Een dashboard zonder stuur

Verzamelde columns

2006 - 2013

Peter Rietveld

About the cover illustration

Norfolk, Va. (Mar. 8, 2004) – Sailors practice repairing leaks in the "wet trainer" on board the Submarine Training Facility (SUBTRAFAC) in Norfolk, Va. The trainer is designed to test the teamwork and damage control capabilities for crews preparing to deploy aboard submarines. Sailors are exposed to leaks from pressurized service pipes within an enclosed space, in effort to provide a controlled yet realistic training environment. U.S. Navy photo. (RELEASED)

Date 8 March 2004

This file is a work of a sailor or employee of the U.S. Navy*, taken or made as part of that person's official duties. As a* work *of the* U.S. federal government*, the image is in the public domain.*

Voorwoord

Utrecht, Maart 2015

Voor u ligt een reeds columns die verschenen zijn op security.nl. Ik trad voor deze site zeven jaar op als vaste columnist. Deze verzameling bestrijkt de periode van 2006 tot 2013. In de eerste jaren heette het gebied nog IT security en het was voorbehouden aan een vrij kleine kring specialisten, maar de omslag was al ingezet naar de situatie van vandaag de dag waarin cyber security met vaste regelmaat de voorpagina van de dagbladen inneemt en formeel als grootste bedreiging voor onze manier van leven geldt.

Iedere verzameling columns is gegeven de aard van het columnisme primair een geschiedenisboek, een tijdsbeeld. Deze verzameling als het goed is, ook. Een column is immers gebonden aan de actualiteit, en een tijdje later niet meer actueel. Wat een lezing van deze columns echter duidelijk maakt is dat er uiteindelijk erg weinig verandert en verbetert, ondanks tal van ferme maatregelen, kloeke besluiten en heel veel meer geld en aandacht. Ook in 2015 zijn computers inherent veilig door telkens dezelfde fouten, mislukken overheids ICT-projecten met voorspelbare regelmaat, is security een grote hype met grote woorden en zeer magere resultaten. Ook nieuwe systemen worden ondoordacht en dus nog steeds onveilig gebouwd en gebruikt en zo rent de wereld nog steeds rond als een krankzinnige kip zonder kop. Het grootste verschil is dat er meer koploze kippen rondrennen dan ooit.

Wat kunnen we nu met deze verzameling? Vakinhoudelijke lering? Ik denk weinig. De geschiedenis leert ons immers dat mensen niet leren van de geschiedenis. Het is dan ook bovenal bedoeld als vermaak, soms lichtvoetig, soms wat zwaarder op de hand. Ik wens de lezer dan ook een paar uur van herkenning en gegniffel.

Peter Rietveld

Inhoudsopgave

Groot slaat dood

23 augustus 2006

Het NRC-Handelsblad meldde dinsdag op pagina 13 dat het niet goed gaat met de grote ICT-dienstverleners. Dit naar aanleiding van de koersval van Ordina na een winstdaling in plaats van de door de goeroes aangekondigde 20% stijging. De oorzaak: loonstijgingen. Simpel, toch?

Het probleem is het overdenken waard: de strategie van grote contracten waar de 'dienstverleners' en analisten zo tuk op waren, heeft geen rekening gehouden met de loonstijgingen die volgen uit de grote vraag naar ervaren IT-ers. De aangekondigde financiële zekerheid valt tegen.

De analisten beginnen nu de keerzijde te zien van de zekerheid die ze zélf enige jaren geleden dwingend als medicijn voorschreven: langlopende contracten, grote concerns en megadeals. Allemaal leuk voor de beurskoers toen ze afgesloten werden, maar nu een financiële molensteen. Ik ben benieuwd of de logische volgende stap komt: opsplitsen. Het blijft vreemd dat het wondermedicijn voor Ahold, Tyco en Stork nog niet in de IT voorgeschreven wordt.

Door het meerjarig vastleggen van prijzen hebben de grote spelers geen speelruimte om mee te gaan met de snelle loonstijgingen die nu hangen aan jobhoppen. Het patroon is vertrouwd: als het goed gaat met de branche, dan gaat het slecht met de grote spelers. Alleen dit keer versterkt door de grote contracten.

Het patroon versterkt zichzelf: iemand die overstapt, begint met een paar weken op de bank bij de nieuwe club. Het duurt immers even voor een opdracht gevonden is. Tel je de hieraan verstookte manjaren bij elkaar op, dan heb je zó plaats voor nog een paar duizend nieuwe IT-ers. Die er niet zijn. Dit drijft de lonen en tarieven op - tot de ballon klapt. Dan stokt de mobiliteit en slaat het tekort heel snel om in een overschot.

Ja maar, hoor ik al zeggen, dan leiden we toch nieuwe mensen op? Prima, maar dat kost écht geld. Omdat de grote clubs toch moeten leveren kunnen de trainees intussen het werk doen wat ze later gaan kunnen. Leerzaam voor de mensen, daar niet van, maar zelden goed voor de resultaten.

De kleinere concurrenten gaan op dit moment op de loop met de ervaren mensen en uiteindelijk, met de klanten. De grote partijen kunnen wel kleintjes opkopen om toch aan mensen te komen, maar in deze markt doen die de hoofdprijs. Plus dat de mensen toch weer weggaan.

De prijsdruk op de mantelcontracten en uitbestedingsconstructies leidt tot snijden waar het niet direct opvalt - en beveiliging is de beste kandidaat: het duurt immers een tijdje voor iets afstort. Dit is geen bewuste keuze, maar gaat sluipenderwijs door een cocktail van onervaren mensen en uitstel van preventief onderhoud.

Wat is de les? Manteldeals kopen geen zekerheid, integendeel zelfs. Hoe het dan wel moet zal weer een boel consultancy-uurtjes opleveren. Maar niet voor de werkloze ICT-er van 2008.

Waarom beveiligingsbeleid faalt

8 september 2006

Kenmerkend voor de meeste vormen van beleid is dat het de doelstellingen bepaald. Daar zit altijd een stuk gevoel in, zo van: we gaan die kant op, doen dat en dat en daarmee worden/bereiken we dat en dat. Nu kennen de meeste organisaties ook een beveiligingsbeleid. Hierin staan zinnen als: "Er zijn passende technische maatregelen genomen ter ondersteuning en aanvulling van de procedurele en organisatorische maatregelen." Nou, daar kun je wat mee. Dit soort zinnen staat garant voor eindeloze discussies, meestal met het volgende patroon: techneuten vragen apparatuur aan die ze toch al wilden hebben, en als ze er echt zin hebben, richten ze een database in. De staf bedenkt een nieuwe managementlaag, claimt resources, stemt af en treedt krachtig op, procesboeren gaan de spelers in kaart brengen en processen beschrijven. En zo ontvouwt zich het vertrouwde landschap van regels, methodieken, systemen en processen waar de IT al jaren in grossiert en waarin verdacht weinig verandert. Alleen dit keer moet het 'vanwege de beveiliging'. Is beveiliging familie van Rupsje Nooitgenoeg?

De gemiddelde organisatie beperkt het beveiligingsbeleid tot een kantje of 12. Kort en helder, raden de specialisten aan, anders zou niemand het lezen, laat staan ernaar handelen. In de regel meldt het dat we de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie borgen en als het wat nieuwer is wordt het woord processen genoemd. Bestaande functionarissen krijgen extra doelstellingen en rollen opgelegd. Zo ontstaat een virtuele beveiligingsorganisatie die “ingebed is in de staande processen.” Klinkt prachtig, maar het betekent niet meer dan dat een boel mensen worden opgezadeld met vage doelstellingen waarvan ze geen idee hebben wat ze er mee moeten. Ondanks dat het beleid kort is, is het helemaal niet helder, wordt het niet gelezen en wordt er al helemaal niet naar gehandeld.

Voor de gemiddelde bestuurder is aan dit alles weinig eer te behalen. Met een beleid dat nauwgezet voorgeschreven is (zoals door VIR en ISO), dat in de praktijk leidt tot nog meer kansarme discussies en projecten zonder aantoonbaar nut dan je normaal al hebt, kun je je niet profileren. Het is een verplicht nummer: inwisselbaar, ongeïnspireerd en zonder draagvlak. Dat zijn de symptomen van de échte ziekte: het beleid is niet geïntegreerd met de rest van het beleid, waarmee het alleen in naam beleid is. Het is dan ook verbazingwekkend als je een manager tegenkomt die zich er bij betrokken voelt: in tien jaar informatiebeveiliging moet ík de eerste nog tegenkomen.

Maar zodra er een groot incident is, stort het kaartenhuis in elkaar. Verbazing en verwarring bij de top, want alle nodige stappen zijn toch gezet? Het kan toch niet zo zijn dat we - vul maar in - niet geregeld hebben? We hebben zoveel jaren álles gedaan en niet op geld gekeken!

Arme bestuurder. Het beleid werkt niet. Wordt het onvoldoende nauwgezet of hardnekkig uitgevoerd? Of zou het kunnen dat er iets ánders, iets veel fundamentelers, mis is? Jawel, dat zou best kunnen. Dat er iets fundamenteel mis is in de aanpak van informatiebeveiliging.

De gangbare aanpak is al in 1989 beschreven door Fites en via RFC2196 in alle handboeken beland. Het uitgangspunt is dat je assets (data, systemen, applicaties) classificeert en dan bepaalt wat er mee mis kan gaan. Je kiest vervolgens de meest waarschijnlijke scenario’s. Daar baseer je je maatregelen en beleid op.

Dit klinkt als een goed uitgangspunt, maar dat is het niet. Want: hoe weet je als schrijver van een document of als beheerder van een systeem wat een ander daarmee kan? Voor veel beheerders is een systeem veilig omdat het achter een firewall staat en er voor een hacker niets belangrijks op staat. Dus hoeven ze alleen spyware en virussen tegen te houden. Maar is dat zo? Hetzelfde geldt

voor bestanden: wat voor een normale gebruiker slechts data is, kan voor een aanvaller informatie zijn. Wie zegt dat een aanvaller uit is op wat je zélf belangrijk vindt? Hoe goed kun je denken als een hacker, spion of spammer? Nooit goed genoeg. Dat maakt het uitgangspunt onbruikbaar.

Ook stap twee is niet goed: de gemiddelde beheerder of IT-manager weet immers niet welke rottigheid anderen met je spullen kunnen uithalen. En zeker niet hóe ze dat zouden doen. Dus de bedreigingen waar je maatregelen tegen wilt nemen, hoe relevant zijn deze nu eigenlijk? Werken de maatregelen die je voorstelt wel? Kun je de waarschijnlijkheid van misbruik bepalen? De fout in de aanpak is dus heel fundamenteel: Garbage In, Garbage Out.

Uit de loopgraven

22 september 2006

Mijn vorige column ging over onjuiste uitgangspunten van de gangbare methodieken rond informatiebeveiliging. Naast de asset based benadering bestaat een aanpak vanuit, zeg maar, de business architectuur filosofie: je gaat uit van de doelstellingen van de organisatie, vertaalt dit naar het belang van veiligheid en dan heb je wel managementsupport. Maar: wat is dan precies de relatie tussen een meetbare behoefte aan veiligheid en een specifieke maatregel, zoals de bestelling van een paar IDS-en? Juist. Da's lastig. In de regel geeft deze benadering dan ook geen betere resultaten, behalve misschien in een paar uitzonderlijke gevallen waarbij de organisatie een vertrouwens- dan wel een veiligheidstaak heeft en een ongelimiteerd budget. Bovendien: dit is een mes dat snel bot wordt. De verwijzing naar de bedrijfsdoelen wordt al snel een mantra. Een beetje bestuurder krijgt jaarlijks tal van voorstellen ter goedkeuring onder ogen. De kans is reëel dat hij dat stuk over de beleidsdoelstellingen gapend overslaat.

Maar vergis je niet. De afwezige ondersteuning voor het beleidsdocument bij de top is iets volledig anders is dan weinig aandacht voor beveiliging. Het probleem is dat beleidsstukken gortdroog zijn. Met formaliteiten win je geen oorlog. Dat je wél budget krijgt, is dus ook geen zeker teken van managementsupport. Iedereen met kinderen weet dat het toestoppen van een koekje of een paar euro's iets heel anders is dan het ergens mee eens zijn: je geeft toe om van het gezeur af te zijn. Gegeven dat iets doen aan beveiliging verplicht is, zal ook een matig voorstel ondersteuning kunnen krijgen. Immers, als je er niets van snapt, dan zullen de specialisten wel gelijk hebben. Als het niet té duur is, dan. Een afwijzing kan heel goed betekenen dat het voorstel aandachtig gelezen is. Maar daar willen de beveiligers dan weer niet aan. Managers zijn immers categorisch dom. "Als ze het niet eens zijn met onze aanpak, dan zien ze het belang van beveiliging niet in." Terwijl het ook zou kunnen dat de aanpak gewoon niet goed genoeg is. Zou toch kunnen?

Het gebruik van een bedreigingencatalogus zoals CRAMM en BSI werkt in de praktijk ook niet echt goed. Zeker als de catalogus heel generiek is, en het te beveiligen object dat niet is. Een wijs man zei ooit: "A Fool With A Tool, Is Still A Fool". Als je vervolgens een kruiskopschroevendraaier als bandenwipper moet gebruiken .....

De catalogi beogen een zeer breed scala aan omgevingen te kunnen bedienen. Er staan dan ook tal van niet relevante zaken in. Vervelend is dat gebruikers van een methodiek vaak de neiging niet kunnen onderdrukken deze heilig te verklaren. Bedreigingen aan de catalogus toevoegen als geïnterviewde is in hun ogen een gotspe: alsof je je als simpele beheerder op hetzelfde niveau durft te plaatsen als de auteurs van De Schrift. Dat laat je dus de volgende keer maar. Met als gevolg dat je als systeembeheerder vragen moet beantwoorden over de waterbeheersing in de eigen regio en de kwaliteit van het justitiële optreden tegen digitale criminaliteit. Meld je dat dat allemaal goed geregeld is, dan hoef je niets te doen. Dat de uitkomst een verzameling goedbedoelde onzin is, zal niet verrassen.

Ik zie nog een andere, essentiële, tactische zwakte in de gangbare benadering. Wat doen we in de praktijk: rond de te beschermen assets richten we een cordon op van gelaagde beveiligingsmaatregelen. Landmijntje hier, rolletje prikkeldraad daar, wachtposten her en der en een loopgraaf als de grond niet te hard is. Het resultaat is een statische beveiliging, die er vanuit gaat dat je alle aanvalsroutes kunt overzien. En dat de aanvaller via bekende paden komt.

Gegeven echter dat het initiatief bij de aanvaller ligt, voeren we eigenlijk een bewegingsoorlog, ofwel een blitzkrieg. De bewegingssnelheid van een aanvaller is extreem groot. De statische benadering is ongeveer even kansrijk als de Maginotlinie in 1940: binnen enkele seconden heb je de zwakke plek te pakken. In de jongste vakliteratuur zie daarom je een voorzichtige verschuiving optreden van een statische naar een dynamische aanpak van beveiliging. De nadruk ligt op het vermogen om op te treden. Hierbij hoort een grote mate van Intelligence: je moet weten hoe je omgeving in elkaar zit, welke mogelijkheden je hebt om te 'manoeuvreren' én je moet aanvallen vroegtijdig kunnen signaleren. Alles draait om het oplossend vermogen van de (beveiligings) organisatie. Deze benadering vereist een radicaal andere aanpak.


Bundesarchiv, Bild 121-0486
Foto: o.Ang. | 1940 Mai - Juni

Inherent aan deze aanpak is het concept van de 'denkende soldaat', wat we in de burgermaatschappij wel kennen als empowerment: de ruimte om te handelen naar eigen inzicht. Wat NIET hetzelfde is als: we zijn in paniek en zoek het maar uit.

De huidige trend dicteert echter dat alle acties vaststaan in protocollen en procedures, waarbij beheerders als gedresseerde aapjes doen wat in het lijstje staat. Los van het gegeven dat de lijstjes in kwestie vaak weinig met het desbetreffende systeem van doen hebben en dus nogal eens genegeerd worden (we nemen immers hooggeschoolde mensen aan- hbo-ers - die we de bewegingsruimte van een wasknijper geven), eist de dynamische aanpak een grote cultuuromslag. Het geïnstitutionaliseerde wantrouwen zal plaats moeten maken voor handelingsvrijheid, vertrouwen en mandaat voor de eigen mensen. Zoals alle veranderingen zal ook dit top-down moeten worden aangepakt. Vis rot immers aan de kop.

Een goed idee is niet genoeg

27 september 2006

Managed Security - mijn gedachten gaan terug naar de tijd dat Gartner dit concept een grootse toekomst voorspelde. In 2002 voorzag Gartner dat Managed Security het grootste segment zou worden van de totale Infosec. En in 2003 heette het dat in 2005 60 % van alle grote bedrijven delen van de bewaking zou hebben uitbesteed.

Nu, vier jaar later, leven we nog steeds onder het juk van de dozenschuivers en dominees: het leeuwendeel van de taart gaat naar leveranciers en adviseurs. Blijkbaar ging er iets vreselijk mis? Nee hoor. Ik voorspel - à la Gartner "met een waarschijnlijkheid van 90%" - dat in 2010 Managed Security nog steeds een zeer beperkte nichemarkt zal zijn die juist hoofdzakelijk kleine en een paar middelgrote bedrijven bedient.

Uitbesteding is in de praktijk vaak een vlucht naar voren. We doen niet meer zelf wat toch al niet lukte! Een andere reden voor uitbesteding is dat het elegante manier kan zijn om van een vergrijsde en uit haar krachten gegroeide IT-afdeling te komen. Ze doen niet wat we willen maar de markt zal ze wel leren. Bovendien geldt bij dit soort uitbestedingen een omgekeerde gouden handdruk: de organisatie krijgt geld toe en ze hoeven ook niet langs het UWV voor een aanvraag voor collectief ontslag.

Voor beveiliging zijn dit soort redenen niet aan de orde. Niets doen, of een beperkte symboolpolitiek voeren werkt meestal prima. Het is bovendien goedkoop, dus dat houd je dan maar binnenboord. De enige situatie waarin je zult besluiten structureel beveiligingstaken uit te besteden, is als je toch al georganiseerd omgaat met beveiliging. Dit vraagt een behoorlijke maturiteit van de ICT en haar relatie met het bedrijf. De basis moet stevig zijn: een behoorlijk inzicht in wat van waarde is, van wat er eigenlijk allemaal is aan data en infra, een structureel budget en een heldere verdeling van rollen, taken en verantwoordelijkheden. Als de organisatie hiermee vervolgens afdoende ervaring heeft opgedaan, wordt het wellicht mogelijk te bepalen of en zo ja, welke, bewakingstaken en beveiligingsrollen zich lenen voor uitbesteding.

Op zich is Managed Security een goed idee. Je legt immers voor een aantal jaren vast dat een bewakingsfunctie door een professionele partij wordt uitgevoerd. Maar een goed idee is niet genoeg.

Een papieren tijger in een zilveren lijstje

20 oktober 2006

Heeft alle aandacht voor Security geleid tot meer veiligheid? Tot een jaar of drie, vier terug was er in de Security geen droog brood te verdienen; nu rollen de CISSPs van de lopende band zoals vroeger de CCNA's en MCSE-ers. Gewapend met een massa kennis zoals dat http-verkeer poort 80 moet gebruiken, vinden ze een goedbetaalde baan. Naast deze grote groep gecertificeerde specialisten is er een reeks bindende voorschriften gekomen die organisaties dwingen nu eindelijk allerhande zaken te regelen. Zelfs de schone slaper VIR kreeg na 2003 opeens allerlei vormen van aandacht. En om het allemaal nog mooier te maken werden technieken als Enterprise patch management, Intrusion Detection, Identity Management en laag 7 firewalls in een bloedstollend tempo volwassen. Al met al zou de spullenboel dus een stuk beter moeten zijn.

Er is geld en aandacht, er zijn mensen en bruikbare oplossingen. Toch is het hoofdzakelijk puin, als vanouds. En als je nadenkt over de ROSI, de Return On Security Investment, wordt je al helemaal niet vrolijk.

Tabaksblat, Sox en NEN7510 zijn wellicht de bekendste voorbeelden van opgelegde beveiligingsinspanningen. Deze formaliseren de best practices van BS7799, VIR en CVIB, die dateren uit de vroege jaren negentig. De enterprise automatisering was toen nog pre-Internet en zelfs pre-Windows. En dus richten de voorschriften zich primair op informatiebeveiliging conform het aloude - en alleen voor infosec valide - adagium dat aanvallen grotendeels van binnenuit komen. Terwijl de problemen waardoor er meer aandacht voor beveiliging kwam zoals Melisa, Iloveyou en code red, volledig uit de hoek van de Compusec kwamen. Een virus kijkt heus niet naar de informatie op een systeem voor het besluit te nemen al dan niet te infecteren. De voorschriften hebben 15 jaar oude oplossingen voor een ánder probleem tot wettelijke norm verheven. Is er dan geen vooruitgang?

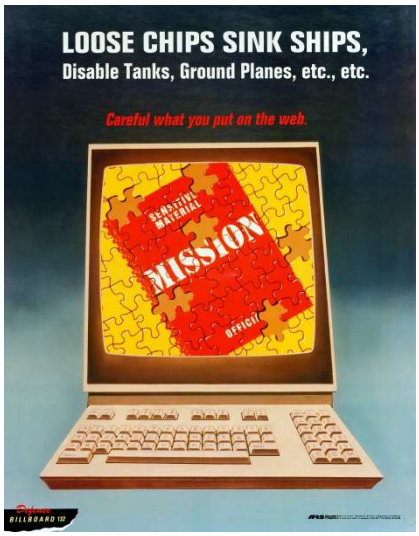
Eens even denken. Dit jaar zag ISO27001 het levenslicht: het Information Security Management Systeem. Eindelijk kunnen we beveiligen met een druk op de knop. Een weelde van informatie van alle incidenten, anomalieën in de logs, actuele patchlevels van systemen, einddatums van SSL-certificaten, zombie machines, wat je maar wilt.

Stop met dromen. We krijgen dus een database waarin alle getroffen maatregelen opgeslagen worden. Dat noemen wij boekhouden. Daar vang je echt geen virus mee. Dit is Compliance, en heeft met het verder verouderen van de regelsets iedere dag minder te maken met de realiteit van Security.

We hadden een Compusec probleem en de specialisten kwamen met een oplossing voor een ander probleem wat ze blijkbaar interessanter vonden: Informatiebeveiliging. Wat de jongste ISO-telg ons brengt is een boekhoudkundig sluitstuk om aan te tonen of je aan de aloude voorschriften voldoet. Voor je het weet bereik je Security Maturity Level 3 en kun je onder het genot van een Cola Light een certificaat in de hal ophangen naast je ISO 9000. De papieren tijgers fokken papieren tijgers zodat je ingelijste papieren tijgers aan de muur kunt hangen. Intussen is driekwart van alle computers in het gemiddelde bedrijf van boven tot onder verziekt, verliezen we het gevecht tegen spam en heeft niemand een idee wat er op het netwerk gebeurd. Want ja, dát moet Beheer maar doen: beveiligingsspecialisten vinden techniek tegenwoordig maar vies.

Awareness, Best Belangrijk

17 november 2006



We moeten leren om geen risico's te nemen op het gebied van beveiliging. Daarom zijn er awareness campagnes. Die vertellen ons dat we moeten patchen, een goeie antivirus installeren, back-ups draaien, niet zomaar attachments openen en niet naar verdachte sites moeten gaan. Raadzame adviezen - voor een thuisgebruiker met een brakke Windows op een Aldi-pc.

Mijn voornaamste probleem met dit soort campagnes is De Verkeerde Toon. We nemen continu volwassen, rationele beslissingen, bijvoorbeeld over investeringen en klantgesprekken, maar als het over computerbeveiliging gaat zijn we kennelijk ineens nooit ouder geworden dan een jaar of zeven. We krijgen leuke screensavers, slogans, posters en massale bijeenkomsten, liefst met rollenspelen en berouwvolle ervaringsdeskundigen die hun lesje geleerd hebben. Zo'n aanpak doet eerder denken aan campagnes uit de DDR dan aan een dynamisch 21ste eeuws bedrijf vol hoogopgeleide, zelfstandige professionals.

SURFnet pakt het nog grondiger aan. Met rolletjes pepermunt en freecards, die de studenten oproepen zich niet te laten pakken. Zijn dit nu de middelen die onze huidige studenten moeten aanspreken? Je zou toch bijna gaan denken aan emigreren.

Dreigen is ook niet slim. Sancties tegen opzettelijke overtredingen, ja, daar is wat voor te zeggen. Maar sancties op fouten en stommiteiten? Misschien handig om van je personeel af te komen, maar voor het personeel zelf leidt het natuurlijk vooral tot onzekerheid over wat wel en niet kan met je primaire gereedschap. En uit onzekerheid gaan we vooral dingen níet doen. Zeg maar dag tegen je productiviteit.

Een ander probleem is dat je voor de meeste awareness-adviezen rechten nodig hebt, die de IT-afdeling eigenlijk niet aan een gebruiker wil geven. Je kunt ze toch moeilijk de rechten geven om hun eigen computer te beveiligen, zoals ze thuis doen. Dat leidt geheid tot misbruik. Althans, dat zal de IT-afdeling zeggen. Dilemma: als ze het niet kunnen stort het bedrijf in, als ze het wel kunnen zit de IT-afdeling zonder werk. En het netwerk vol met illegale beveiligingssoftware.

Gebruikers willen nu eenmaal bediend worden door de stofjassen van de IT-afdeling, die daarvoor overigens ook betaald worden. Ze hebben nooit gevraagd om systemen die niet bestand zijn tegen dagelijks gebruik met een open pijp naar Internet. Als je ze vervolgens het advies geeft dingen te laten, onderstreep je het onvermogen van de IT-afdeling. Zo bevestig je het donkerbruine vermoeden van veel gebruikers, dat die IT-ers over het algemeen maar overbetaalde prutsers zijn.

Systeembeheerders hanteren het motto: gebruikers laten zich niet opvoeden. Ook helpdeskmedewerkers weten al jaren dat uitleggen niet helpt. Waarom zouden beveiligingslessen uit een bedrijfsfilm en op de verpakking van de bedrijfskoekjes dan wel werken?

Het grappige is dat dit allemaal ook helemaal niet hoeft. Je kunt zo'n beetje alles dichtspijkeren en eruit kieperen wat echt niet te redden valt – er is niets mis met een goeie, ouderwetse BOFH die iedereen een thin client geeft (kan ook met windows, hoor) en continu met een bus peur langs alle kieren in het netwerk gaat.

"Ja, maar, thuis hebben we Windows ME en die thin client werkt heel anders, dan moeten we op cursus." Awareness is ook een cursus. "Ja maar, de beheerders hebben geen verstand van thin clients". Zij kunnen ook op cursus. En wie het niet wil leren, moet maar de kost gaan verdienen met virussen van thuisPC's afhalen, of kan zich melden bij de spoelkeuken. De meesten zullen het echter alleen maar leuk vinden. Nieuwe spullen!

Toch modderen we voort met extreem zwakke netwerken. Waarom?

Kennelijk willen we de IT-club niet te veel macht geven, bijvoorbeeld om alles tegen te houden wat niet wenselijk is. Dat herinnert te veel aan vroeger. In de jaren zeventig en tachtig had de gemiddelde IT-afdeling meer te vertellen dan de directie. Ieks! Dat nooit meer. Dan maar liever een netwerk dat af en toe niet werkt.

Eigenlijk is het dus verrotte handig zoals het nu gaat met die awareness-campagnes: de IT-club etaleert haar eigen onmacht en bijt zich vast in zijn frustratie dat er nooit naar ze geluisterd wordt. Dat houdt ze volgzaam.

Geen nieuws is goed nieuws

5 december 2006

Een van de meest lastige begrippen in securityland is imagoschade. Je treft het regelmatig aan in risicoanalyses, waarbij gemeld wordt dat als je maatregel y niet treft, je een gerede kans loopt op imagoschade. Pracht van een stoplapargument, maar eentje die als je er goed over na denkt, toch niet zo makkelijk hanteerbaar is.

In het echte leven is de werkelijkheid een stuk minder maakbaar: je kunt maatregelen implementeren tot je een ons weegt, maar die Ene zit er vrijwel zeker niet bij. Stel je voor dat een beperkt aantal beveiligingsincidenten zich afspeelt midden in een veel grotere reeks incidenten die je organisatie toch al voor het voetlicht brengt. Stel je voor dat dit net op een dag gebeurt dat de hele wereld braaf is, en er geen enkel ander nieuws is. Geheid dat je het acht uur journaal haalt. Stort er daarentegen tijdens het opmaken van de voorpagina's van de ochtendbladen een Turks chartertoestel op de forensentrein van Kampen naar Zwolle – nou dan hoor je weinig meer over het informatiebeveiligingsincident. Je speelt dus in een soort lotto, en je kunt moeilijk als maatregel opnemen dat er een ander nieuwsevenement gecreëerd moet worden om de aandacht af te leiden. Je kunt er dus maar het beste vanuit gaan dat je rampenscenario zich afspeelt op een dag dat het grootste nieuws is dat Pino van Sesamstraat de baard in de keel krijgt.

Daar kwam Justitie ten tijde van de Tonino-affaire ook achter: de maatregelen die je als ICT-club kunt treffen reiken namelijk niet tot het privédomein van de kopstukken van de organisatie. Het advies van burger@overheid, naar aanleiding van deze affaire, luidt: "Om te voorkomen dat gevoelige digitale informatie via het privédomein weglekt, moet ervoor worden gezorgd dat die informatie daar überhaupt niet wordt opgeslagen." Mooi gezegd, maar is er wat van te maken?

Laten we dit eens op de technische en op de organisatorische manier doen. Immers, voor een organisatorisch probleem bestaan geen technische oplossingen en geen enkele technische oplossing kan zonder een organisatorische pendant. Tenminste, dat zeggen ze vaak.

Vanuit de organisatorische procedure zie ik een absoluut verbod opdoemen op het thuis werken aan vertrouwelijke gegevens. Mja, klinkt een beetje zoals het VIR voorschrijft. Dat is al een tijdje geleden ingevoerd, en ik kan mij zo voorstellen dat het ook bij het OM niet toegestaan is thuis te werken aan gevoelige dossiers. Het heeft alleen niet echt geholpen.

Vanuit het technische domein zie ik een DRM-achtige encryptie voor mij – op bestandsniveau dus, waardoor je documenten weliswaar elders kunt opslaan, maar niet kunt openen als je geen toestemming krijgt van een validatiesysteem. Laat deze encryptie goed stevig zijn, en bij voorkeur van Amerikaanse makelij, dan pleeg je met het kraken ervan een terroristische daad en dan kunnen we wellicht tot uitlevering overgaan.

Op deze manier wordt het probleem in ieder geval al heel veel hanteerbaarder. Ik vermoed dat Peter R. de Vries hierdoor afdoende geremd zou worden. In dit geval is de technische oplossing wellicht een stuk doeltreffender dan de puur organisatorische benadering. Maar zou het geholpen hebben in de affaire Tonino?

Was de schade voor het OM zo groot dat er vertrouwelijke werkgegevens letterlijk op straat kwamen, of dat de indruk gewekt werd dat Tonino zich bezighield met kinderporno? Kan een organisatie zich wapenen tegen een dergelijke situatie? Onwaarschijnlijk. Hier kun je feitelijk alleen terugvallen op de ruime ervaring die de voedselindustrie heeft met de communicatie rond

glassplinters in Olvaritpotjes en vergelijkbare situaties van crisiscommunicatie. Betrek als ICT de reguliere communicatieafdeling bij het afhandelen van imagovraagstukken. Daar heb je een afdeling communicatie immers voor.

De les is duidelijk: ontkenning van een incident levert de meeste schade op. Als je de beschuldiging in eerste instantie ontkent en later moet toegeven (zoals Shell in de Brent Spar-zaak) beschadigt een organisatie zichzelf maximaal. Net iets minder slecht is herhaaldelijk met andere lezingen komen – zoals Microsoft een jaar of 5 geleden deed toen een paar websites gehacked werden. Met arrogantie en bestuurlijke onzorgvuldigheid maak je extra veel stuk, en blijf je vanzelf lang in beeld. Je kunt beter komen met een consistent, plausibel verhaal, waarbij je in zekere mate het boetekleed aantrekt. Vaak is de waarheid best een goede kandidaat. Als je kunt inspelen op het sentiment dat iedereen fouten maakt, kom je een heel eind en wordt het volgende nieuwtje al snel weer interessant. Een voorlichter die niets te melden heeft is taboe, dan kun je er beter één hebben met de uitstraling van Balkenende die zeer gedetailleerd de pers eindeloos verveelt. Tot er weer écht nieuws is.

Komt het nog wel goed?

28 december 2006

Aan het eind van het jaar is het tijd voor terugkijken en voorspellingen. Wat we de afgelopen periode gezien hebben is een toenemende druk op de ICT-organisaties: meer regelgeving, meer techniek. Daarbij vervagen de traditionele pijlers netwerk, werkplek en applicaties - waarop beheerorganisaties gebouwd zijn - met SOA. En dat nét nu die markt voor ervaren krachten overspannen is...

Afgezien van de inspanningen rond antivirus, richt de bulk van de beveiligingsactiviteiten van de techneuten zich op het inrichten van preventie op de netwerklaag en zijn de consultants druk druk druk met beleidsformulering en beleidsondersteuning. Leuk, de techies steken nog een paar appliances aan en de consultants schurken zich nog eens behaaglijk tegen het management aan.

Het gevolg is dat er geen capaciteit is voor al die ingewikkelde nieuwe dingen of de minder glorieuze operationele aspecten. Hoe gebruik te maken van al die superoplossingen die naar binnen gereden worden? Wat ga je doen met de melding die de IDS uitspuugt? Niets, want er kijkt toch niemand en waarom zou je: de rulebase staat nog op de fabrieksinstellingen dus het zégt ook helemaal niets. Wat doe je als er een probleempje is met IPS: simpel, de regel uitschakelen.

Applicatiebeveiliging? Nou, eh, we definiëren een VPN voor het beveiligen van SOAP over SMTP, we regelen autorisatie in de web front-end terwijl deze de achterliggende databases als system benadert, we gebruiken de default server certificaten die in de developerkit van de leverancier zitten en raken in paniek op de expiry date.

De belangrijkste realiteit is deze 'uphill battle', die op termijn vrijwel niet te winnen is. Kleine organisaties zijn volledig afhankelijk van een paar mensen qua beveiliging. Dit kán goed gaan, zo lang de omgeving simpel is, de mensen het overzicht hebben, het vertrouwen krijgen, het hoofd koel houden en integer zijn. En niet weggekocht worden.

Middelgrote organisaties kunnen niet concurreren met de groten op geld en met de kleinen op vrijheid in de slag om de medewerkers. Het recept: outsourcen of samenwerken/fuseren. Maar het outsourcen van beveiliging is pas mogelijk als je 'in control' bent over het stuk dat je wilt uitbesteden. Een vlucht naar voren gaat niet werken: bij outsourcing is alleen het champagnemoment simpel. En bij samenwerken of fuseren word je een grote organisatie....

... met alle gevolgen van dien. Grote organisaties zijn vrijwel onbestuurbaar geworden op ICT-gebied, wat nog versterkt wordt door de Security clubs. Normale ICT-ers zijn servicegericht: als het niet kan de op ene manier, dan zoeken ze een andere, hoi we mogen weer. Bij grote organisaties en bij Security mensen zie je dat zelden: gewoon nee zeggen, maar komen met een alternatief, ho maar. Misschien ken je die mensen wel: ze zeggen “het kan niet” maar ze bedoelen “ik kan het niet”. Of “ik wil het niet”. Er wordt een autoriteit gevraagd die zich bij onzekere (underskilled) mensen uit in indekgedrag: nee zeggen is risicoloos. Misschien ben je er zelf wel één van.

Als machtscentrum trekt Security bovendien mensen aan die de machtsconcentratie interessant vinden. Ik heb gelijk en ik zal je daarvan overtuigen of tenminste mijn zin opleggen - doe je niet wat ik zeg dan druk ik op de MIP (Management In Paniek) Knop. Die werkt als volgt: ik herinner de directeur eraan dat hij onder SOX hoofdelijk en strafrechtelijk aansprakelijk is. Ziezo, dat nieuwe systeem komt de deur niet in.

Het invoeren van kwaliteitsprocessen om de boel te stroomlijnen, helpt ook niet. CMM en ISO beschrijven inspanningen, geen resultaten. Het metselt de boel nog verder dicht. Wat ook zelden helpt is het werken 'onder architectuur'. Hoe vaak zie je in ontwerpen dat de inleiding onderdanig een hommage brengt aan de formele architectuur, en die vervolgens volledig de eigen gang gaat? Hoeveel hoog abstracte architecturen schetsen niet een artist impression van de 'stip op de horizon' waar geen zinnig mens naar toe wil - als de richting überhaupt te raden is? Zo fungeren 'het proces' en 'de architectuur' als management desinformatiesysteem, een schuimrubber laag tussen sturing en uitvoering. Dat komt bovenop de traditionele en vakkundige invulling van deze taak door het middle management.

Dit leidt tot een bestuurbaarheid als van een winkelwagentje op de ijsbaan. Zo worden grote organisaties kwetsbaar voor de kleinere concurrenten die uit een garage opereren en (nog) geen last hebben van het dichtmetselsyndroom.

Dit zie je ook bij organisaties waarnaar je zou kunnen outsourcen, niet alleen van beveiliging maar van de hele ICT: deze kunnen niet concurreren op vrijheid (metersdikke contracten en de kwaliteitsmanagementregels van de sales pitch) noch op geld (ze moeten immers concurrerend zijn). Mensen willen daar echt alleen maar werken omdat ze anders verhongeren. Vandaar dat de meeste van die clubs in derdewereldlanden zitten, of in de VS. Wie gelooft er nu werkelijk dat er volop hooggeschoolden zijn in een land met honderd miljoen inwoners waar de onderwijsbegroting lager is dan de aanschafprijs van één JSF? En zie die leverancier in Boekiwoekiestan maar eens aansprakelijk te stellen als zijn broer opperrechter is.

Het enige echte voordeel van outsourcing is dat het gepruts vakkundig onzichtbaar gemaakt wordt door een professionele salesorganisatie, iets waar de eigen ICT-club nooit budget voor heeft gehad. Het vermijden van de term outsourcen door over 'On Demand' te praten, is een mooie illustratie van deze kunst. Volgens de India Times steeg het percentage afgebroken contracten in 2005 van 21% naar 51%. Gegeven dat dit alleen gebeurt als het management van de opdrachtgever de eigen fouten durft te erkennen, kunnen we er van uitgaan dat dit het topje van de ijsberg is, dus dat ruim 100% van alle outsourcingsprojecten volslagen bagger is.

En dan nu de voorspellingen, die ik in de inleiding beloofde. In 2007 overschrijdt het aantal rampzalige ICT-projecten de 97%. Alle organisaties die afdoende Security hebben, moeten het eerste personeel nog in dienst nemen. De introductie van nieuwe kwaliteitsmanagementmethodieken stijgt naar gemiddeld één per maand. Het managementboek 'Security & Flexibiliteit In 50 Best Practices' zal de winkels uit vliegen. Het aantal organisaties met meer geïmplementeerde 'best practices' dan medewerkers groeit bij de Fortune 500 naar 85%.

Tegelijkertijd krijgt de tegenbeweging, die Security als de grootste rampspoed voor het bedrijfsleven beschouwt, steeds meer momentum. Het verloop in specialistische functies in de ICT overstijgt de 60%. Bij dit alles zal het salaris in de ICT stijgen met gemiddeld 17%, waarbij de stijging het laagst is voor specialisten met meer dan drie jaar ervaring.

Security Maturity

26 januari 2007

Meten is verleidelijk. Vooral voor managers. KPI's, scorecards, benchmarking trajecten, noem maar op. Wat vooral interessant gevonden wordt, is 'hoe goed doe ik het ten opzichte van mijn gelijken'. Het is belangrijk deze vraag niet te verwarren met het 'wie heeft de grootste' wat je persoonlijk wellicht meer boeit. Goed management is meestal eerder bezig met 'doe ik net genoeg en niet te veel'. Immers, in bedrijven geldt dat te veel doen aan een cost driver, onverantwoord management is. Dit noemen ze alignment.

Een populaire manier van meten werkt met maturiteitsniveaus: hoe 'volwassen' ben je als organisatie. Op basis van oermoeder CMM definiëren we een hiërarchie van te bereiken resultaten, waaraan wij adviseurs een nummertje hangen van één tot vijf.

Het gerenommeerde NIST (de Amerikaanse pendant van ons normalisatie instituut), beoogt met Prisma het gehele beveiligingswerkveld te bestrijken in vier niveaus van maturiteit. Op level 1 staan policies, op level 2 zie je procedures, op level 3 voer je een en ander in, en op level 4 kijk je of het helpt door testen en auditing. Helemaal prachtig, op de onderste twee levels heb je alleen papier, bij de implementatie schaf je 'alle ad hoc' af en op het hoogste niveau ga je (laten) toetsen of de doelen bereikt zijn.

Laten we wel wezen. Policies kun je zo abstract maken dat je ongeveer alle situaties onder een kapstok artikel kan vangen. Level 1 gaat dus wel lukken. Maar procedures moeten concreet zijn, dus Prisma betekent dat je blijkbaar alle eventualiteiten en omstandigheden moet voorzien, inclusief wetswijzigingen en gaten in goedgekeurde apparatuur en software. In level 2 blijf je dus ergens hangen, tot je besluit wat er af is ‘alvast’ te implementeren, vrij naar level 3. Maar ja, je komt naar de methodiek nooit boven level 2. Los van deze zwaktes krijgt de klant op z'n vroegst resultaten op level 4, waarin je de effectiviteit gaat meten. Nu willen sommige mensen wel eerder weten of het hele traject ergens toe leidt - vreemd, nietwaar? - dus die willen eigenlijk al wat sneller resultaten zien. Maar dat kan niet. Of je moet gaan melden 'dat we ergens tussen level 2 en level 4 zitten'.

De premisse is dat je alles wat je doet meetbaar maakt. Dat maakt alle lagere niveaus dan het hoogste voor iedere organisatie onvoldoende. Of zijn er clubs waar er behoefte bestaat aan tal van kostbare maatregelen zonder enige zicht op resultaten? Wat is hier nu het nut van de verschillende niveaus? Immers, je hebt pas iets als je op niveau vier zit. Echter, een kostenbewuste manager wil niet op het hoogst mogelijke, maar op het laagst acceptabele niveau zitten. Hint voor de knutselaars van Prisma: definieer een niveau luchtkasteel, waar niemand op zit te wachten en plak dáár je natte dromen in. Omdat nummertje vijf nog ontbreekt, die de meeste anderen wel hebben, pak je die toch?

Het minstens even gezaghebbende ITGI heeft een 6 niveaus hoog maturity model voor information security assessment uitgebracht. Op niveau 0 kijk je niet naar de business impact van security zwaktes. Je kijkt überhaupt nergens naar, je doet gewoon niets. Op niveau 1 doe je van alles ad hoc, zonder policies, en alles zonder samenhang of beleid. Op level 2 wordt wat de club doet herhaalbaar, maar dat dan wel 'intuïtief'. Toch benieuwd hoe dat gaat, neem je dan alleen helderzienden in dienst? Op level 3 worden de 'processen gedefinieerd', rollen en verantwoordelijkheden 'toegekend', maar niet afgedwongen. Op level 4 is de vrijblijvendheid afgeschaft, en op niveau 5 wordt security geïntegreerd in de 'business'. Ook hier zie je dezelfde

zwakte: alleen het hoogste niveau is goed genoeg - of ga je de 'business' vertellen dat het niveau waarop iemand anders de baas is, goed genoeg is?

Het Duitse Institut für Software- und Systemtechniek Frauenhoff, zo mogelijk nog gezaghebbender dan de beide voorgangers, heeft een eigen smaak in haar Security Maturity Model, SMM. Ook dit kent vier niveaus. Niveau 0 staat voor blind vertrouwen en helemaal niets doen. Niveau 1 staat voor ad hoc in de rondte bewegen. Op niveau 2 is er beleid dat de acties op elkaar afstemt en op niveau 3 (het hoogste) 'evolueert' alles vanzelf naar een hoger niveau, door permanente processen - zonder al te veel managementingrijpen. Onze Duitse collega's maken duidelijk dat ze beter begrijpen wat het moderne management wil dan NIST en het ITGI: dat alles vanzelf goed gaat. Dat ze hiervoor de 'permanente processen' als wondermiddel in stelling brengen, maakt duidelijk dat we hier een evidente winnaar hebben. Maar het maakt even duidelijk is dat de maturiteitsbenadering zelf nog niet volwassen is.

Unified Threat Management: dure mensen, goeie spullen?

12 februari 2007

In 2004 introduceerde de zeer gerespecteerde analistenclub IDC het begrip United Threat Management (UTM). Hierbij voorspelden ze een ontwikkeling waarbij de traditionele functies van een firewall (packet dan wel statefull) in een appliance 'geconsolideerd' zullen worden met nieuwere rollen als Intrusion Detection en Prevention, mail en browse encryptie, packet shaping, antivirus en antispam en VPN terminatie. Volgens IDC is deze ontwikkeling wenselijk voor onder meer banken, overheden en nog 15 andere sectoren die één gezamenlijk kenmerk hebben: het zijn grote clubs. De analisten zijn het er met zichzelf over eens dat er dus een zeer grote markt bestaat voor UTM. Volgens IDC zullen UTM appliances in 2009 de helft van de hele verkoop van security apparaten uitmaken. ITSecurity.com meldt dat deze magische dozen "proactieve bescherming bieden tegen bekende én onbekende aanvallen". Bescherming snap ik. Maar wat is er nu precies proactief?

In de praktijk is 'een UTM' een firewall die voorbij packet filtering of statefull inspection gaat. Gartner geeft aan deze ontwikkeling een iets minder hoogdravende naam: Next Generation Firewalls. Maar ook die term impliceert dat het iets is wat je gaat willen. Feitelijk bouwt de UTM voort op de traditionele application layer gateway, wat tegenwoordig vaak aangeduid wordt als proxy based firewall. De kern is het samenvoegen van alle netwerk perimeter functies. Het probleem dat UTM wil oplossen is dat een Best-of-breed combinatie van tig van deze rollen leidt tot een filtering DMZ waarin rustig een twintigtal kostbare doosjes staan te zoemen: kostbaar in aanschaf en complex in beheer.

Anno 2007 is UTM natuurlijk al passé, we evolueren immers van Anomaly Based naar Identity Based beveiliging. Nou, geen zorg, er zijn al leveranciers die Network Access Management aan het koppelen zijn aan hun doosjes van Pandora. Er komt er vast nog wel eentje op het idee er XML signatures en Windows Rights Management aan te lijmen. Kan het nog járen mee.

Managerial is UTM natuurlijk een zegen: een stuk minder dozen en minder beheerders betekent dat je minder geld uitgeeft en minder zeurpieten op de loonlijst hebt staan. Bovendien heb je aan een appliance geen beheerkosten, nietwaar?

Dit idee wordt ondersteund door certificeringclubs die er een kwaliteitsstempel op drukken. Niemand kan meer hard maken dat de doos in kwestie niet goed is: dure mensen hebben vastgesteld dat het prima producten zijn en dure raad is goed. Ik heb een hint voor iedereen die op die manier met een UTM opgezadeld dreigt te worden: lees het testverslag. Wát is er getest? Wat betékent een 'Common Criteria' level 4 nu eigenlijk? Er is een belangrijk semantisch verschil tussen een kwaliteitscertificaat van een gerenommeerde instelling en kwaliteit zoals normale mensen dat ervaren. Meestal betekent een certificaat dat je een bepaald theoretisch beveiligingsniveau kunt bereiken - mits je allerlei andere zaken rond het product op een bepaalde manier doet, die misschien niet helemaal aansluiten bij je eigen werkelijkheid. Dat niveau beschrijft de inspanning die je doet, maar zegt hooguit indirect iets over de veiligheid. Ik zie de gevolgen al voor me. 'Ja baas, we hebben wel een netwerk vol virussen en wormen die onze belangrijkste klant besmet hebben, en iemand gebruikt onze firewall als Counterstrike server, maar we zijn toch wel mooi wél level 3 qua beveiliging'.

Technisch georiënteerde beveiligers moeten over het algemeen weinig hebben van Multi-functie doosjes. Immers: je creëert een Single Point of Failure. Bovendien is een all-in-one zelden op alle gebieden even goed. Ook hier schiet ITSecurity.com te hulp: ze melden dat een UTM 100% van

alle virussen vangt, antispam 95% scoort en anti-spyware 97%. Blijkbaar detecteert Trend beter virussen als ie op een packet shaper draait. De praktijk zal bewijzen dat de techniek niet beter wordt als je de functies opeenstapelt in een enkele machine.

En is het wel een enkele machine? Als één functie te maken krijgt met een veel hogere belasting (bijvoorbeeld veel gefragmenteerde packets) dan mag dat niet ten koste gaan van de werking van de andere functies. Dit houdt in dat er een reserve rekencapaciteit moet zijn voor iedere functie. Effectief betekent dit dat alle functies hun eigen reserve zullen hebben, met een sterke scheiding tussen de rollen. Is een UTM dan in feite niet meer dan tig doosjes in één omhulsel, met een geünificeerd beheerschilletje? Oftewel: de totale hoeveelheid benodigde rekenkracht neemt niet af, dus in plaats van 6 lichte dozen heb je één doos die zeven keer zo zwaar is - alleen in één chassis met drie netwerk interfaces. Je kúnt ook beargumenteren dat een quad quadcore server met 32GB natuurlijk wel één systeem lijkt, maar er eigenlijk gewoon zestien zijn.

Alleen, dit is een boodschap die je moeilijk over de bühne krijgt bij het gemiddelde management. Bovendien speelt mee dat je nu eenmaal zelden het allerbeste krijgt, misschien wel om te bewijzen dat jij niet de baas bent, maar zij. Daarom is het belangrijk om je te realiseren dat er betere argumenten bestaan.

Vereenvoudiging van beheer wordt voorgesteld als één van de grootste winstpunten. Je hoeft immers minder dozen in de lucht te houden. Hieronder zit een levensgrote denkfout: beveiligingsbeheer is niet het in de lucht houden van beveiligingsdoosjes, maar het zorgen dat ze doen wat ze moeten doen, en acteren op de informatie die ze opleveren. Een firewall is categorisch anders dan een reguliere server: voor een IT club moeten een server 'up' zijn, zodat de gebruikers hun ding kunnen doen. Maar van een beveiligingsdoosje ben je zélf de gebruiker. Het is geen ding dat 'het moet doen', je moet er zélf je ding mee doen. En daarom neemt met een 'unified' oplossing de hoeveelheid beheer niet af. Of je rar parser nu in een UTM zit of in een open source doos die virussen scant, je zult de functie tijdelijk moeten uitschakelen als er weer eens een gat gevonden wordt in de parser en de patch nog niet beschikbaar is. De signatures die de IDS dan wel de IPS gebruikt werken niet out of the box, je zult ze altijd moeten afstemmen op je omgeving. En als ze iets engs zien, moet je wat dóen. Dit beheer blijft, of het nu één appliance, tien appliances of twintig BSD servers zijn.

Erger nog. Het feit dat veel functies in één chassis zitten, compliceert het beheer. Je hebt immers tal van gelijktijdige ingrepen om de verschillende functies goed uit te kunnen blijven voeren. Dan gaat de change kalender je bijten: je wilt immers niet in ieder onderhoudswindow twintig wijzigingen op een enkel systeem doorvoeren. Bij veel verschillende dozen is het risico van interferentie van changes veel kleiner. Kort samengevat: beheer wordt met UTM juist níet eenvoudiger. Het beheer van beveiligingsmiddelen is gerelateerd aan functies en niet aan een enkele doos of een heleboel dozen. Het wordt dus ook niet goedkoper, want de hoeveelheid werk blijft hetzelfde. De enige kostenvoordelen bestaan uit minder inkoop en minder housing. Of dit opweegt tegen de grotere beheercomplexiteit en interferentierisico's, moeten de voorstanders van de geünificeerde toverdoosjes maar aantonen.

IDC roept inmiddels dat Fortinet marktleider is op dit gebied. Grappig, want hoewel een Fortigate een heel leuk doosje is, heeft ze lang niet alle functies die een UTM system zou moeten hebben. Dames en Heren ontwikkelaars: ga niet bouwen wat IDC en vergelijkbare clubjes bedenken. Hoewel het marketingpad voor je klaar ligt, en je weinig moeite zult hebben investeerders te overtuigen, neem je het grote risico iets te ontwikkelen waar niemand op zit te wachten. Laat het UTM verhaal maar voor zich spreken – de zoveelste hype waar niemand ooit van gehoord heeft. Heren managers: zeg die abonnementen op en laat het kiezen van oplossingen over aan mensen die het probleem begrijpen. Ze zeuren wel, maar je betaald ze toch al elke maand hun salaris.

Best Practices Bestaan Niet

28 februari 2007

Organisaties die op de één of andere manier ‘iets doen’ aan informatiebeveiliging, kiezen vaak voor de zogenaamde Best Practice benadering. Dit is ook een heel gangbaar advies van consultants. Een korte uitleg: in een Best Practice benadering haal je de maatregelen uit een boekje of een lijst van een gerenommeerde bron, en gaat ze vervolgens naar de letter uitvoeren. Het is een vorm van checklistmanagement, waarbij je de vinklijst van een externe instelling gebruikt. Een Best Practice impliceert dat de maatregel al ergens succesvol geïmplementeerd is, dus dat het gestelde doel bereikt is.

Vanuit management optiek is dit een valide methode. Je wilt immers niet maanden discussiëren over wat je allemaal moet doen. Het klinkt reuze handig. Het woord Practice benadrukt dat het praktisch is, en Best geeft het autoriteit. Daarom verdienen Best Practices navolging.

De mooiste truc die de salesafdeling van een IT-club kan bereiken, is het presenteren van haar producten en werkwijze als Best Practices. Tegenover elke kritische geest staan er tien angstige consultants en managers die in aanbidding op de knietjes zakken. Met onze quickscan ben je in een handomdraai SOX compliant!

Zo werkt het natuurlijk niet. Wondermiddelen bestaan niet. Kant en klare Best Practices evenmin. Het succes van een maatregel is altijd afhankelijk van de manier en de timing van de invoering. Bovendien is vrijwel iedere uitgevoerde maatregel een compromis tussen wat kan en wat moet. Dat compromis zal niet bij iedere organisatie hetzelfde uitvallen. Maatregelen en praktijken zijn nu eenmaal bedacht in een bepaalde context en zijn in die omgeving al of niet succesvol.

Een voorbeeld. In het Veluwse dorp Putten gold reizen per paard in de negentiende eeuw als Best Practice. Dit had tot gevolg dat het treinstation acht kilometer van het centrum werd aangelegd. Een actie die blijvend bijgedragen heeft aan de landelijkheid van het dorp. Maar de economische voordelen van de kazernes en de psychiatrische inrichtingen gingen naar het volgende dorp, Ermelo. Ermelo deed niet aan Best Practices.

Het geloof in Best Practices rukt ook op in het hoger onderwijs, waar ze door toonaangevende instituten als Inholland als leervoer voor studenten neergezet worden. Hoe dit zich verhoudt tot het streven naar een innovatieve kenniseconomie en het nieuwe leren? Zou er zoiets bestaan als onderwijsconsultants? Laten we hopen dat de nieuwe minister van Onderwijs in staat is dit geloof te ontmaskeren.

Terug naar IT Security. Ook de Code voor Informatiebeveiliging (CvIB) wordt vaak gepresenteerd als een verzameling Best Practices. In strikte zin is het dat echter niet. Het zijn maatregelen, in 1989 begonnen als goede gewoonten voor computergebruikers, met als doel de

veiligheid te verbeteren. Specialisten van allerlei organisaties hebben er sindsdien nog een aantal goede gebruiken bijgejongd, maar wat er nog steeds niet in staat, is wát je nu precies moet doen om die goede bedoelingen te realiseren. De praktijk, dus. De practice. Nogal wiedes overigens dat dit er niet in staat, want het bestaat ook niet. Er is nooit een pasklaar recept.

De CvIB noemt bijvoorbeeld als Best Practice: geen ongecontroleerde modems in het netwerk. Dat is an sich een prima – hoewel een beetje verouderde – doelstelling. Maar een prima doelstelling is nog geen succesvol geïmplementeerde en in stand gehouden maatregel. De vraag is dus: hoe zorg je ervoor dat je die ongewenste modems vindt, en tegenhoudt, zónder de ongetwijfeld beste bedoelingen van de eigenaren te fnuiken? Dat zal niet in iedere organisatie op dezelfde manier kunnen. Ook het feit dat deze Best Practice niet spreekt van ingebouwde wireless access points, zal je even moeten 'vertalen' naar je eigen context.

Helemaal lastig wordt het als de Best Practice letterlijk uitgevoerd moet worden, wat nogal eens de opdracht is. Of als je te maken krijgt met nieuwe bedreigingen, waar nog geen enkele Best Practice voor bestaat. Doe je er dan maar niets aan tot de Best Practice een update krijgt? Of als een Best Practice voorschrijft dat je risicomanagement introduceert. Je moet dan toch echt zélf overal over nadenken en dat wilde je nu net voorkomen.

De CvIB is een lijst met 133 maatregelen die de moeite waard zijn om te bekijken. Wat het niet is, is een hufterproof en compleet recept voor checklistfetisjisten. Er is alleen gekozen om het positioneren als Best Practices, in een tijd dat dit nog niet de bijklank had die het nu heeft.

Nu is het bon ton om op allerlei gebieden werk als meetbare processen in te richten, en daarin past een hoge mate van standaardisatie. Hoe kun je anders benchmarken tegen de competitie? Zie hier de basis van het succes van de best practitioners. Stel je voor dat de auditoren niet uitkomen met hun checklistje – hel en verdoemenis. Dat je IT-club het helemaal anders doet met BSD servers en OSX werkstations – daar bestaan helemaal geen KPI's voor! Hoe kun je dan aantonen dat je het goed doet?

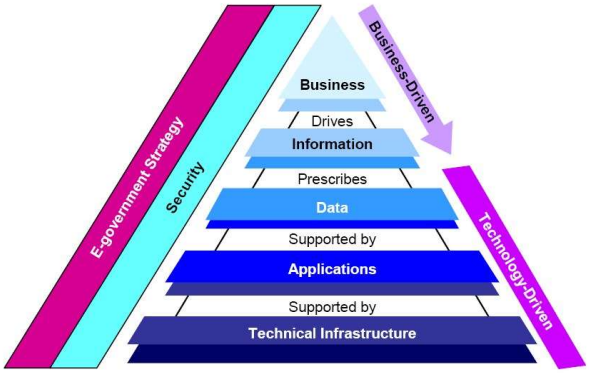
Het fascinerende is dat het hele geloof in Best Practices neerkomt op de angst anders te zijn dan de concurrentie. Daarmee verdwijnt dus het onderscheidend vermogen van de organisatie. En daarmee verdwijnt ook iedere innovatie, ieder concurrentievoordeel en uiteindelijk het bestaansrecht van de organisatie. De neiging om kritiekloos een lijstje van elders te volgen is vooral een uiting van gestold wantrouwen in de eigen medewerkers en gemakzucht. Heren managers, als je je mensen niet vertrouwt of niet naar ze wil luisteren, knikker ze er dan gewoon uit.

Over Security Architectuur

7 april 2007

Iedere zichzelf respecterende organisatie beschikt er al over of is op zijn minst bezig met het opstellen ervan: een IT-architectuur. Dit begrip, overgewaaid uit de Verenigde Staten, staat voor een set van documenten die de informatievoorzieningen van een grotere club beschrijven. De oorspronkelijke opzet, zoals vastgelegd door onder meer IEEE, stelt dat een architectuur beschrijvende documenten omvat op verschillende abstractieniveaus. Zo zijn er netwerkarchitecturen, die op laag 2 tot 4 uitleggen hoe de verkeersstromen komen waar ze horen, en niet komen waar ze niet horen. Onmisbaar voor het oplossen van storingen en voor het aanbrengen van wijzigingen. Vergelijkbaar heb je informatiearchitecturen, die uitleggen hoe applicaties de bedrijfsvoering ondersteunen. Er was niets logischer dan dat er ook een beveiligingsarchitectuur zou ontstaan, die beschrijft hoe een set van beveiligingstechnologieën en processen gezamenlijk zorgt voor een veilige werkomgeving.

Maar helaas, zo is het niet gegaan. Architectuur veranderde van beschrijvend in vóórschrijvend. In het begin was dit niet zo vreemd, immers: je wilde niet alleen een handzame beschrijving van wat er is (de "IST"), maar ook van wat er moet komen (de "SOLL"). Een vóórontwerp zeg maar, een blauwdruk voor de toekomst. Deze verandering kun je terugvoeren op Gartner, die stelt dat een architectuur prescriptief moet zijn, oftewel kaderstellend. Zo ziet een architectuur naar Gartner eruit als een reeks referentiemodellen, en omvat het tal van afspraken over hoe de techniek er uit moet gaan zien, over zeg vijf jaar.



En daar ging het heel erg mis. Deze tweede generatie architecturen is afhankelijk van wat de professionele toekomstvoorspellers aan oplossingen voorzien. Normale leveranciers weten niet wat ze over pak 'm beet zeven jaar verwachten te leveren. Maar Gartner cum suis weet dit natuurlijk wel. Waarmee een hele nieuwe klantenkring gecreëerd werd.

Het voorschrijven van hoe iets moet worden, raakt de essentie van de macht. Zeker als je het hebt over beveiliging. En zo schoven architecten op naar de contreien van de beleidsmakers. Een beveiligingsarchitectuur werd een soort zusterdocument voor het beveiligingsbeleid, waarin staat hoe beveiligingsdoelstellingen gerealiseerd moeten worden. Maar dan wel op de abstracte manier van de stip op de horizon. Met deze ontwikkelingen belandde architectuur in de buurt van de burelen van het beleid en in handen van mensen die wat verder afstaan van de operationele werkelijkheid. En dat verhoudt zich heel slecht met het ontwerpen van een doelmatige beveiliging.

Het is hiermee dus niet gezegd dat Security architectuur niet kan, of niet nodig is. Wat wel gezegd moet worden is dat er een hele berg kolder verkocht wordt. Architectuur verzorgt de juiste balans (de alignment) van noodzaak en middelen, dus een Security architectuur zorgt voor alignment (en daarmee de rightsizing) van Security middelen. Zodra het over verder in de toekomst gaat, ontbreken de parameters om de juiste maatvoering te bepalen, zoals de effectiviteit van de middelen en de realiteit van de bedreigingen. Vijf jaar geleden vonden we bijvoorbeeld spam en spyware onbelangrijke zaken. Zo hebben we nu hooguit een heel vaag idee van waartegen we in

2012 moeten optreden. Om dat nu te lijf te gaan met plannen die gaan over stippen op horizonnen?

Je herkent ontspoorde beveiligingsarchitecturen in de regel snel. Het eerste weggevertje is door het spelen van Bullshit Bingo met de architectuur als geheel: veel platitudes en een ver doorgetrokken beeldspraak. Bestemmingsplan. Modellentypologie. Richtinggevend en kaderstellend. Referentiekader voor projecten & auditoren. Landkaarten en positionering.

Een tweede weggever is het gebruik van oudere mantra's uit beveiligingsland. De meest kenmerkende is Deming, modieus in de jaren negentig. Bedenk je dat veel architecten al een tijdje mee hobbelen en doorkneed zijn in oudere concepten – en wat verder afstaan van de alledaagse werkelijkheid. Als ze er al ooit mee te maken hebben gehad. Wat was dat ook al weer, Deming? In het kort: Plan, Do, Check, Act. Klinkt heel goed, van een tijdloze schoonheid. Je begint met Plan, waarin je bedenkt wat je allemaal moet gaan doen. Grappig, maar bij beveiliging begin je eigenlijk liever met kijken wat er aan de hand is.

Deming is geleend uit kwaliteitsbeheer en in het verleden kritiekloos overgenomen, toen informatiebeveiliging nog in de kinderschoenen stond. En zo vind je in nieuwste beveiligingsarchitecturen stapels oude koek: zaken uit het INK-model, inzichten uit Six Sigma, zelfsturende teams, balanced scorecards en andere begrippen die na het eerste deel van Dilbert afgevoerd leken. Maar goed, die voer je dus allemaal in, met een procesgeoriënteerde watervalmethode, en dan komt het helemaal goed.

De BSA in de bocht

www.security.nl 07 mei 2007 en in ICT-rendement van juli 2007.

De Business Software Alliance, belangenbehartiger van de commerciële software industrie, heeft het gerenommeerde marktonderzoeksbureau Gfk NOP een onderzoek laten uitvoeren naar het bewustzijn van de risico's van het gebruik van illegale kopieën van software bij het MKB. Dit meldde Computable afgelopen donderdag. Het MKB blijkt zich wél bewust van de juridische risico's, maar niet van de veiligheidsrisico's.

"Bedrijven die illegale software gebruiken, kunnen niet rekenen op dezelfde ondersteuning, services, patches en upgrades als gebruikers van legale versies", aldus Jacco Brand, voorzitter van de BSA. Zo is maar 13% zich bewust van het feit dat het gebruik van illegale software kan leiden tot minder functionaliteit, weet maar 11% van meer kans op virussen en maar 12% dat illegale kopieën vaker crashen. De BSA: "Het is opvallend dat het Nederlandse MKB dit onvoldoende onderkent en meer oog heeft voor externe factoren als schadevergoedingen en juridische procedures."

Nu zal een marktonderzoeksbureau de vragen kritiekloos afgevuurd hebben, maar op dit podium zijn de stellingen van de BSA wellicht wat kritischer te beschouwen. Hoe reëel zijn de genoemde veiligheidsrisico's en zijn deze specifiek voor illegale software?

BSA Stelling 1: zonder services van de leverancier van software is je systeem onveiliger. Nu hebben de meeste organisaties die wél betalen voor al hun software geen servicecontract met alle leveranciers, zeker niet in het MKB. Een supportcontract is gangbaar voor de grotere pakketten zoals Exact, maar niet met Microsoft of Adobe. Services zijn optioneel, en het rendement is blijkbaar nooit bewezen, gegeven de geringe verspreiding daarvan bij legale software. Deze stelling klopt niet.

BSA Stelling 2: zonder patches van de leverancier van software is je systeem onveiliger en minder stabiel. Patches dichten beveiligingsgaten. Zonder patches heb je dus gaten. Op het eerste gezicht is dit valide. Maar dat is het niet: beveiligingspatches zijn van de meeste leveranciers (en zeker bij MS) gewoon te downloaden en te installeren, ongeacht de licentie. En dat blijft ook zo: leveranciers zouden wel gek zijn om de toch al geringe verspreidingsgraad van de updates nog verder te verkleinen. Je wilt immers niet te boek staan als de bakker van die baggersoftware die altijd onveilig is. Dat is nu eenmaal, terecht of onterecht, slecht voor je omzet. Dus deze stelling is niet correct.

BSA Stelling 3: zonder upgrades van de software is je systeem onveiliger en minder stabiel. Upgrades brengen extra functies aan in je software. Afgezien van beveiligingsfuncties (zoals een malicious software removal tooltje) voegen extra functies wellicht gebruikersgemak en zinvolle mogelijkheden toe, maar geen veiligheid of stabiliteit. En voor dergelijke zaken zijn tal van al dan niet legale tools te vinden, zoals Adaware. Maar die komen er niet vanzelf op. Updates om je systeem stabiel te krijgen? Die zijn er niet. Geen leverancier meldt ooit dat de dure software eerst instabiel was. Deze stelling is hooguit een heel klein beetje waar.

BSA Stelling 4: in illegale kopieën werken bepaalde functies niet. Als je een gecrackede trial versie hebt, komt dit voor. Meestal gaat het dan op door de leverancier aangebrachte beperkingen die de crack niet wegwerkt. Heb je de verkeerde crack te pakken. En om nu te zeggen dat dit veel voorkomt? Nee. Bovendien gebruiken de meeste mensen maar een zeer beperkte set van de functies van de programma's, dus of het opvalt? Deze stelling is hooguit zeer beperkt waar.

BSA Stelling 5: virussen propageren beter in illegale software. De essentie van een kopie is dat deze gelijk is aan het origineel. Dus de virusgevoeligheid is ook gelijk. In sommige software die illegaal verspreid wordt, of in crackerstools om beveiliging te omzeilen, zit wél troep. Maar die vindt je Antivirus wel, behalve bij de installatie van een OS. Als je AV de troep niet vindt, ligt dat niet aan de al dan niet legale status van de software, maar aan de afwezigheid van de juiste signature. Ook deze stelling is niet waar.

Het meeste illegale gebruik betreft niet gedownloade iso's of gepatchede trial versies. En zelfs als dit wel zo zou zijn, kunnen we dit testen. Koop twee identieke PC's waarvan één met een OEM XP. Zoek op reliz.ru een iso-tje van Windows op een vage Litouwse FTP-server. Er staan ook Engelstalige, hoor. Installeer deze op de andere PC. Laat beide zich automatisch upgraden, waarbij de illegale machine geen WGA, IE7 en WMP11 installeert. Koop voor de legale machine een officiële Kaspersky en zet op de andere de testversie en haal via wat gegoogle een licentiefile op voor Kaspersky. Leuk het nog wat verder op met een legale en een illegale WordPerfect, een trial versie met een beschrijving hoe je het serienummer erin krijgt (zie het nfo-bestand). MS Office kan ook, maar er bestaan ook andere softwareleveranciers... Ga vervolgens met beide machines een avondje vieze plaatjes, films en muziek opzoeken (we emuleren de gemiddelde MKB-gebruiker, voor het realisme). Onderzoek vervolgens beide machines en vergelijk de mate van vervuiling. Ik vrees dat ze identieke malware hebben opgelopen. Oftewel: ook deze stelling houdt geen stand.

BSA Stelling 6: illegale kopieën crashen vaker. Dit is alleen geloofwaardig als je te maken hebt met een aangepaste kopie. Anders zullen ze precies even vaak crashen. Bovendien hebben de meeste crashes te maken met de onderliggende hardware, zoals elke warme periode weer blijkt. Dus ook deze onderzoeksvraag mag in het ronde archief.

Het lijkt mij dat partijen die niet willen betalen voor hun software, gebruik moeten maken voor software waarvoor dat niet hoeft. Daar is ruimschoots voldoende aanbod in en de kwaliteit is best aardig. Als ik de BSA mag geloven zelfs heel goed, want bij open source kun je legaal de software downloaden van gerenommeerde servers en automatisch patchen en upgraden. En omdat het legaal is, crasht het ook nog eens minder. Alleen een servicecontract kan misschien een beetje lastig worden. Maar ik denk niet dat de BSA reclame mag maken voor open source.

Het lijkt er op dat de BSA het aandikken van zeer beperkte beveiligingsrisico's en het verzinnen van niet-bestaande nodig acht, om gebruikers van illegale software te overtuigen dat betalen toch echt beter is. En passant worden ze nog wat servicecontracten in de maag gesplitst. Blijkbaar worden Nederlandse ondernemers niet bang genoeg van de dreiging met boetes, dus dan maar dreigen met hel en verdoemenis. Dit naar het aloude calvinistische principe dat gestolen goed niet gedijt. Jammer voor de BSA is dit niet zo, een gestolen fiets krijgt niet eerder een lekke band. Als dat wel zo is, had je die fiets ernaast moeten stelen.

De kleren van de keizer zijn dood, leve de nieuwe kleren van de keizer!

08 juni 2007

Security 2.0 is overleden. Officieel. Sinds een aantal dagen draagt Gartner bij monde van beroemdheid John Pescatore het evangelie van Security 3.0 uit. Nu zal de geboorte van het nu verscheiden v2.0 de meesten van ons al ontgaan zijn. Voor de mensen die het allemaal gemist hebben biedt de IT-auditeur Noordbeek gelukkig een overzicht in de memorabele whitepaper Security 3.0. Security 1.0 was het projectmatig bottom up benaderen van risico's op basis van incidenten, dus vooral reactief en gedreven vanuit de handjes en de techniek. Security 2.0, a.k.a. de Operational Risk Management aanpak, bleek een 'inconsistente benadering van beveiliging' waarmee nog 'gerelateerde problemen, voortkomend uit de onwil om beveiliging of risicobeheersing als volwassen bedrijfsonderdeel aan te pakken en aan te sturen' voorkomen. Het is dan ook fijn om te weten dat Security 3.0 de 'noodzakelijke geïntegreerde benadering' introduceert die 'voor wie bereid is veel werk te verzetten, het perspectief van deugdelijke beveiliging en efficiënte en effectieve beheersing van de negatieve aspecten van Bedrijfsvoering biedt'.

Volgens Symantec lukte het Security 2.0 "een betrouwbare omgeving te creëren, diefstal van identiteitsgegevens te bestrijden en transacties veiliger te maken" onder meer door detectie en blokkade van nepsites om te beschermen tegen oplichtingspraktijken als phishing en pharming. Bovendien beschermde Security 2.0 "uw kinderen en uw privacy" in een 'natuurlijke en intuïtieve aanvulling op computergewoonten'. Symantec introduceerde Security 2.0 afgelopen 1 mei in ons land.

Security 2.0 is ondanks deze indrukwekkende resultaten jammer genoeg maar kort meegegaan. Volgens Gartner worstelde de IT ten tijde van Security 2.0 met de stortvloed van nieuwe technologie rond consumerisatie en Web 2.0 en onderging een oplopende achterstand in de middelen deze te beveiligen. En dat in één maand tijd.

Met Security 3.0 krijgen organisaties een voorsprong op opkomende dreigingen door het integreren van beveiliging in de grotere infrastructuren. "It's about moving from whack-a-mole to a chess game where we can deploy security in one place so the attacker has to move in another direction," volgens Gartner goeroe John Pescatore "The idea isn't necessarily to win, but to always be a couple steps ahead of the bad guys and force them into a stalemate." Zodat we, om met de woorden van Noordbeek te spreken, ons weer kunnen wijden aan 'leuke dingen'. Zo te zien is Security 3.0 de eerste versie die belooft dat je een keer 'klaar bent' in plaats van eindeloos door te moeten werken. Jammer genoeg is nog niemand er aan toegekomen om vast te stellen hoe je Security 3.0 kunt dóen. Dat waren we bij 2.0 ook al vergeten. Misschien dat het daarom zo kort mee is gegaan.

Het is officieel: de Security bedrijfstak is de onbetwiste kampioen Bullshit Bingo.

Ethiek en Security

27 juni 2007

Uit reacties op mijn stukje over het vinden van software via ranzige .ru en .lv domeinen blijkt dat er nogal hoge verwachtingen bestaan over de ethiek van de Security consultant. Kennelijk vinden sommige lezers het onwenselijk dat een senior consultant kennis heeft van de wat meer duistere zijden van het Internet. De kreet jeugdzonde is gevallen. Dank, dank, zo jong ben ik niet meer....

Maar het aangesneden punt, ethiek, is wel belangrijk en verdient zeker aandacht. Er zijn al tal van schrijfsels over en het onderwerp heeft zelfs geleid tot een aparte beroepsgroep, de 'Ethical Hackers'. In de jaren 90 dook het begrip al eerder op, waarbij de huidige variant impliceert dit niet alleen ethisch verantwoord bezig te zijn maar dat ook gecertificeerd te doen. Als ik de EC Council moet geloven is een ethical hacker een gecertificeerde persoon die, gewapend met 'dezelfde kennis als een hacker' de beheerder bijstaat. Iemand dus die denkt als een dief om zo dieven te vangen maar zelf niet steelt. Klinkt helemaal toppie.

Om dit body te geven hebben ze er een opleiding voor gestart - die van alles vertelt over allerlei types aanval, maar helaas erg gemakkelijk voorbijgaat aan het 'niet stelen'. Zoals de meeste mensen weten maakt de gelegenheid de dief: als je in staat bent in te breken voor je eigen baan, waarom zou je dat dan niet doen om indruk te maken op dat pittige meisje en haar antiglobalistenvriendjes? Daar gaat de EC Council in haar curriculum voor de Certified Ethical Hacker (CEH) niet op in - wel een beetje jammer.

Ik wil hier even dat traditionele religieuze debat over hackers en crackers maar het laat zich niet helemaal vermijden. Waar het vaak op neerkomt is het volgende: Crackers zijn illegaal en passen alleen domme tooltjes toe voor verderfelijke, criminele of commerciële zaken, hackers hebben een aura van intelligentie en integriteit. Om aangeduid te worden als hacker geeft dus ook dat aura. Omdat niet iedereen dat gelijk doorheeft, kun je dat aura versterken door dit expliciet te maken, bijvoorbeeld met een voorvoegsel als über of leet, of meer van deze tijd, Ethical.

Terug naar de CEH. Blijkbaar is er voor hackers een standaard 'Body Of Knowledge', zoals er ook bestaat voor de project manager. Welke kennis zit daar in? Volgens Ankit Fadia in de tweede uitgave van zijn officieuze gids voor 'Ethical' Hacking uit januari 2005, is de essentie van een ethical hacker dat hij over de volle breedte van het veld elementaire kennis heeft en alle tooltjes kent. Niks mis met SAINT en NATAS, maar om het anno 2005 nog als serieuze hulpmiddelen te positioneren.... Maar goed, Ankit is als professional zeer omstreden, omdat hij zijn materiaal bij elkaar gegoogled zou hebben. Bij hem schittert de beroepsethiek door afwezigheid, terwijl het vak nota bene gedefinieerd wordt als een ethische activiteit. Nu moge Ankit omstreden zijn, ISECOM is dat zéker niet. ISECOM geeft in haar trainingen voor tiener hackers (www.hackerhighschool.org) diep weg in het opleidingsmateriaal een schets van de werkwijze van een ethische hacker. Ook hier hetzelfde patroon: een volgorde van zeven stappen van een aanval over het internet .... en daar houdt het hoofdstuk op. Het zelfde overkomt je bij een bezoekje aan www.ethicalhacker.net; geen spoor van denken over ethiek. Het enige wat je ziet zijn mensen die lekker willen hacken, maar dan 'legaal'.

De 'ethische' cursussen schetsen het volgende beeld van een aanvaller: hij is goed thuis in 'UNIX', kan scripten en proggen, beschikt over een breed arsenaal aan tools en weet ongeveer wat hij ermee kan doen. Dat is blijkbaar de Body Of Knowledge van de hacker, die verdacht veel lijkt op die van allerlei andere security opleidingen. Een hacker weet dus hetzelfde als een consultant.

Mijn ervaring is anders. Een aanvaller hoeft maar een beperkt aantal trucjes te kennen in een smal stukje, maar wél heel erg goed. Vergelijk het met een fietsendief. Hij hoeft maar van één type gangbaar slot één manier te weten om hem open te krijgen en hij kan aan het werk. Er staat altijd wel ergens een fiets met het slot dat hij kan kraken. Bovendien zijn niet alle trucjes technisch. De über-fietsendief weet waar z'n collega's de opengebroken fietsen die ze nog moeten verkopen, verstoppen. Die steelt hij, zonder ooit een slot te kraken. Of is dit nu juist een ethische fietsendief?

Het beeld van een aanvaller die op een Unix prompt van een doos die hij zojuist geroot heeft 'dir' intypt wordt vaak gebruikt om de effectiviteit van toolies versus de onkunde van de scriptkiddie te onderstrepen. Dat kán inderdaad zo zijn, maar het kan net zo goed betekenen dat de aanvaller nu eenmaal weinig weet van Unix maar heel veel van de ISA-box of de content switch die in de stap daarvoor gehacked is. De gangbare definitie van een 'echte hacker' als iemand met in ieder geval verstand van Unix en C is écht passé. Je hebt andere skills nodig, als je de Blackberry van Balkenende wil kraken.

De protagonisten van 'Ethical' Hacking laten wel meer steken vallen. Zo wordt erop gewezen dat een penetratietester bijna hetzelfde is als een hacker, maar het verschil wordt nergens uitgelegd. Een penetratietest is een ondersoort van het fenomeen testen en maakt gebruik van een gestructureerde methodiek. In alle stukken van de ethische hackers gaat het over hoe de tools werken, niet over wat en hoe je test, of wat de waarde is van de testresultaten.

Samengevat: Blijkbaar is ethisch hacken hetzelfde als de wet niet overtreden. De protagonisten van ethisch hacken hebben uit marketingoverwegingen de kreet gekozen, zonder enige moeite te doen om eens te kijken wat er mee bedoeld wordt. Aan de vervolgens geboden brede, oppervlakkige en enigszins verouderde technische kennis en de ongestructureerde werkwijze is echter niets ethisch. Eerder het tegendeel: ondermaats werk voor te veel geld.

Ethiek is iets anders dan het zich al dan niet houden aan de wet. Tussen je aan de wet houden (de legaliteit) en maatschappelijk verantwoord gedrag (hoe het hoort) zit een groot verschil. De wet is in veel gevallen ook niet heel expliciet dus je moet per situatie interpreteren. En over wat maatschappelijk verantwoord is, lopen de meningen ook wel eens uiteen. Dit is nu het speelveld van de ethiek.

Blijkbaar is dit lastig, dus ik zal het even uitleggen met een voorbeeld. Je zit de avond na de InfoSecurity beurs tijdens een hevige onweersbui in een taxi van Utrecht naar Den Haag. De chauffeur vloekt hartgrondig, omdat iemand zonder licht 90 rijdt op de middenbaan van een verder uitgestorven A12. Wat doe je? Bel je het taxibedrijf om te klagen over het gedrag van de chauffeur, omdat de chauffeur de bestuurder van de andere auto voor lid van een etnische minderheid met een dodelijke ziekte uitmaakt? Doe je aangifte wegens discriminatie? Of ben je blij dat de chauffeur er niet tegenaan gereden is en geef je hem extra fooi?

En zo komen we terug bij de oorspronkelijke vraag; wat zouden de ethische standaarden van een consultant in beveiligingsland dán moeten zijn. Volgens leidende instanties in het vakgebied is een beveiligingsconsultant een lichtend voorbeeld, iemand die door de zuiverheid van zijn daden anderen weerhoudt van het overtreden van regels. Zo moeten leden van de ISSA (Information Systems Security Association) de 'hoogste ethische standaarden toepassen', 'de wet niet overtreden' en 'intellectueel eigendom beschermen'. Bovendien moeten zij de 'algemeen geaccepteerde' beveiligingstandaarden en 'best practices' uitdragen. Wat niet wordt toegelicht wélke hoge standaarden, best practices en intellectueel eigendom, al dan niet ethisch of beveiligingsgeoriënteerd... De ISSA wil toch niet beweren dat je niet naar closed source mag kijken of er toevallig een gat in zit, omdat de vendor dat in de EULA heeft gezet? ISC2, bekend van de CISSP, doet het in haar code al heel wat beter. Maar door in het geheel niet op in te gaan

op intellectueel eigendom, blijven actuele en belangrijke vakspecifieke vragen open en dat is erg jammer.

Praktisch gezien gaat de ethiekdiscussie hierover: hoe vind je dat je je kennis op niveau moet houden? Hoe weet je van gangbare en nieuwe aanvalstechnieken zonder bepaalde sites en communities mee te lezen? Hoe weet je welk internetgedrag riskant is als je de websites niet kent? Hoe weet je of een systeem veilig is? Of hoef je alleen maar bij te houden wat de 'best practices' en productcertificeringen voorschrijven, en laat je de donkere zijde over aan de onbekenden die de best practices en de default rules van je IDS opstellen? Ik houd mijn handen schoon en ik kijk neer op de mensen die dat niet doen? Wie zo denkt, accepteert een structurele kennisachterstand van járen. Dat mag natuurlijk. Maar nu wordt het nog ethischer: dan moet je wél je klant vertellen dat je hem alleen beschermt tegen aanvallen tot pakweg 2005.

Nee, dat is niet aardig. Maar wil je goed genoeg zijn, dan zul je je hackerskennis up-to-date moeten houden. Met een mes kun je ook hele nare dingen doen. Toch is een mes an sich geen moordwapen. Als we messen gaan verbieden omdat je er iemand mee kan neersteken, hoe snijden we dan onze uien?

Okee, okee, virale code is iets anders dan een mes. Als niemand zou weten hoe virussen in elkaar zitten, zouden ze er niet zijn. Er is geen ander nut voor virale code. Dat is over het algemeen wel juist, ja. Kennis verdwijnt echter niet omdat dat moreel beter is, en virussen gaan écht niet meer weg. Om virussen te kunnen onderscheppen moet je écht heel goed weten hoe ze werken; zelfs een junior bij een firma als Kaspersky zal meer van virussen (moeten) weten dan de meeste virusbakkers in het wild. Pogingen om kennis te verbieden, ook in een recent verleden door onze regering, zijn een zekere koers om moreel verheven naar de bliksem te gaan.

De ethische vragen waar je in de praktijk voor komt te staan, zijn gewoon niet eenvoudig. Ze gaan bovendien niet alleen over het opdoen van kennis maar ook over daden. Mag je je kennis inzetten voor een organisatie die wellicht kwaad in de zin heeft? Mag je de systemen van zo'n 'kwade organisatie' opzettelijk zwak laten? Laat je je rekruteren om stiekem iets in het systeem van een ver buitenland te doen? Mag je de details van een gat in een stuk software publiek maken als de leverancier niet thuis geeft? Mag je een worm uitbrengen die andere aanvallen voorkomt of de schade herstelt? Kun je het maken om een systeem in een ver land wat dieper te bekijken om vast te stellen of het een zombie is of misschien de doos van de aanvaller zélf? Breek je bij forensisch onderzoek de veiligheidsmaatregelen van de verdachte? Doe je dat ook als je het vermoeden hebt dat er politieke motieven meespelen? Als je een exploit verkocht hebt, wat doe je als blijkt dat de exploit ook na zes maanden nog niet is doorgegeven aan de maker van de software, zodat het gat blijft bestaan en de hele wereld kwetsbaar blijft?

Een specialist die op al deze vragen direct een pasklaar antwoord heeft, is hetzij helderziend, hetzij arrogant en gemakzuchtig. Iedere situatie kent nuances, en in iedere situatie handel je - zeker in het begin - met onvolledige en deels onjuiste informatie. Een zinvolle beroepsethiek zal dan ook hiermee moeten samenhangen: blijf onderzoeken, blijf nadenken, en blijf communiceren, ook over je twijfels en de onvermijdelijke fouten. En voor de omgang met 'de duistere zijde' geldt het aloude adagium: wel ín de wereld maar niet ván de wereld, met alle verleiding van dien. Mensen die er prat op gaan dat ze bepaalde kennis niet willen opdoen vanwege 'morele' overwegingen, kun je maar beter mijden.

Incident Headhunter

16 juli 2007

Het waarderen van assets is het beginpunt van alle beleid - dat is de theorie van informatiebeveiliging. Zeg maar de traditionele kwetsbaarhedenanalyse van VIR en GRIB. Daar worden maatregelen aan gekoppeld, die worden ingevoerd en vervolgens wordt de effectiviteit bewaakt en waar nodig worden de maatregelen bijgesteld. "Regelmatige controle van beveiligingsmaatregelen en terugkoppeling van de resultaten waarborgen het niveau van beveiliging" meldt sogeti dan ook. De waardering van assets is in de regel een éénmalige exercitie. Ten onrechte. De waardering van assets kent méér dan nuances en kleine fluctuaties. Kijk maar naar de huidige arbeidsmarkt voor ICT-ers.

Enkele jaren geleden was een "profiel" van een medewerker niets waard. Het hoogste doel was het zo snel mogelijk wegwerken van deze last- en kostenposten, middels banenmarkten en zelfs via al dan niet louche outplacementbureaus. Maar nu geldt dat niet meer. Datzelfde profiel is voor veel organisaties juist hun meest waardevolle asset. De outplacementspecialisten van weleer zijn de headhunters van vandaag geworden. Deze volledige omkering van waarden is iets waar weinigen in infosec rekening mee houden.

Binnen de klassieke trias van Confidentialiteit, Integriteit en Authenticiteit valt dit vraagstuk onder confidentialiteit van bedrijfsinformatie. Het lastige is dat de informatie waar we het over hebben niet per definitie woont op het eigen netwerk. Het bevindt zich ook en vooral in de hoofden van medewerkers en in de SIM-card. Bovendien verspreidt de informatie zichzelf, bijvoorbeeld over Hyves en andere modieuze sociale netwerken.

Het treffen van maatregelen tegen de mogelijke negatieve gevolgen van headhunting is iets wat weinig voorkomt in infosec-beleid. Nu is headhunting op zich een reguliere bedrijfstak met een nuttige rol, vooral voor de medewerkers, maar het verlies van een goede medewerker kan aardig in de papieren lopen. Of een project vertragen. Laten we de exercitie maar eens uitvoeren.

Je begint met het vaststellen wie de key-medewerkers zijn en wat hun waarde voor je organisatie is. Vervolgens hang je daar beleid aan en bepaal je je maatregelen. Dit wordt over het algemeen gezien als een HRM aangelegenheid. Als beveiligingsmensen hierover iets opschrijven, zullen managers denken dat ze om opslag komen vragen. En dat is natuurlijk ook zo. Maar dit neemt niet weg dat het waar is: in tal van bedrijven zijn de medewerkers de voornaamste asset. Kijk naar de gemiddelde detacheerder. Ook voor andere organisaties zijn IT-medewerkers waardevolle assets. Heel banaal: als je dezelfde persoon moet inhuren op basis van een hunt, verdrievoudigt het uurtarief.

Met de huidige ontwikkelingen op de arbeidsmarkt voor specialisten wint dit punt snel aan belang. We zijn al zo ver dat er om één specialist bij een klant te krijgen twintig managers, salesmensen, aanbestedingsspecialisten, procesbegeleiders en bemiddelaars nodig zijn. Wordt de specialist in kwestie weggekocht, dan is de economische schade duidelijk. Er is binnen de ICT-branche vrijwel geen ander stukje informatie dat tot zo veel schade leidt als het verloren gaat. Bescherming tegen hunting hoort dan ook bij infosec.

Hoe komen headhunters aan de 'profielen' die ze zoeken? Er zijn drie paden: adverteren, viavia en profile scavinging. Adverteren hoort strikt genomen niet thuis bij de headhunters, omdat het kopiëren van een personeelsadvertentie en deze geanonimiseerd overal neerzetten, net zo veel op jagen lijkt als achter een struik gaan zitten en het geluid van een worteltje nadoen. Dit leidt

overigens soms tot dolkomische taferelen: sommige hooggespecialiseerde bureaus hebben 'zoek en vervang' ontdekt, waarbij de klantnaam vervangen wordt door het woord 'klant'. Zo zag ik een vacature voor een manager 'tactklanth beheer'. Deze moest samen met de 'technklanth specialisten' oplossingen bouwen. Enig zoek-en-vervangdenken maakt duidelijk dat de klant het ISC is, en de functie tactISCh beheer. Dat er mensen zijn die 18% van een jaarsalaris van een overheidsmanager (toch misschien 9k) neertellen voor dit soort prutswerk geeft wel te denken. Of medewerkers nu reageren op een advertentie van een headhunter of op een gewone, maakt voor de casus hier niets uit: ze hebben zélf het initiatief genomen. Anders wordt het als er gerichte actie naar je personeel ondernomen wordt.

Via-via werken houdt in: mensen stimuleren om namen en telefoonnummers door te geven van specialisten die ze kennen. Misschien dat die mensen het vervelend gaan vinden door de zoveelste hunter gebeld te worden, maar verder is er weinig wat dit tegengaat. Werkgevers die hierover iets in het beleid opnemen zijn schaars. Wat wel voorkomt is dat medewerkers die uit dienst gaan geconfronteerd worden met een beding dat ze niet wat collega's mogen meenemen naar de nieuwe baas. Maar je kunt ze natuurlijk wel aan een ándere baas doorgeven. Er zijn hunters die hier geld voor betalen en betaald worden om je irritante ex-collega's een beter betaalde baan te geven, is helemaal zo erg nog niet. Zo lang ze maar niet bij dezelfde baas als jij terechtkomen. Zo heb je tenminste nog iets aan die telefoonlijst met alle nummers en verjaardagen van mensen die je niet kent en niet wilt kennen.

Profile-scavinging is sterk in opkomst, zeker nu mensen meer en meer privé informatie online neerzetten. Populair is het afgrazen van sites als LinkedIn, Tweakers en Hyves. Als je een firmanaam hebt gevonden plus de naam van een medewerker, kun je de firma bellen en je met een wazig verhaal langs de receptioniste kletsen. Als je niet al direct doorgeschakeld wordt. Zoals laatst nog gemeld door Computable denkt 31% van de ICT-ers na over een andere functie. De kans dat je de medewerker kunt interesseren is dat ene telefoontje dus wel waard.

Wat kan een organisatie doen tegen headhunters? We kunnen vaststellen dat headhunters een hogere impact hebben dan een virus of een hacker. De waarschijnlijkheid van een dergelijk incident is tamelijk voorspelbaar, en op dit moment gewoon hoog.

Uit de voorbeelden komen een aantal mogelijke preventieve en correctieve maatregelen naar voren, met wisselende succeskansen.

Preventief:

"Boeien en Binden". HR-middelen kunnen de band met de eigen organisatie wellicht versterken. Corporate identity en zo. Charismatisch management schijnt ook te helpen. Als je onderscheidend vermogen echter niet meer is dan de naam die op het loonstrookje staat en het type handsfreeset in de Megane, maak je weinig kans. Maar misschien zijn er nog mensen die vallen voor barbecues en abseilen. Karten en laserquesten zijn overigens helemaal uit.

Afspraken met de externe leveranciers maken: als je in een groot en langlopend project van in huur gebruik maakt, kun je van de verhuurder waarborgen eisen tegen de risico's van verloop. De meerkosten zie je alleen wél terug in het tarief.

Blokkeren van de telefoonnummers van headhunters. Lastig als je ze zelf ook inzet. Bovendien is deze blokkade gemakkelijk te passeren, anonieme SIM-kaarten genoeg.

De receptioniste en andere medewerkers instrueren nooit direct door te schakelen en altijd te laten terugbellen ná een screening. Zullen je klanten overigens niet op prijs stellen.

Medewerkers verbieden namen en telefoonnummers van collega's door te geven aan headhunters. Is een juridisch novum waarvan we maar moeten afwachten hoe dat uitpakt. Bovendien: hoe lang wil je dat dit beding geldig is?

Je medewerkers uitleggen dat het gras elders net zo bruin is. Nadeel: soms is het niet waar. Bovendien is dit een boodschap die je niet eenvoudig op het intranet slingert. Waarom zouden ze je geloven?

Als je medewerker bij een opdrachtgever zit, zullen medewerkers van andere detacheerders of van de klant zélf net zo vrolijk het profiel doorgeven. Hierover zou je met je opdrachtgever afspraken kunnen maken, wat alleen wel lastig wordt het op het gebied van sancties. Bovendien wil je ook dat je eigen medewerkers 'profielen' spotten bij de opdrachtgever....

Geen adreslijsten van medewerkers verspreiden. De veronderstelde kennisdeling moet dan maar op een andere manier.

Medewerkers uitleggen wat de nadelen zijn van Hyves, LinkedIn, Second Life en andere sociale sites. Een hele uitdaging: leg maar uit wat het nadeel is van meer salaris krijgen voor hetzelfde werk bij dezelfde eindklant. Bangmaken over het verlies van privacy misschien?

Medewerkers uitleggen dat de kostenopdrijving die voorkomt uit headhunting slecht is voor de bedrijfstak en dat dit ze op termijn als 47-jarige in de bijstand zal doen belanden, ná het consumeren van de overwaarde op de woning. Het lastige is dat mensen veronderstellen dat dit alleen anderen zal overkomen. Bovendien zullen ze je er dan fijntjes op wijzen dat je zelf ook zaken doet met headhunters.

Correctief:

Heb je het vermoeden dat een van je medewerkers gehunt wordt, leg hem dan in de watten. Als al je personeel gehunt wordt? Tja, dan is de kans groot dat je aan het einde van het jaar rode cijfers schrijft. Bovendien is het emuleren van een 'hunt' een wel heel succesvolle methode om opslag of een grotere leasebak te krijgen. Of een andere klus.

Zo te zien kun je als organisatie weinig doen aan het infosec-vraagstuk dat samenhangt met headhunting. Voor de meesten zal er dus niets anders opzitten dan te wachten tot de markt weer instort.

Bovenstaande maakt hopelijk duidelijk dat een statisch beveiligingsbeleid met een heel gebouw aan correctieve en preventieve maatregelen niet altijd een zinnige investering is. Misschien moeten we de methodes maar eens aanpassen. Daar kunnen we de klanten vast wel tegen een heel schappelijk tarief bij ondersteunen.

Nederland is goed voorbereid

28 augustus 2007

"Ga maar rustig slapen". Volgens de legende zou premier Colijn tot aan mei 1940 hiermee de Nederlandse bevolking in slaap gesust hebben, terwijl Duitsland tot de tanden toe bewapend klaar stond binnen te vallen.

Nu wás Colijn op dat moment helemaal geen premier en heeft hij deze uitspraak dan ook tóen niet gedaan. Maar wel vier jaar eerder: op 11 maart 1936, na de bezetting van het gedemilitariseerde Rijnland door Duitse troepen in strijd met internationale afspraken, verklaarde hij op de radio over de dreiging van Duitsland; "Ik verzoek den luisteraars dan ook, wanneer ze straks hunne legersteden opzoeken, even rustig te gaan slapen als ze dat ook andere nachten doen. Er is voorshands geen enkele reden om werkelijk ongerust te zijn." Hij doelde hiermee expliciet op de korte termijn, zeker niet op de situatie in mei '40. Eerder bedoelde hij het tegenovergestelde: in de toespraak merkte hij ook op dat de kans dat Nederland buiten een nieuwe oorlog zou kunnen blijven hem aanmerkelijk kleiner scheen dan in 1914. Dit laatste stuk is er in de legende vanaf gevallen.

Regelmatig wordt 'Ga Maar Rustig Slapen' geciteerd, bij zo'n beetje alle onderwerpen die in een willekeurige perceptie aan de nationale veiligheid raken en waarbij de overheid als laks wordt ervaren. Zo ook vorige week, toen wij geconfronteerd werden met een uitspraak die in potentie uit kan groeien tot een herhaling van deze geschiedenis: onze premier beweerde dat ons land lang niet zo slecht is voorbereid op rampen van diverse aard als het openbaar gemaakte rapport van het project Nationale Veiligheid suggereerde. Dat Nederland niet goed voorbereid is, is volgens onze premier "gedateerde informatie". Het project hield zich in 2005/6 ondermeer bezig met de kwetsbaarheid van de dijken, onze digitale infrastructuur en de dreiging van het terrorisme.

Als er de komende jaren een ramp gebeurt, zullen deze woorden JPB om de oren geslagen worden. Ik neem dan ook aan dat de voorlichters van Algemene Zaken met kromme tenen hebben zitten luisteren. Maar kon hij wat anders zeggen? Dat er géén vooruitgang is geboekt? Ik denk dat hij de uitspraken met samengeknepen billen heeft gedaan en hoopt en bidt dat er geen ramp gebeurt voordat zijn regeerperiode erop zit. Anders zal hij net als Colijn in het geschiedbeeld belanden, als laks en onverantwoord bestuurder.

Volgens Balkenende doet het kabinet er alles aan om risico's zo klein mogelijk te houden, maar zijn rampen nooit helemaal uit te sluiten. De premier zette vervolgens omstandig uiteen dat het van de aard van een crisis afhangt welke minister als eerste verantwoordelijk is. Volgens Balkenende is de minister van BiZa in een aantal gevallen verantwoordelijk voor de coördinatie, maar ligt bijvoorbeeld de coördinatie bij een ramp met een terroristische achtergrond bij Justitie. Als je de rapporten van het project Nationale Veiligheid erop naslaat, zie je dat een digitale aanval via het Internet initieel onder EZ valt, maar als er sprake is van een criminele intentie moet Justitie het voortouw nemen. Blijken de criminelen politiek gemotiveerd waardoor er sprake is

van terrorisme, neem de NCTb de leiding. Raakt de aanval ook de infrastructuur van de rijksoverheid, dan komen BiZa en Defensie in beeld, de één als beleidsmatig bevoegd en de ander als leverancier van het overheidsnetwerk. Dat de digitale verlamming net zo snel zal optreden op bestuurlijk niveau als in de aangevallen systemen, zal niemand ontgaan.

Volgens de minister van BiZa Ter Horst is het beter als het in alle gevallen bij haar zou belanden. Daar is wat voor te zeggen. Als je er halverwege een ramp achterkomt dat die dijkdoorbraak door een aanslag veroorzaakt is, ga je tijdens het pompen en evacueren toch liever niet de coördinatie overdragen aan Justitie? En als vervolgens blijkt dat er een vijandige mogendheid achter zit, nog een keertje aan Defensie? Doe even normaal!

De aandacht voor rampen is gegroeid naar aanleiding van Enschede, Volendam en Schiphol. Rampen waarbij maatregelen ter voorkoming gefaald hebben en het optreden van de nooddiensten (mede daarom) niet optimaal was. Sindsdien is er een aantal rampenoefeningen geweest, om op dit gebied lessen te trekken, en er zullen nog oefeningen meer volgen. Zo is er een oefening geweest waarbij gekeken is naar de effecten van een zeer massale computeruitval ("digitale verlamming"). De uitvoerende mensen van de verschillende clubs kennen elkaar nu, weten een beetje hoe de andere eilanden in elkaar steken en daar houden ze voortaan rekening mee. Dat klinkt misschien als weinig winst, maar het maakt in de praktijk een wereld van verschil. Het heeft - om maar iets te noemen - ervoor gezorgd dat de bedrijven die op 9/11 hun hoofdkantoor in het WTC hadden, binnen enkele dagen weer operationeel waren terwijl de hele directie en iedere procedure en sturing in rook op was gegaan. De lagere goden, die elkaar persoonlijk kenden van cursussen en het sigaretje op straat, regelden het gewoon onderling.

De vooruitgang zit niet op het gebied van preventie: preventie is niet wat je onderzoekt bij een rampenoefening. De premier wees in zijn verdediging abusievelijk op vooruitgang in tal van preventieve programma's, zoals die om overstromingen te voorkomen. Daar is echter bar weinig bereikt. Iedereen kan zien dat de dijken niet zijn verhoogd, de klimaatplannen nog steeds alleen maar plannen zijn, de computersystemen op hún werk niet beter beveiligd zijn, er nog dagelijkse krakkemikkige vliegtuigen laag over de Bijlmer en over de olieopslag bij Zestienhoven vliegen, dat bedrijven nog steeds illegaal gevaarlijke stoffen opslaan, en ga zo maar door. Het gaat er om wat je doet ná een overstroming en hoe dát verbeterd kan worden. Voor preventie is gewoon meer tijd nodig, probeer maar eens een dijk te verhogen in een jaar. Zeker nog nooit een paar dijkhuizen verplaatst? En een beetje budget zou ook wonderen doen, vermoed ik. Blijkbaar is het subtiele onderscheid tussen crisispreventie en crisisbeheersing ook de tekstschrijvers van onze premier ontgaan. Of zou hij deze tekst zelf bedacht hebben?

Hoog tijd om eens naar ons eigen aandachtsgebied te kijken. Informatiebeveiliging kent ook beide componenten: voorkómen en bestrijden. Bijna alle aandacht gaat uit naar preventie, er is vrijwel geen aandacht voor het optreden tijdens incidenten. Alsof het optreden tijdens incidenten triviaal is. Onze onvolprezen trits aan methodieken gaat in alle detail in op het voorkomen van ieder denkbaar scenario, zonder veel aandacht voor hoe je als organisatie moet optreden als een maatregel niet afdoende blijkt, als een bedreiging over het hoofd is gezien of nieuwer is dan onze standaard.

Niet ieder probleem is te voorkomen - volgens de leerboekjes accepteren we dan ook een aantal risico's. Al was het alleen maar omdat preventieve maatregelen de hele organisatie zodanig kunnen verstikken dat er vanzelf niets te beveiligen overblijft. Of dat er gewoon niets preventiefs denkbaar is; als middelgrote saunaketen ben je wellicht niet geëquipeerd om het Internet virusvrij te maken. Accepteren kan als het spreekwoordelijke konijntje op de A12 in de koplampen van een wit busje, maar kan ook betekenen dat je de organisatie enigszins voorbereidt om er bij een eventualiteit het beste van te bakken.

De aanname van veel bedrijven is impliciet dat de bestuurlijke structuur die de organisatie door haar dagelijkse perikelen loodst dit ook zal kunnen bij een veiligheidsincident. Dit is op zich niet zo gek - er gebeuren wel ergere dingen bij organisaties dan de blacklisting van je domein. Maar organisaties die vrijwel alleen ICT hebben of er bovenmatig afhankelijk van zijn, moeten zich wel degelijk voorbereiden op de specifieke vormen van crisisbeheersing die bij ICT horen. In de ICT komt een ongeluk zelden alleen: als je wordt aangevallen, trekt dat meer aanvallers aan. Aanpalende systemen vallen als dominostenen om, hoewel ze niet rechtstreeks geraakt worden. Bovendien duren incidenten vaak veel langer. Een stevig brandje is doorgaans na zes uur wel uitgewoed, maar een veiligheidsincident lijkt meer op een veenbrand die opeens op tig plekken tegelijk zichtbaar wordt.

Waar wij onvoldoende rekening mee houden is de uitputting die optreedt bij een aanhoudende reeks incidenten. Hoeveel dagen van zestien uur kan een gemiddeld mens scherp blijven? Een aanval kan weken of maanden doorgaan. Hoeveel weken van moeizaam beteugelde paniek kan een gemiddelde directie overleven? Hoe lang blijven overlegstructuren tussen ministeries functioneren? Denk aan de doemscenario's van de koude oorlog: als gedurende een paar weken er dagelijks alarm zou zijn, zou iedere persoon in de bevelstructuur uitgeput zijn en ieder hulpmiddel om op te treden versleten. Dit geldt ook voor de beveiliging van computers: de beheerder die blijft zitten totdat de aanval gekeerd is, maakt de organisatie kwetsbaar voor de volgende aanval. Welke manager stuurt de enige persoon naar huis die snapt wat er aan de hand is? Welke manager gaat zelf naar huis, met het risico het verwijt te krijgen dat ie lekker thuis zat terwijl de boel uitfikt? Toch zullen we het zo moeten regelen dat er ook na drie dagen frisse mensen zitten, die weten wat ze kunnen doen. En dat er tijdens een incident op één vlak ook alert gereageerd wordt op andere meldingen. Zo lang dit onder de radar blijft, is de zekerste methode om een digitale verlamming van onze samenleving te bereiken het creëren van het bestuursinfarct.

Een kwakkelend dossier

18 september 2007

Nederland moet aan het elektronisch patiëntendossier, het EPD. Nu is het nog zo dat als je in een ziekenhuis belandt, de kans erg groot is dat de behandelend arts niet over al je gegevens beschikt. Een deel ervan ligt nog op de afdeling waar je de vorige keer was, of in een ander ziekenhuis. En wat je huisarts, de bedrijfspsycholoog en de bloedbank allemaal over je weten, is zéker niet bekend. Dit kan heel vervelend uitpakken. Je loopt een grotere kans op extra onderzoeken, bijvoorbeeld omdat ze nu nog steeds je bloedgroep niet weten, of je krijgt pillen waar je allergisch voor bent, je been wordt eraf gehaald terwijl je voor een ooglidcorrectie kwam, enfin, dat soort narigheid. Om dat te voorkomen en om de bijbehorende budgetten wat zinniger te kunnen gebruiken zijn een paar knappe koppen op het idee gekomen om een landelijk dekkend patiëntendossier te maken. Nou ja, dat hebben we van het buitenland afgekeken. En passant moet het EPD ook de wachtlijsten oplossen, evenals de effecten van de vergrijzing, het tekort aan zorgverleners en zorgcapaciteit en de onbeheersbare kosten. In 2009 moet het EPD in ons land een feit zijn.

Het EPD vormt de grootste ICT-operatie in de vaderlandse geschiedenis. Alle zorgverleners, van ziekenhuizen tot apothekers, en alle verzekeraars worden gekoppeld aan een systeem dat meta-informatie over alle burgers bevat. Via deze meta-informatie krijgt de gebruiker toegang tot alle brokjes informatie die her en der over een patiënt geregistreerd zijn. De toegang tot het EPD wordt beveiligd met smartcards en het PKI-trucje. Oftewel, de authenticatie is keurig geregeld.

De discussies omtrent privacy bij het EPD worden vaak gesmoord met de mededeling dat het 'slechts een elektronische versie' is van wat er toch al vastgelegd werd. Dit is strikt genomen waar, maar gaat voorbij aan het essentiële verschil met papieren dossiers: toegang. In securitytermen: de autorisatie. Een papieren dossier zal niet zo snel in 50.000 exemplaren bij jan en alleman op het bureau gekwakt worden. Bij een digitaal dossier doe je dat bijna per definitie – behalve als je daar maatregelen tegen treft. Waarbij je moet zorgen dat iemand die de gegevens wél nodig heeft, er zonder vertraging bij kan.

Het risico dat de meeste mensen bij het EPD zien, is dat verzekeraars onoorbare dingen kunnen uithalen met de kennis die in de medische dossiers zit – het klassieke autorisatievraagstuk. Nu is er zeker wat voor te zeggen om het risico van de meest vatbare typjes uit je polissen te kunnen managen – dan kun je de premies tenminste concurrerend houden zonder aan de marges te komen. Dit risico heeft voor de rechtstreeks betrokkenen (zorginstellingen, medici en verzekeraars) niet voldoende aanleiding gevormd om écht strikte beveiligingsmaatregelen te eisen op het gebied van autorisatie voor het EPD. Dergelijk misbruik zou immers gewoon niet voorkomen en bovendien, technisch zal het erg lastig zijn, zeggen de IT-specialisten. Dus er is afgesproken dat volstaan kan worden met procedurele maatregelen, 'geborgd' met controle achteraf. Er is echter meer aan de hand. Niet alleen de cliënten, ook sommige betrokkenen kunnen klappen krijgen - in het bijzonder de artsen.

Op 18 juni 2007 heeft het College Bescherming Persoonsgegevens (CBP) op verzoek van het Ministerie van VWS een advies ingediend over de beveiliging van patiëntgegevens in het EPD. Het CBP is stelt dat alleen zorgverleners die op dat moment bij de behandeling zijn betrokken, toegang mogen krijgen tot het elektronische dossier. Dat is op dit moment niet zo. In de discussies rond het EPD wordt vaak als uitgangspunt genomen dat dit soort behandelingsgebonden - dus dynamische – autorisatie op digitale patiëntgegevens technisch niet haalbaar is. De stand van zaken in ICT is op dit moment dat we al behoorlijk tevreden met onszelf

zijn als we de juiste statische autorisaties tot computersystemen kunnen uitdelen - en we gaan al helemaal aan de champagne als we die weer op tijd kunnen intrekken. Aan de granulariteit van dynamische autorisatie op délen van informatie en gegevens binnen applicaties zijn we nog nooit toegekomen.

Op dit moment ligt er een wetsvoorstel bij de Raad van State voor het EPD. Het lijkt er op dat maatregelen om 'need to know' en daarmee patiëntvertrouwelijkheid te waarborgen, niet afgedwongen zullen worden en het advies van het CBP zal worden genegeerd. Nu kun je natuurlijk beweren dat medici gewend zijn de privacy van patiënten te respecteren en dat is voor het overgrote deel ook zo. Al was het alleen maar omdat de aandoening van een patiënt alle aandacht (en tijd) trekt en het privéleven van de patiënt niet. Je bent niet mijnheer van Baalen, maar 'die dubbele botbreuk met complicaties', zeg maar. Maar het kan ook anders gaan. Bijvoorbeeld wanneer de patiënt een bekende Nederlander is. Dan slaat de nieuwsgierigheid tóch toe, zoals bij de politie gebeurde toen voetballer Robin van Persie beschuldigd werd. Het dossier bleek voor veel medewerkers van de politie toch té interessant om met rust te laten. De bijbehorende publiciteit was erg vervelend voor de politie. Maar goed, burgers kunnen niet zelf een ander politiekorps kiezen. De bedoeling van marktwerking in de zorg is dat burgers echter wél een ander ziekenhuis kunnen kiezen.

Het CBP heeft het ministerie al in een eerder stadium de suggestie gedaan de technische uitvoerbaarheid van dynamische, behandelingsgebonden autorisatie te laten onderzoeken. Het ministerie is echter (nog) niet overgegaan tot het laten uitvoeren van een dergelijk onderzoek, en gegeven dat de wet al door het kabinet goedgekeurd is en bij de Raad van State ligt, zal dit ook wel niet meer gebeuren. Dit is een gemiste kans, want voor een dergelijke voorziening zijn de meeste informatie-bouwstenen met het Burgerservicenummer BSN, het UZI register van medici en de diagnose-behandelcombinatie (DBC) al lang voorhanden. Alleen is er geen kant-en-klaar product beschikbaar. De technologie bestaat vooral niet omdat er geen vraag naar is geweest, waarschijnlijk omdat het op dat moment niet bestond. Typisch een kip en ei verhaal. Het lijkt mij echter bepaald niet onmogelijk iets dergelijks te bouwen met een workflowaanpak en ik vermoed dat de politie na de zaak Van Persie ook wel geïnteresseerd is in een dergelijke oplossing. Het VIR-BI schrijft immers ook het Need To Know beginsel voor, wat blijkbaar nog niet overal ingevoerd is. En de ultieme kandidaat is het Elektronisch Kind Dossier, dat blijkbaar straks voor deze en gene in jeugdzorg en onderwijs zonder Need To Know toegankelijk is. Dit dossier bevat nog veel gevoeliger informatie dan het gemiddelde EPD. Nu is er al geklaagd dat er alleen medische informatie in zou staan – blijkbaar is geloofsovertuiging of het wonen aan open water een ziekte. Sla de basisset er maar op na.

Maar goed, terug naar het EPD. Het niet voorschrijven in de wet van de dynamische autorisatie tot patiëntgegevens lost het échte probleem niet op: artsen zijn als vrije beroepsbeoefenaars in hoge mate aansprakelijk voor fouten. Op dit moment laat minister Klink van VWS een onderzoek uitvoeren naar de aansprakelijkheid bij medische missers. Volgens Klink kunnen artsen die het elektronische dossier van hun patiënten niet goed bijhouden, boetes krijgen, maar ook uit hun ambt worden gezet. Een interessante stelling, want wat is goed? Gegeven dat het EPD ook 'clinical notes', oftewel kladjes en geheugensteuntjes zal moeten bevatten, is het stellen van een dergelijke kwaliteitseis dapper te noemen. Bedenk je dat als je diagnostische kladjes of observaties tijdens behandelingen de toets der kritiek moeten kunnen doorstaan – en je je carrière kunnen kosten, je ze heel wat minder snel en gedetailleerd zult maken. En zéker niet op een plek zult opslaan waar iedereen bij kan.

Diagnostische- en behandelnotities zijn geen objectieve informatie; het is ontstaan in een context en moet geïnterpreteerd worden. In het denken over het EPD wordt medische informatie echter gezien als absoluut bewijsbare informatie die eenduidig is en niet interpretatiegevoelig. Nu is dit

een selffulfilling prophecy: artsen zullen het risico mijden door alleen de 'objectieve werkelijkheid', dus het minimum aan informatie, vast te gaan leggen in het EPD. De dossierplicht voor hulpverleners (Artikel 7:454 BW, wet op de geneeskundige behandelingen) schrijft immers niet in detail voor wat er vastgelegd moeten worden. De kans is dan ook groot dat veel relevante informatie niet in het EPD terecht zal komen maar in andere registers, die voor eigen gebruik worden gehouden. Of in het geheel niet vastgelegd worden. Waardoor de beoogde kwaliteitsverbetering van de zorg door de invoering van het EPD wel eens behoorlijk tegen zal kunnen vallen. Voor de geïnteresseerden in deze materie geeft de oratie van de Leidse hoogleraar klinische informatiekunde Zwetsloot fascinerende stof tot nadenken.

Bij het EPD zijn medische missers niet het enige risico dat artsen lopen. Bedenk je dat, zolang niet traceerbaar is wie er allemaal toegang tot de dossiers kan krijgen of – belangrijker nog - gekregen heeft, het verantwoordelijk stellen van de arts een wassen neus is. Hoe kan deze ooit aantonen dat de dossiers goed bijgehouden zijn als weet ik wie er allemaal in kunnen krassen en poetsen? Daarom moeten de medici aandringen op een wettelijke borging van de bescherming van patiëntgegevens in het EPD op de manier zoals het CBP dit adviseert.

Dit is niet de zaak van zorgverzekeraars of de IT-afdelingen van zorginstellingen, de clubs die een mildere vorm van regulering voorstaan. Zij draaien hooguit op voor de kosten van herstel van de fouten in de informatie, zolang ze zich tenminste aan de regels hebben gehouden. Artsen lopen buitenproportionele risico's; uit het ambt gezet worden is als sanctie even wat anders dan een negatieve beoordeling door de Inspectie voor de Volksgezondheid. Ja maar, zo'n oordeel kan zelfs op het Internet gepubliceerd worden. Nou, nou, dat komt aan. Zelfs al zou de instelling moeten opdraaien voor de kosten van extra behandelingen en het smartengeld moeten betalen, valt dit in het niet bij wat een medicus kwijt kan raken, zeker een jongere arts. Daarbij is geld van je baas kwijtraken van nogal andere ordegrootte dan uit eigen zak betalen. De kosten van het uitgebreid inspectiecircus zoals dat nodig is in de huidige opzet, zullen ook niet meevallen. Dit soort 'borgende kwaliteitsinstrumenten' leidt in de regel tot een bureaucratie en een starheid waar de oude sovjets jaloers op zouden zijn.

Vergelijk het 'verliezen' van patiëntgegevens met een beleidsambtenaar die ontslagen wordt omdat hij onbedoeld wat staatsgeheimen gelekt heeft. Deze laatste wordt misschien ook ontslagen (en zijn screening kwijtraken), maar hij zal zijn vaardigheden elders kunnen inzetten. Medici zijn technisch specialisten; zij kunnen weinig anders dan waar ze voor opgeleid zijn. Zij zullen een ander vak moeten kiezen, of emigreren. Gezien deze sanctie zijn patiëntgegevens categorisch geheimer dan de identiteit van onze spionnen. Of dit allemaal wel zo reëel is, mag je je wel even afvragen.

Gelukkig kan het management rond de zorg nog wel wat slimme mensen absorberen, dus in de bijstand zullen de uit het ambt ontzette artsen niet snel komen. Maar het gaat in ieder geval niet bijdragen tot het verhelpen van het tekort aan artsen.

Een alternatief voor de arts is van de zorginstelling een verzekering te eisen tegen de schade uit een dergelijk scenario - zoiets als de gangbare verzekeringen voor de bestuurders tegen claims van wanbestuur. Dan kan een andere verzekeraar vervolgens de ICT afdeling en het bestuur weer verzekeren tegen claims van de eerste verzekeraar.

De megaoperatie om het EPD in te voeren is zonder deze losse eindjes uit beveiligings- en informatieland al zeer ambitieus. Al zou het op tijd lukken, dan hebben we op deze manier hooguit een systeem met zeer beperkte voordelen, tegen torenhoge kosten.

De Chinezen komen! Of niet, natuurlijk.

www.security.nl, verschenen in twee afleveringen op 1 oktober 2007 en 17 oktober 2007

De laatste periode is er weer een reeks berichten geweest over hackers uit het Chinese leger. Zij zouden aanvallen uitvoeren op kritieke infrastructuren van allerlei westerse overheden en technologiebedrijven. Het Pentagon, Whitehall en de Franse en Duitse overheid geven gelijkluidende signalen. Het is niet nieuw. Dit soort berichten zien we sinds 1999. Volgens de autoriteiten zou China streven naar digitale dominantie rond 2050. Veel indruk maakte het programma Titanenregen in 2003, waarvan menig inlichtingendienst danig gestrest raakte. Via de e-mail kwamen er MS Office-bestanden binnen met trojans aan boord, die niet herkend werden door allerlei virusscanners. Eerder dit jaar hebben we digitale schermutselingen gezien rond Rusland en haar voormalige wingewest Estland en recent meldde China zélf veel last van hackers te hebben. Deze gebeurtenissen voegen een nieuwe dimensie toe aan het verantwoordelijkheidsgebied van Security: overheidshackers en nationale veiligheid. Externe bedreigingen dus, terwijl wij nog middenin het paradigma van interne bedreigingen zitten.

Hoe komen dit soort berichten tot stand? Immers, afgezien van allerlei James Bond fantasieën is het onwaarschijnlijk dat er zekerheid bestaat over de identiteit en al helemaal de motivatie van de verspreiders van de trojans. Overheden denken over het algemeen dat succesvolle aanvallen op hun digitale infrastructuur boven de macht van een geïsoleerde script-kiddie gaan - ze besteden immers veel aan beveiliging. De logica is dat als er succesvolle aanvallen plaatsvinden, er dus sprake moet zijn van een grote organisatie, en dat kan alleen een vreemde mogendheid zijn. Om de grote beveiligingsinspanning teniet te doen, is dus een grote aanvalsinspanning nodig. Lt. Gen. Robert Elder, commandant van het US Air Force Cyberspace Command: "To seriously disrupt us, you're not going to be able to do this with a 'teenage hacker' capability." Een succesvolle trojan op de PC van minister Gates of Angela Merkel die niet ergens anders gemeld is, geldt in deze denkwijze dan ook als het bewijs voor een gerichte aanval van een vreemde mogendheid. En als er verkeer richting China gaat, is dat dús in opdracht van het Chinese leger, dat immers zelf zegt bezig te zijn met cyberwar.

Een kenmerkend aspect in cyberwar dat juist militairen bekend voor zou moeten komen, is het asymmetrische ervan. A-symmetrische oorlogsvoering houdt in dat de inspanningen van aanval en verdediging in de verste verte niet op elkaar lijken: om alle zeewegen te beveiligen tegen één terrorist in een rubberbootje heb je nu eenmaal honderden marineschepen en vliegtuigen nodig. Om een groot netwerk te verdedigen houdt je bendes maatregelen en systemen in stand: om het te kraken is één miniscuul gaatje genoeg. Een aanvaller kan dus volstaan met de inspanning die een hobbyist moet doen, ook al krijgt hij zijn opdrachten van officiële agentschappen.

Laten we Ockhams scheermes eens erbij nemen - "entia non sunt multiplicanda praeter necessitatem", vrij vertaald: de eenvoudigste verklaring is meestal de beste. De conclusie dat er andere overheden achter zitten kan maar zo voorbarig zijn. Want dat anderen de aanval niet gevonden hebben kan ook betekenen dat ze gewoon iets minder goed opletten of het niet melden. Als je een trojan aantreft op een machine in je netwerk of in de mailserver, neem je dan de moeite om de code veilig te stellen en uit te zoeken welke het nu precies is? Nee, je AV verwijdert hem gewoon. Stel, je hebt hem toch nog, neem je dan de moeite om dat te melden bij een AV leverancier? Weet je hoe dat allemaal moet? Maakt het voor je organisatie eigenlijk uit welke trojan het precies is? Nee, nee, nee. Een goede beheerder zal een besmette machine gewoon opnieuw inspoelen. Ik denk dat erg weinig mensen buiten de overheid de moeite nemen om Govcert te bellen.

Een paar AV producten sturen de gevonden malware automatisch op voor nadere analyse, maar bij een geringe verspreidingsgraad zullen de AV makers er geen signatures voor ontwikkelen. En dat geldt voor zeer veel trojans. Slechts een enkeling komt in grotere aantallen voor. Een niet gedetecteerde trojan zegt dus niets over de geavanceerdheid ervan. Het zegt eerder iets over de gangbaarheid ervan. De kans is groot dat dit ook bij de trojans op de overheidsmachines het geval is.

Iets slimmere trojans verspreiden zich via sociale netwerken. Als een aangevallen persoon toevallig een netwerk binnen de veiligheidshoek van de overheid heeft, dan zal een aanval automatisch over dat netwerk propageren. Is er dan sprake van een gerichte aanval?

Als je vervolgens leest dat de aangetroffen spyware gebruik maakt van belegen exploits in oudere Windows-software, dan wordt de claim van een 'goedgeorganiseerde militaire operatie' bijna kolderiek. Het zou in ieder geval niet zo best zijn als dit het beste is wat wij van een goedgeorganiseerde militaire operatie mogen verwachten.

Het lijkt erop dat we van deze sfeer van interpretaties en giswerk afhankelijk zullen blijven. Want als je probeert te achterhalen waar een aanvaller écht vandaan komt, zoals de free-lancer bij de Amerikaanse overheid Shawn Carpenter deed bij de titanenregen in 2003/4, die hij traceerde naar een drietal routers in Guangdon, loop je al snel het risico van een diplomatiek incident. Dan krijg je bezoek van mensen in een donkerblauwe Audi met getinte ramen. Meer bewijs dan bovenstaande logica zullen we dan ook niet snel krijgen. We moeten maar leren leven met grote verhalen en onzekerheid. Het is daarbij verstandig ons niet te verliezen in een angstpsychose: als het waar is dat vreemde mogendheden gerichte aanvallen uitvoeren op onze bedrijven en onze overheid is dat zeer ingrijpend voor ons leven en onze maatschappij. Het zouden maar zo de eerste schermutselingen kunnen zijn van een volgende wereldoorlog, nietwaar?

De verdenkingen richting het Chinese volksleger brengt ons bij de klassieke vraag van de casus belli: kan er op enig moment sprake zijn van een oorlogshandeling, waarbij een digitale daad leidt tot een echte oorlog? De VS beschouwen het Internet als Amerikaans grondgebied. Iedere aanval over het Internet zou in het traditionele denken dus een aanval op de VS zijn, zelfs als deze gericht was op een ander land. Het zou prettig zijn te weten of het Internet ook onder het NAVO-verdrag valt - zijn wij gebonden aan het geven van militaire assistentie?

Zoals we in het eerste deel van deze column zagen, is de ontwikkeling richting cyberwar onmiskenbaar. Landen die nu nog geen vermogen tot cyberwar hebben, zullen het snel gaan opbouwen. Of de verhalen waar zijn en 'De Chinezen komen' ... is daardoor niet relevant. Ik denk dat dát nog wel even zal loslopen. Als China economische schade wil toebrengen aan de VS hoeven ze alleen maar wat dollars te dumpen. En daar hebben ze meer dan genoeg van. Spionage is natuurlijk iets anders, maar dat is niet nieuw, hoewel het vaak genegeerd wordt. Maar goed, wat we wél zeker weten is dat cyberwar de komende tijd hoog op de agenda staat. Naar ik aanneem, zelfs in ons land.

De bedreiging van digitale oorlogsvoering mag dan op dit moment overtrokken worden, de kwetsbaarheid is zeer reëel. Het militaire overwicht van de VS (en in het verlengde, het Westen) is gebaseerd op beweeglijkheid en de kwaliteit van de troepen en de middelen, niet op de hoeveelheid. Daarbij is informatie essentieel: als je alleen een paar supertanks hebt, wil je die precies op tijd op de goede plaats hebben. Het verstoren van het informatieoverwicht kan de militaire balans snel doen omslaan - waarbij de supermacht bij uitstek geraakt wordt in zijn achilleshiel, de informatievoorziening. Digitale oorlogsvoering is bij uitstek een wapen voor de zwakkere partij in een hedendaags conflict. Het beschermen van het informatieoverwicht is voor de sterkere partij dan ook een zaak van levensbelang.

Een aanval hoeft niet gericht te zijn op de militaire infrastructuur om dit informatieoverwicht te ontwrichten. Het zwaartepunt van een land ligt eerder in de economische stabiliteit dan in haar vermogen kruisraketten op een ver doel te laten landen. Hierbij gebruik ik de term zwaartepunt in de betekenis van Clausewitz, als het zenuwcentrum van een mogendheid. In onze tijd vormen informatie en communicatie samen met mobiliteit (olie) het zwaartepunt van een land.

Dat de VS zenuwachtig zijn, is terecht. Ze zijn kwetsbaar. De combinatie van middelen (mobiliteit en informatie) die zo succesvol was bij de verovering van Irak en Afghanistan, is in gevaar. In het Chinese militaire denken, zoals verwoord door Wang Pufeng in 1995, is het breken van dit overwicht essentieel. Of China nu of later, of een andere mogendheid voor onze achilleshiel gaat, is eigenlijk niet zo heel belangrijk. Zwakte in het digitale domein bedreigt de grondslag van het militaire overwicht en daarmee de welvaart van het westen. Dit geldt mutatis mutandis ook voor ons land: die paar opgepoetste Leopards of ge-midlifede F16's kunnen een veel grotere partij aan, maar zijn kansloos als er geen informatieoverwicht is. Dit vind je niet terug in de NDD, de Nederlandse Defensie Doctrine. Evenmin als andere dimensies aan cyberwar, overigens.

De keuze is: óf veel aandacht voor beveiliging van onze informatievoorzieningen, óf terug naar de veel omvangrijker krijgsmacht van weleer, met navenante budgetten. Dit laatste zal sommige ijzervreters wel aanspreken, maar er zijn gewoon te weinig potentiële zandhazen om weer een paar legerkorpsen te kunnen opstellen. Bovendien is het hedendaagse oorlogstuig volledig afhankelijk van de informatievoorziening dus dan zullen eerst weer allemaal nieuwe spulletjes moeten gaan verzinnen. Ik denk niet dat Wouter Bos hiervoor de knip wil opentrekken. Er blijft dus niets anders over dan veel meer aandacht voor wat ons bedreigt. Kortom, het is tijd voor een nieuw paradigma in zowel de civiele als de militaire sfeer.

De nieuwe wapenwedloop is begonnen, maar dit is er niet één van zoveel mogelijk ijzer uit de kast rukken en dat in nette rijtjes neerzetten. Het is er één van het aanhaken van kennis en talent, ongeacht rang of stand... De Chinezen hebben dát goed begrepen, zie hiervoor dit artikel van Wei Jincheng uit het dagblad van het volksleger uit 1996. Dit schetst een losse organisatie met een hoge mate van empowerment in de lagere echelons, zodat de inventiviteit en kennisontwikkeling gewaarborgd wordt.

Het wordt wennen voor de heren en dames bureaucraten hier te lande, want inhoudelijke kennis en een procesgeoriënteerde autoritaire organisatie gaan slecht samen. Maar goed, onder druk wordt alles vloeibaar en er is hier wellicht sprake van druk, dus wie weet.

Als we dan toch aan de vooravond staan van een cyberwar is 't minste dat ik kan doen een stappenplan aanreiken, waar we heel voorzichtig over kunnen nadenken:

1. De digitale casus belli: De NAVO zou kunnen uitdragen dat er ook zoiets kan bestaan als een casus belli in het digitale domein. Meer duidelijkheid hierover zou een zekere mate van terughoudendheid kunnen stimuleren bij andere partijen. Via onze diplomatieke kanalen kan de discussie aangeslingerd worden.
2. Afscheid van de silo's: Het is onmogelijk iedere kilometer van de digitale grens te bewaken - we weten geeneens waar die ligt. Het vergaren van betrouwbare informatie in deze 'grensbewaking' is echter cruciaal. De overheid zou haar eigen informatieverwerving moeten versterken zodat zij feiten van fictie kan onderscheiden. De inlichtingendienst zullen meer naar buiten moeten treden: afspraken en daadwerkelijke oefeningen met ISP's, elektriciteitsbedrijven, banken, telco's en meer van dat - op een hoger bestuurlijk niveau en minder vrijblijvend dan van de huidige CERT-verbanden.
3. Eenheid van commando: Overheidsdiensten vormen een lappendeken. Ongeacht wat er op dit moment precies aan de hand is, is er een cyberwapenwedloop op til. Daarom is het

verstandig duidelijkheid te creëren rond de verantwoordelijkheden en spelers op het digitale slagveld. Unity of command is een absolute vereiste om te kunnen handelen. Internetveiligheid is op dit moment ondergebracht bij EZ, en een beetje bij Justitie en BZK, maar als oorlog in zicht komt ruikt het toch naar de Eerste Hoofdtaak van Defensie. En dat zal dan een volledig nieuw krijgsmachtonderdeel moeten worden, zo eentje die je niet binnen enkele weken uit de grond stampt. Iets als het Amerikaanse Cyber Command, de 8e luchtmacht, dat sinds 2006 operationeel is. Maar wél graag met een bredere scope dan bij onze bondgenoten, die moeten leven met een beperking tot 'militaire systemen'. Je mag alleen groene bitjes aanvallen, hoor! Een dergelijke knieval voor departementale territoriumdrift maakt een Cyber Command gelijk zinloos. Nu zul je zeggen dat die beperking natuurlijk direct van de baan is als er iets aan de hand is... Maar oorlog en vrede zijn nu eenmaal niet gekaderd langs de overzichtelijke lijnen van overheidsdiensten, en kunnen bovendien tegelijkertijd en door elkaar heen bestaan. Dus of je op tijd je scope aangepast hebt en tijdig kunt optreden, is maar afwachten.

   De digitale inlichtingendienst die zorg draagt voor deze 'grensbewaking' zal een onderdeel moeten vormen van dit apparaat, en dus ook in het Defensielandschap terechtkomen.
4. Herziening van de best practices: De manier en invulling van defensieve maatregelen zal herzien moeten worden. De huidige best practices zijn opgesteld om bescherming te bieden tegen vandalen en criminelen, waarbij de beveiliging naar binnen is gericht, omdat de meeste aanvallen daarvandaan zouden komen. Aanvallen van buiten zijn eerder puur technisch van aard dan die van binnenuit, dus het accent in security zal verschuiven richting techniek. Omdat de hulpbronnen van de tegenpartij groter zijn of groter worden dan die van de gemiddelde briljante hobbyist al dan niet als lid van een criminele organisatie, zal er zeker een snellere evolutie van aanvalstechnieken optreden. Dit zal de levensduur van onze nog te ontwikkelen best practices onder permanente druk zetten.
5. Primaat van de kennis: Het kunnen acteren in crisissituaties van cyberwar zal minimaal het vermogen tot een tactisch offensief vragen. Het ontplooien van dit vermogen zal een zware wissel trekken op de toch al schaarse expertise bij de overheid en in de markt. Zeker als we terugschrikken voor die briljante Chinese informaticastudenten die onze universiteiten bevolken....

Geavanceerde onvoorspelbare aanvallen kun je alleen met een hoog kennisniveau pareren of - beter nog - omdraaien. Het zal waarschijnlijk niet genoeg zijn om een paar goeie studenten van de Nederlandse Defensieacademie hierop te zetten. Een kweekvijver voor het benodigde talent zal niet eenvoudig zijn - de markt lonkt immers en voor een schaal 10 of 11 Rijksoverheid komt een Security specialist zijn bed niet uit. Een oplossing kan wellicht gezocht worden in het creëren van een mobilisabele strijdkracht - maar niet één van security managers graag, we hebben technische kennis nodig, geen procedures. Het idee van dienstplichtige hackers, net als in China, zal overigens wél even wennen zijn voor de gemiddelde sergeant-majoor. Maar het wordt vast gezellig.

Afscheid van het netwerk

vrijdag 05 oktober 2007

Een netwerk is niet meer wat het geweest is. Sommige mensen hebben het daar best moeilijk mee. Door de groeiende toepassing van mobile devices, koppelingen naar buiten en het werken buiten de eigen kantoorlocaties is het niet altijd duidelijk waar het eigen netwerk ophoudt en de buitenwereld begint. Waar is de buitenmuur gebleven? Vooral 35-plussers in onze branche moeten nog wel eens wennen aan het idee dat de buitenmuur níet meer het focuspunt van de beveiliging is.

Voor wie het niet (bewust) meegemaakt heeft: er was een tijd dat een netwerk bestond uit aan elkaar geknoopte pc's die – met een vaartje van maximaal 2 Mb – over coax printers en bestanden deelden. Centraal stond wat groot ijzer, waarop alle belangrijke dingen gebeurden. "Buiten" was waar je wat kon "ophalen". Dat deed je bij wazige dingen als BBS-en, later compuserve, en nog later Internet. De buitenmuur bestond uit modempools waarop onverlaten zo maar inbelden. Beveiliging was het geheimhouden van die nummers. Dat was best overzichtelijk.

Wél een uitdaging was het om binnen een netwerk verschillende classificatieniveaus van informatiebeveiliging aan te kunnen. De grootste bedreiging vormden hobbyende gebruikers. Toen bleek dat het toch wel zeer lastig was om een granulaire autorisatie af te dwingen en te onderhouden, ontstond System High. Kwade tongen beweren overigens dat System High een semantische truc is voor het afschaffen van beveiliging.

In System High wordt alle informatie binnen een netwerk als even waardevol beschouwd, omdat het op dat netwerk staat. Het netwerk wordt dan ook als geheel gerubriceerd. Het concept is met name binnen de overheid en bij grote financiële instellingen formeel omarmd, maar heeft ook daarbuiten veel invloed op het denken van beveiliging gehad. In System High is het netwerk een geïsoleerde omgeving, en ieder koppelpunt met de buitenwereld een controlepunt waar alle informatiestromen tot in detail gecontroleerd worden. De oplossing die System High biedt voor het probleem van hobbyende medewerkers is dus een strikte selectie aan de poort.

Het klassieke alternatief voor System High is Multi Level Security (MLS): in een MLS-netwerk worden verschillende classificaties onderkent en er worden technische en procedurele maatregelen getroffen om vermenging van deze te voorkomen. Nu is het adagium dat MLS niet realistisch was en System High wél, gegeven de kosten en de technische stand van zaken. Maar dat was in 1974.

System High is nog steeds een belangrijk beginpunt van veel beveiligingsdenken, bij een incidentele tent zelfs nog formeel. Hier wreekt zich dat het theoretische kader onder informatiebeveiliging niet echt onderhouden wordt. Dat laat zich volgens mij verklaren uit dat je eerst techneut wordt en als je het allemaal niet meer kunt of wilt volgen op grond van je leeftijd het management mag versterken. In beleidsland heet dit conservatisme proven technology en best practices. Laten we eens dieper ingaan op de theorie.

ICT-beveiliging kent twee deelgebieden, te weten informatiebeveiliging (InfoSec) en computerbeveiliging (CompuSec). Het gaat natuurlijk allemaal om het beveiligen van de informatie. Het beveiligen van de computersystemen, waarop de informatie zich zou kunnen bevinden, de CompuSec, wordt daarom meestal ondergeschikt gemaakt aan de informatiebeveiliging.

Voor Informatiebeveiliging geldt als randvoorwaarde het labellen van informatie en hulpmiddelen als applicaties en systemen, om deze te kunnen besturen. Dit betekent dat objecten voorzien worden van een uniek kenmerk, een identiteit. In de regel bestaat deze identiteit alleen in de beleidsstukken, omdat bitjes, bestanden en computers geen label kunnen krijgen.

In feite wordt CompuSec als "Next Best Thing" ingezet voor het bereiken van InfoSec: we kunnen de informatie niet beveiligen omdat we niet daadwerkelijk labellen, dus we steken de inspanning in het beveiligen van de computersystemen en netwerken. In het "System High" denken wordt dit tot in extremo doorgetrokken: we schaffen labelling af en concentreren ons op de afscherming van het netwerk als logisch geheel. Zo wordt informatiebeveiliging indirect gerealiseerd, met weinig zekerheid rond de resultaten.

Maar de jaren 70 zijn toch echt voorbij. Het aantal koppelpunten met de buitenwereld is zo groot en complex geworden dat het eigen netwerk zelfs in beleidsstukken niet meer af te kaderen valt. De theoretici van informatiebeveiliging zien het ook. Op deze schokkende ontdekking zie je verschillende reacties.

De ene school roept dat 'het lokale netwerk' niet meer bestaat ('deperimeterisatie'), en dat iedere machine dus beschermd moet worden als ware het onderdeel van het Internet. Dit slaat vooral aan bij mensen die privé al lang geleerd hebben om te gaan met de risico's van Internet. Meestal door een gemengde aanpak: lokale beveiliging, het besef dat afgeschermde informatie eigenlijk niet bestaat, en de acceptatie van het feit dat virussen en aanvallen net zoiets zijn als de files op de A2 – ze horen er kennelijk bij. Deze school wordt ondersteund door een merkwaardige coalitie van makers van desktopfirewalls, antivirusproducten en aan de andere kant Linux en Mac adepten. Dit leidt immers tot onkwetsbare systemen, nietwaar.

De andere school roept dat de buitenmuren nog hoger en beter moeten en kunnen en dat je binnen 'gelaagde beveiliging' moet opstellen. Hierin vind je vooral de meer klassieke enterprise automatiseerders en bestuurders die het individualistische van de deperimeterisatie niet zien zitten – het categorisch vertrouwen van gebruikers en het accepteren dat écht vertrouwelijk niet bestaat is voor hen een aantal bruggen te ver. Deze school wordt ondersteund door de leveranciers van 'oplossingen' van laag 2 tot en met 8, met schitterende appliances die IDS, IPS, IdM, IAM, DomSec en de hele verdere afkortingenbrij in hapklare brokken kunnen 'implementeren'.

Beide stromingen weerspiegelen in feite een veel dieper liggend wereldbeeld. De eerste school is een liberale school waarin mensen zelf kunnen – en moeten – denken. De vrije stroom van informatie levert meer op dan het monopoliseren ervan. Deze school gelooft in intern ondernemerschap en innovatie.

De tweede school heeft een meer autoritair wereldbeeld, waarin een organisatie een koekjesfabriek is waarvan de medewerkers de processen moeten uitvoeren zoals ze 'in het beleid' voorgeschreven zijn. Mensen worden in dit beeld tegen zichzelf en elkaar beschermd en het onthouden van informatie ('Intellectueel eigendom') is de basis van concurrentievoordeel. Je kunt deze posities in feite zo projecteren op de klassieke links-rechts verhouding. Het is dan ook niet erg waarschijnlijk dat er een hanteerbare synthese zal ontstaan. Waarschijnlijk blijven we tot in lengte van dagen de concrete dingen uit beide scholen naast en door elkaar implementeren. Keuzes maken blijft immers lastig.

Wat niet meet, wat niet deert

13 november 2007

Bewakingsystemen zien bepaalde zaken wel en andere niet - dat is inherent aan iedere vorm van geautomatiseerde detectie. In feite zijn er twee manieren om te bewaken: de eerste het is signaleren van vooraf gedefinieerde foutsituaties (het herkennen van een virus-signature of een reeks verdachte instructies in verder onbekende trojan, maar ook zoals iets te hard rijden). De tweede is een aanpak om situaties door hun ongebruikelijkheid op te laten vallen. Denk hierbij het uitproberen van meerdere IP adressen in een subnet of het slingeren over de hele rijbaan. Dit is een vorm van anomaliedetectie. Bij IDS systemen zie je vaak dat beide benaderingen mogelijk zijn, zodat de kans dat een gevoelige situatie opvalt, groter is. Dat is reuze handig.

De praktijk van anomaliedetectie is echter weerbarstiger: om een anomalie terug te vertalen naar een concreet incident, moet er onderzocht worden wat er aan de hand is. En daar wreekt de gladde interface van de mooi vormgegeven appliances zich - de bedienende mens moet complexe patronen kunnen analyseren, terwijl het apparaat en bijgevoegde salespitch de indruk wekt dat een aapje het trucje wel zal kunnen. Je treft dan ook zelden een beheerder of eigenlijk IDS operator aan die in staat is de onbekende situaties te herkennen. En nog schaarser zijn die, die het ook daadwerkelijk en met enige regelmaat dóen.

Wat ook niet helpt bij IDS-en is het kunnen finetunen van het instelbare alarmniveau, waarbij je bij foutsituaties een rood stoplicht kunt laten tonen. Dat moet, omdat sommige patronen voor het specifieke netwerk dat je moet bewaken daadwerkelijk een bedreiging zijn en anderen foutsituaties weer niet. Het is heel verleidelijk dit zeer spaarzaam in te stellen, omdat rode stoplichten ertoe leiden dat je iets moet gaan doen. Daarbij vraagt de analyse van een verdachte reeks packets veel kennis van kwetsbaarheden en het eigen netwerk. Zoek je een patroon uit, dan kan het zijn dat deze verwijst naar een aanval die systeemspecifiek is. Zo lang je niet weet wat voor applicaties je feitelijk allemaal hebt, weet je niet waar je gevoelig voor bent. Het is heel verleidelijk om te veronderstellen dat je een bepaald script nergens hebt. In de gemiddelde CMDB vind je de informatie niet, dus....

Er zijn nog andere showstoppers. Veel incident-tickets staat behoorlijk beroerd in de SLA rapportage, en een paar onduidelijke meldingen in een bewakingssysteem zijn geen moeilijk gesprek met de service manager waard....

Bedenk je dat in veel organisaties incidenten waarbij geen storing in de dienstverlening optreedt, helemaal niet kúnnen bestaan, volgens het servicemodel. Zonder ticket heb je geen werkorder, en mag je er helemaal geen tijd aan besteden.

De laatste nagel in de doodskist is de natuur van een techneut. Een echte automatiseerder streeft er naar om bij voorkeur niets met het handje te hoeven doen, dus een waarschuwingsysteem zó instellen dat er vaak bellen afgaan, is tegennatuurlijk. Omdat het IDS-systeem zélf gewoon werkt, is het uitsluiten van een wazige foutmelding een prima manier om een incident te sluiten.

De consequentie is dat de overgrote meerderheid van de IDS systemen alleen bekende issues zal detecteren, waar je veelal - als je een beetje bij blijft met patchen en virussignaturen - toch niet gevoelig voor bent. Dit leidt tot een complete vervreemding van de werkelijke situatie op de perimeter. Meten is weten, maar zolang je alleen meet wat je al weet, weet je niet wat je niet weet. En dan weet je dus niets. Bij security-managementinformatie geldt helaas ook het bekende adagium van garbage in en garbage out.

De resulterende "veilige" situatie is in feite die waarbij de bestuurder die 's nachts met 97 km/h over de randweg Eindhoven rijdt, een prent krijgt, en die andere chauffeur die stomdronken met alleen stadslichten op de middenbaan slingert met 70 km/h, ongezien door mag. Intussen meldt de politieke leiding een toename van de veiligheid op het baanvak. Dat doel kan echter alleen gerealiseerd worden door ook een ouderwets concept als een agent die zelf kijkt in te zetten. Maar daar is helaas geen budget of mankracht meer voor.

This Is Me

woensdag 28 november 2007

Naymz.com is een 'sociale netwerksite' voor Reputation Management for Professionals. Een soort LinkedIn dus. Maar met een interessant verschil: voor een heleboel mensen is er alvast een profiel aangemaakt. Ben je één van die gelukkigen en tref je je eigen naam aan, dan kun je zeggen "This Is Me". Vervolgens kun je een wachtwoord kiezen en je profiel verder aanvullen en in gebruik nemen. Volgens de Terms of Use mag je je niet voor een ander uitgegeven. De rest van de Terms of Use gaan over vunzige content, de belangen van de aanbieder - kortom het feit dat je volledig aan de wolven bent overgeleverd als er iets misgaat. En als iemand anders je naam en profiel inpikt, ben je gebonden aan Terms of Use die je nooit gezien hebt... Op Naymz.com heb ik lekker zitten rondklikken en nu ben ik een heleboel verschillende mensen.

Nayms.com maakt het wel heel eenvoudig om iemands identiteit te kapen. Hij bestaat immers al. Eén klikje en je bent binnen. Heb ík dan een identiteit gestolen? Of heeft Naymz dat gedaan door alvast een profiel aan te maken en dat vervolgens te grabbel te gooien...?

Dergelijk misbruik kan - hoewel iets minder eenvoudig - op alle sociale netwerksites. De feitelijke identificatie is namelijk meestal het e-mail adres. Ik kan een profiel aanmaken dat verdacht écht overkomt, zeker als ik het échte CV van iemand heb. Een leuke query op google met CV en filetype:doc levert genoeg kandidaten op om vrolijk te gaan klieren.

Soms is het e-mail adres dat de identiteit bepaalt een bedrijfsgebonden adres. Dan is er een redelijke kans dat dat ook het echte adres is. Maar de meeste mensen kiezen een gmail of ander pseudo-anoniem adres, omdat het doel van de site toch zeer sterk richting jobhoppen gaat en je niet wilt omkomen in de spam.

Als je een verzoek ontvangt om te linken, kun je eigenlijk alleen afgaan op het gevoerde mailadres en als je dat kent, kun je het accepteren. En daar speelt natuurlijk een klassiek probleem: een mailadres als (ik noem maar wat) piethein.donner@minswz.nl ziet er geloofwaardig uit. Maar wimdevries@gmail.com? Welke Wim de Vries heb je dan voor je? De keuze voor een mailadres wordt bepaald door de beschikbaarheid van de naam, niet door de representativiteit ervan. Als ik jeroen.pauw@jeroenpauw.tk wil gebruiken, is er niemand die mij daarvan weerhoudt. Misleiden is extreem simpel. Zeker in e-mail, waarin je met outlook een displaynaam in plaats van een SMTP-adres ziet.

De aanbieder van het tk-domein meldt opgewekt dat jeroenpauw.tk mijn 'new web identity' is, onder de briljante leus "Renaming the Internet". En met dit adres kan ik dan netwerken - er zijn vast veel mensen die erin trappen. Wie wil er nu niet op TV?

Het internet is in essentie voor de gebruikers anoniem. Ja maar, roepen de wijsneuzen dan, je kunt het IP-adres opvragen. Ja duh, niet iedereen werkt bij de politie of een ISP. En zeg nu zelf, als je daar wel werkt, verifieer je ieder mailtje of het IP-adres van de afzender geloofwaardig is in relatie tot het mailadres en het tijdstip van verzenden? Het internet zal altijd tot op behoorlijke hoogte anoniem blijven, ongeacht kentekens, PKI-spullenboel en andere warrige ideeën uit overheids- of commerciële kokers. Gegeven dat de gemiddelde westerse opsporingsdienst al heel veel moeite moet doen om handelingen terug te voeren op een natuurlijke persoon, is het onwaarschijnlijk dat het particulieren ooit zal lukken.

Natuurlijk zijn er meer manieren mogelijk om een digitale identiteit te creëren. Ik kan een digitale handtekening aanmaken, al dan niet met PGP, om mij voor mijzelf uit te geven. Dat levert wel een zekere geloofwaardigheid op. Maar in feite geloven de mensen dan niet mij, maar het heilige PGP of het zalige PKI.

Het punt is, dat gebruikers de geloofwaardigheid van een systeem afmeten aan de gangbaarheid daarvan. Er worden aannames gedaan over de echtheid van een gebruiker op basis van het vertrouwen in de aanbieder van het stuk achter het apestaartje of het gele slotje in de statusbalk. Dit is zo'n beetje de essentie van 'Identity 2.0' waarin de 'community rating' van een 'identity provider' de geloofwaardigheid van een digitale identiteit zal garanderen. Dus als het merendeel van de username@provider.id identiteiten in de praktijk klopt, zullen ze allemaal kloppen. Identity 2.0 zal nog wel in Beta zijn. En zoals je ziet, als je zelf geen online identiteit creëert, doet een ánder dat wel voor je. Met de toename van het aantal psuedo-identiteiten, zal het misbruik verder toenemen en kunnen mijn collega's en ik niet vervroegd met pensioen.

Minister Hirsch Ballin heeft wel een oplossing. Het moet gewoon verboden worden je voor een ander uit te geven op het internet. Nou, ik daag je uit je eens voor jezélf uit te geven. Dat gaat mij alvast niet lukken; de naam Peter komt in mijn nogal groot uitgevallen familie heel wat keren voor. Toen ik mij bij mijn ISP aanmeldde, bleek ik nummer 446. Ha! Al die 445 anderen geven zich voor mij uit! Het moet verboden worden! Nee, dan mijn Mijn Oom Wim, die écht de Vries heet. Hij heeft een nog veel groter probleem....

Zin en Onzin

dinsdag 11 december 2007

In het kader van de themaweek Managed Security vorig jaar betoogde ik dat het uitbesteden van beveiliging een hoge mate van maturiteit in de organisatie vraagt: je moet immers weten wat je aan beveiliging moet doen, voordat je dat door een ander kan laten doen. Om een smart buyer te zijn moet je méér materiedeskundigheid hebben dan als je het zelf doet, want bij zelf doen geval kun je nog 'Iteratief' kennis opbouwen. En bijgevolg zul je er meer van moeten weten dan je leverancier. Maar goed, dit jaar wil ik iets minder filosofisch naar deze materie kijken.

Het concept Managed Security Service Provider (MSSP) lijkt bedacht te zijn door Counterpane – nou ja, dat zeggen ze zelf. Gartner heeft dit MSSP concept eind vorige eeuw omarmd en massaal aanbevolen. Volgens het magic quandrant Noord Amerika van 1/8/07 staat Verisign bovenin (zowel in visie als in het vermogen tot uitvoering), op de voet gevolgd door IBM, AT&T en Symantec en meer op afstand gevolgd door BT en onze eigen KPN (nou ja, Getronics dan). In de Europese Magic Quadrant van April 2007 staan eigenlijk alleen Cybertrust en Integralis als partijen die een geschiedenis hebben in Security, de rest zijn dezelfde doorsnee mix van systeem integrators en telco's die alles aanbieden wat een beetje potentie lijkt te hebben. Wat overigens niets hoeft te zeggen over de kwaliteit. In dit licht moet je ook de overname van GPR door de KPN zien: BT heeft Counterpane, Deutsche Telecom heeft debis en dan kun je niet achterblijven. Deze 'me too' scenario's spelen een grote rol, waardoor grote bedragen worden gespendeerd om het portfolio op hoofdlijnen vergelijkbaar met dat van de concurrentie te maken. De vraag of het allemaal even zinvol is voor de klant, krijgt minder aandacht zo te zien.

De uitkomst van Gartner is niet verwonderlijk, als je je realiseert dat het zwaarst wegende aspect in deze weging de omvang van de firma en de financiële positie is. Met dit soort vergelijkingen zul je als je een auto koopt thuiskomen met een Opel of een Fiat. Prima auto's hoor, maar als je naast iemand parkeert in een Donkervoort of een Spyker, steekt het wat schraal af. Als je een auto moet hebben om indruk te maken op de buren, is een Kadett of een Panda duidelijk een mismatch. En helemaal als je nog geen rijbewijs hebt – het gaat op den duur toch opvallen dat je er nooit in rijdt.

Wat is er te koop?
Managed Security is een containerbegrip, waarin allerlei beveiligingszaken in een doosje met een strik erom aangeboden worden. Om te voorkomen dat je appels en peren vergelijkt, is een korte rondgang noodzakelijk. Bij het vergelijken van abstracte, samengestelde proposities als Managed Security moet je nu eenmaal onder de motorkap kijken om te zien wat het aanbod nu precies inhoudt.

Het resultaat van een rondgang langs de aanbieders lijkt dat het beheer van security devices geouttasked wordt. Security Devices variëren een beetje, waarbij sommige leveranciers zich beperken tot de klassieke firewalls, maar het merendeel woont inmiddels wat hoger de OSI stack in door ook allerlei IDS/IPS-achtigen en crypto spul te beheren. De meeste aanbieders concentreren zich bij het beheer van devices op de netwerk perimeter, sommigen durven de sprong het interne netwerk in, aan. Een specifieke categorie zijn de aanbieders van Managed PKI services, maar in de praktijk lijkt deze markt zeer beperkt. Nu ja, de meeste bestuurders krijgen nog steeds puistjes als je PKI roept…. Als toefje op de taart wordt over het algemeen 'threat management' in allerlei varianten aangeboden, waarbij je eerder dan de rest van de wereld weet dat er een gat zit in een stuk software, zonder dat je daarvoor zelf allerlei bronnen in vele talen moet gaan doorwaden om deze informatie te vinden.

Om eens te gaan kijken wat je aan Managed Security zou hebben of wat je zou willen aanbieden, moeten we nader ingaan op de verschillende onderdelen van de dienstverlening.

Managed Security Devices
Deze categorie omvat het bulk van alle aanbieders. Met het uitbesteden van het beheer van een stel appliances is op zich niets mis, omdat die dingen ook beheerd moeten worden. Bij de producten die zich op de applicatielaag begeven is er een behoorlijke patchcyclus en als het volgende gat in een rar of chm parser gepubliceerd wordt, zal een externe leverancier wellicht sneller patchen dan je dat zelf zou doen. Doen dus.

Als je vervolgens leest dat 'Managed Firewall Services' een 'totaaloplossing voor de implementatie en beheer van een effectief Security beleid binnen een organisatie' bieden “door inzet van ervaren, gecertificeerde security engineers en consultants”, ga je toch weer twijfelen. Firewalls die uitstekend helpen binnen een netwerk? Is dit een leverancier die voldoende kennis heeft?

Het in de lucht en gepatched houden van een firewall, een VPN concentrator, een IDS of een log correlatiedoosje is het simpelste stuk, je moet echter nog steeds iets dóen met dergelijke apparaten. Zeker met de meer geavanceerde. Zoals ik laatst als predikte op dit platform moet je als bewaker weten wat je bewaakt omdat je anders niet weet wat je ziet. Dit houdt in dat je als MSSP-klant je leverancier in detail op de hoogte moet brengen van wát en wie er bewaakt wordt en of er intern (of extern) operationeel iets speelt waardoor normaliter valide verkeer dat op eens niet hoeft te zijn. Dat kan zoiets banaals zijn als een medewerker die uit dienst is gegaan. Het “detecteren van afwijkingen in het netwerk van de klanten en het onmiddellijk op de hoogte brengen van de klant” is dan ook grotendeels wensdenken: alle beperkingen en nuances van bewakingssystemen gelden, ongeacht of deze nu in-house dan wel geoutsourced bediend worden.

Managed Security Devices zal helaas zelden meer voorstellen dan het in de lucht houden van onderbenutte geavanceerde doosjes. De bijdrage aan de veiligheid is dan ook gering, de rationale is puur kosteneffectiviteit. Hoewel effectief, je geeft minder uit aan iets wat je net zo goed kan laten, omdat je er nog niet aan toe bent. Haal eerst maar je rijbewijs voordat je die Panda koopt.

Managed Secure Internet Hosting
Feitelijk is dit gewoon hosting met een modieus verkooppraatje, vrijwel iedere echte hosting provider regelt de beveiliging goed. Ze moeten wel. Dit is de meest volwassen vorm van Managed Security.

Managed Secure Internet Access
Deze vorm kan wel interessant zijn om te outsourcen: voor je inbound proxy staat een filtering proxy die virussen en spyware vangt en de meest omineuze sites op een blacklist zet. Deze extra laag kan veel ellende voorkomen. Hierbij geldt dat dit alleen het algemene basisniveau kan leveren. Een nadeel om in de gaten te houden dat een filter op de proxylaag de feitelijke bandbreedte aanzienlijk beperkt. Dit is ondanks de uitvoerbaarheid en het evidente nut verassend genoeg een weinig gangbaar product bij de grote MSSP. Het concept wint wél terrein bij de reguliere ISP’s, waar het waarschijnlijk beter past.

Managed Secure E-Mail
Deze categorie wordt door een paar gespecialiseerde aanbieders geleverd, en maakt vaker deel uit van een pakket van weer een andere aanbieder. Het beveiligen van mail laat zich goed outtasken, zo lang de afnemer niet verwacht dat het fire and forget is en een tamelijk algemeen beveiligingsniveau vraagt, net als bij de Secure Internet Access. Een aandachtspunt is mail integratie met andere functies zoals webmail: mailscanners werken op SMTP niveau waardoor de

eigen mailinfra niet meer extern zichtbaar mag zijn. Het kan daardoor conflicteren met webmail en de wens op userniveau verschillende regels neer te zetten.

Het wordt anders als je bijvoorbeeld meer dan de standaard beveiligingsfuncties vraagt; wil je dat alles wat positief herkend wordt als virus of spam verwijderd wordt zijn er tal van prima aanbieders die dit wellicht goedkoper kunnen dan je het zelf zou doen met dezelfde standaardproducten. Wil je dat informatielekken door eigen medewerkers of alle 0-day's worden tegengehouden, dan zul je merken dat iets anders dan een kadett niet in het assortiment zit.

Managed Threat Management
Wat je uitbesteedt met deze dienst is het afspeuren van de boze buitenwereld op nieuwe bedreigingen. Je MSSP koopt het op haar beurt weer in bij een hierin gespecialiseerde speler. Threat Management is prima etalagemateriaal, want je laat zien dat je proactief goed op de hoogte bent wat je bedreigd. En de besparing kan op het eerste gezicht reëel zijn, omdat het doorlezen van duizenden berichten per dag in allerlei moeilijke talen op zoek naar dat ene puntje dat een eigen systeem kan raken wellicht niet kosteneffectief is. Maar de vraag is wát je er überhaupt aan hebt. Immers, je hebt een tijdje eerder het nieuws dat er een gat zit in een PHP script op een specifieke Linux distro of je kent eerder de details over een gat in Excel. Bij de eerste moet je je afvragen of je dat script eigenlijk wel hebt, en of het in een kwetsbare opstelling draait, en bij het tweede of de organisatie het gaat vreten dat je een tijdlang – tot er een fix is – het gebruik van Excel uitsluit. En als er géén fix komt, dat je het hele product per direct overboord gooit…. Hetzelfde geldt de gedetailleerde informatie over virussen: wat heb je aan de informatie in realtime, als je antivirus producten het vervolgens niet kunnen onderscheppen? Ga je de internetpijp dichtgooien omdat er mogelijk een virus aankomt? Wanneer mag die dan weer open? Kennis zonder dat je er iets mee kunt veranderen, leidt hooguit tot een gefrustreerde Security Officer.

Zonder een zeer goed functionerende beheerorganisatie en/of een dringende behoefte een hoog veiligheidsniveau te realiseren, is Threat Management dan ook meer bezigheidstherapie voor Security-knutselaars dan zakelijk zinvol. Hoewel je de directie goed de stuipen op het lijft kunt jagen met het aantal bedreigingen waar je geen middelen tegen hebt. Maar of en wanneer het nuttig is je eigen onvermogen zo te etaleren behoort tot de arena der politiek.

Andere diensten
Naast deze vormen van managed service worden incidenteel nog andere zaken onder de noemer geschaard, om een nog breder en indrukwekkender portfolio te bouwen. Forensische Opvolging, Managed Vulnerability Management of Managed Security Audit zijn niet meer dan terugkerende diensten in deze of gene vorm. Kan helemaal zijn wat je zoekt, maar ik zou dit onder koppelverkoop scharen; het woord Managed staat ongeveer gelijk aan een strippenkaart of een abonnement en ik zou het feit dat ik iedere twee weken de Bobo door de brievenbus krijg toch niet als Managed Service durven omschrijven.

Het Managen van Managed Security
Een vereiste voor iedere managed service is dat je een manier hebt om de resultaten te meten. Tenminste, als het goed is, je gaat toch geen contract afsluiten vanwege een buikgevoel en mooie taartpunten en stoplichten? Nou dan!

Security Metriek geldt als een soort holy grail, net zoiets als ROSI (Return On Security Investment) dat is. Uitbesteding geeft nog een extra dimensie aan deze queeste. De uitdaging der metriek is in Managed Security van een hele andere ordegrootte dan bij normale outsourcing, en ga er van uit dat de gemiddelde service manager hier inhoudelijk niet op voorbereid is. Een Security incident is geen storing die 'opgelost' is als de stack van een doosje weer antwoord geeft

op een ping. Eindgebruikerstevredenheid zegt bij Security niet of de gestelde doelen bereikt zijn, misschien eerder het tegendeel. De klassieke KPI's gelden hier niet.

Het gaat meestal mis in de discussies als het subtiele verschil tussen de beveiliging en de resulterende veiligheid niet voldoende onderkend wordt. Het meest realistische is het meten van de inspanning van de leverancier in plaats 'resultaten'. Als je de leverancier op de resulterende veiligheid wilt afrekenen, moet je immers de detaillering van het beveiligingsbeleid en de dagelijkse interpretatie overlaten aan de leverancier. En dat wil je wellicht niet, niet in het minst omdat je dan maar één leverancier kunt hebben. Je kunt de bewaker van de voordeur niet afrekenen op het resultaat, behalve als je geen achterdeuren hebt én dat aan kunt tonen. Je loopt bovendien al gauw vast in oeverloze discussies over hoe dat virus op het netwerk is gekomen of waarom je niet gezien hebt dat de echtgenoot van een ex-medewerkster informatie uit een systeem steelt. Forensisch onderzoek kan dan – in sommige gevallen – uitsluitsel geven, maar de zakelijke relatie staat op dat moment al zó onder druk, en digitale bewijsvoering is zó ondoorgrondelijk en inhoudelijk betwistbaar, dat je die kant écht niet op moet willen.

Het laatste aandachtspunt dat ik mee wil geven, is het verschil is tussen het meten van de beveiligingsinspanning en het meten van goede bedoelingen. Dat een Managed Security provider ISO27001/CMM-SSE of whatever gecertificeerd is, zegt niet noodzakelijker wijze iets concreets over hoe goed deze de informatie van een klant beveiligd. De gangbare methodes zijn te abstract voor een dergelijk gebruik. Ze stellen statische doelen, zonder beschrijving van de middelen, en zijn niet gedimensioneerd op uitbestedingsrelaties waarbij een leverancier meerdere partijen met verschillende beveiligingsbehoeftes bediend. Deze noodzakelijke nuanceringen maken het er niet verkoopbaarder op, behalve als de afnemer bereid en in staat is diep op de materie in te gaan. Of blind te tekenen.

'Managed Security' is al met al een gemengd pakket van onrijpe en rijpe diensten. Voor de meeste organisaties zal de bezuiniging van uitbesteden inhouden dat ze minder uitgeven aan iets wat ze net zo goed kunnen laten, behalve als ze het doen met het expliciet doel ervaring op te doen. Als ze deze eerste horde genomen hebben en een echte smart buyer zijn geworden, is het verantwoord bepaalde diensten in te kopen. Ik acht de kans groot dat ze dan weer té goed weten wat de beperkingen van de meeste proposities zijn, en hoeveel ze nog steeds zelf moeten doen, zodat ze het liever helemaal zelf blijven doen.

Niemand is de baas

donderdag 20 december 2007

Er was eens een tijd waarin de baas de Baas was. Omgaan met fouten was eenvoudig: de slechte Baas gaf de medewerker de schuld, de goede Baas nam zelf de schuld op zich. Hij had immers bepaald wat er gedaan moest worden en hoe. Als de fout te erg was, stond de goede Baas op straat. Hij was immers verantwoordelijk. Daarom moest hij ook wat meer salaris hebben dan de anderen. En toch waren er best veel goeie Bazen.

Toen werden de bazen gebusinessprocessredesigned en vervangen door Managers. Managers zijn verantwoordelijk voor het proces. Medewerkers voeren het proces uit. Het proces wordt bepaald in het beleid. De directie keurt het beleid goed. Auditoren bewaken de kwaliteit.

Deze opzet is ooit bedoeld om de 'kwaliteit te borgen'. In gebieden waar de risico's het grootst zijn, is dit recept als eerste ingevoerd. Dat was in het begin vooral financiën, met de Register Accountant in de rol van de ultieme specialist. Met enige vertraging volgde informatiebeveiliging onder het bezielend toezicht van de Register EDP Auditor. In deze gebieden worden de gevolgen van deze standaardisatie van middelmatigheid dan ook het eerste voelbaar, met de sub-prime crisis als huidig hoogtepunt.

De directie laat het maken van beleid over aan specialisten. Deze beleidsmedewerkers bepalen wat er moet gebeuren, hoe dat moet en wie er verantwoordelijk is voor de uitvoering. Managers zijn alleen impliciet aangewezen als verantwoordelijke voor de resultaten. Vallen de resultaten tegen, dan kan de Manager de verantwoordelijkheid dragen en de schuld op zich nemen. Ze bestaan nog, ik ben er begin 2005 eentje tegengekomen. Hij is inmiddels boventallig. Wat de Manager ook kan doen, en dat gebeurt vaker, is de schuld geven aan de medewerker. Deze moet zich gaan zitten schamen in een hoekje. Dat doet ie niet, hij haalt gewoon z'n schouders op en neemt nog een kopje sterrenmix. Wat ook soms gebeurt, is dat een medewerker gaat uitleggen dat het ingerichte proces de huidige situatie niet dekt en hoe het dan wél zit. De Manager die een dergelijk verweer ontvangt kan twee dingen doen. Hij kan het negeren en hopen dat een volgende crisis de aandacht afleidt. Of hij kan het verweer doorgeven aan de beleidsmakers.

De beleidsmedewerkers op hun beurt begrijpen dat het tijd is voor nieuw beleid - de situatie die zich voordeed was immers niet voorzien, onder de 80/20 regel kon natuurlijk niet overal rekening mee gehouden worden. De beleidsmedewerker kan ook de bal terugkaatsen naar de Manager, die formeel verantwoordelijk is. Het blijkt immers dat de Manager vergeten is de medewerker op z'n dwaalleer te wijzen en het is een boel werk hoor, nieuw beleid ontwikkelen en dat goedgekeurd te krijgen. Daar zit niemand op te wachten.

Krijgt de beleidsmedewerker het toch te verduren over zijn beleid, dan heeft hij in het uiterste geval altijd een onfeilbaar excuus achter de hand: een verwijzing naar de bron van het beleid. Het proces is immers ingericht conform de best beschikbare richtlijnen (Sox, SAS, ISO en noem de verzamelde adviezen van gerenommeerde firma's maar op). Het adagium luidt: 'Niemand is ooit ontslagen omdat hij Gartners adviezen knipte en plakte'. Wat de beleidsmedewerker nóóit zal doen is naar de eerder genoemde medewerker gaan, die staat immers te dicht op te materie om deze te kunnen begrijpen. Deze spiraal van verkleuteren, duiken en blame shifting gaat door totdat iedereen het beu is en overgaat tot het managen van de volgende crisis. Verrassend genoeg is die er altijd precies op tijd.

Toen ik studeerde, in de jaren '80, wilden universitaire studenten met hoge cijfers Baas worden. Die functie bood de voldoening en de creativiteit van het leidinggeven, veel zelfstandigheid, eigen verantwoordelijkheid, en een mooi salaris. Tegen de tijd dat we ver genoeg waren in onze carrière om Baas te worden, waren er alleen nog maar Managers. Ook goed, dachten wij. Gewoon een nieuwe naam voor Baas. We zaten ernaast.

De Manager van de 21e eeuw heeft alleen nog het mooie salaris van de Baas. Vaak nog mooier. Er zijn alleen veel meer Managers dan er ooit bazen waren en je hebt lang niet altijd medewerkers. De verantwoordelijkheid stelt in de praktijk geen bal voor. En de zelfstandigheid al helemaal niet. Je bent resultaatverantwoordelijk maar niet gemandateerd om te bepalen hoe je iets aanpakt. De processen zijn in beton gegoten en als Manager word je geacht zodanig te 'sturen' dat de processen worden gevolgd. Je bent proceseigenaar en resultaatverantwoordelijke, maar niet de procesverantwoordelijke. Erop toezien dat de processen de verwachte resultaten opleveren, is dan weer de taak van de business controller.

Wat je vooral niet moet doen als Manager, heb ik inmiddels geleerd, is vaststellen dat een proces niet goed is ontworpen en daarom niet de beoogde resultaten oplevert. Dan houd je je bezig met de inhoud van het werk, waarmee je jezelf te kijk zet als een blauwe boord. Dat heeft hele nare gevolgen in je beoordelingen en in de dagelijkse omgang met je collega's. Als je een compleet onbruikbaar proces terzijde schuift word je bovendien bij de eerste daadwerkelijke afwijking afgefikt door een auditor die het proces kwaliteitsbewaking uitvoert. Hoewel er veel meer Managers zijn dan er ooit Bazen waren, staan juist de Managers veel verder van de materie. Kortom, je hebt als Manager minder bewegingsvrijheid dan een lopendebandmedewerker in een koekjesfabriek. Je enige troost is hooguit dat iedereen dit lot met je deelt.

Je organisatie heeft de collectieve onverantwoordelijkheid ingericht langs de lijnen van 'zelfsturende teams', die continu bezig zijn met het verkleinen van de scope en het vergroten van het budget, en je dagtaak is het bijwonen van alle bijbehorende overleggremia. Mis je één vergadering, dan heb jij de taak van een ander, en weer een ander je budget.

Een standaardgrapje tijdens mijn studie luidde dat als je een zesjesstudent was, niet tegen bier kon en zelfs geen sjans had in de darkroom, je nog altijd beleidsmedewerker kon worden bij een ministerie of een multinational. Werd je zelfs dáárvoor afgewezen, dan zat er niets anders op dan IT-er te worden. IT-ers, dat waren de mensen die computers neerzetten met programma's erop die je kon gebruiken. De IT-projectManager zorgde dat dat zo ongeveer op tijd gebeurde - desnoods op z'n tandvlees. En IT-Security mensen maakten de boel dan veilig. Of zo.

Die tijd is gelukkig voorbij. IT heet nu ICT. De hoogste ICT-er anno 2007 is de Business Consultant. Business Consulting heeft niets te maken met organisatiekunde of met wat een bedrijf doet. Ja, ook dat was ooit wel zo. Nu is de Business Consultant een inhuur beleidsmedewerker die alleen iets mag zeggen over ICT processen. Hij noemt dit Beleid en roept om het hardst dat de techniek het probleem niet zal zijn. Vorige week zag ik het summum: een vacature voor een Business Security Consultant. Dit klinkt als heel wat, maar stelt nog minder voor dan een Business Consultant. Wat hij mag doen, vrees ik, is het kopiëren van beveiligingsprocessen uit een generieke methode en die dan in een mooi PowerPoint plaatje zetten. Zolang beleid maar bovenin staat, is het allemaal goed. In de regel is hij al weer naar een volgende klant, als blijkt dat ook deze keizer geen kleren aan heeft.

Niemand is de baas. Onze polder is vervangen door een moeras. Deze geïnstitutionaliseerde collectieve onverantwoordelijkheid mist zijn uitwerking niet. De grote organisatie waar we zo graag Baas wilden worden, is geïnfantiliseerd, opgeknipt, ge-insourced, ge-outsourced, ge-resourced en uiteindelijk in stukjes gehakt en verkocht als sloopafval aan buitenlandse opkopers.

Waarom zouden we de informatie eigenlijk nog beveiligen, als niemand de organisatie zélf beschermt?

Het anti-terrorismehoesje

vrijdag 11 januari 2008

Op 31 december 2007 besloot het Amerikaanse ministerie van Buitenlandse Zaken een rfid-chip in de Amerikaanse paspoortkaart te bouwen die tot een afstand van zo'n 6,5 meter afleesbaar is. Deze kaart is bedoeld als een goedkoper en kleiner alternatief voor een echt paspoort. De kaart zal geldig zijn om over land en zee (maar niet per vliegtuig) te reizen naar Canada, Mexico, Bermuda en de Cariben.

De op dit moment ingebakken chip is maar tot 7,5 cm afstand leesbaar. De nieuwe chip biedt dus een veel groter bereik. Dat is handig: je zwaait wat met je pas en kunt meteen doorlopen bij de grens. Critici menen echter dat de privacy van staatsburgers in het geding is, zeker daar de kaart met speciale lezers tot op 13 meter uit te lezen zou zijn! Een woordvoerder van het Amerikaanse ministerie van Buitenlandse Zaken werpt tegen dat er geen 'biografische gegevens' via rfid afleesbaar zullen zijn, het enige dat uitgelezen kan worden is de foto van de kaarthouder. Nou en met alleen een pasfoto kun je geen identiteitsdiefstal plegen. Toch? Zeker niet als hij net zo goed lijkt als die van mij.

Alle gekheid op een stokje, de pasfoto kan niet uitgelezen worden, alleen de signature die eruit afgeleid wordt. Dat zijn stiekem toch 'biografische' gegevens. Of geloof je nu echt dat al die tig pixels ingelezen worden over die bandbreedte? Als aanvullende maatregel gaat het Amerikaanse ministerie aan de kaartleverancier (die nog geselecteerd moet worden) vragen om een beschermend hoesje te ontwerpen zodat je kaart alleen uitgelezen kan worden als jij dat wilt. Ziezo, probleem opgelost. Althans, voor mensen die dit graag willen geloven. En: zo lang je die kaart in dat hoesje houdt.

Tegelijk verschijnen er meldingen rond het 'breken' van de rfid die onder meer gebruikt wordt in autosleutels. Geinig. Leg dat maar eens uit aan de verzekering als al je geleaste auto's van een bepaald type tegelijk gestolen worden... We gaan leuke tijden tegemoet: ik zie het helemaal al voor me, een grote terugroepactie van alle BMW X-3s omdat de signing key gestolen is, of gekraakt door een Duitser met roze haar.

De discussies rond de veiligheid van rfid worden gedomineerd door privacy en de bedreigingen die uitgaan van allerlei geavanceerde vormen van criminaliteit. Maar vergeten we niet juist de minder geavanceerde bedreigingen? Hightech criminaliteit wordt pas zinvol als gewone vormen van criminaliteit niet meer werken. Je gaat toch niet uit stelen als je houdt van veel inspanning voor weinig resultaat - dan kun je net zo goed een baan zoeken.

Als ik kan uitlezen dat de eigenaar van die Mercedes CL600 binnen 6 meter loopt, is dan het grootste risico voor de eigenaar dat ik de chip uitlees en de auto steel met een kopie? Is het grootste risico dat een Amerikaan loopt dat ik van z'n nieuwe kaart een stukje van z'n digitale identiteit lees en doorgeef aan een winkel? Of, om meer actueel te blijven, dat iemand je kaart kopieert en onder jouw identiteit en op jouw kosten de tram neemt in Rotterdam? Dat de RET weet wanneer je welke tram genomen hebt en dat doorgeeft aan de coordinator terrorismebestrijding, maar dat jij dat niet was maar iemand met een kopie van je kaart? Dit zijn toch een beetje triviale scenario's. Als dit het enige is wat er aan de hand is, ben ik helemaal voor alle rfid-toepassingen. Zeker omdat ik als rechtgeaarde IT-er toch nooit met het openbaar vervoer ga.

Maar dit is - uiteraard - niet het enige wat er aan de hand is. De bestuurster van die zwarte Mercedes wordt op d'r bek getimmerd tot ze haar sleutels afgeeft. Via de sniffer weet je op dat moment ook al welke creditcards zij op zak heeft en welke elektronische gadgets ze heeft - verrotte handig als je op zoek bent naar iemand om uit te schudden. Die Prada handtas en het Cartier horloge melden zich ook keurig, dus die gaan ook mee. De heler kan de echtheid ook controleren met de tag, dus je krijg ook meer geld voor je buit. Ah, de zegeningen van de technologie.

Dan stoppen we er toch gewoon sterke cryptosleutels in? Tja, het lukt al niet om een PKI project voor 5.000 medewerkers rond te krijgen, denk je dat we dat dan wel kunnen voor alle 50.000 goederen in een gemiddelde supermarkt? O ja, maar dan stoppen we er toch een Firewall in, zoals RFIDSec uit Denemarken levert? Vast wel, ik vermoed dat de eerste RFID anti-virus producten ook binnenkort op de markt komen.

De risico's gaan nog verder dan alleen de doodgewone beroving met grof geweld. Ook voor de terrorist ontstaan er tal van nieuwe kansen. Met een afstand van 6,5 meter is het mogelijk om een bermbom te laten afgaan als iemand met een Amerikaans paspoort voorbijkomt. Daarbij maakt 6,5 of 13 meter ook niet echt uit, zo duur is kunstmest immers niet. Een slimmere bom gaat pas af als er binnen twee minuten drie Amerikanen langskomen. Dan hoef je ook geen vrijwilligers meer te zoeken voor zelfmoordaanslagen. En huurmoordenaars kunnen hun geweer aan de wilgen hangen en gepersonaliseerde bommen gaan strooien. Eigen schuld, dikke bult, had je die pas maar in het beschermende hoesje moeten doen!

Het drama beperkt zich niet tot alleen paspoorten - tags die aan apparaten of spullen worden gehangen introduceren immers vergelijkbare risico's. De bermbom zal volgens een typespecifiek patroon afgaan als er een Hummer of een Patria langskomt zodat de schade maximaal is. Met active tags is het bereik ook een stuk groter - tot 500 meter, en het gerucht is dat sommige legers een grote voorkeur hebben voor active tags omdat deze veel betrouwbaarder zijn. Betrouwbaarheid is inderdaad een groot goed.

Je kunt de bom ook laten afgaan bij een passerend voertuig omdat er een boel mensen inzitten met een Calvin Klein onderbroek aan of een Walmart tag in hun zonnebril. Rfid stamt af van IFF (Identification Friend or Foe) en dat zul je weten ook.

Dit soort bedreigingen zijn nogal andere koek dan een beetje identiteitsdiefstal. Overigens is dit al gedemonstreerd op Black Hat 2006 door Flexilis en roept Bruce Schneier dit ook al een tijdje in de woestijn.

Ik denk dat we de firma van die beschermhoesjes moeten vragen een kledinglijn op de markt te brengen met dezelfde eigenschappen. Wordt vast ook erg populair bij winkeldieven. Of we vragen de maker van onze telefoon om er een rfid-jammer in te bouwen. Dit soort nieuwe producten zal goed verkopen, zeker als je bovenstaande scenario's in een smeuïge, wat smakeloze campagne giet. Ik verwacht dan ook een terugkeer van Benetton als topmerk, totdat het kabinet dergelijke producten verbiedt voor gewone burgers. Dan mogen alleen opsporingsambtenaren en militairen dat dragen - dat geeft werkenbijdeoverheid.nl opeens een hele andere dimensie. Of ze gaan alleen Extended Capability tags toestaan, die geen last hebben van shielding.

Blijkbaar zitten de beveiligingsspecialisten weer eens te slapen. Wij zijn allemaal ethische consultants met te weinig fantasie om échte bedreigingen serieus te nemen. We erkennen alleen hightech risico's die passen in ons knusse belevingswereldje, zodat we alleen daartegen beveiligen. Voor mensen met een ondernemende geest aan weerszijden van de wet, breken er interessante tijden aan.

De Chinezen Komen Niet - Ze Zijn Er Al!

donderdag 24 januari 2008

Volgens Alan Paller, directeur van het gezaghebbende SANS Instituut, heeft de Chinese overheid op grote schaal databases van Westerse overheden en bedrijven geïnfiltreerd. Paller vindt dat we onze beveiliging fors moeten opvoeren ‘to find the enemy within’. Hij geeft deze dreiging een prominente derde plaats in de top 10 van bedreigingen voor 2008, nog boven aanvallen door eigen medewerkers (op 5) en spyware (op 7).

Dit is nogal een boude bewering. Als – zoals het dogma luidt - 80% van de aanvallen van de eigen medewerkers komt, moet de Chinese bedreiging fenomenaal groot zijn. Ter onderbouwing voert Alan Paller de volgende ‘smoking guns’ aan:
1: in de logs zie je dat de aanvallers niet, zoals gebruikelijk, veel typefouten maken.
2: het massale en repetitieve karakter van de aanvallen. ‘This is not amateur hacking. They are going back to the same places 100 times a day, every day. This kind of an effort requires a massive amount of money and resources.’

Het verhaal sluit mooi aan op de aanhoudende reeks berichten op dit vlak. De Amerikaanse overheid vroeg in november $154 miljoen extra aan, voor een 7-jarig programma om de eigen kwetsbaarheid te verminderen. Zo moeten in het kader van het Einstein project 2.000 experts toegevoegd worden aan US-CERT, die voltijds de koppelvlakken van de overheid naar het Internet in de gaten gaan houden. Dit gaat in 2008 $115 miljoen kosten. Het aangevraagde budget lijkt zwaar onvoldoende – alleen als je de experts beroerd betaalt (voor $57.500 bruto krijg je weinig specialisten) en bovendien een organisatie opbouwt zonder enige overhead, zou het misschien kunnen. Bovendien moeten ze van dit geld ook nog 2.000 internetconnecties samenvoegen tot 50. Een prima maatregel, maar bepaald niet gratis.

Congresleden hebben hun zorgen geuit over de privacyrisico's en hun verwondering uitgesproken over de afwezigheid van details in het voorstel. Zo te zien zijn de details echter niet weggelaten maar gewoon nog niet ingevuld, omdat het hele plan helemaal niet doordacht is. De aanvraag maakt deel uit van een totaal budget van $ 436 miljoen voor cybersecurity, de toegekende extra 154 miljoen wordt onder andere gefinancierd door korting op de hulp aan veteranen, korting op hulp aan Katrinaslachtoffers en uit de opbrengsten van olie uit Irak.

De omvang van het cybersecurityprobleem werd afgelopen week nog onderstreept door de U.S. Director of National Intelligence (DNI) Mike McConnell in The New Yorker. Volgens de DNI signaleert het Amerikaanse ministerie van defensie dagelijks ongeveer 3 miljoen aanvallen, het state department ongeveer 2 miljoen. Cybersecurity heeft van de DNI bij de verschillende inlichtingdiensten de hoogste prioriteit gekregen. Volgens de DNI is het aantal aanvallen uit China sterk toegenomen de afgelopen maanden, terwijl de aanvallen uit Rusland op het niveau van de koude oorlog zitten. Volgens Ed Giorgio, een security consultant verbonden aan de NSA, heeft China 40.000 professionele hackers in dienst om de VS en haar bondgenoten aan te vallen. McConnell meent dat het grootste probleem niet de beveiliging van de overheid zelf is, maar de beveiliging van bedrijven. SANS beweert dat China en andere landen terabytes aan informatie gestolen hebben in 2007 en Paller verwacht dit jaar een verdere toename. De Chinese overheid noemt deze beschuldigingen overigens potsierlijk.

SANS beschrijft als 'attack of choice' spear-phishing, e-mail met attachments die zich uitgeven als zijnde afkomstig van een betrouwbare bron. Daarbij wordt misbruik gemaakt van zwaktes in MS-producten en van methodes om virussen te verbergen voor scanners. Bij de gesignaleerde enorme aantallen aanvallen tellen e-mailtjes dus mee. Het gebruik van gerichte fishing zou de meest gangbare methode zijn omdat het zo eenvoudig en doeltreffend is. Nu bevat 80 – 95% van alle e-mail dergelijke zut. Zoals ik vorig jaar al beargumenteerde heb je daar geen militaire organisatie voor nodig en hoeft een dergelijke aanval, hoe gericht ie ook overkomt, helemaal niet gericht te zijn.

Oplossingen voor dit type aanvallen zijn overigens prima uitvoerbaar. Bijvoorbeeld door alleen attachments toe te staan die voldoen aan bepaalde regels – zoals whitelisting van controleerbare en onmisbare bestandstypen. Een interessante technische tool hiervoor is een magic byte filter: daarmee kieper je alle bestanden die voorgeven iets anders te zijn dan ze zijn, gewoon weg. Dit magic byte filter is noodzakelijk voor whitelisting, omdat je anders alleen op extensie kunt filteren en dat helpt niet zo veel. Een kleine kanttekening is hierbij op z'n plaats – ook vertrouwde bestandstypen kunnen zwaktes bevatten zoals MS bewees door de ondersteuning voor oudere Office varianten te laten vallen.

Als je een waarschijnlijk doelwit voor Chinese spionnen bent moet je de e-mailbescherming dan ook verder aanscherpen, bij voorkeur door alleen attachments door te laten van vertrouwde mailadressen. Als je slim bent doe je dit voor hele domeinen en niet voor individuele adressen, want anders blijf je intikken. Natuurlijk kan een aanvaller afzenders spoofen, maar dit laat zich op meerdere manieren ondervangen, waarvan DomSec m.i. de mooiste en simpelste is – berichten worden ondertekend door de verzendende mailserver en uitgepakt door de ontvangende mailrelay in je perimeter. Heb je en passant ook je mail over Internet tegen meelezen beveiligd. Daarvoor hoef je geen enkele versleuteling ín je netwerk toe te laten of moeilijke migraties te doen, terwijl je tóch een hoge mate van zekerheid hebt omtrent je trusted sources. Natuurlijk, als een aanval vanuit een vertrouwd netwerk komt is er een slagingskans, maar zonder deze maatregel heeft iedere aanval uit ieder willekeurig domein die slagingskans.

Gewone vormen van e-mailversleuteling als PGP en S/MIME maken allerlei beveiliging zoals Antivirus kansloos. Bovendien moet je dit op heel veel plekken tegelijk inzetten (denk aan

mailarchieven), en dat is een prijs die je met DomSec niet hoeft te betalen. Het bestaat al geruime tijd maar wordt toch slechts mondjesmaat toegepast. Waarschijnlijk is deze oplossing té simpel en té eenvoudig te implementeren om interessant te zijn. Veel mensen hebben liever DNSSec, maar dat kun je niet zelf Internetbreed regelen. DNSSec geeft je een prima excuus om veel te overleggen, maar je kunt er feitelijk niets mee.

Een puntje van deze aanpak is natuurlijk het kostenaspect: DomSec vraagt het uitwisselen van PKI-certificaten met allerlei partijen en dat moet je inrichten en onderhouden. De kosten kunnen best meevallen – je hoeft daarvoor geen certificaten te kopen. Immers, je communiceert in dit scenario niet met onbekende partijen, wat de raison d'etre is van een reguliere PKI. Een groot voordeel, want als je ze zelf bakt word je ook niet verrast door allerlei critical extensions waar je niets aan hebt, behalve sores. Maar ja, je PKI zelf doen geldt als iets dat je aan gespecialiseerde firma's moet overlaten, omdat het anders onbetaalbaar zou zijn. En die firma's komen weer met certificaten aan die alleen in de meest simpele scenario's te gebruiken zijn. Als je dan toch besluit om infrastructurele certificaten zelf te bakken is er vast een auditor die je met ETSI 101 456 om de oren slaat. De koers is simpel: laat de boel onveilig, of tem de auditor en bak ze lekker zelf.

Whitelisting is arbeidsintensiever dan blacklisting, dat alles doorlaat en alleen tegenhoudt wat de beveiliging toevallig kan onderscheppen. Blacklisting is voor de organisatie op termijn een recept voor rampen. Alles wat versleuteld is, kan gewoon door en als de Chinese spion nostalgisch aangelegd is, gebruikt ie vast wel één of andere crypto. Een hybride opzet waarbij je bij alle niet-vertrouwde domeinen whitelist en de vertrouwde domeinen blacklist maakt e-mail beveiliging wel hanteerbaar, lijkt me.

Het lastigste aan whitelisting is het grote aantal bestandsformaten van minder gangbare programma's. In veel organisaties is e-mail feitelijk de opvolger van FTP en wordt gebruikt om bestanden uit te wisselen van allerlei soorten en maten die je niet met een magic byte filter kunt herkennen en dus op extensie moet doorlaten. Je kunt je afvragen of dit heel erg is – een bestandextensie die een systeem niet snapt, kan nooit leiden tot een op dat systeem uitgevoerde aanval. Het wordt lastiger als je een custom product gebruikt dat een .XLS extensie gebruikt maar niet excel compatible is. Maar meestal zie je .000 of .ZUT extensies, en daar kan Windows echt geen chocola van maken. Zo lang je dat tenminste niet zo ingesteld hebt. Je moet je computer dus niet vertellen om .ZUT bestanden altijd met Powerpoint te openen of zo. In een normale opzet gebruik je alleen whitelisting voor bestandstypes die silent execute dan wel anderszins default begrepen worden door je standaard OS.

Verkeer van custom applicaties onttrekt zich op dit moment toch al aan iedere vorm van inspectie. Mochten er onverhoopt geen exploiteerbare gaten in Windows of Office meer zitten, zullen 'kleinere' bestandstypen een nieuwe aanvalsvector voor gerichte aanvallen vormen. Hoe je het ook wendt of keert – als je veel verschillende systemen hebt, heb je veel kwetsbaarheden en is de beveiliging tegen aanvallen arbeidsintensief. En als je bovendien weinig gangbare spullen gebruikt, verminder je het risico van ongerichte aanvallen omdat er geen standaard gaatjes in zitten. Maar je verhoogt juist weer het risico op succesvolle gerichte aanvallen door enge spionnen, omdat specialisten die er een exploit voor gaan maken bijna altijd raak zullen schieten.

Het sluitstuk van een wat zinniger beveiliging is outbound filtering. Er zijn nog verrassend (of schokkend) veel organisaties die alleen binnenkomend verkeer in de gaten houden. Dit is echter een kritieke verdedigingslinie: als je een rootkit via de e-mail naar binnen hebt gekregen moet deze uitgaande sessies opbouwen om z'n verderfelijke werk te kunnen doen. Nu gaan deze sessies veelal over http of https, maar dit betekent niet dat je er niets tegen kunt doen. Een beetje webproxy kan ook filteren, en daarmee kun je deze deur heel wat verder dichttimmeren. Het scannen van https is ook geen probleem zolang je https überhaupt scant en niet blindelings

doorlaat. Een Trojan die een covert channel over bijvoorbeeld DNS opent zou net zomin een probleem mogen zijn als je je enigszins verdiept in je firewall. De vectoren die de Chinezen volgens SANS zouden gebruiken mogen voor een beetje beveiligde organisatie dan ook écht geen probleem zijn.

Laten we even teruggaan naar de genoemde 'smoking guns' van Paller. Als belangrijke aanwijzing wordt genoemd dat de gebruikelijke typefouten niet opduiken in de logs. Nu ben ik benieuwd over welke logs hij het heeft. Als de primaire aanvalsvector e-mail is, dan zul je geen kromme commando's in je IDS-log aantreffen, zelfs niet naar je mailserver. Immers, je mailserver accepteert verkeer van allerlei domeinen dus er is geen restrictie die je moet omzeilen. Typefouten zie je bij probing van webservers en database servers. Deze smoking gun heeft dus op z'n best een relatie tot minder belangrijke en minder frequente aanvallen. Als die 40.000 Chinese hackers enkele honderdduizenden e-mailtjes per dag versturen, hebben ze een luizenbaantje. Een beetje spammer doet dat makkelijk in z'n eentje. (Waar kan ik solliciteren?)

De tweede smoking gun is de frequentie en herhaling van de aanvallen, tot maar liefst enkele honderden keren per dag, wat een gewone hacker niet zou kunnen. Als het een e-mailaanval betreft is een simpele 'resend' voldoende, en dat doet je mailserver vanzelf. Deze smoking gun gebruikt volgens mij rookloos kruit – hij rookt niet. In mij komt het angstige vermoeden op dat onze leiders en beschermers het niet helemaal begrijpen.

Gaan ze het dan beter doen? Ze gaan 2.000 man extra inzetten. Dat is goed. Die tweeduizend specialisten waar nu budget voor vrijgemaakt zou zijn kunnen de belangrijkste gaten dichten, de infiltraties opsporen en uitsnijden en het aantal kwetsbare koppelvlakken verminderen. Maar dat gaan ze mooi niet doen, ze worden toegevoegd aan project Einstein, dat houdt de gaten in de gaten.

Een mooie verdere indicatie van de ernst en kunde van onze beschermers is de opmerking dat het gesignaleerde aantal aanvallen uit Rusland 'op Koude Oorlogsniveau' is. Jongens, jongens, denk eens éven na. Vertel je ons nu werkelijk dat Rusland evenveel digitale aanvallen doet als zeg maar tijdens de Cubacrisis, de Berlijnse blokkade of de Olympische Spelen van Moskou? Of is de koude oorlog een aantal jaren geleden opnieuw uitgebroken, en zijn ze vergeten dat aan ons te vertellen? Ik hoor hier toch eerder een manager die z'n budget en mandaat wil vergroten door de Russen erbij te halen, dan een specialist die waakt over uw en mijn veiligheid. Maar ach, met zo'n evident te laag budget is dat normaal gesproken wel vergeeflijk. Als je SANS of de DNI bent is de gecreëerde paniek echter besmettelijk.

Mijn conclusie: als de officiële berichten over de aanvalsvectoren waar zijn, is het mogelijk om met relatief eenvoudige middelen die al jaren bestaan de gaten te dichten. Dat betekent dat we de afgelopen jaren ons werk niet goed hebben gedaan en ons met de verkeerde dingen hebben beziggehouden. Aangezien het verhaal van de autoriteiten aan alle kanten rammelt en ze blijkbaar geen idee hebben waar ze mee bezig zijn, wat dat kost of hoe dat moet, zullen we ons werk ook de komende jaren niet goed gaan doen. Als de Chinezen er al zijn, zoals SANS volhoudt, dan kunnen ze tot in lengte van dagen hun gang gaan. Want dat half miljard dollar is in dat geval een druppel op een gloeiende plaat. Maar goed, met een dergelijke leiding is iedere dollar weggegooid geld. De enige andere logische verklaring voor het hele verhaal is dat het van A tot Z verzonnen is om iemand z'n winkeltje te sponsoren. Maar dat zal toch wel niet? Toch?

Voortschrijdend Inzicht Mag Niet

vrijdag 8 februari 2008

Als ik de laatste berichten mag geloven, is de totale schade van mislukte projecten groter dan alle ICT beveiligingsincidenten bij elkaar. Kijk naar Walvis. Kijk naar het Elektronisch Kind Dossier. Of P-Direkt. VIDI. Project Toeslagen bij de belastingdienst. GPS bij justitie. MULAN, Indigo, SUB, Sagitta. Nu ook het megaproject Gemeentelijke Basis Administratie gestrekt is gegaan, is er veel aandacht voor de projectaanpak. De SP heeft een meldpunt ingericht en de Kamer wil een parlementair onderzoek. Met deze reeks aanhoudende ICT-fiasco's bij de overheid komen langs alle kanten de beste stuurlui belangeloos langswaaien met hun adviezen. Hopen op een parlementaire enquête dus, want dan kun we misschien wel op TV vertellen dat we het beter weten.

De communis opinio is dat er een gebrek is aan kennis en dat er onrealistische tijdspaden opgelegd worden aan de projecten. Het is wel interessant te zien hoe deze twee zaken aangepakt worden. Ik wil dat zelf ook wel eens leren.

Alle adviezen bieden ongeveer dezelfde drie recepten - strakker managen op de plannen en de procesinrichting, kopiëren van succesvolle systemen en projecten elders en meer controle op alle stappen. En omdat het de overheid betreft zie je ook een vierde recept: uitbesteden. Deze – uiteraard goedbedoelde - adviezen zijn staan garant voor nog meer probleemprojecten. Ze leiden tot afgeraffelde en slecht doordachte systemen, die opengebroken kunnen worden zodra iemand de moeite neemt. Een vooruitzicht dat, gezien de toename van overheidsbrede informatiesystemen met privacygevoelige informatie, niet vrolijk stemt. Laten we de recepten eens nader bekijken.

Recept 1: Strakker Managen
Strakker managen is het management-equivalent van keihard aanpakken: iedereen is het direct met je eens. Als je de stukken van de ministeries bekijkt, lees je zinnen als "Er is voor de ontwikkelprojecten van P-Direkt een op PRINCE II gebaseerde aanpak, inclusief kwaliteits- en risicomanagement en een sluitende overleg- en informatiestructuur. Op gezette tijden vinden audits plaats." Nou, dat is dus al lang strak geregeld.

Of toch niet? Prince II is een besturingsmodel voor IT-projecten uit de jaren '80 en het vertoont dan ook wat sleetse plekken. Het richt zich bijvoorbeeld op kleinere en middelgrote projecten van een paar maanden tot hooguit een jaar, en veronderstelt een Controlled Environment. De complexiteit is sindsdien enorm toegenomen (zo is de rekenkracht en de hoeveelheid data verduizendvoudigd en gaan projecten niet meer over losse systemen maar over geïntegreerde systemen, dus 1000x1000x1000) en tegelijkertijd is de macht van de ICT behoorlijk afgenomen. En passant zijn we de Controlled Environment ook kwijt geraakt. In 1988 kon je tegen de klantorganisatie misschien nog zeggen dat ze gedurende het project de werkelijkheid maar even moesten bevriezen. Nu kan dat niet meer.

En dan de bureaucratie die voortkomt uit Prince II: een enorme hoeveelheid papier- en tijdsverbruik, waardoor de tijdspaden inderdaad onrealistisch kunnen worden. Een beetje PID (Project Initiatie Document onder Prince) heeft de toon, omvang en detaillering van een regeerakkoord van tot elkaar veroordeelde partijen. Dat opstellen kost al gauw een jaar, die afgaat van het budget, de ontwikkeltijd en de bouwtijd. Als de PID ook nog gepaard gaat met een aanbesteding kun je het qua omvang en realisme eerder vergelijken met het verzameld werk van Tolkien. Vaak kost de voorbereiding meer dan 80% van de tijd en het budget. Het bouwproject

houdt zich vervolgens maanden bezig met dit alles weer overboord gooien. Dat sommige projecten onder politieke (tijds)druk de PID fase overslaan is dan ook begrijpelijk, maar niet automatisch de oorzaak van eventueel later falen.

Een manier van 'strakker managen' is het project opknippen in meerdere, kleine projecten en dat dan in een programma onderbrengen. Dat moet de stuurbaarheid ten goede komen. Maar een project is pas interessant voor je status als het groot is. Dus het stuurbaar maken op de manier die de rekenkamer aanraadt, zal de ambitie van de bestuurders en projectmanagers doen verschuiven naar de programma's waar die projecten onder vallen. Dus er komt een extra laag middenkader bij, en de projectmanagers worden allemaal programmamanagers. Dat is reuze fijn voor ze, maar hoe dit helpt tegen de kwaal is mij niet geheel duidelijk. Zo storten niet alleen projecten, maar ook hele programma's af.

Wat ook kan, en heel modieus is, is 'dakpansgewijs plannen': al aan de volgende stap beginnen als de vorige nog niet helemaal (of helemaal niet) klaar is. Het is daarbij niet erg dat iets niet lukt, we gaan al bouwen aan de volgende stap als we alleen maar een schets hebben. De aanname is dat de eindsituatie niet veel zal afwijken en alle problemen binnen de gekozen aanpak oplosbaar zijn. Hiermee wordt niet alleen de tijdsdruk opgevoerd, maar de inhoudelijke druk op de ontwerpers nog veel meer - als iets inherent verkeerd blijkt, kun je niet meer veranderen. Dit leidt ertoe dat alle initiële aannames koste wat kost overeind moeten blijven. We zetten de dominosteentjes heel dicht op elkaar, dan vallen ze vast niet om. Als dit tot een goed systeem leidt terwijl je met een samengeraapt team werkt aan iets complexers dan een Winzip implementatie, is dat stom toeval.

Intussen pleit Binnenlandse Zaken voor Centrale Coördinatie van de grootschalige ICT-projecten. Niet verrassend is dat het ministerie zélf deze verantwoordelijke taak wel op zich wil nemen. Gegeven de traditionele interdepartementale kippendrift en het algemene landjepik lijkt mij dit een geheid recept voor nog veel grotere drama's. Of hebben ze een medicijn uitgevonden tegen de 'Not Invented Here' en 'Over de Schutting'-syndromen?

De kritiek op de overheidsprojecten gaat duidelijk een bepaalde kant op: de kwakzalvers geven de patiënt de schuld. Dat noemen we met een memorabele term alibimanagement, en als recept roepen wij projectmanagers in koor: strakker managen. Geen Changes, gedetailleerdere ontwerpen, uitgebreide inventarisaties, meer kwaliteitsbeheer, meer rapportages. Allemaal versterkt door een extra laag als Centrale Coördinatie, al dan niet overheidsbreed. Kortom: meer macht voor de projectmanager! De kwaal wordt als medicijn voorgeschreven, maar niet in een afgezwakte vorm zoals bij een vaccin.

Recept 2: Successen kopiëren
We weten niet waarom sommige projecten lukken, maar als we gewoon blind alles hetzelfde doen dan boeken wij óók succes. Zo werkt de methode Best Practice. Onze OV-kaart bijvoorbeeld zou een exacte kopie worden van de Octopus kaart in Hong Kong. Need I say more? De managerial insteek bij kopiëren is dat je alle risico's al kent en de oplossingen daarvoor dus ook. De Octopus kaart is in 1997 in gebruik genomen, en wordt anno 2008 nog steeds als argument gebruikt dat het hier helemaal goed gaat komen.

Maar Octopus gebruikt onder meer single DES, dus moest Translink voor die andere chip kiezen, die nu gekraakt is. Maar goed, je kunt nog altijd de schijn van kopiëren ophouden en vervolgens schijnsturen en je schijnsuccessen vieren op de noodzakelijke champagnemomenten. Wat TLS dan ook maar deed. Waar TLS vervolgens achter kwam is dat Hong Kong geen Nederland is. Zo is de overgang in Hong Kong bot afgedwongen en is een stad - hoe groot dan ook - iets anders dan een land met tig vervoersmaatschappijen. Een deel van het succes in Hong Kong was ook dat de

Octopus feitelijk tevens een chipknip is. En die hebben we hier al. Bovendien kampten de inwoners van Hong Kong met een nijpend gebrek aan muntgeld. Wij niet.

Translink wilde in haar megalomanie niet alleen de strippenkaart vervangen maar ook de chipknip. Dat de chipknip hier ook maar niet wil aanslaan, ondanks de gezamenlijke dwang van overheid en financiële sector en tegen een beduidend hoger budget dan de hele OV-kaart, had toch iets duidelijk moeten maken. Dezelfde misser hebben we gezien bij dat andere megasucces, C2000. Lesje projectmanagement: een succesvol project kún je niet kopiëren. Zit in de definitie van het woord project - het is eenmalig. Oftewel ook dit recept is de kwaal zélf.

Recept 3: Meer Controleren
Dit recept ligt in het verlengde van 'lekker strak managen' en wordt vooral door auditoren en consultants aangeraden. Huur mij in en het komt hélemaal goed. Auditing controleert of je doet wat je op papier hebt gezet – of je dat op de goede manier doet. Maar of je het goede doet? Dat zou de vraag moeten zijn. Zo lang de auditor echter niet helderziend is kan hij alleen afwijkingen op de plannen zien. Veranderingen in de werkelijkheid of fouten in de initiële aannames komen niet boven tafel. Een audit op een lopend project is een apart vak, zeker als het project niet conform waterval werkt. Auditing is zeker nuttig maar zal bij onrealistische verwachtingen al snel in een verdomhoekje belanden – er is immers niets ergers dan falend toezicht op de publieke zaak, nietwaar? Dat rijdt in een Saab leasebak en kan geeneens toveren... Tssk.

Zo lang een audit impliceert dat alles conform een vooraf in detail vastgelegde planning gebeurt – daar wordt immers tegen geaudit – is de inzet van een auditor een symptoom van de kwaal.

Een 'second opinion' van onafhankelijke specialisten zoals recent in zwang is geraakt, zou de traditionele beperking van de audit moeten ondervangen. Maar als projectmanager heb je erg veel mogelijkheden om een ongewenste uitkomst van een second opinion buiten scope te plaatsen: de koers veranderen is immers vreselijk kostbaar, vertragend en anders stel je de competentie van de ander ter discussie. Feitelijk is een second opinion die sterk afwijkt gezichtsverlies voor het hele project én de opdrachtgever. Als je de second opinion 'meeneemt' is dat meestal alleen voor de vorm, anders loopt je hele team boos weg. En daar gaat je continuïteit.

Bedenk je ook dat alleen helderzienden een goede second opinion zó uit de mouw kunnen schudden. In de twee weken die er meestal voor gegeven wordt aan iemand die even op de bank zit, krijg je doorgaans niet veel meer dan wat platitudes in een standaardrapportje: strakker scopen, meer communiceren en meer tussentijds rapporteren. Menig adviseur zal – al dan niet impliciet – voorstellen een collega van dezelfde firma in te huren. Dit medicijn heeft hooguit een placebo-effect.

Recept 4: Uitbesteden
De ondertoon in veel commentaren op de falende projecten bij de overheid is dat je maar beter kunt uitbesteden, want de overheid maakt er maar een potje van. Leuk hoor, maar laten we deze marketingvariant op de aloude ambtenarengrappen maar even vergeten. Veel van de genoemde projecten zijn juist uitgevoerd door 'gerenommeerde marktpartijen'. Dat die hun klant de schuld geven wil niet automatisch zeggen dat dat daadwerkelijk zo is. En de niet-uitbestede projecten krijgen te maken met uitbestede delen van de eigen organisatie en da's ook geen feest, hoor. De veronderstelling dat de procedures niet worden gevolgd is evenzeer onjuist. Er wordt ook bij de overheid al jaren lustig en grootschalig ge-in-, ge-out- en ge-resourced, geaudit, gemanaged en gerapporteerd en het helpt geen bal.

Bij uitbesteden of met een politiek correcte term 'sourcen' ga je systemen langs arbitraire lijnen opknippen en versnipperen over tal van leveranciers. Alleen: een systeem is helaas geen stuk ijzer

waar toevallig wat applicaties op wonen. Het is een complex geheel van vele lagen en componenten. Er is geen mate van strak aansturen en auditen die de puzzel kan oplossen als je dat verspreidt over verschillende partijen. Je kunt immers niet naar één partij outsourcen want dan krijgt die te veel macht, toch?

In dit geval is het recept nog veel erger dan de kwaal: uitbesteden over meerdere partijen is sturingstechnisch een kansloze opgave. Je besteedt het LAN uit aan de één, de back-end aan de ander – maar zónder de applicaties, die gaan naar een paar anderen, weer een ander doet het rekencentrum, en als klap op de vuurpijl laat je nog een andere leverancier de Security 'doen'. Echt waar, dit bestaat. Schuiven met lucifersdoosjes, terwijl je op je vingers kan natellen dat dit een recept voor drama's is. Security gáát over macht, zeker de macht over de ICT maar meer en meer ook over de hele organisatie. 'Ik ga eens lekker het systeem en de processen van mijn concurrenten afkeuren. Want wij hebben een breder portfolio dan alleen Security, zeker sinds die laatste fusie'. Jij zal zoiets misschien niet denken, maar je Security vakgenoten zijn jammer genoeg meestal wat minder integer.

Wat fascinerend is dat niet één van de voorgeschreven medicijnen zich richt op de kwaal ‘gebrek aan kennis’ en alleen als je het erin wilt lezen op de kwaal onrealistische tijdspaden. Iedereen wijst als schuldige 'de klant die telkens wat anders wil' aan. Dit veronderstelt dat als je vooraf precies bepaalt wat je wilt en daar verder niet aan sleutelt, het helemaal goed komt. Nu is één van de vaak genoemde oorzaken de tegenvallende complexiteit van de beveiliging, die telkens wat anders wil en niet precies weet hoe..... Is dat iets anders willen of iets anders moeten - omdat zoiets triviaals als de werkelijkheid zo af en toe verandert en dat je vooraf gewoon niet alles kon weten?

Van PID en aanbesteding tot in de projectuitvoering heerst de fictie dat de requirements niet zullen veranderen en dat alle aannames kloppen. Maar gedurende het project verandert de werkelijkheid toch. Heus wel. Zeker als het project 5 jaar loopt. O tjee, wéér een tegenvaller. De waterval benadering is het werkelijke probleem, een gedetailleerde planning die niet gebaseerd is op realistische veronderstellingen houdt in dat het project van tegenvaller naar tegenvaller strompelt tot het uit zijn lijden wordt verlost.

Om te adviseren om dan maar uit te besteden aan 'marktpartijen' die niet in staat blijken om in zeven jaar een MS Access 2.0 bestandje te porten naar een ASP.Net-applicatie en nooit van testen hebben gehoord maar wel mooie kwaliteitscertificaten en processen hebben, is nog erger. Als drie pleisters niet helpen tegen een acute depressie, zou een hele doos dan wel helpen? Er wordt al veel te veel geborgd, belegd en afgekaderd in de wondere wereld van de digitale Betuwelijn.

Maar ik ben bang dat we ook in de toekomst strak zullen vasthouden aan het oorspronkelijke plan, omdat iedere verandering nu eenmaal tot vertraging en gezichtsverlies leidt. Er komt geen ruimte voor voortschrijdend inzicht. We blijven nare ontwikkelingen als het kraken van kerncomponenten negeren. En naar aanleiding van de reeks fiasco's die nu in de publiciteit zijn gaan we nóg krachtdadiger sturen, projecten nog complexer maken, nóg meer 'naar de markt brengen' en nóg steviger vasthouden aan het oorspronkelijke megaplan. En daardoor gaan we dus nóg grotere megafiasco's meemaken, met systemen die live gaan met vijftien jaar oude technologie, die niet getest zijn en waar alle rafels dus nog aanzitten. Er is de komende tijd nog zat te pappen en nat te houden, dus als je je verveelt, kun je ook in de Security komen werken.

Een lesje in beveiliging

maandag 25 februari 2008

De spraakmakende editie Nederland Undercover, waarin journalist Alberto Stegeman

ongehinderd een imitatie semtexbom aan boord van een vliegtuig plaatste, toont aan dat compliancy blijkbaar iets heel anders is dan Security, ook al gaat compliant zijn over aan een waslijst beveiligingsvoorschriften.

Minister Hirsch Ballin benadrukt dat de beveiliging van Schiphol voldoet aan de Europese regels "en in zijn algemeenheid goed is". Al met al is er dus op alle fronten adequaat gehandeld, vinden de verantwoordelijken. Bestuurlijk gezien hebben ze gelijk: iedereen heeft zich aan de regels gehouden, is dus 'compliant'. Afgezien dan van die arme kleumende bewaker die in de televisie-uitzending te zien was. Schipholdirecteur Cerfontaine: "Zo iemand moet je gelijk ontslaan." Dat deed hij dan ook. Goed man.

Ook de Nationaal Coördinator Terrorismebestrijding (NCTb) Tjibbe Joustra, wijst "de menselijke factor" aan als zwakke schakel. De irisscan die per 1 juli van dit jaar voor alle medewerkers op de luchthaven gaat gelden, maakt daar volgens Joustra definitief een einde aan.

Al eerder zorgde gerommel met de beveiliging van Schiphol voor gedonder. Donner (CDA) beloofde in zijn vorige functie dat de beveiliging verscherpt zou worden. Hij spendeerde naar verluidt een slordige kwart miljard voor uitbreiding van toegangscontroles, hekjes, stempels, processen, procedures, pasjes, irisscans, vingerafdruksystemen en ook het preventief fouilleren en willekeurig aanhouden van bezoekers en vakantiegangers. Trots verkondigde hij begin 2005 dat Schiphol een van de veiligste luchthavens van Europa was geworden. Kort daarop roofden verklede criminelen op klaarlichte dag diamanten met een waarde van 76 miljoen euro. Een maand later nam een jager zijn dubbelloops geweer met bijbehorende munitie zonder problemen in zijn koffer mee naar Spanje. Vervolgens liet Peter R. de Vries zien hoe eenvoudig het was om met paspoorten van iemand anders van Schiphol te vertrekken en er ook weer mee binnen te komen. Volgens Donner zouden voor het eind van 2005 alle passen van de luchthaven zijn voorzien van biometrische kenmerken. Opvolger Hirsch Ballin belooft nu dat deze irisscan per 1 juli 2008 voor alle medewerkers zal zijn ingevoerd. Drie jaar vertraging maar. Lang niet slecht.

Bovendien zal een terrorist "waarschijnlijk niet zo handelen als de bewuste journalist", volgens operationeel directeur Ad Rutten, verantwoordelijk voor de veiligheid op Schiphol. Weet Rutten iets wat wij niet weten? Zijn er dan nóg betere manieren om een bom in een vliegtuig te krijgen?

Hoe zit het eigenlijk met de screening van Schipholmedewerkers? Journalist Stegeman maakte gebruik van de toegangspas van een collega, die via een uitzendbureau op Schiphol werkte. Die

collega moet gescreend zijn, waarschijnlijk door de Koninklijke Marechaussee. En ondanks het feit dat hij werkt bij Nederland Undercover, kon hij direct aan de slag op Schiphol. Is dat vreemd? Een screening is een controle of iemand een verdacht profiel heeft, en een gevaar voor Nederland of haar bondgenoten kan vormen in de functie waarnaar gesolliciteerd is. Een positieve screening van een journalist op een functie van dokwerker is niet verrassend. Als de screenende medewerker al doorhad dat er een 'Nederland Undercover' actie gaande was, heeft hij dit kennelijk toegestaan. En waarom ook niet? Vrije nieuwsgaring is een existentieel onderdeel van onze samenleving, en het beschermen daarvan is de taak van de AIVD en gedelegeerd gemachtigde KMar. Het dienstverband bij een SBS-productiebedrijf geldt blijkbaar niet als een staatsgevaarlijke activiteit. En als je heel cynisch bent, kun je ook nog veronderstellen dat ophef over onveiligheid rond Schiphol juist gunstig zal zijn voor de KMar, die dan eindelijk het geld krijgt voor de mooie spullenboel die al jaren beloofd wordt. Maar als je dat gelooft ben je wel heel erg cynisch, hoor.

Wat kunnen wij nu met dit alles?

Er zijn een paar interessante observaties te maken. De eerste is dat de ultieme oplossing op dit moment kennelijk de irisscan is. Zo lang deze niet ingevoerd is, mogen we niet nadenken over de restrisico's; de irisscan is een waterdichte oplossing, vindt Joustra. Zo zet je de discussie inderdaad wel stop, ja. Totdat ook dit tovermiddel niet tovert.

Een irisscan is een technische oplossing voor een organisatorisch probleem, namelijk menselijk falen. Als het werkt, kunnen we nooit meer beweren dat technologie geen organisatorische problemen kan oplossen. Ik ben benieuwd. De irisscan op Schiphol houdt ongetwijfeld de undercover journalisten buiten. Maar of een terrorist of een diamantendief er een been in ziet om een uitgerukt oog voor dat apparaat te houden? Of minder bloederig, een laptop met een filmpje van het betreffende oog? Er zijn overigens nog wel meer manieren, maar die krijgt SBS beslist niet gratis van mij.

Tweede observatie: beveiligers gaan minder strikt met de regels om als ze nut en noodzaak niet onderschrijven. Dan zeggen we dat 'de aandacht verslapt'. Als de professionals (de bewakers) de dreiging lager inschatten dan de bestuurders, kan er ook iets anders spelen. Hoe erg vindt de gemiddelde laagbetaalde bewaker het dat een slimme jongen voor een paar miljoen aan spulletjes jat bij een groot en anoniem bedrijf? Hoe waarschijnlijk achten de bewakingsprofessionals een bomaanslag op het vliegveld? Het is niet uit te sluiten dat ze zelf mee de lucht in gaan en dat weten ze. Je kunt ook niet beweren dat de bewakers niet op het belang gewezen worden. Maar het zou maar zo kunnen dat ze niet overtuigd zijn en een aanslag onwaarschijnlijk vinden. Wanneer was de laatste hier ook al weer? Nou, daar helpt geen awareness training meer aan, dan moet je toch eerst een handboek hersenspoelen uit Noord Korea invoeren.

Het kan ook zijn dat er in de risicobepaling niets stond over journalisten. Ze moesten beveiligen tegen dieven en terroristen, niet tegen journalisten. Een aardige illustratie van het toch al vrij hoge stiptheidsactiegehalte van Security.

De belangrijkste les is van het geheel is dat het ruimschoots en voortijdig voldoen aan eisenlijsten vol strenge regels kan samengaan met de lekheid van een mandje. Dat alle losse maatregelen 100% 'geïmplementeerd' zijn, maar het gestelde doel toch niet is bereikt. Dat een strikte pasjescontrole blijkbaar niet overgelaten kan worden aan feilbare mensen. Dat techniek sterker is dan procedures.

Of heeft dit nog steeds niets te maken met ICT-security? Is informatiebeveiliging categorisch anders? Hmm. Bewijs het maar eens.

Wie zwijgt stemt toe

vrijdag 7 maart 2008

Op deze site woedt de laatste weken bijna dagelijks een Privacydebat. Wat vinden we van camera's in vliegtuigen, databases voor vingerafdrukken, DNA en gelaatstrekken, de OV-kaart, rekeningrijden? We zijn tegen! Op het forum debatteren onze vaste bezoekers over de aangekondigde volksopstand, maar in het Haagse pruttelt alleen D66 zachtjes over het einde van de privacy - de rest van het politieke spectrum is zo te zien vóór de ontwikkelingen. Of ze vinden miepen over Wilders belangrijker. In elk geval: Security.NL is één van de condensatiepunten van het burgerlijk ongenoegen over de oprukkende Big Brother-samenleving. En zal als zodanig genoeg aandacht trekken van de Powers That Be. Beschouw je als gewaarschuwd.

De behoefte aan privacy confronteert ons beveiligers met het feit dat meer beveiliging kan leiden tot scherpe afname van het veiligheidsgevoel. De tegenstanders van de huidige regels ter bescherming van onze privacy voeren aan dat alleen mensen die iets te verbergen hebben zich zorgen moeten maken en dat er nu eenmaal geen andere manier is om deze mate van beveiliging te realiseren. De voorstanders van zoveel mogelijk privacy werpen tegen dat technologie faalt, dat mensen niet bespied willen worden, dat de overheid als toezichthouder niet 100% integer en foutvrij is. En dat dat laatste vooral de reden is dat er zoveel privacyregels bestaan. Een gebruikelijke insinuatie is dat de overheid de totale controle over de burger nastreeft, en het internationaal terrorisme aangrijpt om dat erdoor te jassen.

Het argument "niets te verbergen" veronderstelt vooral een integere en kundige overheid. VVD-kamerlid en voormalig crimefighter Fred Teeven zei het 7 januari ronduit: 'Daarbij hebben wij hier zo'n betrouwbare overheid, dat ik me geen zorgen maak om misbruik'. Komt dat voort uit de ervaring die hij als ambtenaar bij justitie heeft? In elk geval zal in de toekomst iedere ambtenaar 100% integer moeten zijn, als de huidige koers doorzet. Het is immers nu al niet ongebruikelijk dat een politieagent even kijkt of de auto die hij wil kopen ooit bij een aanrijding betrokken is geweest. Met zijn salaris kan hij zich inderdaad geen miskoop veroorloven, maar dat terzijde. Het mag gewoon niet en het is niet integer. In de nabije toekomst kan deze agent ook zijn aanstaande schoonfamilie of zijn nieuwe buren doorlichten. Of alle kinderen in de klas van zijn dochter.

Bovendien krijgen steeds meer mensen toegang tot dit soort informatie. Mensen wier integriteit tot op heden nog niet op de proef is gesteld en die daar niet op geselecteerd zijn, in tegenstelling tot de politie. Leerkrachten, vroedvrouwen, procesbegeleiders, beoordelingsambtenaren, maar ook de medewerkers van de bedrijven waar de computersystemen aan uitbesteed zijn. En de inhuur daar. Beveiligingstechnisch is dit een nachtmerrie. Of zoals mijn collega bij sales zegt, een gouden kans.

Kenmerkend voor de tegenstanders van privacy is dat zij het verlies van privacy in alle gevallen als onvermijdelijk zien. Jawel, om veilig te kunnen vliegen is het noodzakelijk dat iedere passagier z'n vingerafdrukken, politieke voorkeuren en DNA afgeeft en een camera op z'n gezicht krijgt gedurende de hele vlucht. Om het milieu te verbeteren moeten meer mensen met het OV, en daarvoor moet nu eenmaal de persoonsgebonden OV chipkaart een succes worden. En de gegevens op die kaart moeten niet alleen bewaard worden, maar ook beschikbaar gesteld voor marketingdoeleinden. Dat is kennelijk nu eenmaal zo. Zoals ook rekeningrijden de enige oplossing is voor de files en dat kan niet anders dan dat de gegevens waar iemand op enig moment is of was, centraal opgeslagen, voor de eeuwigheid bewaard en toegankelijk worden voor alle diensten die daar vanuit veiligheidsbelang bij willen.

Als techneut zeg ik: als je wilt zijn er voor al deze kwesties prima oplossingen die de privacy meer respecteren en nog beter werken ook. Realiseer je dat de kosten om data te beveiligen oplopen naarmate je meer data hebt. Het opslaan van zo min mogelijk gevoelige data waar zo min mogelijk mensen toegang toe hebben, is de beste manier om de veiligheid haalbaar en houdbaar te maken. Onder de huidige koers zullen de beveiligingskosten van rekeningrijden, OV-kaart en luchtreizen een zwart gat zijn. Met als gevolg een lekke beveiliging, want de behoefte tot beveiliging van deze data wordt zo structureel gebagatelliseerd dat je wel heel naïef bent als je denkt dat de moeite überhaupt genomen zal worden. Mijn collega bij sales heeft dan ook pech - Henk, dit jaar weer geen bonus!

Zolang er geen mens aan de andere kant zit, maar een computer, zou er geen sprake zijn van verlies van privacy. Computers schenden immers geen privacy. Zo lang er niemand op die computers aan kan loggen is dat semantisch gezien waar. Toch zullen ook die systemen in de lucht gehouden moeten worden en op dit moment bestaan er geen kaders en middelen die dit zonder menselijke ingrijpen mogelijk maken. Beheerders kunnen nu eenmaal bij de data, zeker als ze enige moeite doen. En om computers beslissingen te laten nemen zonder menselijke interactie, omdat de mens onveiligheid meebrengt, introduceert weer heel andere risico's. Een drogredenering dus.

Een ander gangbaar argument is dat computers alleen gegevens opslaan die al ergens anders bekend zijn. Telefoon- en e-mailgegevens zijn immers bekend bij de provider, dus daar kan iemand geen privacy verliezen. De buschauffeur ziet dat je instapt, dus ook dat is geen geheim. Er is dus helemaal geen sprake van vermindering van privacy! Ja, zo lust ik er nog wel eentje. Het maakt nogal wat uit of hier en daar kortstondig een snippertje van je informatie rondzwerft, of overal en voor de lange termijn je geconcentreerde en gecorreleerde informatie. Geheim en privacy zijn niet lineair hetzelfde. Wie dit serieus als argument aanvoert, begrijpt er helemaal niets van. En wil het waarschijnlijk niet begrijpen, gegeven de inventiviteit van deze drogredenering.

Big Brother is Watching You
Een groeiend aantal mensen ziet inmiddels een link naar de klassieke samenzweringen van Illuminati, New World Order, vrijmetselaars of joden. Is de wereldwijde ontwikkeling inderdaad een vastomlijnd programma? De wezenlijke vraag bij deze veranderingen is die van het waarom. Waarom achten zo weinig beslissers privacy beschermenswaardig? Is Big Brother werkelijk onder ons?

Om de afbraak van onze privacy tegen te gaan is het niet kansrijk om per situatie het gevecht aan te gaan. Versnippering ontkracht ieder verzet. Laten we vaststellen wat de gemeenschappelijke noemer is in de afbraak van onze privacy.

Als je onder de oppervlakte kijkt zie je *wel degelijk* een soort wereldwijde beweging, die zich over vrijwel de volle breedte van het politieke en bestuurlijke spectrum afspeelt. Op de meest onverwachte punten duiken opeens bepaalde mantra's op. De centrale persoon hierin is de Israëlische socioloog Etzion en zijn Communautaire beweging. Deze beweging heeft onder politici een grote aanhang verworven, zonder zichtbaar te worden bij het grote publiek. Als we het al kennen, kennen we het als de Derde Weg, en meer recent van het Normen en Waarden debat.

Etzioni betoogt dat alle mensen verantwoordelijk zijn voor zichzelf en voor elkaar, binnen hun groep. Hoewel Etzioni op het eerste gezicht een protagonist is van de beschaafde dialoog tussen verschillende groepen als matigend tegenwicht tegen markt en overheid, heeft zijn leer behoorlijk scherpe kantjes. Niet verwonderlijk, in zijn jonge jaren was hij lid van Palmach, een marxistisch georiënteerde zionistische beweging van Kibbutzim die de Britten in Palestina tussen 1943 en 1947 met bommen bestookte en hoog op de lijst van terroristische organisaties stond. En hij was recent actief in het neoconservatieve "Project for A New American Century" van Cheney, Wolfowitz, Rumsfield, Libby en Perle. De PNAC kun je toch moeilijk als een gematigd gezelschap zien.

De Derde Weg wordt tactisch gepositioneerd als de aanpak tussen het reëel bestaande staatssocialisme en het pure marktliberalisme, als een morele middenweg tussen links en rechts, van een problematiek die in beide andere benaderingen vooral economisch is. Voor velen een aanlokkelijk model sinds de val van de muur, waarin onze leiders zelf zonder ideologisch houvast kwamen te zitten. Het enige alternatief op dat moment was het neoconservatisme van Cheney en Wolfowitz of de beginselloosheid van paars. Tot Etzioni in het vacuüm stapte. Voor zijn derde weg koos vrijwel ons hele politieke en bestuurlijke spectrum. Google een beetje en je ziet wel wie ik bedoel.

In de leer van Etzioni is de 'dialoog' tussen groepen mensen de lijm van de samenleving. Uit een echte dialoog volgt volgens Etzioni overeenstemming, een gezamenlijk beeld, en dat is de basis voor beleid en gedrag. Alle culturen fuseren magischerwijs naar een gezamenlijk beeld in deze 'dialoog'. Alleen een paar lastige onderwerpen vallen hierbuiten, zoals ras en godsdienst. Er wordt dan ook niet over raciale en godsdienstgrenzen heen gelijmd: inburgeren is het motto.

The Limits of Privacy
Wat vinden de communitairisten nu van privacy en individuele vrijheid? In het traditionele westerse denken zijn privacy en rechtstaat immers een twee-eenheid, die in wetten en verdragen is vastgelegd. Deze relatie ontbreekt in het denken van Etzioni volledig. In zijn "The Limits of Privacy" uit 1999 beargumenteert hij dat de veiligheid van de samenleving in alle gevallen boven ieder individueel recht op privacy gaat. Hij onderkent in zijn model van de behoeften van de mens in navolging van Maslov geen enkele specifieke behoefte aan privacy en individuele vrijheid. Etzioni stelt zonder omwegen dat burgers moreel verplicht zijn de traditionele normen en waarden van de eigen omgeving te volgen. De waarden die van generatie op generatie overgaan, dus. De vrijheid van de burger is volgens Etzioni gedefinieerd in de groep, niet buiten de groep. En de groep beschermt de burger tegen de overheid en tegen de markt. Typische sociologenreutel, omdat sociologen zich beroepsmatig bezighouden met groepen en het individu buiten scope houden.

De enige uitzonderingen op de groepsdynamiek zijn in de visie van Etzioni de psychopaten. Op die manier weet je meteen waar je ingedeeld wordt, als je niet 'gezellig meedoet' met de groep. Want wie beschermt een individu tegen de groep waar hij toevallig in geboren is? Wat is wél een groep en wat niet? Wie beschermt de burger tegen overheid en markt als de groep faalt, of niet als zodanig erkend wordt? Wat mag een 'groep' doen om haar leden te beschermen tegen de overheid als de dialoog niets oplevert? Wat doe je met psychopaten? We zagen al dat een groep die niet meewerkt aan de 'dialoog' buiten het systeem valt. En dat een groep ook als geheel kan

worden uitgesloten, moge ook duidelijk zijn. Wie beschermt de leden van zo'n groep dan tegen de markt, de overheid en de andere groepen? Wat nu als je bij de groep 'Bunnik Side' of 'cobolkrassers' wordt ingedeeld terwijl ze toevallig net even uit de mode zijn? Mag je een andere groep kiezen? Of oprichten? Helaas niet.

Etzioni stelt dat de Westerse waarden van vrijheid en democratie aangevuld moeten worden met algemene waarden uit het Midden Oosten, zoals meer respect voor autoriteit en inzet voor de gemeenschap. Respect moet je erin rammen. Of verwar ik het nu met angst? Hij stelt onder meer voor om jeugdige delinquenten kaalgeschoren en in hun onderbroek naar hun familie terug te sturen en vervolgens hun misdragingen met naam en toenaam op lokale TV en in kranten te vermelden. Een bordje om hun nek waarop staat wat ze misdaan hebben is ook een probaat middel uit de stal van Etzioni, voor wie schaamte een belangrijk sturingsmiddel is. Mensen moeten zich schamen als ze niet 'meedoen', voor hun uitkering, hun afzondering, hun Wasteland bezoek, hun individualisme, hun dik-zijn, hun roken, hun hoerenlopen, hun dronken autorijden. Zet ze met kenteken, naam en toenaam op Internet, in de krant, op TV. Geen privacy voor non-conformisten: hun lot is Naming and Shaming. Vernedering en stigmatisering zijn geaccepteerde middelen in de aanval op privacy door de discipelen van Etzioni. Zo is de schandpaal na een afwezigheid van 154 jaar terug in ons land, maar dan één waar je de rest van je leven niet meer uit komt. En je kunt al aan de schandpaal komen voor zaken die niet eens strafbaar zijn, en voor zaken waar je niet voor veroordeeld bent.

Mocht je niet geloven dat dit in ons land speelt: het OM in Limburg maakt van milieuovertredingen verdachte bedrijven bekend op het Internet. Let wel, verdáchten, niet veroordeelden. Dit middel wordt op deze manier vaker door pseudo-overheden ingezet: ziekenhuizen en scholen met slechte gemiddelde scores, de Autoriteit Financiële Markten (AFM) en de Voedsel en Waren Autoriteit (VWA). Het is niet geheel toevallig dat de voorbeelden toezichthouders zijn in sectoren waar we marktje zijn gaan spelen, maar dat moet maar wachten tot een andere column.

Etzioni lobbyde ook intensief voor Key Escrow (wat hij overigens steevast aanduidt als public key recovery, maar ja PKI is nu eenmaal moeilijke materie), waarbij van alle cryptografische systemen op voorhand een sleutel of een loper bij de overheid ingeleverd moet worden. Het beste was eigenlijk is het gebruik van door de overheid gemaakte cryptografie, zoals Skipjack. Je hebt immers niets te verbergen, en bovendien is PGP of een commerciële crypto hoogstwaarschijnlijk voorzien van een backdoor van een bedrijf, stelt hij. De nadelen van Key Escrow voor de cryptografische sterkte zijn genoegzaam bekend, en de aanname dat de sleutels bij 'de overheid' als niet nader gespecificeerde entiteit, in veilige handen zijn, is op z'n best wereldvreemd. Deze naïeve houding is toch vreemd voor iemand die zich 25 jaar geleden vooral druk maakte over corruptie in de Amerikaanse senaat. Maar goed, daar was de ultieme vijand, 'big business', aan het werk.

Niets aan de hand

Etzioni ziet in overheden per definitie geen bedreiging voor de burger. Toen Bush eind september 2001 een waslijst van beperkingen oplegde was zijn reactie: "The notion that the government is the oppressor and is just trying to use this occasion to deprive citizens of our liberties is distressing and uninformed". Hij vindt Internetfilters dan ook een goed plan, om onschuldigen te beschermen tegen porno, tabaksreclame, geweld en verkeerde ideeën. Toegang tot 'Harmful Cultural products' en commerciële content vallen buiten hetgeen de wet dient te beschermen, beargumenteerde Etzioni in 2004, en mag dus afgesloten worden. Dat de 'kinderpornofilters' ook gebruikt worden tegen vermeende schendingen van auteursrechten, zoals nu in Denemarken en Zweden, daar is dan ook niets mis mee, vindt hij. Ook op andere plekken vind je Etzioni's weerzin tegen het bedrijfsleven. Hij heeft vooral een hekel aan de

tabaksindustrie, Microsoft en Intel, en strijdt al lang voor strenge straffen voor bedrijven die de regels overtreden.

Waar Etzioni wel een serieus risico ziet rond privacy is dan ook in de commerciële sferen, vooral in de gezondheidszorg en op Internet, omdat de bedrijven burgers en eigen medewerkers zullen schaden in hun jacht op commercieel gewin.

Voor de rechtsbeginselen van de veronderstelde onschuld tot het tegendeel bewezen is en nemo tenetur (niet meewerken aan de eigen veroordeling) heeft de socioloog ook geen enkel begrip. Als de overheid geen fouten maakt, bestaan er immers ook geen onschuldige verdachten. Waarheidsvinding en rechtsgang zijn in deze visie hooguit rituelen zonder echte inhoud. Het hele concept van dialoog door groepen is zó flinterdun dat er alleen een almachtige overheid overblijft die burgers en bedrijfsleven er onder moet houden. Etzioni's Derde Weg onderscheidt zich hooguit in de details van het 'reëel bestaand socialisme', de tweede weg die we in 1989 begraven dachten te hebben. De vraag wanneer de afbraak van privacy en rechtstaat ophoudt, is daarmee duidelijk beantwoord: pas als er geen privacy en rechtstaat meer is. Om privacy, rechtstaat en individuele vrijheid te behouden kun je niet om het ontkrachten van Etzioni en zijn gedachtegoed heen. Het motto is hier wie zwijgt, stemt toe. Maar wie spreekt, spreekt tegen.

En daar zijn nog andere valide redenen voor. Zo pleitte Etzioni in 2004 voor preventief militair ingrijpen door de NAVO in Iran, Rusland en Pakistan. Deze 'falende staten' vormden in zijn beleving een groot risico waar terroristen kernwapens voor het oprapen hebben. Toch interessant om te weten is onder welke definitie van falende staten het Rusland van Poetin dan valt. Het is evident dat er voor de NAVO geen enkele kans is om deze 'falende staten' te overwinnen, laat staan overwonnen te houden. Een morele wereldoorlog beginnen om de veiligheid veilig te stellen is namelijk heel erg slecht voor onze veiligheid.

Koud Onderzoek

donderdag 27 maart 2008

De bekende Amerikaanse onderzoeker Edward Felten heeft onlangs aangetoond dat de versleuteling van harde schijven minder veilig is dan algemeen verondersteld wordt. De sleutels worden tijdelijk in RAM opgeslagen en zijn daaruit op te halen met een zogenaamde Cold Boot encryption Hack. Het punt is dat de sleutels niet gelijk weg zijn na het uitschakelen van de machine, maar tot een halve minuut of meer nog in het geheugen achterblijven. Dus als je de stekker uit een machine trekt en deze weer gelijk aanzet, heb je een kans om de cryptografische sleutels uit het geheugen te vissen. Als je snel genoeg bent dan. Maar volgens de onderzoeker zijn de zoekmiddelen hiervoor de laatste tijd sterk verbeterd.

De Cold Boot Hack is natuurlijk geen wereldschokkende aanval, die dan ook weinig aandacht heeft gekregen. De meeste machines die gestolen worden, staan immers uit, of gaan uit terwijl de dief door het verbrijzelde raam stapt en naar de vluchtauto loopt. Dit geldt echter niet voor laptops: die staan vaak in hibernation. Als het goed is zal software met het inschakelen van de hibernation mode de sleutels uit het geheugen verwijderen, maar helaas, het is niet altijd goed. Dat cryptografische sleutels eenvoudig gevonden kunnen worden op een systeem is al een aantal jaren bekend. Hebben we dan het detail met hibernation gemist met z'n allen, of zo?

Het is dus tijd voor een nieuwe policy, nieuwe software en nieuwe images. Voor de meeste organisaties hoeft er buiten de beveiliging van PC's en laptops niet veel te veranderen. Of toch? Het onderzoek beschrijft namelijk aspecten die juist in andere scenario's erg nuttig kunnen zijn. In het bijzonder geldt dit voor de ontdekking dat het gebruik van kou het verval van de data in RAM tegen gaat. En dat werkgeheugen in vloeibare stikstof vrijwel eindeloos de informatie vasthoudt. Dit is goed nieuws voor forensisch onderzoekers, die een manier krijgen om het werkgeheugen van een verdachte machine te bevriezen. Letterlijk. Machines moeten onder de huidige protocollen uitgezet worden, gedetailleerd beschreven en dan vervoerd naar een veilige plek voor nader onderzoek (zoals bijvoorbeeld het NTI voorschrijft[1] en Fox IT impliceert[2]). Het nadeel hiervan is dat het werkgeheugen leeg is voordat de data op een onweerlegbare manier is veiliggesteld. Dus alles wat alleen in het geheugen zit, is weg. Iemand die een beetje handig is met computers, kan het de gemiddelde forensische onderzoeker dan ook knap moeilijk maken. Maar dat wordt een stuk minder als de onderzoeker gewapend wordt met een busje kou en nieuwe protocollen. Bovendien is sinds een tijdje duidelijk dat je met een aanval via de Firewire-poort ook het geheugen van een systeem kunt leeglepelen. Daar zou een forensisch onderzoeker ook heel gelukkig van kunnen worden. Laten we eens aanzien hoe snel de formele forensische protocollen deze nieuwe inzichten absorberen.

Een heterdaadje is bij digitaal forensisch onderzoek op dit moment onmogelijk te bewijzen. Een daad kan hooguit in meer of mindere mate aannemelijk worden gemaakt. Hierbij wordt veel gebruik gemaakt van de minder bekende features van het besturingssysteem. Daarbij zijn de meeste computer seizure guidelines volledig op Windows geënt. Helaas weten de meeste rechters en openbare aanklagers erg weinig van digitale bewijsvoering, zodat nogal wat zaken struikelen tijdens de behandeling. Zeker als de verdediging zich enigszins verdiept heeft in de materie.

---

[1] http://www.forensics-intl.com/evidguid.html

[2] http://www.brainspark.nl/downloads/EDP_Auditor_nr_2_2007_Introductie_Forensisch_IT_Onderzoek.pdf

Mijn tip van de week voor de bad guys: gebruik exotische besturingssystemen als NeXTstep, Warp 4 of HELIOS. En de tip voor forensische onderzoekers: werk alleen voor de verdediging.

De nieuwe manier om cryptografisch materiaal uit het RAM te halen is goed nieuws. Zeker voor de rechtstaat: de kans dat juridische dwang nodig is om de verdachte de sleutels te laten afgeven - en daarmee mee te laten werken aan de eigen veroordeling - wordt een stuk kleiner. Dit is wel weer een tegenvaller voor de protagonisten van deze omgekeerde bewijslast - het feit dat forensische onderzoekers iets zouden kunnen, maakt het niet toepassen van de nieuwe inzichten tot falen.

De onderzoeker Felten signaleert dat in het verleden wel vaker mensen op het trage dataverval in RAM gestuit waren, maar dat de beveiligingsimplicaties niet eerder onderzocht waren omdat er geen publicaties over te vinden waren - behalve een Duits artikel uit de jaren '70. Het is te hopen dat het met dit onderzoek anders loopt. Door de relatie met één specifiek beveiligingsaspect te leggen is Felten helaas wel in dezelfde valkuil getrapt. Na tien minuten was het al oud nieuws en verdwenen zijn conclusies in de vergetelheid. Of had iemand hier het bericht wel gezien?

Laten we de omissie rechtzetten: de welopgeleide en uitermate kundige lezers van dit platform kunnen vast nog meer Security implicaties van de Cold Boot Hack deze bedenken. Die overigens evenmin zullen doordringen tot de officiële handboeken, zelfs als we er een prijsvraag van maken. Ach, als we onze plaats maar kennen, nietwaar?

We kunnen er in ieder geval in onze directe omgeving ons voordeel mee doen. Nou heb ik thuis een laptop die van nature beveiligd is: je bent al gauw een kwartier aan het hannesen voordat je bij de geheugenmodules kunt en dan is het geheugen echt wel leeg. Die is af fabriek beveiligd tegen de koude aanval. Er zit alleen wel een PC-card slot in en daar kun je wel een firewire in prikken. Dan maar géén laptop meer. Ik ga bovendien mijn desktops beveiligen door de dimms met druiplijm in te pakken en de systeemkasten met superlijm dicht te kitten. Die firewire kaarten moeten er uit, helaas. Hoewel, zo lang forensisch specialisten nog in de problemen komen met iets anders dan Windows en inzichten van ná 1998, hoef ik mij helemaal niet druk te maken. CSI bestaat namelijk alleen op TV, niet in onze wondere wereld van ICT beveiliging.

Een triviaal bureautje in de periferie

donderdag 10 april 2008

Er was deze week een ICT beveiligingsnieuwtje dat het nieuws niet gehaald heeft, wat erg jammer is. De feiten: de NAVO heeft in de opbouw van het vermogen tot cyberwarfare de volgende concrete stap gezet met het instellen van de Cyber Defence Management Authority (CDMA). Dit internationale centrum wordt in Brussel neergezet en moet eind 2008 operationeel zijn, zo is besloten tijdens de NAVO-top in Boekarest. Dit CDMA krijgt een coördinerende taak, zodra een nationale overheid daarom vraagt. Tot een dergelijk fenomeen zich voordoet, zal het CDMA standaarden en procedures ontwikkelen om aanvallen te voorkomen en af te schrikken. Het CDMA heeft haar kenniscentrum al geopend in Tallinn (Estland) en IJsland heeft haar concrete steun hiervoor al toegezegd. Tja, een nieuwe papierfabriek in Oost-Europa klinkt inderdaad niet zo nieuwswaardig. Maar toch is het bericht interessant genoeg om eens nader te bekijken.

De Amerikaanse pendant van het CDMA (het US Air Force cyber-operations command) heeft recent bij monde van Lt. Gen. Robert J. Elder Jr. verklaard dat de VS in de toekomst mogelijk tot de inzet van network warfare overgaat om de communicatie van tegenstanders te ontregelen, een taak die op dit moment nog met conventionele middelen als kruisraketten en ander slim bommentuig gerealiseerd wordt. Lager in het geweldsspectrum zullen de Amerikanen bloggers inhuren om bepaalde denkbeelden over de bühne te krijgen, en om eventueel het bepaalde personen moeilijk te maken.

Zo zie je dat het denken evolueert en de linies op het digitale slagveld opgebouwd worden. Hoe ver is de NAVO intussen? Het CDMA heeft een beduidend minder ambitieuze opzet. Het wordt opgezet als defensieve instelling om 'internationale systemen' te waarborgen. "The keynote is defence, whether an attack comes from state, criminal or other sources," aldus de NAVO-woordvoerder. Heeft de NAVO een nieuwe taak in criminaliteitsbestrijding?

De verschillende nationale entiteiten die door het CDMA gecoördineerd moeten worden, verkeren in verschillende fasen van opbouw. Volgens Gartner zijn wereldwijd 120 landen bezig om een offensieve capaciteit voor digitale oorlogsvoering op te bouwen, waarvan 30 al een daadwerkelijke capaciteit bereikt hebben. Deze instanties vallen binnen de NAVO niet onder de gezamenlijke paraplu, die zich immers a priori beperkt tot defensieve capaciteiten. De kans dat de CDMA iets zinnigs te coördineren zal hebben tussen nationale instanties in Europa lijkt dan ook al niet groot, een defensie zonder vermogen tot een tactisch tegenoffensief is weinig meer dan een papieren Maginotlinie. Bovendien zijn veel van de genoemde 30 landen geen NAVO-lid. Gelukkig is het aantal standaarden, normen en procedures dat je kunt opstellen voor theoretische eventualiteiten onbeperkt, anders zouden ze zich eens gaan vervelen. Maar het wordt vast geen club waar de echte security-talenten bij zouden willen werken.

De NAVO is voorlopig gepreoccupeerd met het beschermen van de eigen infrastructuur. Dat hangt wellicht samen met de recente resultaten van de inzet van Telindus om de eigen systemen te beveiligen; men is geschrokken van het aantal aanvallen dat de Cisco spullen signaleren. Dat gaat wel over, na enige tijd krijg je wel een beeld van wat ruis is en wat niet.

Als de CDMA iets moet betekenen in een echte oorlog (met bijvoorbeeld de Russen) is een plek vlak bij de grens van het NAVO-territorium niet echt handig - de kans dat het kenniscentrum lang operationeel zal zijn, lijkt dan ook minimaal. Dat het bureaucratische hoofd in het verre Brussel zit, maakt daarbij ook niet veel uit. Het lijkt er op dat de NAVO met deze actie een signaal heeft willen afgeven richting Poetin dat ie met z'n tengels van onze kritieke digitale infrastructuur moet

afblijven. Of is het meer iets van een triviaal bureautje neerzetten om onze jongste bondgenoten ook iets te geven?

Het echte nieuws is dus blijkbaar dat we met onze bondgenoten niet zullen samenwerken als het op digitale oorlogsvoering aankomt, en dat we daarvoor een bureautje openen in de periferie van ons grondgebied. Een duidelijker signaal dat de er in beleving van de NAVO weinig aan de hand is, lijkt mij moeilijk denkbaar.

Volgens gerenommeerde ICT security specialisten is er juist heel veel aan de hand en is het de hoogste tijd voor een stevige digitale defensie. Een aanval op de internationale digitale infrastructuur klinkt wellicht wat vergezocht, maar - zo meldt John Walker, vice-president van de Information Security Systems Association (ISSA) – ook 9/11 klonk vergezocht en is toch gebeurd. "It is therefore feasible that something could happen on that scale in the cyber world, via the Internet". Zo is er vlak voor kerst 2006 een internationaal alarm uitgegaan omdat er een digitale aanval op de financiële sector ophanden was. Nu ja, zou zijn geweest, want het werd een stille en vredige kerst. Volgens Walker is een frontale digitale aanval op onze kritieke infrastructuur binnen twee jaar zeer waarschijnlijk. Nu deed hij deze uitspraak in april 2007 - dan hebben nog maar héél weinig tijd.

Een prachtige logica gebruikt Walker hier: als één onwaarschijnlijk verhaal gebeurt, moeten we rekening gaan houden met andere onwaarschijnlijke verhalen; de natte droom van alle FUD artiesten. Ik houd persoonlijk dan ook serieus rekening met de dreiging dat de hemel op ons hoofd zal vallen, waar Asterix ons immers al jaren voor waarschuwt. Overigens was 9/11 niet onwaarschijnlijk, zoals de onderzoekscommissie van het Amerikaanse congres vaststelde, maar werden de signalen niet opgepakt. Het gebruik van passagiersvliegtuigen als bommen was al in 1993 als scenario onderzocht, na de eerste aanslagen op het WTC. Bovendien zijn er in 1994 drie van dergelijke pogingen mislukt en heeft de dader van de eerste WTC aanslag in 1995 gemeld dat een dergelijke aanval overwogen was. Wat er dan nog overblijft van de redenering van de gerenommeerde specialist dat we onwaarschijnlijk klinkende verhalen serieus moeten nemen? Ik denk dat de ISSA een betere vice-president verdient, en die in ieder geval dringend nodig heeft om nog enige geloofwaardigheid te houden.

2007 was in ieder geval het jaar van de waarheid voor de Idolen van de Internetbeveiliging: ook Instant Messaging en VoIP schijnen het afgelopen jaar door gerichte aanvallen onbruikbaar te zijn gemaakt. Daniel Ingevaldson, directeur technologie strategie van de X-Force (IBM, vroeger ISS) achtte dat eind 2006 onvermijdelijk omdat VoIP volgens [3] hem op dezelfde onveilige protocollen draait als e-mail. Hij denkt toch niet dat VoIP op SMTP draait? Of bedoelt hij IP? Ik heb een nieuwtje voor onze IBM-er: het hele Internet draait op IP. Er bestaan geen 'veilige' protocollen.

Phyllis Schneck, directeur van het FBI programma Infragard noemt het gegeven dat 9% van alle spam in Azië van computers in China afkomt als bewijs van de betrokkenheid van de Chinese regering. Ik ben toch benieuwd hoeveel procent van alle pc's in Azië in China staat, hoe ervaren de gebruikers zijn en of die 9% dan nog zo statistisch significant is. De opmerking van Kaspersky hierover is opvallend afwijkend van het koor van gerenommeerde specialisten, en beduidend geloofwaardiger: de Chinese politie is zo beroerd en corrupt dat iedere hobbyist alles kan doen wat digitaal verboden is zonder enig risico te lopen. Duidelijk toch, zolang het maar niet openlijk bloggen over Tibet is. Daarbij leidt de Internet censuur tot een boel creativiteit onder de dikke 200 miljoen internetgebruikers in China. Deze activiteiten zijn primair tegen de Chinese regering

[3] http://www.information-age.com/briefing-rooms/security-and-continuity/273356/the-state-of-security.thtml

gericht, niet tegen het Westen. Met censuur leer je ze hacken, wat niet de bedoeling zal zijn van de Chinese overheid. Maar een genuanceerde visie op deze materie hoor je vrijwel nergens, we vinden het juist het heel fijn om bedreigd te worden. Goed voor de omzet of de status. Deze georkestreerde paniek doet denken aan het werk van spindokters, en lijkt verdacht veel op de bomber-gap en missile-gap hysterie uit de Koude Oorlog. Het heeft al met al een hoog Fitnagehalte, dit opkloppen van de angst uit de behoefte om een bekwaam bestuurder te lijken.

Het is blijkbaar een groot wonder dat je anno 2008 deze column nog kunt lezen over een extreem vijandig, door Chinese en Russische spionnen en terroristen gemanipuleerd Internet. Want als de leidende specialisten aan onze kant zulke koeien van vergissingen maken, is het niet meer dan terecht dat we het gevecht verliezen zodra we echt aangevallen worden. Gegeven dat de boel nog werkt is dat niet zo. Gelukkig is de NAVO slim genoeg en gebruikt het de FUD alleen om de Estse regering te paaien en de lokale economie te stimuleren. Het zal namelijk nog wel even duren voor het Internet een serieus digitaal slagveld is voor nationale legers en internationale terroristen.

Security volgens WC-Eend

dinsdag 6 mei 2008

"Wij van WC-eend adviseren WC-eend". Kent u 'm nog? Het was de briljante slogan van de reclameklassieker uit de jaren '80, uitgesproken door een ernstige man in een witte jas, in een laboratorium-achtige setting. Met dank aan GeenStijl is het vorig jaar nog door Trouw uitgeroepen tot de beste reclameslogan aller tijden. De ultieme parodie op het gebruik van pseudo-onderzoek om een product aan de man te brengen, indertijd zeer gangbaar voor schoonmaakmiddelen, maakte meteen een einde aan dit gebruik. Althans, in de schoonmaakmiddelenbranche. Onze bedrijfstak heeft de WC-eendenles nog niet geleerd en blinkt nog altijd uit in reclame van het soort "onafhankelijk onderzoek wijst uit...."

Een paar recente voorbeelden. "Uit onderzoek, dat onder 370 Britse bedrijven is uitgevoerd, blijkt dat 65% van de bedrijven zichzelf onnodig in gevaar brengt, omdat zij het gevaar onderschatten van USB-sticks, flash drives, iPod's en PDA's, die een bedreiging vormen voor de veiligheid van hun netwerk". Lulkoek. Dat bedrijven de risico's onderschatten is geen feit – er is immers niet onderzocht of voor de specifieke bedrijven er sprake is van grote risico's. Het zou best kunnen natuurlijk, maar dit onderzoek wijst dit niet uit. GFI gaat verder: "Het gebruik van draagbare opslagmedia is een grote bedreiging als bedrijven geen record hebben van de bestanden die van het netwerk naar het medium worden overgebracht en vice versa. Slechts 29% van de bedrijven registreert daadwerkelijk welke gegevens naar en van het netwerk worden overgebracht". Nog mooier: aan het niet onderzochte feit wordt vervolgens een niet bewezen oplossing gekoppeld. Alsof het registreren van de bestandsnamen als losse actie wél afdoende zou zijn. GFI sluit dit merkwaardig stukje proza af met de opmerking dat het onderzoek "door een onafhankelijk mediabedrijf werd uitgevoerd". Mediabedrijf? Was het komkommertijd in Hilversum of zo? En let op het woord onafhankelijk. Er staat al bijna wetenschappelijk. Je ziet de witte jas zó voor je.

"Wereldwijd onderzoek van PriceWaterhouseCoopers en CIO Magazine toont aan dat informatiebeveiliging verbetert, maar tevens dat toename van kwetsbaarheden en bedreigingen noodzaken tot een planmatige aanpak". De toename van kwetsbaarheden en bedreigingen waaraan gerefereerd wordt is volledig afkomstig van de door de 8200 leidinggevenden gesignaleerde incidenten, maar wordt gepresenteerd als een vaststaand feit dat tot een bepaalde aanpak leidt. Terwijl het feit niet onderzocht is maar alleen de perceptie geturfd, noch dat de effectiviteit van de voorgestelde aanpak onderzocht of bewezen is.

"Uit recent onderzoek, dat is uitgevoerd in opdracht van NetIQ, onderdeel van Attachmate, blijkt dat IT-managers VoIP-security dreigingen ernstig onderschatten. Het wereldwijde onderzoek is gehouden onder 155 organisaties die gebruik maken van VoIP-systemen of van plan zijn deze te gaan inzetten. De enquête toont aan dat veel IT-managers hun ogen sluiten voor bedreigingen van de VoIP-infrastructuur". De dreigingen worden gebracht als vaststaand feit. Onderzocht

hoefden ze blijkbaar niet te worden. Wedden dat NetIQ een prachtig doosje heeft voor dit soort problemen?

Een prachtig voorbeeld van hoe dit effect werkt is het regelmatig terugkerende onderzoek van onder meer CompTIA en Information Week naar “de grootste Security risico’s”. Aan een groot aantal Security managers, ICT managers en allerhande consultants wordt gevraagd wat zij als grootste bedreiging zien. Het antwoord levert vervolgens koppen op als ‘Gebruiker nog steeds de grootste bedreiging’. Dit wordt door de Security en ICT managers, net als door de consultants vervolgens geabsorbeerd als absolute waarheid. Zo is de cirkel vicieus: de meeste aandacht gaat naar interne beveiliging waardoor de incidenten daar meer indruk maken zodat ze het meeste aandacht trekken. En ja, dat is tevens een neerwaartse spiraal. Ook Computable meldde onlangs nog dat “onderzoek heeft aangetoond dat meer dan 80 procent van alle beveiligingsinbraken van binnen de eigen organisatie komen!” in een artikel over een autorisatie query tooltje.

David Lynch van Apani, marketing directeur van een bedrijf gespecialiseerd in het beveiligen binnen bedrijfsnetwerken, meldde in 2005 al: “Insider attacks have been with us almost as long as networks have been with us. It is a phenomena that has been extensively studied over the years, and depending on which study you believe, anywhere from 40% to 70% of ALL attacks come from the inside - and this ratio has held ever since the first time I ever saw a Cyber crimes report, well over 10 years ago”. Het beeld is al tien jaar hetzelfde, dus het is kennelijk zo. Nu was het aantal outsider attacks tien jaar voor 2005 (in 1995 dus) logischerwijs erg klein, zo zonder internet en e-mail. Maar toch is er niets veranderd en er zal er nooit wat veranderen.

Het kan ook nog zo zijn dat dit een typisch Amerikaans fenomeen is dat hier niet geldt, maar kritiekloos overgenomen wordt. Zoals onderzoeken in één land vrijwel altijd van toepassing worden verklaard op de hele wereld. De incidenten in Amerika worden grotendeels getriggerd door de rottige manier waarop personeel behandeld en ontslagen wordt, wat wraakacties oproept. Een onderzoekje bij één van onze grootste ministeries wees uit dat we, ondanks het grootschalig opheffen van diverse locaties en het overbodig maken van het bijbehorend personeel, wat vervolgens door de opheffing de eigen huizen niet meer aan de straatstenen kwijtraakte, er geen enkel intern misbruik kon worden gevonden. Tijd voor een echt onderzoek in Nederland?

Statistieken en leugens

“Cybercriminelen lijken een voorkeur te hebben voor Apache servers voor het besmetten van documenten en websites. Maar liefst 51 procent van de servers die ten prooi zijn gevallen aan de praktijken van de kwaadwillende hackers, is van dat type” meldde Sophos. Hoeveel procent van de webservers draait Apache? En daarbij, is besmetten de enige activiteit van kwaadwillende hackers? Of zelfs maar de ergste activiteit?

Veronderstelde causaliteit

"88 procent is ervan overtuigd zich goed voorbereid te hebben op de grootste bedreigingen; slechts 56 procent van deze bedrijven heeft procedures om op incidenten te reageren," aldus Chris Potter, partner van PWC in het BERR onderzoek van 2008. Het klinkt wel logisch, maar het zou toch kunnen dat procedures om op incidenten te reageren niet de enige mogelijke voorbereiding is op de grootste bedreiging.

McAfee in 2005: “One in five workers (21 per cent) let family and friends use company laptops and PCs to access the internet, dramatically increasing the chances of infection of the device and potentially the corporate network”. Want? Als mijn buurman op mijn bedrijfslaptop zoekt naar een illegale Photoshop CS3 waar de spyware van Adobe uitgesloopt is, loopt hij een grotere kans een virus op te lopen dan als ik dat zelf doe? Ja vast.

Deloitte heeft in een onderzoek in 2006 vastgesteld dat bedrijven de noodzaak van goede beveiliging onderschatten. Het bewijs: maar liefst 54 procent van de Chief Cecurity Officers (CSO’s) vindt dat de investeringen achterblijven op de toenemende dreiging van virussen en

aanvallen. Is dat bewijs? Is het niet waarschijnlijker dat menig CSO gewoon vindt dat ie een hoger budget nodig heeft, en iedere argumentatie welkom is?

“Organisaties die het bouwen van applicaties uitbesteden, lopen grotere kans gehackt te worden’, meldt analistenbureau Quocirca. Uit hun telefonische onderzoek blijkt dat alle Europese organisaties die programmatuur elders hebben laten bouwen, doelwit zijn geweest van kwaadwillenden. Nu zou het interessant kunnen zijn te weten hoeveel organisaties die al hun programmatuur zelf bouwen, geen doelwit zijn geweest van kwaadwillenden. Dat zou wellicht enige diepte geven aan de bewering, die nu alleen geldt als oproep niet uit te besteden. Maar het trekt de aandacht, en dat is waar het natuurlijk om te doen is. Bovendien, organisaties die al hun applicaties zelf bouwen bestaan niet, tenminste ik ken geen club die de eigen besturingssystemen bouwt en onderhoudt. Of is het kopen van off-the-shelf producten categorisch iets anders dan het uitbesteden van softwarebouw? Wat bewijst het?

“Tijdelijk personeel heeft wel toegangsrechten, maar gaat niet op dezelfde manier om met bedrijfsgegevens” ontdekte beveiligingsbedrijf Websense. In het onderzoek werden honderd tijdelijke medewerkers van verschillende bedrijven ondervraagd. 62 procent van hen gebruikte wel eens (met toestemming) de inloggegevens van een interne collega en 52 procent gebruikt e-mail accounts van een collega. Dit noemt Websense “Schrikbarende aantallen, zeker in combinatie met de 81 procent van de ondervraagden die altijd toegang had tot internet, zonder restricties”. Het ondervragen van 100 inhuurkrachten zal je weinig feiten kunnen geven, zeker als je de uitkomsten niet afzet tegen het gedrag van de interne medewerkers in vergelijkbare posities. Waarschijnlijk is meestal gewoon zo dat je het mailaccount van een collega gebruikt omdat je er zelf (nog) geen hebt, en ook geen eigen werkplek. De meeste mensen hebben immers geen idee hoe een mailclient naar een andere account om te zetten. Maar wat heeft dit met Websense te maken? Het lijkt eerder een geleend ‘onderzoek’ van een IDM vendor dan van webfiltersoftware. Maar zie daar de slotzin: Er is een “schrikbarende” combinatie met ongefilterde internettoegang! Is dat onderzocht dan? Nee? Dan vraag ik mij toch af waarom niet. Ik vermoed omdat een dergelijk onderzoek aan zal tonen dat inhuur hetzelfde doet als de eigen medewerkers en de dag doorbrengt op ongevaarlijke websites als nu.nl, de rabobank, viva, marktplaats en ouders.nl. Tja, dan heb je geen Websense meer nodig.

Kortom, WC-eenden te over in securityland. Als ik zie hoeveel aandacht onwetenschappelijke, oppervlakkige en kromme onderzoeken trekken kan ik maar één conclusie trekken: dat wil ik ook! Ik wil graag gezaghebbend, onafhankelijk én wetenschappelijk aantonen dat het niet lezen van security.nl, en dan in het bijzonder mijn columns, gevaarlijk is voor organisaties en zal leiden tot imagoschade, faillissement en zelfs gevangenisstraf voor de bestuurders. En dat graag uitgesproken door iemand in een witte jas.

Als ik nu het oplezen van mijn vragen door een aantal studenten communicatie van een hogeschool als stageonderzoek laat uitvoeren, kost het niets. Daarbij zijn studenten aanstaande wetenschappers en omdat ze niet op de loonlijst staan zijn ze onafhankelijk. Zo, dat is het begin. Welke vragen zouden de studenten moeten stellen? Enquêtevragen zijn alleszins te manipuleren en indachtig de reeks eerdere columns kom ik uit de losse pols tot de volgende:

De Security.nl WC-eend enquête:
1. Heeft uw organisatie een beveiligingsbeleidsdocument ja/nee?
2. Heeft uw organisatie een security architectuur ja/nee?
3. Heeft uw organisatie een security awareness programma ja/nee?
4. Heeft uw organisatie (delen van) uw ICT uitbesteed dan wel extern ingekocht ja/nee?
5. Werkt uw organisatie conform best practices ja/nee?

6. Is het aantal CISSP's in uw organisatie de afgelopen drie jaar toegenomen ja/nee?
7. Heeft uw organisatie in de afgelopen drie jaar meer beveiligingsincidenten ja/nee?

Als het antwoord op de laatste vraag en één van de anderen ja is, is het bewijs geleverd dat het niet opvolgen van mijn adviezen leidt tot meer beveiligingsincidenten. En voor al die partijen die mij niet ingehuurd hadden in de afgelopen jaren, kan dit alleen maar komen door het niet lezen van security.nl. Als ze de site wel lezen maar er zijn nog steeds beveiligingsincidenten, dan zijn ze te eigenwijs. Als het antwoord op de laatste vraag echter is dat er niet meer incidenten zijn, bewijst dat, dat de detectie van beveiligingsincidenten ver onder de maat is. Iedereen weet toch dat het Internet steeds gevaarlijker wordt? Dus het antwoord is altijd ja.

Mijn enquête gaat onafhankelijk en wetenschappelijk bewijzen dat er geld over de balk gesmeten is terwijl er zeer grote belangen te beschermen zijn. Dergelijke onvergeeflijke incompetentie op beveiligingsgebied leidt in het beste geval alleen maar tot imagoschade. Het nemen van zulke grote risico's met ICT zal bovendien niet ontsnappen aan de aangescherpte blik van de auditoren die opereren volgens het 'Show Me' beginsel, dus naar de SAS70 statement kun je fluiten. Bovendien is er geen geld over om de hackers buiten te houden, dus de organisatie en haar klanten worden aan alle kanten leeggeroofd door Russische hackers. Dat leidt weer tot het verlies van omzet en sterk dalende koersen, en uiteindelijk faillissement.

De VEB zal er dan ook niet voor terugdeinzen om de artikelen over bestuurdersaansprakelijkheid uit de kast te trekken. Ik zal in dat geval onbezoldigd als getuige-deskundige optreden, zodat een ieder duidelijk is dat er buiten security.nl geen onafhankelijke waarheid bestaat. Het wordt tijd de lezers te laten betalen voor alle goede adviezen.

Leuke speledingetjes

maandag 26 mei 2008

Mobiele veiligheid is hot. Smart phones, PDA's en laptops, ja, daar zijn leuke dingen mee aan de hand. Neem de Blackberry, de smart phone voor de elite, van het Canadese bedrijf RIM.

Is een Blackberry veilig? Vast wel. Ze zijn in elk geval in ons land goedgekeurd voor het bevatten van (lage categorieën) staatsgeheimen. Nu was niet iedere regenjas hier te lande daar even blij mee, en de Franse collega's hebben het tegen een vergelijkbare set beveiligingseisen afgekeurd. Ook elders is blijkbaar niet iedereen even overtuigd van de veiligheid van de BB. Onlangs ontstond nog ophef over de vermissing van twee toestellen van Amerikaanse diplomaten bij een internationale top. Als de BB's superveilig waren, zou er geen ophef zijn geweest. Het Witte Huis geeft geen commentaar.

RIM stelt zich over het algemeen terughoudend op met claims over de veiligheid van het eigen product. Leveranciers echter geven er torenhoog over op. Brian Reed, chief marketing officer van BoxTone: "The Blackberry is the Sherman tank in terms of a secured device, as security has always been a focus for RIM". De Sherman tank stond er echter vooral om bekend dat hij zo snel in de fik vloog. De bemanningen gaven hem de bijnaam Ronson, naar de aansteker. Maar dat bedoelt Reed denk ik niet. Hij bedoelt denk ik gewoon dat je een Blackberry moet kopen en verder geen ingewikkelde vragen moet stellen. En dat zal je bedrijf gewoon doen, of je nu tegensputtert of niet.

RIM heeft met de laatste versie van de Blackberry server weer een boel extra beveiligingsfeatures toegevoegd. Zo kan de beheerder gewaarschuwd worden als het toestel zich op een onwaarschijnlijke plek bevindt. Ook kan de server instellen dat de telefoon zichzelf vernietigt als hij wordt aangevallen. De zwaktes van een paar jaar geleden met certificaten en trojans lijken nu ook onder controle. Dat is goed.

Met het sterker worden van de toestellen verschuift het beveiligingsvraagstuk richting de infrastructuur. De Blackberry servers in het eigen netwerk vormen een kritiek onderdeel van de beveiliging. Hoe je die inricht is een zeer prominent vraagstuk. Immers, de server is de sleutel tot het koninkrijk.

Nu word je door de consultants aangeraden een Blackberry router in een DMZ op te stellen vóór de BES server, die immers onderdeel van het LAN moet zijn. Denk echter niet dat de Blackberry router een echte router is: het is een Windows machine met een routerende functie erop. Gegeven het feit dat de BES 'router' berichten verwerkt, en dus input van buiten afhandelt, is dit systeem categorisch kwetsbaar. De input moet afgehandeld worden en dat brengt risico's met zich mee. En die zijn niet denkbeeldig. Volg de berichten van 0day kwetsbaarheden en virussen maar: packers en parsers – daar gaat het om. Bovendien vraagt het veilig opstellen van een Windows server in een DMZ expertise en hulpmiddelen die in veel organisaties ontbreekt.

Verder luidt het dringende advies om een firewall tussen de BES router en de BES server in het LAN te plaatsen. Dat klinkt goed. Alleen moet het wel een hele slimme firewall zijn – hij moet toch eerst het verkeer snappen. Een simpele statefull firewall zal er weinig van bakken.

Zonder een DMZ/BES Router architectuur geldt het geheel als onacceptabel zwak. Maar ook als je alle adviezen opvolgt wordt het nooit heel sterk. Als het strengste dat je kunt doen is zorgen dat alleen de BES router kan communiceren met de BES server, is je winst eigenlijk niet zo groot. Deze structuur kan weliswaar een aanval vertragen en de pakkans vergroten, maar zeker niet uitsluiten. Helemaal niet op de lange termijn.

Als de server voor gaas gaat bij een aanval, gaat bovendien niet alleen het hele mobiele gebeuren mee, maar ook het interne netwerk. BES is een Windows applicatie die gebruik maakt van active directory. Een significant deel van de beveiliging ligt dus buiten BES en in de inrichting van de Windows omgeving. Met het introduceren van geavanceerde beveiligingsfeatures voor de telefoons krijg je vanzelf de neiging om de apparaten in te zetten voor meer kritieke rollen. En zo ontstaat dan juist meer onveiligheid: BES kan voor een aanvaller een mooie en permanente toegang vormen tot een beveiligd netwerk, dus het is het al snel waard.

De gaten zullen wel gevonden worden. Daarvoor staat de klantenlijst van Blackberry garant. Bij het zien van die lijst zal immers menig ondernemend of spionerend hart in Rusland of China al sneller gaan kloppen. En die melden hun exploits niet op Full Disclosure.

Tips

De complexiteit waar je mee te maken krijgt als je de puzzel die Blackberry heet wil beveiligen in een bedrijfsnetwerk overstijgt het denkraam van vrijwel iedere beveiliger. En zodra niemand het overzicht kan bewaren, maak ik me zorgen. Daarom een paar tips:

- Bedenk je dat mobiele veiligheid niet alleen de beveiliging van het apparaat zelf is. De verkopers hebben het wél alleen daarover. Het is namelijk hun product. En ze willen het verkopen.
- Beveiligingsfeatures dienen om toestellen te verkopen, niet om je data te beveiligen. Hoe beter je oplet en hoe meer je vraagt, hoe beter die beveiliging zal worden. Praat met de makers. De leverancier zal immers alles doen om je een nieuw apparaat te verkopen. En als dat inderdaad beter is, ach, waarom niet – je hoeft niet te doen alsof je het uit eigen zak betaalt, hoor.
- Vroeg of laat wordt de back-end kwetsbaarder dan de front-end. Een sterke beveiliging van de front-end via de back-end kan gebruikt worden als aanvalsmiddel. Als een toestel remote gesloopt kan worden met een beveiliginsfeature, zal er altijd iemand zijn die gaat uitzoeken hoe deze functie te misbruiken. Niet elke feature is een aanrader.
- Zodra een telefoon te breken is met een e-mailtje, zijn e-mailtjes een groter risico dan telefoondiefstal.
- Met Blackberry neemt de vervlechting van je systemen binnen en buiten toe, dus ook de kwetsbaarheid. Op enig moment zul je SAP en Putty op de toestellen aantreffen. Beveiliging per laagje, per clubje en per silo is dan kansloos.
- E-mail is grotendeels zut; e-mail op een telefoon is niet anders. Filtering van mail op onwenselijke zaken wordt dus nog belangrijker dan het al was. Daarbij moet je je realiseren dat bestaande mailfilters hoofdzakelijk bedreigingen voor Windows onderscheppen. Die zijn niet goed genoeg.
- Als berichten door een parser moeten, is een systeem zeer kwetsbaar. Het is fijn dat je bestanden in Word en Acrobat kunt bekijken op je minuscule schermpje, maar ieder format erbij introduceert ook tientallen mogelijke nieuwe gaten. Ook antivirusproducten

gebruiken een parser. Stel je er dus op in dat je regelmatig bepaalde bestandstypen moet tegenhouden tot je kunt patchen. Zorg dat je dit kunt en dat de gebruikers dat weten.
- Het beveiligen van browseverkeer tegen malware en gerichte aanvallen staat in vergelijking tot mail al helemaal in de kinderschoenen. Zelfs de beste middelen die je kunt inzetten zijn zeer beperkt qua mogelijkheden, dus stel grove beperkingen in de sites die de BB-gebruikers mogen bezoeken.
- S/MIME en HTTPS certificaten mogen dan wel beveiligingsmiddelen zijn, als ze van onbekende herkomst zijn kunnen ze zelf een bedreiging vormen. Zij zijn immers óók input van onbekende users, die je eerst moet verwerken voordat je weet of het goed is.

Spionage en cyberterreur

Dan zijn er ook nog mensen die zich druk maken over het feit dat alle berichten via het RIM-netwerk lopen, en dus via Noord-Amerika. Dan zou de NSA ze kunnen onderscheppen en kan alle gevoelige informatie bij onze militaire bondgenoot annex economische concurrent terechtkomen. Eng? Misschien, maar het introduceert geen extra risico: hetzelfde geldt voor alle andere communicatiekanalen, behalve postduiven en buizenpost. (Rooksignalen niet: die worden door satellieten in de gaten gehouden.)

Andere overheden kunnen de berichten juist weer niet onderscheppen – zo lopen er discussies met de Indiase regering die de berichten van BB-gebruikers uit India wil kunnen onderscheppen. Hoewel het projecteren van dit soort nationale behoeftes op een grensoverschrijdend systeem als BB té 1952 voor woorden is, zal er toch heus wel een afluistervoorziening ingebouwd worden. RIM zal de groeimarkten in Azië immers niet willen missen. Nu vinden wij het over het algemeen niet zo heel erg dat Amerikaanse spionnen onze diepste geheimen kennen, maar om hun collega's uit India of China hetzelfde privilege te geven gaat wel erg ver.

Wat belangrijker is, is dat een aanval op RIM zelf een mega-impact op de Command and Control keten van het Westen zal hebben, een kwetsbaarheid die steeds groter wordt met het groeiend gebruik. Nu zullen de verschillende krijgsmachten hopelijk hun eigen separate communicatiekanalen hebben, maar bedrijven en andere overheden zullen in dat geval strategisch onthoofd worden. Toch lastig, vooral in spannende tijden. Bovendien zal het lang niet altijd duidelijk zijn dat het aanval is – het zou ook een storing van een aantal dagen kunnen zijn.

Het onderuit schoffelen van het RIM netwerk zou een goede stap zijn in een cyberaanval, waarbij laagje voor laagje het weerstandsvermogen van een land afgebroken wordt. Misschien is het een idee om bij een rampenoefening een dergelijk scenario eens uit te proberen. Niet dat zo´n aanval eenvoudig zal zijn - RIM neemt de zaken vast wel serieus - maar de les van alle andere complexe en samengestelde systemen is, dat er altijd een aanval mogelijk is. Dus Blackberry: een leuk statusverhogend gadget, waar voor echt serieus gebruik een goed alternatief achter de hand gehouden moet worden.

Certificeringen

maandag 23 juni 2008

We zijn CISSP of A+, onze bedrijven zijn ISO27000 of SAS70 Type 2, onze software is Common Criteria of ICSA certified: certificering is verplicht in ons vak. Discussies over dit onderwerp gaan over de waarde en de beperkingen van specifieke papiertjes. Maar wat is het nut van certificering op zich? Dat is kennelijk een moeilijke vraag. Meestal krijg je als antwoord het soort argumenten als bij de Europese Grondwet: niemand kan je precies uitleggen waarom het goed is, maar als je het niet doet volgt armoe en uitsluiting. Dus ben ik GSEC, zijn mijn collega's CISSP en CISM, en kijken we neer op degenen die dat niet zijn. Onze organisatie is ISO en CMM, dus dat eisen we ook van onze leveranciers en partners. Als topwerkgever ben ik natúúrlijk CRF certified en mijn omgeving is zo belangrijk dat ik EAL4 als minimum stel. Bovendien ben ik lid van register zus en clubje zo met allerlei gedragscodes en goede gebruiken. Laat niemand beweren dat ik niets aan kwaliteit doe!

De discussie over de waarde van bepaalde certificaten heeft nogal een hoog 'wie heeft de grootste'-gehalte. We zouden bijna vergeten dat certificatie in de rest van de wereld veel minder gebruikelijk is. Niet IT-ers kijken verwonderd naar de alfabetsoep achter de naam op het visitekaartje en naar de rijen ingelijste partnerships en kwalititeitscertificaten in de hal van de IT-boer. Alsof je daarmee je geloofwaardigheid aantoont, zoals de krantenknipsels op het prikbord van de paragnost. Staat er op het kaartje van je tandarts dat ie gecertificeerd is voor een XE-Day draagbare boor? Hangt er bij de topkok een reeks certificaten van Sabatier als bewijs dat ie weet hoe hij zijn messen op orde moet houden? Is de verloskundige Gold Business Partner van de Beter Baby? Nee dus. Maar wij weten kennelijk van geen ophouden.

Onzekerheid, angst en gezichtsverlies

Wat willen we toch bewijzen met al onze labels en keurmerken? In mijn ervaring tonen zij vooral onze onzekerheid, en onze angst voor gezichtsverlies. Maar waar komt die onzekerheid dan vandaan?

Er zijn wel vergelijkbare bedrijfstakken. Neem de wereld van de garages. De BOVAG doet met zijn keurmerk al jaren zijn best om de sector uit de kwalijke reuk van beunhazerij te krijgen. Het werkt niet altijd; zo bleek toen ik laatst met mijn leasebak voor de eerste APK opging. Het reservewiel was stiekem vervangen door een afgereden exemplaar met een kromme velg. De auto is alleen onderhouden bij merkdealers die lid zijn van de BOVAG. Welke dealer het wiel gestolen heeft, is na drie jaar niet meer vast te stellen; ik controleer niet na elke beurt of alles nog in de auto ligt. (Dus ik bel de BOVAG niet, hoewel de organisatie dat echt wel wil. Waarom zou ik, het leasebedrijf draait voor de schade op. Of de verzekering. Of mijn baas. Maar ik niet. En intussen zeur ik op ieder feestje en bedrijfsuitje over dat stelletje oplichters bij de garage.)

Feit is dat de BOVAG in haar 78-jarig bestaan de verhalen over louche garages er niet veel minder op heeft weten te maken. De BOVAG is als brancheorganisatie breder dan garages alleen, maar heeft geen kwaliteitskeurmerk voor tankstations. Bij de pomp merk je het best snel als iemand de boel loopt te flessen. Bij garagebedrijven komen kwalitatieve manco's of andere wanprestaties pas laat aan het licht. Maar voor de klant is het ondoenlijk om na ieder garagebezoek de hele auto na te lopen. En dus loopt de hele bedrijfstak imagoschade op als één van de bedrijven een grove fout maakt. De strijd van de BOVAG tegen het negatieve imago is dan ook niet te winnen: er komt echt geen moment dat iedereen denkt dat het garagebedrijf een structureel schone bedrijfstak is.

De bouw heeft ook zo'n imago van onbetrouwbaarheid, verkapte criminaliteit en amateurisme. Toen ik een grote verbouwing aan mijn huis voorbereidde werd ik overstelpt met goede raad hoe om te gaan met de aannemers, waarbij altijd de ondertoon was dat alle aannemers boeven waren. Als je kijkt naar de bouwfraude zie je dat het imago van de bedrijfstak volkomen ruk is. Toch kent de bouwwereld geen keurmerken met de bekendheid van BOVAG. Het verschil is natuurlijk dat je veel vaker bij een garage komt dan dat je een aannemer over de vloer hebt. En dat je van garage nog makkelijk kunt wisselen, iets wat je met een aannemer tijdens een klus niet moet doen, tenzij je graag nóg langer zonder keuken zit, of zonder dak. Garagebedrijven zijn dus kwetsbaarder dan aannemers. Daarom voelen garages een grotere noodzaak om aan hun imago te werken.

Ons vak lijkt meer op de garages dan op de aannemers. Gebreken in ons werk komen ook vaak pas laat aan het licht. Klanten kunnen onze kwaliteit – of het gebrek eraan – niet zo snel zien. Wij voeren veel kleinere werkzaamheden uit en klanten kunnen zo overstappen naar een concurrent. Dat maakt ons net zo kwetsbaar als een garage, en stelt ons voor dezelfde uitdaging: het aantonen van onze kwaliteit. Maar er zijn ook grote verschillen. Bij de BOVAG kun je klagen over het werk van haar leden. Kun jij bij ISC2 klagen over het werk van een individuele CISSP? Of bij de Norea over een auditor? Of bij de CRF over de 'top ICT werkgever'? Volgens mij niet. In elk geval lopen de organisaties achter de labels er niet mee te koop. Maar stel dat het wel kan, wat zouden ze dan moeten doen bij een klacht? Mensen of bedrijven schrappen als lid heeft weinig zin: dan halen ze gewoon het vergelijkbare certificaat van de concurrent. Dus als kwaliteitslabel zijn zelf ook niet voor hun taak geschikt.

Nog een verschil: waar de garagebranche één label heeft, hebben wij er honderden. Waarom eigenlijk? Komt dat alleen omdat alle predicaten onvolwassen en niet op hun taak berekend zijn? Lijkt mij niet logisch, met zoveel labels zitten er vast wel een paar goede tussen. Ik zie het meer als onze eigen onzekerheid. Gaat er iets mis, dan willen we graag kunnen zeggen dat onze voorgangers er een potje van hebben gemaakt. Dat we veel beter zijn dan onze concurrent, en ook beter dan onze jongere collega's die voor lagere tarieven werken. Dat de mensen die Algol, SNA en kloppen in C niet mee hebben gemaakt er nooit iets van zullen bakken. Dat ons bedrijf beter is óók. Terwijl we eigenlijk onszelf niet goed genoeg vinden. We hobbelen maar voort, van het ene mislukte project naar de andere halve implementatie. Dat knaagt toch vroeg of laat, ergens diep van binnen. Het is dezelfde existentiële onzekerheid die ons gedram over best practices en proven technology veroorzaakt.

Onze verslaving aan certificaten wordt versterkt door het grote verloop in bedrijven en medewerkers. Hoe lang bestaat een IT-bedrijf gemiddeld? Hoeveel nieuwe banen, schaalvergrotingen, reorganisaties en fusies maak je mee in een gemiddelde carrière? In al die situaties moet je als ICT-er je waarde binnen enkele seconden administratief kunnen aantonen. En net als een garagebedrijf kunnen we dat niet. Dan is alles meegenomen, al is het maar een lullig certificaatje waar we feitelijk geen waarde aan hechten.

Security is nog erger dan de ICT in het algemeen. De onzekerheid over ons eigen kunnen is dan ook groter: de meeste mensen lopen hooguit een jaar of drie, vier mee, de meeste bedrijven niet meer dan zeven. Het zijn juist de jonge, intelligente mensen die doorhebben dat ze met grote belangen aan het spelen zijn. Voor veel geld. Die dan ook van alle kanten onzeker zijn: ben ik mijn geld wel waard? Hoe overtuig ik mensen die al twintig jaar meedraaien van mijn gelijk? En wat blijkt dan: we overtuigen de anderen helemaal niet. We zijn namelijk van onszelf ook niet overtuigd.

Deze onzekerheden duwen ons steeds verder de mallemolen van certificering in, nog verder aangejaagd door een veelheid van leerinstellingen en andere overheadachtige bedrijfjes die hiervan leven. Tel eens na hoeveel mensen er nodig zijn om één Security specialist aan het werk

te krijgen; delivery manager, contract manager, mantelcontract manager, PZ, tussenhandel, brancheorganisatie, opleiders en maak de lijst maar af. Want daar komt het uiteindelijk op neer: de marges in de Security zijn zodanig dat het zeer lonend is een probleem op te blazen als je leeft van het oplossen ervan. Dat hebben de opleiders goed van de IT afgekeken.

Nu ik het er toch over heb, ik ben ook te huur als trainer. Ik moet alleen nog even een mooi klinkende afkorting voor een certificaat verzinnen en een register oprichten. Wat denken jullie van RSA, Register Security Analyst? Of moet er toch een C in?

Outsourcing: Horen, Zien, Zwijgen?

dinsdag 8 juli 2008

Met de volgende economische dip aanstaande en de voortgaande slag om het talent, zullen nog meer grote organisaties hun systemen en hun data uitbesteden. Uitbesteding wordt op enig moment offshoring: met de consolidatie onder de aanbieders en de bijbehorende bedragen is een leverancier die zegt vanuit Nederland te blijven werken een illusie. Het moment nadert – of is al daar – dat echt kritieke systemen voor economische en politieke veiligheid ons land zullen verlaten. En daarmee krijgt informatiebeveiliging een paar extra dimensies.

Data in een ander land is onderhavig aan lokale wetgeving: als je je bedrijfsgegevens op Google Docs neerzet, mag de Amerikaanse justitie dit inzien en mag dezelfde Amerikaanse justitie tevens opleggen dat Google je dit niet vertelt. Dit geldt in diverse gradaties bij alle vormen en plekken van uitbesteding. Je bedrijfsgegevens bevatten niet alleen puur interne spullen, maar ook gevoelig materiaal over je leveranciers en partners: offertes, afspraken en financiële transacties. Daar kunnen ze ook voor langskomen, dus ook als je niets verkeerd doet kun je ermee te maken krijgen. Als justitie bij je inhouse rekencentrum aanklopt, hoor je dat vanzelf – als je het uitbesteed hebt hoor je het níet.

Als de beheerder van je systemen overzee toegang verstrekt aan derden, moet hij daartoe de mogelijkheden hebben. Beheerdersrechten (vaak gewoon root) geven feitelijk toegang tot alle informatie op de systemen. En de lokale beheerder zal echt niet de lokale wet breken om je te beschermen. De aanbieder van outsourcing loopt het risico dat hij de klant schade toe moet brengen. Dat gaat hij niet aan de grote klok hangen. Als hij verstandig is, neemt hij intussen alle maatregelen die mogelijk zijn.

Je kunt bijvoorbeeld zeggen: we nemen alleen gescreende beheerders in dienst. Maar welke garanties geeft dat eigenlijk? Feitelijk is screening dan de énige beveiliging tegen een gerichte actie. En wat zegt gescreend in de praktijk? Dat iemand de wet naleeft en geen foute vrienden heeft. Dus gehoor geeft aan de lokale opsporingsambtenaar die inzage in een systeem eist. Zeker als die ambtenaar een negatieve aantekening in een dossier kan zetten waardoor de beheerder z'n screening en daarmee z'n bron van inkomsten kwijtraakt. Dan zal deze de formulieren van die ambtenaar niet al te kritisch lezen. Niet alle ambtenaren in alle lage lonen landen zijn zuiver op de graat. Zo kan screening het tegenovergestelde bereiken van wat de bedoeling is.

Andersom is het al niet veel beter: een beheerder in een ver warm land die de data hergebruikt of vernielt, is juridisch erg moeilijk aan te pakken. Het hemd is altijd nog nader dan de rok, dus de lokale opsporingsambtenaar en zijn organisatie zullen daar nog minder aandacht aan besteden dan hier. India zit niet te wachten op berichten dat de informatie daar onveilig is, dus reken op politieke druk. Wat een vervelende bijkomstigheid is dat je als klant de beheerder geen computervredebreuk kunt aanwrijven – omdat hij de toegang al had - dus juridisch sta je ook nog heel zwak.

Veel inlichtingendiensten beschouwen het als hun taak de economische groei van hun land veilig te stellen, zoals we vorige week nog konden horen van de Britten die Liberty aftapten[4]. Verder in het verleden hebben iets vergelijkbaars mogen meemaken met de Amerikanen die Boeing 'hielpen'. Hiermee stellen de diensten dat ze zich bevoegd achten om bedrijfsspionage en misschien zelfs bedrijfssabotage toe te passen. Met het samenklonteren van de

[4] http://www.security.nl/article/19024/1/Britse_overheid_krijgt_boete_wegens_schenden_privacy.html

informatievoorzieningen van grote bedrijven in outsourcingscentra wordt dit een stuk eenvoudiger; het inbreken in vijf omgevingen is nu eenmaal simpeler dan in vijfduizend. Zeker als die vijf bij elkaar in de buurt staan, misschien wel in je eigen land. Dat het eenvoudiger is geldt overigens ook het opblazen ervan, in een low-intensity Cyberwar scenario.

De hamvraag is of je als leverancier van outsourcing de beveiligingsrisico's van de klant moet dragen. En dan ook die van de ene klant voor de andere? Hoe kun je je verweren? De risico's zijn fiks – spionage maar ook sabotage: stel je klant publiceert cartoons met de Profeet in een van haar dagbladen en intussen verhuis je de data van je rekencentrum in Delhi naar het nieuwe rekencentrum in Jakarta. Jij houdt heus niet bij wat al je klanten zoal doen, maar de moslimbroederschap wél! De klanten zadelen je op met een extreem moeilijk kwantificeerbaar risico: je weet immers niet op welke lange tenen ze kunnen gaan staan. Dat een onderdeel van een klant werkzaamheden verricht voor de JSF zullen ze je ook niet vertellen, en al helemaal niet dat ze die informatie neerzetten op het netwerk dat jij beheert: ze overtreden immers zélf de formele regels. Je gaat omgevingen beveiligen zonder zicht op de waarde van de informatie; een garantie voor niet-passende maatregelen.

Het is dan ook zeer interessant als aanbieder om deze gevaren af te sluiten. Als je systemen beheert maar géén toegang tot de informatie erop hebt, of die alleen hebt op een manier dat de eigenaar het merkt, kun je niet in deze onmogelijke positie gebracht worden. Nu zullen niet alle activistische groeperingen deze nuance zien, maar toch. Dit gaat helaas niet zo gemakkelijk met bestaande middelen. Het is een verworven recht van een beheerder om alle rechten op systemen te hebben, hij dreigt gewoon de manager dat hij anders niet kunt garanderen de problemen op te kunnen lossen. Druk op de management-paniekknop, en voilá.

Zorgen dat beheerders geen toegang hebben tot applicaties en informatie van klanten doe je normaliter met het minimaliseren van rechten. Het is een grote inspanning om het te regelen en de techneuten zullen het als omslachtig ervaren en dat zul je horen ook. Least privilege stelt in een niet-gehardende omgeving in de regel bovendien ook niets voor: een beheerder kan op tig manieren meer rechten krijgen. Hernoem cmd.exe naar de screensaver, doe een "net user administrator " en zet je favoriete wachtwoord. Of zoiets. Dat zijn de eerste trucjes die je als beheerder wilt weten. Er bestaan steviger platformen, maar algemeen geldt dat besturingssystemen niet gebouwd zijn om lokale aanvallen van geautoriseerde beheerders te weerstaan. Dus je techneuten lastig vallen met 'beperkingen' die geen enkele serieuze aanval overleven is weggegooid geld. Je moet wat beters verzinnen.

Als aanbieder zul je verregaande eisen moeten stellen aan de systemen die je beheert – en dus aan de budgetten van je klanten die bij je komen om hun kosten te drukken. Je kunt deze vraagstukken niet oplossen in je eigen systemen: daar staat de informatie niet. Bovendien zijn de extra beveiligingskosten in dat geval helemaal voor jou. Daarbij wil de klant om de paar jaar een andere leverancier kunnen kiezen, dus je kunt geen al te complexe eisen stellen. Als het een beetje meezit heb je bovendien meer dan één klant, dus je moet je ook druk maken over de scheidingen onderling. Daarbij heb je elke paar weken een nieuwe beheerder, en na enige tijd verplaats je de boel ook nog naar een ander land met een ander rechtsstelsel en lagere loonkosten. Dat levert geen eenvoudige set funcspecs op, al met al.

- Harde scheiding tussen beheerders en informatie. Gegeven de rechten van beheerders zal dat op de meeste platformen een 'uitdaging' vormen. In principe kom je uit op eisen die het meest lijken op wat militaire automatisering onder MLS-capable verstaat. (MLS staat voor Multi-level Security). Een goede start is besturingssystemen met EAL5 of meer te nemen: een Linux, BSD of Solaris met trusted extensies. Of XTS-400 met STOP, maar die

beheerders zijn weer zo schaars. Bovendien is het lastig als de klant tóch vasthoudt aan Exchange en Sharepoint.
- Beveiliging niet alleen op de netwerklaag, maar ook in de informatie en de transacties. Daar komt een heleboel crypto bij kijken. Met de gangbare producten kom je er niet.
- Volledig gecentraliseerd beheer van rechten en accounts. Zeg maar dag tegen oncontroleerbare 'functionele' en decentrale accounts. Gegeven dat de klant ook accounts op die systemen zal willen hebben (misschien zelfs voor bepaalde beheertaken, al dan niet uit te voeren door concurrenten) is dit een zeer grote en complexe operatie.
- Zonering van het netwerk waarbij beheer volledig out-of-band is. Daarmee voorkom je dat klantomgevingen elkaar beïnvloeden via je beheervoorziening. Dit legt weer een extra druk op het systeem voor gecentraliseerd beheer van rechten en accounts; de huidige generatie IDM systemen is niet ontworpen om over meerdere gescheiden omgevingen te werken. De beheersystemen moeten zo gebouwd zijn dat er via een ander kanaal toegang is als het OS door z'n hoeven gaat. Gegeven de mogelijkheden van virtualisatie of de management console van je bladeomgeving is dat te doen.
- Dynamische toegang. Enveloppenprocedures moet je afschaffen, ze kunnen echt niet meer. Dit traditionele gat in de beveiliging wordt altijd in stand gehouden met de argumentatie dat de beheerder in extreme noodgevallen met alle rechten moet kunnen aanloggen. Leuk argument tegen angstige managers, maar achterhaald. Zeker als de server 3000 kilometer verderop staat. Dynamische toegang kan als er een noodsituatie optreedt met een koppeling van een identity management systeem aan het helpdesksysteem. Als er een incident is geeft dat toegang via de out-of-band voorziening, met een eenmalig wachtwoord - en als het ticket sluit is die autorisatie weer weg. Dit mechanisme moet je ook inzetten om ongeautoriseerde changes tegen te gaan: geen change request, geen toegang.

Met het stellen van dergelijke eisen – er zijn er nog meer – zul je in je eigen vlees snijden: de concurrent die de kop in het zand steekt is ongetwijfeld goedkoper. MLS-capability is notoir duur, dus onveiligheid loont. Het is geen zekerheid dat je rampenscenario ook daadwerkelijk plaatsvindt, dus beveiliging is een twijfelachtige investering. Bedenk echter dat je, als je voor één klant een risico accepteert, je dat automatisch ook doet voor al je andere klanten. Als je dat vertelt aan die andere klanten, zullen ze wel twee keer nadenken voor ze het contract verlengen. Leg dát maar eens uit aan je aandeelhouders.

De nachtmerrie van security managers

maandag 28 juli 2008

Het is de nachtmerrie van iedere security manager: een norse, mottige beveiligingsspecialist geeft een directielid de wind van voren. In onbegrijpelijk jargon snauwt hij dat beveiligingsregels overtreden zijn, dat het echt niet zo kan en dat het oerstom is. Dan weet je wat er volgt: van ergens bovenaan wordt de security manager toegesproken over de specialist die ver buiten zijn boekje is gegaan. Oepsie!

De security manager, al dan niet CISO of CSO, is op bestuurlijk niveau erg kwetsbaar. Hij is de man van het slechte nieuws – dit mag niet, dat is fout gegaan, dit moet anders. Hij is nooit populair. De norse verongelijkte specialist maakt zijn positie er niet beter op. Zijn carrièrepad leidt dan ook meestal niet naar boven maar de deur uit. Security manager is een eindfunctie, je zit de tijd uit tot je pensioen.

Ben je security manager en niet suïcidaal, dan instrueer je je specialisten om belangrijke gebruikers nooit meer toe te spreken. Dat vinden ze jammer, want preken tegen overtreders is heel lekker, vooral als de overtreder flink hoog in de boom zit. Maar ze luisteren wel naar je, en klagen onderling gewoon iets harder over stupide gebruikers en het incompetente management. Dat schept dan weer een band in het team, dus dat is goed. Een ander gevolg van het verbod is dat uitsluitend overtreders op lagere posities op hun gedrag aangesproken worden. En na een tijdje niemand meer.

Wie spreekt de gebruikers dan wel aan? Beveiligingsbureaus en CERT's delegeren deze hete aardappel naar het reguliere management, dat er evenmin zin in heeft. Of het wordt alleen op papier gedelegeerd: de mensen die je verantwoordelijk maakt weten het niet. Je gooit het over een muur waar niemand achter staat. Een creatievere oplossing: delegeer het naar HR of de afdeling communicatie - omdat het gaat over interne medewerkers. Waar het op neer komt is dat deze politionele taak vrijwel nergens goed wordt uitgevoerd. Het gevolg laat zich raden: een reeks ongelukkige beveiligingsincidenten waartegen niet adequaat opgetreden is, waarna de security manager op straat geknikkerd wordt.

De security manager kan proberen te vluchten in het bedenken van beleid. Hij trekt een rookgordijn op van ondoorgrondelijke bureaucratie en holt wat achter virussen aan. Maar feitelijk laat hij de situatie op z'n beloop. Dat is geen ramp als je organisatie de marktleider onder de mottenballengroothandels in Stroe is. Maar voor serieuze organisaties is het dansen op de vulkaan.

Wat kan de security manager wél doen? Nou, zelf weggaan en ergens senior security consultant worden bijvoorbeeld. Het betaalt beter en adviseren is risicoloos. Je moet alleen wél de files voor lief nemen. En het is jammer voor het bedrijf dat je verlaat.

Maar ja, weggaan kan altijd nog. Er zijn meer opties. Het gaat in dit probleem vooral om imago en communicatie. Les 1: zorg dat je af en toe goed nieuws hebt. Dat klinkt eenvoudiger dan het is. Koffiemokken uitdelen ís geen goed nieuws. Spreken op een congres ook niet. Je kunt ook niet succesvol systemen bouwen, want die moet je dan weer controleren. Bovendien zal ICT je van broodroof beschuldigen. Overtreders pakken en aan de schandpaal nagelen kan ook al niet, want daartoe heb je geen mandaat. Melden dat je een viruscrisis hebt overwonnen: ja, dat is goed nieuws. Maar doe het niet te vaak, dan wek je de indruk dat je de boel eigenlijk niet onder controle hebt. Uitleggen dat ICT de technische keuzes maakt en dat je alleen maar achteraf kunt

signaleren is ook verkeerd, dan veeg je je eigen straatje schoon. Het gaat niet om gelijk hebben. En ook niet om gelijk krijgen. Het gaat helemáál niet om gelijk. Het gaat om geluk.

Kortom, je hebt vrijwel alleen maar slecht nieuws. Les 2: breng het anders. Laat met rapportages en post-mortems zien dat je van je fouten leert, goede afspraken maakt, goed samenwerkt en je processen onder controle hebt. Wijs iemand in het team aan als beveiligingsvoorlichter. Kies een gladde prater en goede schrijver die slim en technisch genoeg is om de boodschap te vertalen zonder hem te verminken. Hij is je filter. Laat alle externe communicatie via dit filter lopen. Stuur alleen hem en niemand anders naar de probleemgevallen. Er zijn mensen die dit een leuke klus vinden en hem ook aankunnen. Crisiscommunicatie is een hooggewaardeerd beroep en bovendien een uiterst interessant carrièrepad.

Met een beveiligingsvoorlichter kun je de technisch specialisten in hun hok laten; dat vinden ze zelf ook veel fijner. Maak echter niet de fout één van de specialisten uit te roepen tot voorlichter. Hij kan het misschien wel, maar zal het niet willen. Een specialist beschouwt iedere baanverandering waardoor hij minder achter het scherm zit (e-mail, boekhouding en PowerPoint tellen niet mee) als een achteruitgang. Minder beeldscherm = meer vergaderen, en dat vraagt nu eenmaal een ander slag mensen. Voormalige journalisten, salesmensen en recruiters zijn een betere keuze. Zij zijn bovendien veel minder schaars dan kundige techneuten.

Communicatie, daar gaat het om. Beter en verstandiger communiceren is de belangrijkste vooruitgang die je als security manager kunt maken. Het is natuurlijk niet zo dat een beveiligingsvoorlichter in één keer alles oplost. Bij een grote crisis zullen je mensen zelf op pad moeten; bereid ze daarop voor. Maar de samenwerking met een voorlichter als lid van het team is al mooi. Een beetje communicatietraining sorteert al gauw meer effect dan nog maar weer eens een productcertificaat voor beveiliging. Let daarbij overigens niet op uiterlijk. Een slobbertrui beschermt tegen boze geesten en scheren is slecht voor je aura, schijnt. Laat het gaan. Presenteer het maar als excentriek of Esprit de Corps. Als duidelijk is dat de specialisten onmisbaar zijn en niet alleen om mensen lastig te vallen, dan wordt dat wel geaccepteerd. Niet van harte wellicht, maar toch.

Les 3: gebruik het mediamedicijn met mate. Een hype werkt tegen je: als je continu je eigen successen roeptoetert, graaf je voor jezelf een mooie kuil. Maar indien met mate gebruikt, kan een basale marketing- en communicatiestrategie je uit de negatieve spiraal helpen. Verrassend genoeg neemt de veiligheid dan ook toe. Hopelijk volgt er dan ook een intern carrièrepad voor de security manager. Want die files, die worden er niet minder op.

Zet RBAC bij het grof vuil

woensdag 27 augustus 2008

In de slag om compliance aan SOX en vergelijkbare 'hoge normen' stellen beveiligingsspecialisten RBAC voor als conditio sine qua non. Deze trend wint nog steeds terrein. Er zijn ook al consultants die RBAC-compliancy eisen van software zoals Active Directory of IDM, in het kader van SOX. RBAC-achtige features in allerlei software wordt ook verpakt in compliancy termen - sommige leveren 'GRC'-modules en sinds enige tijd is er zelfs 'Compliancy As A Service (CaaS). Dit is niet heel vreemd: RBAC is eind jaren tachtig bedacht om dit soort problemen op te lossen. Maar noch SOX noch PCI-DSS schrijven het voor; er wordt alleen een "adequate internal control" geëist, en vendors en consultants roepen in koor dat RBAC in allerlei subsmaken de enige manier is. Was dat maar waar. RBAC is een slecht plan en brengt je juist verder van adequate interne controls omdat het niet werkt.

Rollenexplosie
Het uitgangspunt bij RBAC is dat medewerkers die hetzelfde werk doen, dezelfde rechten en applicaties nodig hebben. RBAC wekt daarmee de schijn van efficiency en 'consolidatie', van rechtvaardigheid. Deze schoonheid trekt mensen met een ordelijke geest aan, waarvan er velen in de ICT werken. Maar wat is hetzelfde werk? Het idee dat verschillende mensen dezelfde rol hebben en dus gelijk zijn, is een misvatting. Een secretaresse heeft meestal rechten op de mailbox van de baas. Een programmeur heeft toegang tot de source code repository. Maar welke baas? Welke repository? Sommige bazen hebben meerdere secretaresses of delen secretaresses. En programmeurs hebben de hebbelijkheid niet altijd aan alle projecten te werken.

Medewerkers hebben altijd meer dan één rol. Sommige medewerkers hebben sóms maar één rol. Zelfs in de spreekwoordelijke koekjesfabriek hebben mensen meerdere petten - denk aan lijn en projectrollen, interimtaken en allerlei vormen van samenwerking en taakwaarneming. Bovendien zijn er ook autorisaties nodig voor eenmalige taken, zoals toegang tot een dataset voor het maken van jaarrekeningen of root toegang tot een systeem om een storing op te lossen.

Ieder RBAC project stuit dan ook op het feit dat er meer rollen dan gebruikers zijn. En dan gaan ze groepen samenstellen op grond waarvan mensen rechten krijgen. Iedereen krijgt alle rechten die een ander lid van het groepje nodig heeft. Je krijgt dus altijd meer rechten dan je nodig hebt. Dat draagt niet bij tot meer veiligheid, integendeel, want als iemand expliciet rechten krijgt dan is misbruik wel heel moeilijk aan te tonen. Op dit vraagstuk struikelen de meeste implementaties. Maar er is meer mis.

Autorisaties waarop?
In normale omgevingen zal RBAC alleen de toegang tot applicaties, devices en directories kunnen regelen. Dit zijn hooguit indirecte waarborgen van de veiligheid van de informatie; er is immers geen mechanisme dat afdwingt waar de informatie staat. Door deze beperkingen is RBAC een puur IT-feestje, waarbij je niet op medewerking van 'de business' of 'Corporate Security' hoeft te rekenen. Een goed werkende RBAC zou ervoor kunnen zorgen dat gebruikers sneller en met minder fouten toegang tot IT resources krijgen, maar dat heeft niets met compliancy (het voorkomen van misbruik immers) te maken.

Niet alles is rolgebonden
Het klassieke rollendenken kent twee variabelen, rollen (functies) en autorisaties. RBAC koppelt autorisaties alleen aan functies van personen. Beveiligingseisen zijn echter niet alleen afhankelijk van medewerkers. Sommige taken mogen niet op bepaalde systemen worden uitgevoerd, omdat

ze op minder veilige plaatsen staan. Denk daarbij aan balie PC's en thuiswerkplekken, maar ook aan meer en minder beveiligde zones en panden.

Op jacht naar de bron
RBAC vraagt aan een bronsysteem actuele attributen op grond waarvan rechten uitgedeeld kunnen worden. Het bronsysteem voor rollen is meestal de HR administratie. Daarin staat wel op welke afdeling iemand zit (of zat) en wat de functienaam van iemand is (of was). Maar je hebt veel meer input nodig als je niet met heel grove schetsen autorisaties wilt uitdelen, veel meer informatie dan HR heeft. Die moet je gaan bijhouden. Als je geen bron hebt, dan moet je alles handmatig gaan doen. Nu zijn er soms wel andere registers die de benodigde informatie bevatten. Maar om het urenschrijfsysteem, de prikklok en het helpdesksysteem te koppelen als bron voor deze onmisbare informatie, gaat nogal ver. Het zal slechts incidenteel kunnen, omdat vrijwel al deze registraties achteraf vastleggen, terwijl RBAC de informatie vooraf nodig heeft.

Datakwaliteit
RBAC en ieder ander geautomatiseerd autorisatiebeheer is 100% afhankelijk van triggers in bronsystemen. De datakwaliteit is kritiek, en hoe meer brongegevens je moet gebruiken, hoe meer data die nu nog informationeel is, kritiek wordt. Voor HR is het kamernummer een leuk extraatje, maar als je er provisioning aan koppelt moet het kloppen. En blijven kloppen.

Het gebruik van meerdere bronnen leidt tot interessante synchronisatievragen en arbitraire keuzes over welke gegevens wanneer leidend zijn. Als één systeem 90% goede data heeft, dan gaat 10% van de autorisaties fout. Met vijf bronsystemen met ieder 90% kwaliteit mag je blij als er wel eens een transactie lukt. Bedenk je dat als data op twee plekken staat in plaats van op een plek, iedere waarde in het eigen systeem kan kloppen maar dat ze ten opzichte van elkaar kunnen verschillen waarmee de datakwaliteit daalt. Hoge kwaliteit van data is fijn, maar zeker niet gratis.

Onderhoud
Naast bronnen voor triggers heb je voor alle geautomatiseerde provisioning business logica nodig: iedereen die op kamernummer A213 zit krijgt default printer B11787_VNS. Zit iemand in project HUPSA dan moet hij bij de projectenshare, op de testkamer V4_120 kunnen komen, rechten op bepaalde VPN's krijgen en een nieuwere versie van bepaalde software op de PC hebben. Echter, niet iedereen in het project heeft precies hetzelfde nodig. Stopt die persoon bij project HUPSA, dan moet hij nog twee maanden bij de data kunnen voor de nazorg maar niet meer bij de rest, terwijl andere mensen die stoppen met het project geen nazorgtaken hebben en dus ook niet onder de twee maanden regel vallen. Bij een gemiddeld project zijn deze zaken bovendien niet van te voren bekend, dus ze moeten snel.

Als je dit soort vragen projecteert op een organisatie met enige schaalgrootte, een paar projecten en een reorganisatietje hier en daar, dan weet je dat je dagelijks tientallen mutaties in de logica zult hebben. En dit zijn mutaties die in de regel in de applicatiecode zitten. Als dat zo is, heb je na iedere logicawijziging een nieuwe release van de Code. De Change Manager ziet je al aankomen; en met maar één change window per week kom je er in ieder geval niet.

RBAC 2.0?
Jean Pierre Vincent beschrijft in het blad Informatiebeveiliging een concept voor "**RBAC 2.0**" met een structuurwijziging (een extra abstractielaag), om niet persoonsgebonden rules te kunnen bevatten. Een prima idee, waarvoor de 'toolleveranciers' wel even hun systemen moeten aanpassen. Dat zal misschien gebeuren, maar het existentiële probleem van de beschikbaarheid van brongegevens en de realiteit van de almaar wijzigende logica wordt er niet door opgelost. Zij maken RBAC tot een monstrum van complexiteit. De implementatie- en de beheeruitdaging zal

navenant zijn, evenals de foutkans, dus het beweren dat de kosten zullen dalen en de veiligheid zal toenemen is erg optimistisch, ongeacht de wijzigingen in RBAC 2.0 of later.

De belangrijkste argumenten om RBAC in te voeren zijn vermindering van de kosten en het verhogen van de veiligheid. Veiliger en goedkoper, omdat het eenvoudiger zou worden. Welnu, in de zestienjarige geschiedenis van RBAC is aangetoond dat het niet in te voeren is. Mislukte projecten zijn per definitie duur. En het mislukken is echt niet omdat het niet serieus geprobeerd is, knappere koppen dan alle Security.nl lezers bij elkaar hebben de tanden erop stukgebeten. Stukjes van RBAC zie je soms wel, maar het grote geheel is nergens gelukt. Het is net zoiets als PKI en X.500 - er zitten bruikbare zaken in, maar het grote concept is te complex en te ambitieus. Onbruikbaar dus. Het is dan ook hoog tijd dat we met z'n allen afspreken nooit meer te zeggen dat RBAC een bruikbare oplossing is. Voor je het weet staat het daadwerkelijk in een bindende richtlijn. Dan moeten we het bouwen en dat heeft uiteindelijk maar één mogelijke uitkomst: een compleet fiasco. Daarmee verliezen we veel van de opgebouwde geloofwaardigheid die we als ICT Security zo moeizaam opgebouwd hebben.

Rijkspas: Het blijft tobben met die chipkaarten

woensdag 10 september 200

Het was groot nieuws, zes maanden geleden. De staatsveiligheid was in gevaar omdat de toegangspassen voor overheidsgebouwen waren gekraakt. De pasjes gebruiken de inmiddels beruchte Mifare Classic-chip, bekend van de OV-kaart. Op vrijdag 7 maart lichtten onderzoekers van de Radboud Universiteit in Nijmegen minister Ter Horst van Binnenlandse Zaken in. Ter Horst zond terstond een aantal AIVD'ers naar Nijmegen. De conclusie: twee miljoen toegangspassen moeten op korte termijn vervangen worden. Omdat voor elkaar te krijgen moet het project voor één pasje voor de overheid (minus de 400.000 passen van Defensie) versneld en gewijzigd worden. Dan is de staatsveiligheid weer gewaarborgd.

Stichting ICTU (onderdeel van het ministerie van Ter Horst) werkt aan dit project genaamd Rijkspas, dat naast toegangsbeveiliging voor panden van de rijksoverheid ook netwerktoegang en follow-me printing mogelijk moet maken. De minister heeft dit project gevraagd versneld op te leveren, met nog dit jaar de eerste uitrol. Vanaf nu zal het projectteam terzijde gestaan worden door de Digital Security groep van de Radboud universiteit, die roem vergaarde met het kraken van Mifare. Helaas moest er ook een aantal zaken veranderen aan de Rijkspas, waarbij in opdracht van de AIVD de nabijheidchip achterwege wordt gelaten. Deze Mifare-chip wordt nu geschrapt uit de Rijkspas. De vernieuwde nieuwe Rijkspas kan dus niet meer op afstand worden gelezen met speciale apparatuur. Een forse change op een project dat vlak voor de oplevering zit (voorzien voor Q4/2008) en dat nu van de minister nog sneller moet. Andere chips betekent andere lezers - dat gaat niet van de ene op de andere dag. Als je pech hebt moet je zelfs opnieuw aanbesteden. Voorlopig zullen de pasjes dus maar handmatig gecontroleerd worden, meldt het ministerie.

Nu was het probleem van de huidige pasjes niet acuut, omdat de onderzoekers van het Radboud de details niet bekend hadden gemaakt. De opheffing van het spreekverbod door de rechter vergroot echter de druk op het project Rijkspas.

Eerder berichtte RTL Nieuws dat door slordige beveiliging onbevoegden gemakkelijk de departementen binnenkwamen. Dat kwam doordat oud-medewerkers hun pasjes niet inleverden, wist plaatsvervangend secretaris-generaal van BZK, Philippe Raets. Als dat het probleem is, wel, daar helpt geen Mifare classic of andere cryptochip tegen. Dat heeft met de actualiteit van het bronsysteem te maken.

Voor een pasjessysteem is de cruciale vraag op basis van welke gegevens de kaarten worden uitgegeven en ingetrokken. ICTU heeft bij de Rijkspas voor de bestaande directory van rijksambtenaren gekozen - die onder Rijksweb zit, RYX. Vanuit ICTU gezien is RYX een valide keuze: het is het enige register van rijksambtenaren. Met de koppeling van de Rijkspas wordt afgedwongen dat RYX bijgewerkt wordt, op straffe van fysieke buitensluiting van de eigen medewerkers. Om over de inhuur maar te zwijgen. Helaas is RYX niet altijd het toonbeeld van actualiteit - het duurt even voor een ambtenaar opgenomen wordt dan wel afgevoerd. Het is heel knap dat het register nu nog maar drie dagen achterloopt, maar voor provisioning is dat véél te veel. RYX bevat bovendien onvoldoende informatie om de gevraagde beveiliging mogelijk te maken, en zal dus uitgebreid moeten worden. De uitbreiding van de hoeveelheid gegevens in het centrale register betekent per definitie een daling van de datakwaliteit. In rijksbrede projecten is de regie van een verandering nogal een uitdaging - om alleen al de 37 stuurgroepen op één lijn te krijgen is al nauwelijks haalbaar. En al lukt dat wel, dan helpt het nog niets als die stuurgroepen binnen hun eigen organisaties niet een absolute autoriteit hebben; ze zijn er om het project aan te sturen, niet om de eigen organisatie - die vaak een wolk van instellingen, stichtingen en organen

omvat - te sturen. De eerste directeur van de ICTU noemde RYX al de "nagel aan zijn doodskist". Welnu, dat zullen er meer gaan zeggen.

Minister Ter Horst maakte tevens bekend dat de AIVD (op eigen verzoek) een centrale rol gaat spelen bij de beveiliging van ministeries en aanpalende organen, dus dan zal de datakwaliteit in het bronsysteem door de AIVD beheerd moeten worden. Hopelijk bestaat de werkvoorraad van jaren die ze nog niet zo lang geleden hadden met het uitvoeren van screenings, niet meer: het beheren van honderdduizenden personele en organieke mutaties per maand is even wat anders dan een paar honderd screenings. Het is best knullig als elke dag honderden ambtenaren hun gebouw niet binnen mogen en triestig op de stoep tussen de rokers moeten blijven staan omdat de mutaties niet tijdig zijn doorgegeven of verkeerd zijn ingevoerd. ICTU kon als ICT-club niet veel veranderen aan de processen bij de diverse rijksorganen, misschien dat de AIVD meer indruk maakt.

IJdele hoop: de AIVD heeft aangegeven de centrale rol te zien in een adviserende hoedanigheid. Dus gaan ze adviseren over de gewenste datakwaliteit. Wat daar nu centraal aan is? Misschien dat de rokende ambtenaren maar een andere plek voor hun persoonlijke behoeften moeten vinden, want voorlopig zal het wel vol zijn op de stoep.

De koppeling naar RYX is alleen nog maar de bron voor het pasjessysteem. De integratie met de verschillende netwerken om authenticatie op de werkplek en op de printer mogelijk te maken zal ook niet vanzelf gaan. Daar kun je wel tegen wat vragen oplopen: ga je in de huidige LAN omgeving een dergelijke grote wijziging aanbrengen? Vast niet. Dus dat zal in de opvolger van de huidige, op XP gebaseerde overheidsstandaard desktops meegenomen worden. Die opvolgers zijn over het algemeen niet zo ver gevorderd - de migratie naar XP is immers nog niet zo lang geleden afgerond. Het zal eerder 2013 zijn dan 2010 vóór Vista op de desktop te vinden zal zijn. Daarmee zullen de beloofde beveiligingsfuncties in het LAN evenzeer mee opschuiven de toekomst in.

Nu kun je dit scope-technisch oplossen door te stellen dat de Rijkspas deel uitmaakt van de nieuwe rijkswerkplek, het roemruchte project GOUD. Maar dat traject loopt ook bepaald niet zonder hobbels: de aanbesteding was een behoorlijke afgang waarbij drie van de vijf uitgenodigde partijen afzagen van een bod omdat ze het project kansloos achtten. Dat was voor Minister Bos echter geen reden het project te herzien. Gegeven dat GOUD versie 1.0 feitelijk neerkomt op Vista, Office 2007 en een tekenpakket voor SVG (weet iemand nog wat dat is?) met een 2003 back-end voor 15.000 werkplekken bij vijf departementen, blijft er nog een enorm stuk rijksoverheid over zonder de toegezegde veiligheid. Die toch ook nog een keer zal moeten. Tegen die tijd is de storm over de Mifare chip hopelijk al lang gaan liggen.

De minister van Binnenlandse Zaken heeft een boel dingen beloofd en de suggestie gewekt dat dit najaar de staatsveiligheid hersteld wordt. Dat gaat dus never nooit niet lukken. Waar het op neer gaat komen is dat er een pas komt die in theorie gebruikt kan worden voor allerlei beveiliging, maar de komende tijd zelden ergens voor gebruikt wordt. Dit is de traditionele begripsverwarring tussen ICT en de normale wereld; voor ons is een probleem opgelost als er ergens een werkend systeem staat, voor de rest van de wereld is het probleem opgelost als dat systeem overal staat en dan nog steeds werkt.

Minister Ter Horst is ongetwijfeld te goeder trouw, maar het lijkt erop dat het rapport van de rekenkamer over falende ICT projecten bij de overheid niet goed tot haar doorgedrongen is. We zien hier weer torenhoge ambities en bestuurlijke spierballentaal waar iedereen die een beetje logisch nadenkt van weet dat ze niet realistisch zijn: een multifunctioneel Rijkspas-systeem is pas af als alle verschillende stukken op hun plaats zijn, niet als het project de basisvoorziening

oplevert. Uitrollen, reorganiseren en integreren duurt veel langer dan het stukje techniek in elkaar schroeven wat ICTU doet. De hele operatie zal gezien de architectuur in het beste geval tot 2015 duren. 2022 is realistischer. Tegen die tijd is de basisvoorziening die nu in opbouw is, zwaar verouderd, zodat het op de meeste plaatsen niet werkt en bovendien niet meer veilig is. Dit kunnen we nalezen in het rekenkamerrapport dat vlak voor het zomerreces, in juni 2018, verschijnt. Hopelijk hebben we dan samen met de Belgen het WK-voetbal hier te lande, zodat het rapport helemaal geen aandacht krijgt.

Exit – en dan?

woensdag 8 oktober 2008

Vertrekkende medewerkers zijn een zaak voor HR. Maar zij vormen ook een bedreiging van de veiligheid van de organisatie. De maatregelen die getroffen worden benadrukken daarbij de informatie die verloren gaat of op ongewenste plaatsen terechtkomt. Het is dan ook logisch dat dit onderwerp bij informatiebeveiliging getrokken wordt. We hebben de acties rond uit dienst gaan (deprovisioning van toegang) immers al.

Er is een aantal bedreigingen om te overwegen:

Ten eerste heeft de organisatie (dat heb je nu eenmaal met kenniswerkers) geïnvesteerd in de medewerker – en die investering wil je beschermen. Liefst door de medewerker gewoon binnen te houden natuurlijk.

Ten tweede verzamelen medewerkers in de loop van de tijd een hoop digitale informatie thuis – zeker als ze wel eens thuis werken hebben ze na verloop van tijd eerdere versies van zo'n beetje ieder document waar ze mee te maken hebben gehad. Dit risico kan aardig oplopen – en komt juist voor in informatie-intensieve beroepen.

Ten derde kan de vervanging van medewerkers met een spilfunctie de productiviteit en de continuïteit benadelen. Als die 3e lijner die alle moeilijke zaken oplost ermee ophoudt, wel, dan kan het even duren voor je je service levels weer haalt. Hetzelfde geldt voor die boekhouder die door de cijfers heen kan kijken en in alle crisissituaties onmisbaar blijkt. (Het is logisch dat de buitenwereld deze mensen het liefst bij je wegkaapt. Dat doe je zelf ook.)

De laatste is dat medewerkers beschikken over interne kennis van de organisatie, de sterktes en de zwaktes, de klanten, de plannen en de lijken in de kast. Zo lang zij in dienst zijn, is dit zinvolle kennis, en kunnen zij niet zonder. Echter, na uitdiensttreding zou je deze informatie het liefst willen wissen uit hun brein. Dat gaat niet zonder al te drastische stappen. Toch zul je je goed moeten realiseren dat deze informatie (zolang het nog actueel is, en dat kan best wel lang zijn) buiten je beveiligingsbereik is. Zo lang een medewerker in dienst is, beschermt de medewerker zichzelf door echt gevoelige zaken niet aan de grote klok te hangen. Bij uit dienst is het maar afwachten. Dit is informatiebeveiliging pur sang.

Wil je goed omgaan met exits van medewerkers, dan houd je rekening met alle vier de bedreigingen. Dat is niet makkelijk. Omdat het onderwerp ook nog eens zweeft tussen HR, ICT en de business zijn de resultaten meestal niet om over naar huis te schrijven. De aanpak verschilt ook nogal per organisatie.

Amortisatie
Voor het terughalen van investeringen in medewerkers zijn amortisaties bedacht. Amortisaties

kunnen overgenomen worden door een nieuwe werkgever. Amortisaties dekken echter alleen de zichtbare – en recente - kosten (van trainingen waar facturen van zijn); als iemand een tijdje meeloopt bij een toko is er feitelijk veel meer geïnvesteerd. Denk ook aan de projectmanager die een megaproject in de soep heeft laten lopen – die heeft veel geleerd. Maar goed, amortisatie is beter dan niets.

Zwervende informatie
Voor de thuis verzamelde digitale informatie liggen technische oplossingen binnen bereik, met WRM-achtige middelen. Het inleveren van toegang tot informatie is immers gewoon een variant van deprovisioning binnen het mobiele domein – dus ook als die informatie bij de medewerker thuis is. Tot we dat echt invoeren hebben we een procedure waarin staat dat iemand die uit dienst gaat 'alle informatie' van het bedrijf dient te verwijderen van 'alle datadragers'. Wat alleen niemand doet, hetgeen blijkbaar zelden tot problemen leidt.

Spilfuncties
Bij medewerkers op spilfuncties die weggaan, gaat het om het verlies van strategische en tactische kennis. Om dat op te lossen is per geval een nadere analyse nodig. Een paar weken inplannen voor 'kennisoverdacht' boekt in elk geval zelden het gewenste resultaat. Iemand die uit dienst gaat 'alles' te laten opschrijven wat ie weet, ook niet: niet iedereen kan alles wat ie weet in een planbare tijd opschrijven, en bij mensen die in een week alles wat ze weten kunnen opschrijven, moet je blij zijn dat ze weg gaan.

Bij medewerkers op spilfuncties hoor je vaak over het gevaar van "IT helden" die als enige iets kunnen, met daarbij de waarschuwing dat je dat dus nooit moet laten gebeuren. Maar deze IT helden beschikken meestal niet over kennis die ze anderen onthouden (dat is meer iets voor het middenmanagement), zij kunnen gewoon goed kennis opbouwen op basis van informatie. En dat is een vaardigheid, die los staat van de specifieke informatie.

Wie toch bang is om afhankelijk te worden van IT helden, kiest er nogal eens voor om alleen mensen aan te nemen die de procedures naar de letter volgen, omdat ze nu eenmaal niet beter kunnen. Dan stel je dus eigenlijk een maximum aan vaardigheden in. Dat is niet alleen dom, het is suïcidaal voor je organisatie. Daarbij moet je continu mensen inhuren met kennis die je zelf niet in huis hebt – ook niet handig. Het is het bekende verhaal van pay peanuts, get monkeys. Met goeie mensen op spilfuncties moet je gewoon blij zijn, en je moet ze goed behandelen. Gaan ze weg, probeer dan even goede mensen te vinden.

Wat je vanuit informatiebeveiliging moet zeker stellen is een goede overdracht van lopende zaken; een exitgesprekje met 'Security' in goede sfeer waarin een vertrekker zijn losse eindjes kan uitleggen is zó geregeld. Als je toch bezig bent, richt dat dan ook in voor vertrekkende inhuur; kennis die je vrijwel cadeau kan krijgen verlaat de organisatie en het verwerven ervan kost bijna niets.

Non-concurrentie bedingen
Wat kun je nog meer doen? De meeste organisaties nemen een non-concurrentie beding op in hun contracten. Formeel beoogt zo'n beding het intellectuele eigendom van het bedrijf te beschermen. De kennis die een ex-medewerker heeft wordt bestempeld tot bedrijfseigen informatie, die niet mag worden ingezet voor de concurrent in de volgende baan van de ex-medewerker. De bescherming van bedrijfseigen informatie ligt in dit scenario blijkbaar bij HR.

Als medewerkers toegang hebben tot gevoelige informatie, dan moet die informatie afgeschermd worden. Iedereen die erbij kan moet zich aan dezelfde regels houden. Inhuur valt echter niet onder een dergelijk beding. Het hogere management trouwens ook niet. De informatie is

bovendien niet als zodanig geclassificeerd of aangemeld bij Informatiebeveiliging. Blijkbaar is zo evident welke informatie het betreft, dat nadere specificatie niet nodig is.

De wetgever heeft als poldercompromis een maximale duur van een half jaar aan non-concurrentiebedingen gehangen. Voor slechts weinig beroepen geldt dat na zes maanden de organisatie zo veranderd is, dat het niet uitmaakt dat iemand inmiddels voor de concurrentie werkt. Deze zes maanden termijn is even zinloos als het middel zelf.

Als je toch bij 'de concurrent' gaat werken kan je oude baas het boetebedrag opeisen. Bij dergelijke conflicten weegt de rechter het aanmerkelijke belang en stelt eigenlijk altijd vast dat een werknemer die niet kan eten meer schade oploopt dan een bedrijf dat een gehoopt resultaat niet haalt. Onder water speelt mee dat als een werknemer niet meer in het eigen beroep aan de slag kan, de wetgever tevens voor de kosten (van de uitkering en omscholing) opdraait. De werkgever wil gewoon dat mensen helemaal niet weggaan uit zichzelf en gebruikt niet nader gespecificeerde 'gevoelige informatie' als stok om de hond te slaan. Zo hebben we een nutteloze regel gekregen op basis van drogredenen.

Non-disclosure beding
Om hergebruik van kennis bij concurrenten tegen te gaan kennen we ook nog de non-disclosure bedingen (NDA's). Zij gelden vaak wél voor de ingehuurde medewerkers. NDA's opereren goeddeels in grijs gebied. Immers, hoewel ze beogen diefstal van kennis tegen te gaan, zijn ze (net als non-concurrentie bedingen) niet specifiek over welke kennis het dan gaat. Nauwkeuriger definities dan "Alles wat je hoort over project X of product Y" zijn zeldzaam. Dat een zó bot mes niet de beoogde resultaten kan behalen zonder bijwerkingen, is duidelijk. Of je negeert een NDA in je volgende functie en je noemt het 'vergeten', of je gebruikt een substantieel deel van je kennis en inzichten niet bij de nieuwe baas om maar geen risico te lopen. In ieder geval is het aantal rechtszaken rond het overtreden van NDA's zeer beperkt. De vraag is of er veel mensen op halve kracht draaien vanwege eerder getekende NDA's, of dat ze massaal genegeerd worden.

Een andere benadering
Zoals de Amerikaanse economen Bolder en **Levine** omstandig aantonen, vormen belemmeringen op het vrije verkeer van informatie en personen (intellectueel eigendom) een grote rem op innovatie en economische groei. Het meest sprekende voorbeeld komt uit de VS: het grootste verschil in juridische arbeidsvoorwaarden binnen de VS gaat over non-concurrentie bedingen. In vrijwel alle staten zijn de regels min of meer vergelijkbaar met die in ons land. Behalve in Californië (zie het **boek** van Ronald Gilso), daar heeft een non-concurrentie beding geen waarde. En zoals we weten ligt de grootste innovatiekracht van de VS juist daar. Volgens kenners ligt dit aan het vrije verkeer van medewerkers. Dit feit wordt onderbouwd met de cijfers uit Michigan, dat sinds 1985 non-concurrentie bedingen honoreert. Sindsdien is de innovatie daar structureel ingezakt.

Het argument dat tegen een versoepeling of afschaffing van deze bedingen wordt ingebracht is dat de schade voor een onderneming immens kan zijn. Waarom zou je nog in innovatie investeren, als het zó wegloopt? Het antwoord is eenvoudig; innoveren moet los staan van het vertrek van medewerkers. Innovatie kan immers ook beginnen op het moment dat een nieuwe medewerker met een goed idee komt dat bij zijn vorige baas niet aansloeg.

Waarom hindert de wetgever werknemers in het uitoefenen van een gestegen marktwaarde? Omdat 'de economie' in ons poldermodel vertegenwoordigd wordt door lobbies van bestaande grote firma's, die het onderscheid tussen 'de economie' en 'de eigen economie' niet helder zien. Dit argument zou je dan net zo hard kunnen toepassen op de topmanagers en inhuur, die immers ook veel waard zijn. Hebben die een non-concurrentiebeding? Nou dan. Meer marktwerking zou

hier écht geen kwaad kunnen, waarbij het belang van een individueel bedrijf haaks staat op het macro-economische belang.

De gedachte achter non-concurrentie maatregelen is dat innovatie daalt als de resultaten niet via de wetgever veiliggesteld worden. Terwijl creative destruction in alle leerboekjes van het kapitalisme voorkomt als condicio sine qua non voor economische groei, beschermt de overheid de grote ondernemingen (die de kosten en moeite van patenten kunnen opbrengen) omwille van de werkgelegenheid. Via de wet ondersteunen we dus de dinosauriërs onder de bedrijven, met alle gevolgen van dien.

Het is niet toevallig dat de grootste economische bedreiging uitgaat van een land dat een broertje dood heeft aan alle vormen van intellectueel eigendom. China, inderdaad. De economie van het gevestigd belang die we opgebouwd hebben middels regels voor intellectueel eigendom leidt tot zwakke bedrijven die de internationale slag verliezen. Misschien kunnen we beter gewoon weer aan het werk gaan en zelf weer steeds betere dingen maken. Zonder al die idiote regeltjes.

Digitale ongehoorzaamheid

vrijdag 14 november 2008

Met het opsturen van mijn weigering mee te doen aan het landelijk EPD heb ik een grote stap gezet. Ik heb nee gezegd tegen de digitale vooruitgang, tegen mijn eigen boterham. Ik heb ook nee gezegd tegen een systeem waar ik beroepsmatig mee bezig ben geweest en eigenlijk groot voorstander van ben. Mits het goed geregeld is. En daar zit hem de kneep - dat is het niet en dat wordt het niet, als er nu niet iets dramatisch verandert.

Het EPD is symptomatisch voor tal van andere systemen die in het kader van de digitale overheid opgesteld worden. Goedbedoelde systemen, waar je feitelijk niet tegen kunt zijn. Een dossiersysteem waardoor medische fouten tot het verleden behoren. Een computersysteem zodat je sneller geholpen wordt aan een bouwvergunning. Een systeem dat zorgt dat er geen onschuldige kinderen meer vermoord worden. Een beprijzingssysteem dat de files laat verdwijnen. Biometrie in het paspoort en centrale registratie zodat criminelen en terroristen opgepakt worden. Energiemeters die het milieu redden. Dát willen we toch allemaal?

Goede bedoelingen zijn niet genoeg. Op zich is het automatiseren van bekende processen niet echt problematisch. Veel werk, niet eenvoudig, maar te doen. Het automatiseren van matig uitgekristalliseerde of volslagen nieuwe processen is wat anders; dat is heel moeilijk. En heel veel werk. Als er onder grote geldingsdrang, hoge tijdsdruk en met complexe organisaties gewerkt wordt, is de kans op een geslaagd systeem nihil. Dan krijg je wat we zien met al deze systemen; ondoordachte keuzes en bijwerkingen die bewust genegeerd worden. De trein rijdt en hij moet doorrijden, kritiek is uit den Boze.

De realiteit van deze projecten is dat de producten live gaan, ongeacht de 'bekende beperkingen', die vakkundig buiten scope gesplaatst en gebagatelliseerd worden. Dat is ook het gezamenlijke kenmerk van bovengenoemde systemen; ze zijn nieuw, automatiseren iets wat eerder niet bestond, zijn onvolledig, worden afgeraffeld en het gebruik wordt - ondanks eerdere toezeggingen - opgelegd. De investering is gedaan, dus het 'gemak' van het nieuwe systeem is verplicht.

Nu ben ik gereformeerd opgevoed. Als er één ding is wat daarvan is blijven hangen, is dat ik aan alles wat verplicht is, gevoelsmatig niet mee wil doen. Ik wil dus niet meedoen aan deze collectivistische projecten. Het individualisme van Calvijn, zeg maar. 'Samen werken, samen leven' zit niet in mijn bloed. Hoe ons kabinet bij deze slogan is gekomen, met duidelijke verwijzingen naar Hegel, Marx en Mussolini, blijft mij intrigeren.

Hoe zou het leven er uit gaan zien als je al buiten deze systemen wilt blijven? Ik ben benieuwd hoe je anoniem kan blijven, als een vorm van digitale ongehoorzaamheid. Anonimiteit is immers de enige bescherming tegen een overheid die niet in staat is of het niet nodig acht persoonsgegevens te beschermen tegen criminelen of eigen medewerkers.

De volgende opties zie ik als een begin;

- Geen creditcard gebruiken.
- Weigeren deelname EPD - bijzonder raadzaam voor Bekende Nederlanders (zie affaire van Persie). Je kunt helaas niet de formulieren online aanvragen - omdat alles plaintext over het Internet gaat. De verbeteringen in de zorg gaan aan je voorbij. Nu maakt dat mij

persoonlijk niets uit, ik ben alleen nog maar in de zorg geweest om er te werken. Als je iets mankeert is het lastiger.

- Op Internet heb je geen echte identiteit. Waarschijnlijk is dit de omgeving waar je het gemakkelijkst anoniem kunt blijven. Blijf alleen ver van commerciële en overheidssites. Marktplaats is een grensgeval.
- Mobiele telefoon met prepaid SIM uitzetten of in een beschermend hoesje stoppen, als je niet belt of gebeld wilt worden. In ieder geval als je je verplaatst. Beter is geen mobiele telefoon te hebben.
- Strippenkaarten zo lang mogelijk gebruiken. De initiële belofte dat de strippenkaart pas afgeschaft zou worden als 95% van de gebruikers vrijwillig overgestapt zou zijn op de OV-chipkaart is al weggemoffeld. Als het dan niet anders kan: de OV-card alleen in de anonieme variant gebruiken.
- Geen spaarsystemen als bonuskaarten gebruiken waar je gedrag uit kan blijken - of regelmatig je kaart ruilen (hoewel dat weer inzicht geeft in je sociale netwerk).
- Snel een nieuw paspoort ophalen voor het nieuwe model verschijnt komende zomer. Geeft je een paar jaar uitstel van de centrale registratie van vingerafdrukken. Voor de gelaatsscan ben je al te laat – als je niet wilt dat deze gegevens beschikbaar komen voor allerlei centrale systemen moet je geen paspoort meer nemen. Met alle gevolgen van dien.
- Belastingaangifte op papier doen. Best lastig omdat je erg lang op een teruggave moet wachten. Helaas geen optie als je ondernemer bent - het bedrijf kun je maar beter sluiten.
- Geen gegevens laten opnemen in een regionaal EKD. Je neemt dan wel het risico dat je daardoor je kinderen kwijtraakt, beter is maar geen kinderen te hebben.
- Zoveel mogelijk cashtransacties - alleen pinnen uit de muur ín een bankkantoor. PIN is veiliger dan de creditcard, maar niet bij automaten in publieke ruimtes. Treinstations bijvoorbeeld.
- Alle andere zaken ook cash afhandelen. Dit kan alleen als je zwart werkt. Vervelend voor je verzekeringen, maar het is niet anders.
- Als de chipknip verdwijnt, zou cash betalen terugkeren voor parkeren? Vast niet. Nu adviseerde het Planbureau voor de Leefomgeving aan Minister Cramer om overal in de bebouwde kom betaald parkeren in te voeren. Doe die auto dus ook maar weg.
- Als rekeningrijden daadwerkelijk ingevoerd wordt kun je toch al geen auto meer rijden zonder dat je gaan en staan vastgelegd wordt. Hoewel dat met camera's met gezichtsherkenning eigenlijk ook nu al een issue is.
- Stoken op gasflessen en elektriciteit uit eigen generator. Water uit de eigen put. Kost een paar stuivers, maar dat heb je er vast voor over.
- Geen DigID gebruiken. DigID heeft met gebruikersnaam/wachtwoord een erg zwakke beveiliging en je bent zelf verantwoordelijk voor wat anderen ermee doen. Ik ben benieuwd of je je DigID kunt laten disablen, om misbruik te voorkomen. Waarmee je overigens afziet van recht op een uitkering omdat je dat alleen online kunt aanvragen. En op termijn van alle andere sociale zekerheid, maar ook van je paspoort en je stembiljet. Gezien de legitimatieplicht kan dat lastig worden.
- Op straat lopen en fietsen is ook een probleem door het invoeren van camera's met gezichtsherkenning. Met een bivakmuts of capuchon op rondlopen leidt weer tot andere problemen. Binnen blijven dus, je kunt je immers al niet legitimeren.

Het moge duidelijk zijn dat de kwaliteit van leven zeer sterk achteruit gaat als je gaat proberen jezelf te beveiligen tegen de gemakzuchtige of bemoeizuchtige overheid. Bovendien, als je leeft zonder sporen na te laten, zul je alleen daardoor al 'opvallen' en de verdenking op je laden crimineel dan wel terrorist te zijn. Nu zullen ze dat niet snel kunnen bewijzen, maar het is voldoende om je te 'verstoren', je 24 uur per dag hinderlijk te laten volgen door geüniformeerd

personeel.
Kortom, digitale anonimiteit is geen optie in onze samenleving. Niet meedoen aan de collectivistische samenleving leidt tot complete uitsluiting.

Onnodig DNA bewaren – mag niet, gebeurt toch

vrijdag 12 december 2008

DNA-profielen en vingerafdrukken van verdachten mogen niet langer worden bewaard dan noodzakelijk. Is de verdachte niet langer verdacht, dan moeten zijn gegevens vernietigd worden. Klare taal van het Europese Hof voor de Mensenrechten (EHCR) in Straatsburg, in een unanieme uitspraak op 4 december. De zaak was aangespannen door twee Britten: zij hadden de rechter verzocht om vernietiging van hun DNA-materiaal na afloop een onderzoek, maar dat verzoek werd verworpen. Ook een Brits parlementslid, die vrijwillig DNA had afgestaan bij een onderzoek naar de moord op een oom, kreeg nul op het rekest toen hij om vernietiging verzocht. Het bewaren van de gegevens 'could not be regarded as necessary in a democracy' volgens de 17 rechters. Ze vonden het 'disproportioneel' en daarom niet toegestaan.

De Britse regering is teleurgesteld over de uitspraak uit Straatsburg. Tot 2001 was het vernietigen van DNA en vingerafdrukken voorschrift in de UK, sindsdien werden gegevens bewaard. Sinds 2004 mogen opsporingsdiensten zonder toestemming DNA en vingerafdrukken afnemen voor iedere verdenking van een strafbaar feit. De database bevat nu de gegevens van meer dan 7% van alle Britten, waaronder veel minderjarigen. Zo bleek in 2007 dat ook het DNA van een 7 maanden oude baby opgenomen[5] was. En het helpt, zegt de Britse regering. Volgens de Schotse politie bijvoorbeeld konden dankzij de database 10.000 misdrijven worden opgelost, waaronder 88 moordzaken.

Deze cijfers zijn echter misleidend, zo toonde Genewatch al aan: die 10.000 is niet het aantal opgeloste misdrijven, maar het aantal gevonden DNA-matches. Een DNA-match is nog lang geen veroordeling: misschien ben je toevallig een dag eerder op de plek des onheils geweest en heeft de politie je roos en je oorsmeer aangetroffen. Het bewijst dus niets.

Maar er zijn wel degelijk meer zaken opgelost, dat wel. Dat is het gevolg van het vastleggen van DNA-materiaal op de plek van meer soorten misdrijven dan voorheen. Het resultaat is dat veelplegers aan nog meer zaken konden worden gekoppeld. Genewatch[6] heeft vastgesteld dat de Britse DNA-database per jaar tot 0,17% extra opgeloste zaken leidt, meest inbraken en autodiefstallen. Daarbij blijkt DNA slechts in een zeer beperkt aantal zaken een rol te spelen (0,35% van het totaal) waarbij het ook nog eens zelden het doorslaggevend bewijs vormt. Tot hoeveel veroordelingen de 88 'opgeloste moorden' hebben geleid is niet vast te stellen omdat dit soort gegevens niet vrijgegeven wordt. Het lijkt er veel op dat Britse politici hun beleid meer baseren op CSI dan op wetenschappelijk onderzoek.

De uitspraak van het Hof is volgens de Labour-regering echter geen reden de wetgeving te herzien. Volgens haar zijn DNA en vingerafdrukken "vital to the fight against crime". Londen heeft van het Straatsburger Hof tot maart 2009 de tijd om de profielen uit de database te verwijderen. Het socialistische kabinet heeft al aangegeven die periode te gebruiken om haar standpunt te bepalen. Eigenlijk zegt Londen hiermee al het vonnis niet uit te voeren.

---

[5] http://www.dailymail.co.uk/news/article-481997/Outrage-DNA-profile-seven-month-old-baby-added-register.html
[6] http://www.genewatch.org/article.shtml?als%5Bcid%5D=539478&als%5Bitemid%5D=529172

Ook voor Nederland is de uitspraak van het Europese Hof voor de Mensenrechten interessant. Het werpt een geheel nieuw licht op de toekomst van ons paspoort. Dit biometrische paspoort, ingevoerd in 2006, moet binnenkort ook de afdrukken van onze wijsvingers bevatten. Als het bewaren van vingerafdrukken en DNA-profielen al verboden is voor criminaliteitsbestrijding in een democratie, met welke argumentatie kun je het dan wel noodzakelijk maken dergelijke gegevens voor een identiteitsbewijs te verzamelen?

Het voorkomen van terrorisme? Het indammen van de migrantenstromen? Het vangen van verspreiders van illegale MP3"s? Het bewaken van de volksgezondheid zoals bij onze hielprik database?

Ik vermoed dat de verschillende overheden doorgaan met de centrale registratie van DNA en vingerafdrukken. Het is een internationale trend en dan kun je moeilijk achterblijven. Door gewoon de gegevens van iedereen vast te leggen in plaats van alleen rond het strafrecht, kan de overheid niet verweten worden dat ze een uitzondering creëert. Dit argument is al gebruikt in andere landen. Welk formele doel daarbij uiteindelijk de doorslag gaat geven is alleen interessant voor de fijnproever.

Toch is er meer om te overwegen. Als de Nederlandse overheid China op de vingers probeert te tikken over de schending van mensenrechten in Tibet, werpt de Chinese overheid tegen dat ook in ons land mensenrechten worden geschonden. En helaas, dan hebben ze gelijk. Dit kan nooit de bedoeling zijn. Nu de hoogste gerechtelijke instantie heeft bepaald dat vingerafdrukken van niet-verdachten niet bewaard mogen worden, komen ze dus niet in ons paspoort. Regels zijn regels. Toch?

Ik hoop het van harte, in dit geval. De uitspraak van het Hof zou een mijlpaal moeten zijn. Waarom zegt een klein stemmetje in mij dat deze uitspraak dan toch volslagen genegeerd zal worden? En dat we toch allemaal braaf een vingerafdruk zullen laten maken?

Waar zijn de klokkenluiders?

dinsdag 6 januari 2009

Ik heb al eens geschreven over de ethiek van ons werk. Er is een zaak die ik toen niet genoemd heb, maar die nu zeer actueel is. Daarom, vandaag nog eens over ethiek.

Stel, je bent betrokken bij de bouw van één van de nieuwe allesomvattende systemen. Zoals de OV-kaart, het EPD, het EKD, het GBA of het nieuwe paspoort, dat doet er even niet toe. Een systeem dat als er iets misgaat, tot zeer grote problemen kan leiden. Niet voor een bedrijf alleen, maar voor de hele samenleving. Noem het een maatschappelijk kritisch systeem. Je ziet dat het systeem in aanbouw grote beveiligingsgaten bevat. Denk aan: de applicatie draait onder een admin account met onveranderbaar wachtwoord, of is afhankelijk van een anonieme Windows share. Of hangt aan de achterkant met onbeveiligde mail aan elkaar. Zoiets. Een situatie die dus absoluut zwak is, maar niet zonder ingrijpende veranderingen en inspanning rechtgezet kan worden.

Dat levert vertraging en meerkosten op. Het management wil echter koste wat kost opleveren. Tijdig opleveren is immers absoluut noodzakelijk – het gevoel van urgentie van de business case is goed overgekomen; het is een onmisbaar systeem. Zeker voor de carrièreperspectieven van bepaalde personen.

Omdat het systeem door meerdere partijen gebouwd en beheerd gaat worden, is het bovendien de vraag van wie het beveiligingsprobleem nu eigenlijk is. Omdat er geen use case is, komt het defect bovendien niet voor in de testbevindingen, dus formeel is er helemaal geen probleem.

Je voorziet dat de formele checks and balances niet gaan werken. Net als in de financiële sector zijn tientallen mensen bezig om dingen voor een enkele controleur met beperkte tijd en middelen onzichtbaar te maken. Bij veel systemen boeit dat nauwelijks, omdat het geheel toch wel stevig is, of omdat een aanval zeer onwaarschijnlijk is. Voor een goede techneut is er altijd wat te verbeteren, dus in genoeg gevallen hoef je je niet druk te maken. Maar bij maatschappelijk kritische systemen is het soms onvermijdelijk.

Nu kun je lekken naar de pers en gegeven de mogelijke consequenties zullen zeer weinigen dat doen. Plus dat de meeste pers niet geëquipeerd is om dit soort berichten fatsoenlijk in te schatten; je krijgt al gauw een soort schandaal- of hype-pers of er wordt bij de meer serieuze pers niets geplaatst, bij gebrek aan inhoudelijke kennis en afwezigheid van weerwoord. Als je dit meemaakt, is dat best frustrerend. Je bent al gebonden aan allerlei vertrouwelijkheidsverklaringen en je moet rekening houden met je commerciële belang. Probeer je een keer integer te zijn en dan helpt het nog niets. Daarom dat veel mensen in de beveiliging zo cynisch worden als een Parijse taxichauffeur.

De kans is levensgroot dat de gaten onder de pet gemanaged worden. Overigens kan dat met de beste bedoelingen – het inschatten van de impact van een gat in een systeem is nu eenmaal niet eenvoudig. Projecten willen nu eenmaal op tijd klaar en binnen budget klaar zijn, ook als er feitelijk geen mogelijkheid is binnen die kaders een systeem te bouwen dat goed genoeg is. Als je dan tóch aan het projectmanagement gemeld heb wat er mis is – het laatste dat je normaliter zult doen - wordt het defect als ‘known issue’ geregistreerd. Doe je bij alle defecten, immers. Als het goed is, wordt het in de toekomst opgelost. Het beveiligingsprobleem wordt daarmee gelijk gesteld aan een knop die niet werkt.

Meestal is dit registreren van het defect het einde van het verhaal. Het wordt onderdeel van 'het volgende increment' of anderszins verplaatst naar een volgende fase. Zo is het project gered en het issue begraven. Dan kan de controleur er feitelijk niets mee. Het gat is een formeel geaccepteerd risico geworden, en dan wordt er niet over gerapporteerd. Terwijl het gat er dus nog steeds is, en niet gedicht wordt. Garanties over volgende releases en incrementen zijn in de regel boterzacht – één economisch crisisje en het verdwijnt in een diepe la.

Er is blijkbaar geen maximum aan het risico dat een manager formeel mag nemen. En al wordt er wel over gerapporteerd: dit soort rapporten verdrinken snel genoeg in het geheel van vertragingen en budgetoverschrijdingen. Met hetzelfde effect: er wordt niets aan gedaan.

Gehaaide managers hebben nog betere manieren. Zoals het 'in vertrouwen' vertellen aan alle betrokkenen wat er precies mis is; ze mogen er dus niets mee doen omdat ze dan het vertrouwen schenden.

Ook schitterend is het opleveren van een normenkader bij het systeem: wat daar niet in staat, kan niet worden niet getoetst door de auditoren – die immers niet bevoegd zijn eigen normen mee te nemen. De toch al vrijwel kansloze toezichthouder wordt hiermee misleid danwel medeplichtig gemaakt en staat effectief buitenspel.

Zodra de zwakte in het systeem erdoor gedrukt is wordt het afgedekt met het woord 'vertrouwelijk'. Dan is het over en sluiten met de veiligheid. Zeker wanneer 'vertrouwelijk' de vorm aanneemt van een 'staatsgeheim'. De burger en het parlement dat hem vertegenwoordigt heeft daarmee een enorme informatieachterstand, want nauwelijks zicht op de problematiek. Het toverwoord vertrouwelijk of staatsgeheim maakt controle effectief onmogelijk.

Zo is het overigens niet bedoeld: vertrouwelijkheid als middel om het eigen falen te maskeren kan hooguit tijdelijk gebruikt worden, mits er intussen hard gewerkt wordt aan correcties. De praktijk leert echter dat het veel gebruikt wordt in plaats van beveiliging. Geheimhouding via woorden sluit echter alleen de goedwillenden uit. Of in onze termen – Security Through Obscurity.

Het is dan ook tijd dat er voor dit soort situaties van bestuurlijk falen een soort klokkenluidersregeling komt voor de beveiliging van maatschappelijk kritische systemen. Zodat je nog iets meer kunt doen dan klagen tegen je collega's over de projectmanager en de opdrachtgever die het probleem het liefst begraven. Een regeling die wél werkt. En dus eentje met minstens een meldpunt en een uitbreiding van het mandaat (en de capaciteit) van de toezichthouders. Uiteraard moet de melder volledig anoniem kunnen blijven en de risico's voor het systeem – dan vaak al live – en betrokkenen geminimaliseerd. Waarmee de regeling een soort samenwerking wordt van de toezichthouders en mensen van de sectie Stiekem.

Hoe dit zich verhoudt tot de controlerende taak van pers en parlement is lastig en blijft altijd een beetje wringen, maar liever een systeem dat soms faalt dan helemaal niets. En dat is wat we nu hebben: niets.

Een goede regeling voor het luiden der klokken moet er komen. Het belang van de individuele organisatie, hoe groot ook, die haar eigen falen verstopt is altijd kleiner dan het belang van de samenleving als geheel. Dit gaat ook op voor bedrijven die blijkbaar zo verweven zijn in de samenleving dat de overheid ze nooit zal laten omvallen, zoals banken, voetbalclubs, de zorg en het openbaar vervoer. De beslissing om de goedkoopste chips te gebruiken en de regels van De Nederlandsche Bank niet van toepassing te verklaren op de OV-kaart is een goed voorbeeld van

de noodzaak van een goede regeling: de beveiliging ging overboord uit politieke overwegingen, maar Translink en chipleverancier NXP worden erop aangekeken. Ten onrechte.

Zodra blijkt dat een veiligheidsprobleem bewust weggemoffeld of erger nog, gecreëerd is, moet de verantwoordelijke opperbaas (overdrachtelijk) hangen aan de hoogste boom. Dit geldt overigens net zo hard voor pure incompetentie; als je een gevoelig systeem laat bouwen kan een excuus als 'het is een gerenommeerde partij' of 'ik heb het aan de specialisten overgelaten' écht niet. Geen enkele leverancier is zó goed.

Daarom is nu net dat systeem van inhoudelijke controles en inhoudelijke controleurs nodig. Dit systeem is in de huidige vorm erg zwak en laat zich zonder problemen manipuleren; het werkt in opdracht van de hoofdleverancier en heeft nauwelijks ruimte om te manouvreren.

De ontbrekende sluitsteen is bestuurdersaansprakelijkheid via de rechter – ook voor de politiek. Dit om te voorkomen dat de sorrycultuur toeslaat en de bestuurlijke verantwoordelijkheid wordt geofferd op het altaar van het coalitiebelang. Veiligheid is té belangrijk om over te laten aan politici.

De staat is terug

zondag 25 januari 2009

De vorige economische crisis - voor mensen die het zich niet meer herinneren - ging over het opleuken van bedrijfsresultaten zodat opgeklopte verwachtingen nog een maatje hoger werden. Grote bedrijven riepen zichzelf uit tot beste vertegenwoordigers van het zegevierend kapitalisme en de grote directeuren werden stijliconen. De beloning van het management was gekoppeld aan de in de beurskoers vertaalde verwachting. Het afstorten van dit systeem in 2002 doopten we de 'internetbubble' naar de meest zichtbare exponent.

Om herhaling van 2002 te voorkomen namen de verschillende overheden een reeks vergelijkbare maatregelen. De belangrijkste was het ruimhartig hanteren van het rentewapen door centrale banken, de Amerikaanse voorop. Als goede tweede kregen we de regels van SOx (2002), Tabaksblat (2003) en allerlei aanverwanten. Daarmee werd de toezichthouder de bescherming tegen een nieuwe dijkdoorbraak en begon de opmars van Compliance en GRC, inmiddels een zeer goed boerende bedrijfstak.

In 2008 heeft de volgende dijkdoorbraak daadwerkelijk plaatsgevonden. De medicatie van 2003 heeft niet geholpen. Als ik de tekenen goed versta moeten we ons voorbereiden op een grotere dosis: meer regeldruk en toezicht en een rente die naar de 0% of zelfs daaronder gaat. Het laatste is in volle gang, en het eerste zal komen zodra de stofwolken zijn neergedaald.

Door fors te strooien met renteverlagingen werd de crisis van 2002 vakkundig naar de toekomst doorgeschoven. Naar nu dus. In 2002 waren het de graaiende topondernemers die de wereld in een recessie stortten. Nu zouden die door Sox en Tabaksblat in toom worden gehouden. Is de huidige crisis dan nu de schuld van falend toezicht en te weinig regels, zoals Greenspan[7] en oud-directeur Levitt van de SEC roepen[8]. Onder vakmensen is dit toch wel de meest gangbare opinie. Maar er zijn ook andere geluiden die de oorzaak van 2002 én van de huidige kredietcrisis plaatsen in het monetaire beleid van de overheid. Dat zit zo: eerst moest de rente omlaag om de economie te stimuleren. Daarmee daalde en passant ook de kosten van de begrotingstekorten bij de overheid. Doordat de rente laag was, groeide de geldhoeveelheid, werd lenen spotgoedkoop, sparen zinloos en klotste het overtollige geld tegen de plinten. Zo stegen huizenprijzen, grondstofprijzen en boekwaardes van bedrijven explosief, want alles was beter dan 2% rendement op de staatslening. Ieder risico was gerechtvaardigd.

Maar omdat er tegenover dit extra geld geen extra waarde stond zou er toch sprake zijn van een torenhoge inflatie, leert de economische theorie ons toch? Ja en nee. Er wordt gezegd dat de geldhoeveelheid groeit vanwege de opkomende landen als China en India; daar wordt extra waarde gecreëerd. Maar dat is zeker niet het hele verhaal. Inflatie is een nationaal cijfer maar 'flitskapitaal' is internationaal en blijft buiten de boeken. Geen haan die ernaar kraait, en politiek bovendien verrotte handig, gegeven de automatische koppelingen en andere gevolgen van inflatie. Het is je toch ook opgevallen dat de stimuleringsmaatregelen van Bos buiten de inflatieberekeningen van het CBS blijven. Gaat dat geld dan rechtstreeks naar de opkomende landen?

---

[7] http://www.rtl.nl/(/financien/rtlz/nieuws/)/components/financien/rtlz/2008/weken_2008/43/1023_1615_greenspan_eigen_boezem_krediet_crisis.xml

[8] http://www.accountant.nl/Accountant/Nieuws/Arthur+Levitt+Huidige+bedreiging+financieel+syst

Dit verklaart ook waarom de Europese Centrale Bank niet mee wil doen aan de lagerentepolitiek; zij stelt dat dit op de middellange termijn leidt tot grote gevaren voor de prijsstabiliteit. Milton Friedman wees daar ook al op.

En toch wordt hetzelfde middel weer volop ingezet, omdat het spook van de deflatie ook nog rondwaart[9]. En daarom gaat de rente naar nul en draaien de geldpersen op volle toeren. We gaven uit wat we niet hebben, werden daar ziek van en het medicijn is meer uitgeven. Dat is als een biertje tegen een kater - het helpt even maar je blijft lazarus. Met als gevolg dat sparen geen rente meer oplevert. De eerste bank die 0 procent geeft op sparen is gesignaleerd: de Julian Hodge bank in Wales heeft de primeur. Feitelijk (gezien de inflatie) leg je er geld op toe als je het op de bank zet - let wel, dezelfde banken die onvoldoende liquiditeit zouden hebben om normale leningen te verstrekken.

Maar ja, dit verhaal is een stuk moeilijker (en nog vele malen complexer dan hierboven) dan de schuld bij de graaiers of de controleurs leggen. De markt heeft het gedaan, punt uit. Het marktdenken heeft helemaal afgedaan en de liberalen zitten waar de socialisten na de val van de muur in 1989 zaten: in het verdomhoekje. De staat is helemaal terug. En dat gaat wel een paar jaar zijn effecten hebben. Ook op ons werkveld.

In 2002 vervingen we het traditionele interne toezicht door het stelsel van extern toezicht via auditoren zoals we dat nu kennen. Nu de pendule richting de staat gaat, roepen velen dat ook deze vorm van zelfregulering onvoldoende is. Dat zal zeker leiden tot een berg extra regels en een sterke leiband voor de auditor. Dat gaan we merken, zeker als we het projecteren op de Security compliance. Het moment nadert dat je als bedrijf een bepaald stuk software niet mag gebruiken omdat de staatsauditor er nog geen toetsingskader voor heeft opgesteld....

Is er iets te leren uit het falen van de financiële auditing? Zeker wel. Auditing is gebaseerd op de Risk Based Approach, die in de informatiebeveiliging ook een tijdje in de mode is geweest en nog steeds breed gedragen wordt, via methodes en best practices. In het kort is dit: maak een lijstje van alle risico's en neem de bijpassende maatregelen. Gebleken is dat de Risk Based aanpak faalt; je ziet altijd risico's over het hoofd omdat ze je voorstellingvermogen dan wel je kennis te boven gaan. Het is een heel gevaarlijke illusie om te denken dat ieder probleem te voorkomen is of af te dekken met een normenkader. Er is niets zo verstikkend als het uitsluiten van iedere eventualiteit, het afdekken van ieder mogelijk risico. En het werkt niet omdat je niet ieder risico kunt onderkennen. Wil auditing een effectieve rem vormen op riskant gedrag, dan is een betere aanpak nodig. Geen hardere, zoals nu gaat gebeuren.

Kenmerkend voor de Risk Based Approach is de wonderlijke vermenigvuldiging van regels - na iedere ronde blijken er nieuwe voorschriften bij te zijn gekomen, met een stijgende mate van bizarre bijwerkingen. Het voornaamste risico waartegen organisaties zich indekken is nu al het compliance risico in plaats van de risico's waar het allemaal om te doen was. Wat de crisis nu bewijst.

Nu is beveiliging van computersystemen van een andere ordegrootte dan het bewaken van de financiële integriteit van onze economie. Maar toch - de afhankelijkheid van computersystemen begint een grootte aan te nemen die echt bedreigend wordt. En we gebruiken dezelfde methodes als in de financiële wereld gebruikelijk zijn. We houden alleen rekening met risico's die we waarschijnlijk achten.

---

[9] http://www.volkskrant.nl/economie/article1084572.ece/Bernanke_vs._de_deflatiespiraal

Als een volgende DNS Changer Trojan computers naar een nep-CRL in plaats van de echte bij Verisign leidt en een paar strategisch gekozen root-certificaten ongeldig verklaart, gaat er echt een heleboel stuk. Helemaal zodra we DNSSec ingevoerd hebben. Op een dergelijk scenario is vrijwel niemand voorbereid. Dit klinkt wellicht meer als een Tom Clancy scenario dan als een realistisch verhaal, maar ook bij computers is een volledige breuk denkbaar. En bovenstaande kan door een gemiddelde nerd op zijn zolderkamer in elkaar gezet worden. Wat overigens geen oproep is aan de lezers van deze site.

Wat de crisis ons bovenal leert is dat je soms het ondenkbare moet denken. Op dit moment is onze beveiliging gebaseerd op het voorkomen van bekende problemen en het verminderen van bekende risico's. Daarmee maken we dezelfde denkfout als de financiële wereld heeft gemaakt. Door het onverwachte tot onmogelijk te bestempelen nemen we enorme risico's. We hebben nog wel wat tijd om ons leven te beteren, maar niet veel. Een recessie zou maar zo kunnen beginnen met een probleem in het digitale domein. En als we pech hebben is dat de volgende keer al, in 2013 of zo.

SaaS is gatenkaas

zondag 15 februari 2009

Je kunt op dit moment geen brochure of whitepaper lezen of je wordt getrakteerd op een samenstel van Cloud Computing, GRC en Grid. Maar vooral SaaS. SaaS staat voor Software as a Service, het huren van een web based applicatie. Er zijn ook al varianten gesignaleerd als Solutions as a Service, Security as a Service[10] en natuurlijk ook Service as a Service[11].

SaaS is Hot. SaaS Mot! Het is in essentie een heel goed idee: het aanbieden van high-end applicaties voor weinig gebruikers, die te duur zijn om inhouse te hosten, met een 'betalen naar gebruik'-model. Daarmee komen we eindelijk voorbij het punt dat een organisatie de eindgebruiker niet veel meer te bieden heeft dan browsen, e-mail, tekstverwerken en file- en printsharing, wat in 1994 ook al kon.

De IT zou de IT niet zijn als we de roze wolk van SaaS niet om andere 'hot' concepten zouden hangen. Zo zie je dat Google Apps - de moeder van alle cloudware - inmiddels als SaaS gepositioneerd wordt. Als één hype niet verkoopt dan doe je er toch gewoon twee, nietwaar? Als dát niet helpt kun je nog over grid computing beginnen...

De meeste verwarring is ontstaan door web based en internet based door elkaar te halen. Web based wil zeggen dat je de browser als client gebruikt. Wat als het belangrijkste voordeel van SaaS wordt gebracht (eenvoudige deployment), is niet specifiek voor SaaS. Het wordt pas SaaS als het betalingsmodel pay-per-use erbij komt.

SaaS levert op dit moment het vertrouwde tafereel op van af en aan stampende consultants. Straks hoef je geen office meer te installeren! Je nieuwe PC is veel gemakkelijker! Veel sneller! Veel veiliger ook. Volgens Gartner is het concept de kinderschoenen ontgroeid en zal 90% van alle organisaties in 2009 een vorm van SaaS gebruiken. En in 2012 zal 9% gratis officeproducten via de browser gebruiken, dus Microsoft, maak je borst maar nat.

Volgens analistenbureau IDC is het grootste voordeel van SaaS de snelheid en het gemak van deployment. Daarnaast spelen de lagere kosten een grote rol: betalen naar gebruik in plaats van naar aanschaf, minder interne IT-support en gelijkmatige betaling in plaats van met pieken en dalen. IDC ziet dan ook grote kansen in de consumentenmarkt omdat je veel sneller nieuwe features kunt krijgen.

Nou, ik heb nieuws. SaaS is alleen geschikt voor high-end gebruik zoals het begon bij CRM. Grid is extreem zinvol, maar alleen binnen je eigen rekencentrum. Op internet is een grid een mooi woord voor een Botnet. En Cloud computing gaat het ook al niet worden.

SaaS is begonnen met salesforce en vergelijkbare concepten; kostbare business software voor beperkt gebruik. Daarvan is het nut en het beveiligingsprofiel vrij overzichtelijk. Anders wordt het als SaaS voor de meer basale functies ingezet wordt. Een groot vaderlands bedrijf neemt Outlook als SaaS af. Toen de wereld nog gewoon was noemden we dat webmail, maar goed. Wat is daarvan nu de toegevoegde waarde? Dat je intern niet in staat bent zoiets basaals als e-mail kosteneffectief te regelen, zodat het blijkbaar goedkoper is om het door een commerciële aanbieder te laten doen? Het zegt mij vooral dat je intern vreselijk inefficiënt bent. Ik zou wel

[10] http://tarr.uspto.gov/servlet/tarr?regser=serial&entry=77112422
[11] http://samj.net/2008/08/sanity-as-service-marketing-gone-mad.html

twee keer nadenken voordat ik als beursgenoteerde toko mijzelf een dergelijk brevet van onvermogen zou durven geven. Als het nu gratis is, zoals Google Apps, dan is het toch wel goed, zullen mensen zeggen. Dat is waar, als het gratis is, betaal je niet te veel. Maar voor niks gaat alleen de zon op, zeiden ze in de middeleeuwen al. Van de rest hoor je de prijs alleen pas later.

De SaaS-manie wordt gevoed door Google, Microsoft, en de ijzerboeren IBM, EMC, HP, Dell en "We put the dot in dot-com" Sun. De insteek van de laatsten is duidelijk; ze verkopen ijzer aan Google. "Me Too" Microsoft toont bij deze aan dat de beschuldiging van het kopieergedrag niet helemaal uit de lucht gegrepen is. En Google? Nou, dat is het bekende verhaal van te veel geld, te veel consultants en te weinig eigen ideeën. Recycle dan een paar oude, is het devies wat wij consultants uitbrengen. En dat is wat Google doet. Cloud Computing heette ooit Server Based Computing. Een paar jaar daarvoor Network Computer. En in een heel grijs verleden heette het gewoon een domme terminal en time sharing. En Cloud Computing is ook niet meer dan dat, domme terminals met slimme centrale computers. SaaS en Cloud zijn leuke ideeën voor bedrijven die hun terminals willen vervangen. Maar verder? De varianten op Thin computing vonden uiteindelijk allemaal een plaats - in de marge; zinvol, maar zeer beperkt. En dat zal nu ook gebeuren.

Vrijwel overal is het fat client model oppermachtig. Waarom zou je een nieuwe computer kopen die minder kan dan de huidige? Ja maar, zegt de cloudware verkoper, alles wat je nodig hebt kun je van Internet oproepen. Dus dan heb ik maar liefst een tekstverwerker. Die heb ik nu ook al. Ja, maar die online veroudert niet! Vanzelf een update! Wauw. Betekent dat dan dat ie het altijd doet, ook als het netwerk eruit klapt? Niet? Mmm. Kan ie ook wat ik nu allemaal kan met m'n Word? Ook al niet? O, maar in mijn Word 2008 zitten allemaal functies in die ik eigenlijk niet nodig heb, dus waar ik best zonder kan. Dus het is beter om een online tekstverwerker te nemen die dat allemaal niet kan. Ach zo. Is die gratis dan? Niet, zeg je? Waarom zou ik dan de huidige machine eruit gooien die ik al betaald heb? Niet vanwege de nieuwe features die cloud tekstverwerking mij biedt, want die zitten er niet in. Minder zelfs. Voor het gratis kan ik overigens prima met open office toe, hoor. Bovendien heb ik al een tekstverwerker, die niet vervangen is ook gratis en dan hoef ik niet te wennen aan een andere interface. En dan bewaarde ik de vervelendste vraag tot het eind: welke functies aan een tekstverwerker zijn eigenlijk verouderingsgevoelig?

Nu zijn er ook een paar cruciale gebreken in de uitgangspunten van SaaS en Cloud. De belangrijkste aannames zijn dat centrale rekenkracht en storage onbeperkt zijn en veel goedkoper dan die van losse servers en PC's. En bovendien dat netwerktoegang onbeperkt en flat fee is.

Onbeperkte centrale capaciteit is een hoax: storage capaciteit kun je dan wel massaal opschalen, disk I/O schaalt veel minder. Processorcapaciteit kun je een eind opschalen, maar daar is geen tekort aan; het beter benutten van de aanwezige capaciteit in je eigen netwerk is een veel grotere uitdaging. Internettoegang en netwerkbandbreedte zijn helemaal niet onbeperkt. Net neutrality is heus niet bedacht omdat het aanbod ongelimiteerd is.

Over de losse PC's is ook nog wel wat te zeggen. Wat is de behoefte aan een dunnere client dan de traditionele PC? Die nieuwe machine waar je alleen een browser op draait, zal ook een gangbare Intel of AMD processor hebben, waar je prima XP of Ubuntu op kan draaien. Dus met SaaS gaan er nog meer processoren met hun vingers in de neus. Natuurlijk kan het ook zo'n kittig minikastje zonder bewegende delen zijn. Maar de afnemers van Wyse en Sun Ray's zijn erg schaars, dus op de één of andere manier werkt het concept niet. Waarom zou het dan nu wél werken? Mensen willen nu eenmaal een dikke PC, net als die man die elke dag in z'n Bentley in de file staat geen Yugo wil.

SaaS en Security
SaaS buiten de deur houden is voor sommige ICT-afdelingen een kwestie van overleven. Daarbij komen de krachtigste argumenten uit de beveiligingshoek. Voor het commerciële verhaal van SaaS is het Security-aspect inderdaad killing. Het afserveren van de beveiligingsbezwaren als een mythe[12] is het anticiperen op onvoldoende kennis bij de beslissers van de potentiële afnemers.

Andere SaaS-evangelisten stellen de toegenomen beveiligingsvraag juist als reden om hun product te gebruiken. En daar kan wel wat inzitten. Immers, als je als interne IT het extreem slecht doet, dan doet bijna ieder ander het beter. En dat kan ook wel een SaaS-aanbieder zijn. Dit geldt evenzeer de stijgende regeldruk; als je intern de HIPAA, PCI-DSS of een andere vinklijst moet naleven, dan heb je een financiële open einde regeling. Een externe leverancier kan dat ongetwijfeld goedkoper; het is veel rendabeler om de schaarse kennis voor meerdere netwerken in te zetten dan voor één enkel.

Helaas is dat maar beperkt waar: om een netwerk van 1000 PC's goed te beveiligen heb je al enkele fulltime topkrachten nodig. Dus alleen als je klein bent is het snijverlies aanwezig dat geïnsinueerd wordt. Het zal dus nooit zo zijn dat je meer krijgt voor minder geld. De kans is groot dat de wolkenverkopers toch hun invloed op je leidinggevenden zullen hebben (ook hier geldt dat wat je van ver haalt lekkerder is), en je geconfronteerd wordt met de opdracht SaaS te 'enablen'. Daarom hier een Top 10 van vragen die in ieder geval beantwoord moeten worden:

1. Waar is de data van je bedrijf? In welk land? Wie heeft er toegang?
2. En dan in het bijzonder: wie zijn de beheerders en wat kunnen die met de data?
3. Hoe hard is de scheiding naar data van verschillende klanten? De kans dat je een meer dan logisch gescheiden datagebied krijgt is klein, het kan immers altijd goedkoper.

Dit zijn de klassieke vragen, die ook spelen bij reguliere outsourcing. Er zijn ook meer specifieke vragen:

4. Hoe zit het met de life cycle van users? Het ontnemen van de rechten van de eigen werknemers bij vertrek is al een ingewikkelde casus waar veel organisaties nog mee worstelen, bij SaaS moet dat ook. Is dit handwerk en hoe kan je vaststellen dat dit goed en tijdig gebeurt?
5. Je bent voor de beveiliging en het toegangsmodel afhankelijk van wat de aanbieder het beste lijkt. In sommige gevallen is dat prima in orde, maar gegeven de hoge hype waarde zijn er tal van aanbieders voor wie time-to-market alles is. Dit leidt tot zwakke systemen, zoals de deconfiture van het toch niet onbeduidende Sage[13] zeer recent aantoonde. Mag je een penetratie test laten uitvoeren door een zelf gekozen partij?
6. Gebruikers worden bij steeds meer organisatie verwend met een enkelvoudig wachtwoord. Maar bij SaaS is dit niet bepaald gemeengoed. Ik geef je op een briefje dat het wachtwoord onder het toetsenbord ligt. Hoe realiseer je Single Sign On?
7. Als je medewerkers dezelfde userID hebben als op het interne netwerk (dat is makkelijker, nietwaar?), dan zullen ze waarschijnlijk ook hetzelfde wachtwoord kiezen. Deze sleutel tot je koninkrijk staat in het systeem van de aanbieder. Wil je dat?
8. Stel dat je wel Single Sign On hebt met SaaS. Moeten gebruikers iedere keer opnieuw aanloggen als ze van de ene naar de andere applicatie gaan (hint: het zijn cross-domein webapplicaties)? Dan is de winst van portals en ESSO weer net zo hard de deur uit.

[12] http://www.cxotoday.com/India/News/Security_Issues_on_SaaS_Model_Are_Myths/551-81359-911.html
[13] http://blog.kashflow.co.uk/2009/01/28/sage-take-SaaS-product-offline-due-to-security-concerns/

9. SaaS kan een leuk doelwit voor een aanval zijn, door het gedrag van andere klanten. Weet je wat de andere klanten zoal doen waarmee ze de aandacht van dierenrechten-hacktivisten, cyberjihadisten en ander creatief tuig trekken?
10. Voor internettoegang tot gevoelige informatie heb je meer noodzaak tot sterke authenticatie. Met hoeveel RSA tokens kun je je gebruikers opzadelen?

De betere SaaS-aanbieders hebben hun zaakjes op orde en bieden een heel nuttig product. Daar ben ik echt niet tegen. Maar hoe het internet koppelvlak eruit gaat zien als je met meerdere goede SaaS leveranciers zaken doet, is een volledig nieuwe vraag. Dan moet je een soort federatieve 'SaaS hub' bouwen. Daarmee kun je als autorisatie provider optreden: het SaaS-systeem krijgt niet de credentials van je gebruikers maar accepteert de log in van je authenticatiesysteem. Dit systeem moet je tegen het Internet aanhangen en zal stevig beveiligd moeten worden. Het bevat immers je users en hun wachtwoorden. Deze hub zal niet eenvoudig te bouwen zijn, zeker als verschillende SaaS-partijen hun eigen standaardjes hanteren. Zullen we deze uitdaging dan maar het labeltje Identity 2.5 geven?

Mumbai of Nieuwegein

zaterdag 21 maart 2009

Ik moet kennis inhuren voor mijn project. Het systeem dat we neerzetten zal jaren dienst doen, en mijn opdracht is niet alleen het systeem binnen de gestelde tijd op te leveren, maar ook ervoor te zorgen dat het de komende jaren goed en veilig werkt en verder uitgebouwd kan worden. De kennis over het systeem zal pas gaandeweg het project echt ontstaan en het is dan ook zeer waarschijnlijk dat ik daarbij externen ga opleiden; intern zijn er nog wat tekorten aan ICT-ers. Voor het opleiden van inhuur wil de klant – terecht – niet betalen. Investeren in een externe, waarbij de kans groot is dat hij op enig moment weer beschikbaar is, kan ik nog wel enigszins verantwoorden. Anders niet.

Je zou zeggen: een standaard probleem. In Nederland is de gevraagde kennis echter niet beschikbaar, omdat het product in kwestie hier niet gangbaar is. Een voor de hand liggende stap is de benodigde expertise dan van wat verder weg te halen. Gegeven de markt kan dit heel wel India of de Verenigde Staten worden; daar zijn kandidaten genoeg en ze willen graag deze kant opkomen om een paar maanden of een jaar te komen helpen. Probleem opgelost, toch? Nou, nee, dat niet. Ik twijfel.

Voor de kennis wil ik gevoelsmatig helemaal niet afhankelijk zijn van een specialist die we van ver weg hiernaartoe halen. Ik wil liever een aanbieder in de buurt. Dat is politiek niet correct, want protectionistisch: Nederland heeft als open economie meer te verliezen dan te winnen. De politicus die ons een vakantie in eigen land adviseerde, werd bijkans neergesabeld. En tóch twijfel ik.

Een wereldwijde markt voor specialisten werkt namelijk prijsopdrijvend. Dat is tegen de marktreligie in, die stelt dat een wereldwijde markt de prijs juist drukt. Dat is waar, zolang de vraag automatisch het bijpassende aanbod schept. Maar het is niet waar voor specialistische kennis. Schaarste creëert geen extra aanbod, maar een hogere prijs.

Specialisten groeien niet aan een boom: ze groeien doordat ze dingen doen, bóvenop de nodige opleiding en intelligentie. Kennis is geen zak nootjes die je kunt ‘overdragen’ of kopen, ook niet bij een universiteit. Neem een net afgestudeerde ‘specialist’ in de arm en je ziet wel wat ik bedoel. De economie is gebaat bij voldoende specialisten tegen een acceptabele prijs. De kenniseconomie is geen vraagmarkt, maar een aanbodmarkt. Als een paar specialisten de hele wereldvraag kunnen bedienen, ontstaat er vanzelf een soort kartel. Dan kun je beter wat overcapaciteit hebben. Scheelt je bovendien een boel zorgen om de ongezonde levensstijl, de levensovertuiging of het rijgedrag van die ene specialist.

Naast dat ik nú expertise nodig heb, wil ik dat die kennis ook daarna snel beschikbaar blijft. Dus bij een leverancier die een directe binding met mijn organisatie nastreeft. Met een aanbieder in een ander land zie ik nog niet zo snel een echt commitment ontstaan, op alleen de basis van wederzijds belang. Nu zou ik met de Indiase of Venezolaanse leverancier natuurlijk ook een contract kunnen afsluiten, zodat ik wat meer zekerheid heb. Voor een of twee specialisten is dat echter een brug te ver. Bedenk maar hoeveel van dat soort contracten je krijgt bij een beetje grote club. Als je pech hebt moet je ook nog een aanbestedingstraject in. Weer niet leuk. Bovendien, gegeven de zeer verschillende rechtsstelsels is een dergelijk contract overzee toch ook niet altijd wat het lijkt.

Die binding met mijn organisatie is essentieel. Vanuit Mumbai is Hoevelaken echter – psychologisch - even ver als Moskou en Los Angeles, terwijl dat vanuit Rotterdam of Nieuwegein echt heel anders is. In een wereldwijde markt moet ik als afnemer op prijs kunnen concurreren met de hele wereld. Dat loopt in de papieren als de markt weer aantrekt. Wat bij lokale aanbieders een grote rol speelt is dat ze mensen hebben opgeleid die moeten renderen, topmarkt of niet. Dan heb ik dus juist kans op korting, bij gebrek aan vraag van anderen.

Lokale leveranciers zullen ook mensen aanbieden die niet over de hele wereld willen werken. En kijk om je heen: de meeste mensen werken het liefst in het moederland, hoewel een jaartje buitenland (mits zonnig en veilig) veel mensen als idee wel aanspreekt. Als het op een klus in het buitenland aankomt, blijken er opeens toch bar weinig vrijwilligers te zijn. Oftewel, statistisch gezien er is een grote kans dat ik betere mensen krijg bij de lokale leverancier. Mensen die zo goed zijn dat ze niet iedere klus in ieder pestpokkenlandje hoeven aan te nemen om te kunnen eten. Betere mensen leidt zoals bekend tot betere systemen, tegen lagere kosten.

Er is nog iets anders dat een rol speelt. Het gaat hier om een beveiligingssysteem bij een gevoelige organisatie. Diepgaande kennis van dit systeem in een land waarvan de economie nog harder getroffen wordt dan hier, en waar de sociale zekerheid voor de betreffende specialist nihil is, is dan ook een puntje van zorg. Hoe waarschijnlijk is het dat mensen letterlijk door honger gedreven zich laten verleiden tot criminele of wraakzuchtige handelingen tegen mijn systeem? En met een dader ver weg, hoe groot is de pakkans? Daar helpt geen screening tegen. Bovendien: hoe screen je iemand van ver weg? Deze overwegingen gelden bij uitstek voor beveiligingssystemen, maar spelen bij vrijwel alle ICT systemen een wezenlijke rol.

Een beroep op een van verre ingevlogen ervaren type is dus hooguit een noodoplossing. Voor een veilig systeem en een beperking van de kosten en afhankelijkheid, wil je dat de ‘vaste’ leveranciers de expertise in huis hebben. Zo niet, moeten ze deze kunnen opbouwen. Mocht de specialist vervolgens de straat oversteken om bij een concurrent te werken, kun je hem vast daar ook wel huren. Vast is dus tussen aanhalingstekens, het hoeft geen contractuele relatie te zijn. Een gezamenlijk belang met bedrijven en personen werkt ook prima, en zelfs vaak beter. Het werken met vaste leveranciers betekent, gegeven de psychologische afstand, werken met leveranciers in Nederland, alle globalistische retoriek ten spijt.

Toch nog even de andere kant: we moeten gebruik maken van de globalisering, vindt de overheid. Tegelijkertijd moeten we een kenniseconomie nastreven, anders staat ons bittere armoede te wachten. En veiligheid is ook het allerbelangrijkste. Kennelijk gaan die drie gewoon niet altijd samen. In sommige gevallen, zoals ICT-beveiliging, staan ze zelfs haaks op elkaar. Mijn conclusie is dan ook: neemt Hollandsche Inhuur! Je betaalt misschien wat meer, maar je krijgt uiteindelijk veel meer waar voor je geld.

Zouden ze het ooit leren?

maandag 6 april 2009

Dat het verschijnsel privacy nog steeds hoogst verwarrend is blijkt uit de officiële reactie van de politie op de blunder met de flitsfoto website. Via mijnpolitiebureau.nl kunnen mensen die een bekeuring ontvangen hebben, op deze site inloggen met DigiD of Burgerservicenummer en hun wachtwoord. Het was een pilot die net een maand in de lucht was. Deze 'boetevolgservice' is ontwikkeld in samenwerking met BVOM, CVOM en CJIB. Op de site konden bestuurders die tussen Alkmaar, Hoorn en Den Helder zijn geflitst de foto van hun overtreding bekijken op internet. Aardig plan, maar het ging fout: ze konden ook de foto's zien van andere overtreders. Na een smalend artikel in de wakkerste krant van Nederland is de site uit de lucht gehaald.

Op zich een redelijk triviaal misstandje. De site toont kleine verkeersovertredingen en er is dus ook weinig aan de hand. Waar ik wél een groot probleem mee heb is de reactie van de politie. Deze benadrukt dat de privacy niet geschonden kan zijn, omdat overtreders toch al gebruikmaken van de openbare weg en door iedereen gezien kunnen worden. Daarom zijn deze foto's niet privacygevoelig, aldus het korps Noord-Holland. Hetzelfde standpunt neemt Google in met Streetview; wat op straat gebeurt is publiek bezit, en als je het er niet mee eens bent ga je maar naar de rechter. Laten we dit even laten bezinken.

Stel, justitie fotografeert wildplassers en zet deze foto's op het internet. Er is sprake van een overtreding en van iets dat zich afspeelt in de publieke ruimte, dus in de redenatie van de politie moet dit kunnen. Maar de wildplasser staat er wel lullig op. Maakt kennelijk niet uit.

Nog een: je fotografeert politieagenten die onder diensttijd, buiten op straat voor het bureau, staan te roken. Niet strafbaar, maar verzin een leuke reden, zoals schade aan het gezag, of het verkeerde voorbeeld voor de jeugd. Vervolgens zet je de foto's op Internet. Toen Geenstijl een mildere variant van deze grap uithaalde, werd door minister ter Horst het portretrecht in combinatie met het redelijk belang op privacy van de agenten aangevoerd als onvoldoende reden tot maatregelen[14]. De politieagenten kunnen een civiele procedure aanspannen, was het advies van onze minister.

Of, nog erger, je zet een webcam op een naaktstrand. Fout? Ja, natuurlijk! Maar waarom? Ook een naaktstrand is immers openbare ruimte, dus als iemand wil klagen kan hij niet bij de politie terecht. Dit biedt de ondernemende geest leuke kansen; laat de bezoekers van de site betalen om de camera te kunnen richten. Een uitstekend businessmodel, maar de kans is erg groot dat je uit de lucht wordt gehaald. De eerste reden is dat je er geld mee verdient, wat natuurlijk in strijd is met de Oudhollandse zeden. Maar wat je te horen krijgt is dat je de privacy van de mensen op het strand schendt. Waar je weer tegenin kan brengen dat veel mensen toch al allerlei privé-zaken op het internet gooien, en dit dan niet meer uitmaakt. Zie hiervoor bij de politiek populaire verwijzingen naar het gedrag van sommige sukkels op Hyves, CU2, CU2night en Facebook. Een dijk van een argument natuurlijk: omdat sommige mensen niet voor zichzelf kunnen zorgen, is het voor iedereen verboden. Natuurlijk zullen er ook mensen vinden dat die naaktlopers het alleen maar fijn vinden om met hun hele hebben en houwen op het internet te staan. Maar de meeste mensen snappen wel dat hoewel het naaktstrand publieke ruimte is, de privacy geschonden wordt met een webcam. Toch mag het wel, volgens de wet.

---

[14] http://juridischdagblad.nl/index2.php?option=com_content&do_pdf=1&id=5352

Dat kan ook met het Zandpad, de weg in Utrecht waaraan de woonboten met prostituees liggen. Staat je kenteken op de webcam? Nou en, het speelt zich af op de openbare weg, dus hij blijft lekker staan. Ook hier zie ik zakelijke kansen; bied aan de beelden te verwijderen voor administratieve kosten van honderd euro.

Een laatste: de pinautomaat. Stel je richt een webcam die opneemt wat mensen intypen. Zonder de gezichten heel herkenbaar te tonen, want anders schendt je het portretrecht en kan iemand een civiele procedure tegen je aanspannen. Pinautomaten hangen op de openbare weg, dus de wet staat dit allemaal toe. “Als burgers vinden dat ze door de camera’s in hun bewegingsvrijheid worden beperkt, staat het ze vrij naar de rechter te stappen,” zegt de woordvoerder van Ter Horst.

Privacy heeft in het digitale tijdperk blijkbaar een onvoorziene dimensie gekregen, die nog niet vertaald is naar heldere juridische kaders. Het Europees Verdrag voor de Rechten van de Mens, waar privacy liefhebbers zich op beroepen, biedt weinig soelaas. Artikel 8 lid 1 stelt dat een ieder recht heeft op respect voor (onder meer) zijn privéleven. Het tweede lid zegt vervolgens dat geen inmenging van enig openbaar gezag is toegestaan. Maar dan komt het: behalve als dit bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare orde of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Dus als er al sprake is van enige relevante wetgeving, dan is deze erg ruim geformuleerd. Sterker nog, je kunt er alle kanten mee op. Zoals Ter Horst met vaste regelmaat aantoont. De politie van Noord-Holland had vast wel een betere site kunnen laten maken maar ze hielden zich dus wel aan de wet, alle smalende kwalificaties van de Telegraaf ten spijt.

Terug naar de digitale wereld. Waar de kneep zit is dit: dat iets op enig moment voor een toevallige waarnemer (zoals de voorbijganger op de openbare weg waar iemand 7 km/h te hard rijdt) te zien zou kunnen zijn, is categorisch iets anders dan wanneer dit voor in principe oneindige tijd voor alle mensen zichtbaar is. Als je iets digitaliseert kan het niet alleen maar door een paar mensen bekeken worden zo lang het op de site staat, het zal ook oneindig gerepliceerd worden en blijft altijd ergens staan. En je weet nooit welke internetmogelijkheden er over een paar jaar zijn. Het is dus niet vast te stellen wat de schade op termijn zal zijn. Het vrijer interpreteren van de regels door de politiek is dus maximaal het verkeerde signaal.

Dit bewijst het onbegrip van de digibeet in privacyland. Omdat de digibeten voorlopig nog niet met pensioen zijn, zit er niets anders op dan de wet te verbeteren en vervolgens iedereen verplicht bij te scholen. Met de bepaling dat ze ook kunnen zakken voor het bijbehorende examen en dat dit consequenties zal hebben voor de verantwoordelijkheden die ze kunnen dragen. Ik weet dat dit hoogst ongebruikelijk is in bestuurdersland, maar gegeven de belangen die op het spel staan, zoals het aanzien en het gezag van de staat, is dit volgens mij gerechtvaardigd.

DLP, de volgende revolutie?

woensdag 22 april 2009

Het verlies van USB-sticks bij Defensie en andere instellingen heeft geleid tot veel aandacht voor onbedoeld verlies van data. Een groot aantal organisaties heeft met enige spoed een oplossing ingevoerd. Zo werd data-encryptie voor USB-sticks snel gemeengoed. Over het algemeen komt het er op neer dat bestanden versleuteld worden zodra je ze op een stick zet, mits ze binnen het netwerk aangemaakt zijn. Dus: als iemand de stick verliest, dan is hij alleen het ijzer kwijt. Probleem opgelost.

De praktijk is echter weerbarstiger: USB-encryptie werkt niet zoals voorzien - nu ja, de techniek doet het prima maar het concept dekt gewoon niet alle scenario's en creëert weer nieuwe problemen. Een onbedoelde bijwerking is bijvoorbeeld dat mensen, om toch portable te kunnen werken, de bestanden dan maar gewoon naar huis mailen. Op de privé-PC kan je immers de versleutelde USB-stick niet lezen. Hiermee is de kans op dataverlies misschien kleiner dan bij USB sticks, maar zeker niet klein. Thuis-PC's worden zelden netjes gewist alvorens het pand te verlaten. De incidentele PC die letterlijk van de straat geplukt wordt die ik zie, is altijd keurig ingericht, met bedrijfsdata, belastingaangiftes en wat dies meer zij. Naar huis mailen betekent dus op zijn best dat de bestanden met een grotere vertraging lekken.

Een andere bijwerking is dat mensen ook op kantoor meer gebruik maken van handige privé-middelen. Zo zie je steeds meer mensen met "kekke mini-laptops" rondlopen. Dat is geen vooruitgang, beveiligingstechnisch. Er worden weinig auto's opengebroken of mensen overvallen om een USB-stick, zeker met de huidige prijzen, maar voor laptops wél.

Je kunt dergelijke schaduwinfrastructuur natuurlijk gewoon verbieden, maar dat moet je niet zo maar doen. Kijk eerst eens naar waarom mensen eigen middelen gebruiken. Gebruikers (ook beheerders) omzeilen de beveiliging omdat deze te hinderlijk is. Verbieden geeft het signaal af dat veiligheid boven productiviteit gaat, terwijl het gaat om medewerkers die wat extra doen om hun werk af te krijgen. Veiligheid gaat lang niet altijd boven productiviteit, zeker niet als de risico's relatief gering zijn. De meeste mensen die een USB-stick of laptop op straat vinden, gooien de bestanden die erop staan namelijk gewoon weg.

Hoe het wel zou moeten? Met Data Loss Prevention technologie[15] (DLP) zouden we deze problemen beter op moeten kunnen lossen. Deze techniek wordt ook Data Leak Prevention, Information Leak Detection and Prevention (ILDP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF) of Extrusion Prevention System genoemd. Ik houd het op DLP, het lijkt erop dat deze kreet gaat winnen.

DLP is nog niet zo bekend. Het werkt als volgt. Bewerkingen op gevoelige data worden beperkt en beveiligd vanuit het lokale besturingssysteem, het netwerk OS, de netwerkinfrastructuur zoals switches en routers en op de communicatie-infrastructuur (mailservers, portals, web proxies en gateways). Voor DLP werken diverse grote partijen innig samen (zoals EMC/RSA met Microsoft en Cisco). Het is ook erg populair bij de antivirus en firewall boeren. De huidige

[15] http://www.computable.nl/artikel/ict_topics/security/2836097/1276896/dlp-is-andere-aanpak-voor-security.html

marketingcampagne is alleen niet erg succesvol te noemen. FUD[16] verkoopt blijkbaar niet zo goed meer.

Het doel van DLP is het tegengaan van het lekken van informatie. Daarbij gaat het vooral over onbedoeld lekken, van gebruikers die niet weten dat het niet mag, dan wel door technische zaken (zoals auto-forwards op mail). De oorsprong is PCI-DSS, waarbij creditcardnummers extra beveiligd moesten worden. Ook is er andere regelgeving, waar bijvoorbeeld adresgegevens (zoals onze Wet Bescherming Persoonsgegevens) of burgerservicenummers met extra zorg behandeld moeten worden.

Hiervoor doet DLP het volgende: een netwerkbreed zoeksysteem stelt vast (op grond van zoektermen of andere functionele input) wat gevoelig is en waar dat staat. Hiervan wordt een fingerprint gemaakt, die door allerlei interne barrières gebruikt wordt om de gevoelige info te kunnen identificeren.

Zo is een creditcard of burgerservicenummer gemakkelijk te herkennen en zal deze informatie binnen gehouden worden. In zekere zin wordt informatie voorzien van een identiteit, zodat er sturing mogelijk wordt: deze informatie mag je wel printen en intern mailen, maar mag niet naar buiten. Deze informatie mag je inzien, maar niet veranderen. Deze informatie mag je wel e-mailen, maar alleen versleuteld. Het DLP systeem kan op basis van een bestand en een policy de benodigde (zelf te kiezen) acties starten, van een stille blokkade en alarmering, een versleuteling die past bij de handeling, tot een extra ‘Weet U Het Zeker?’-button.

Een belangrijke ontwikkeling voor DLP is het aanhaken van Microsoft met ERM. Hiermee wordt geautomatiseerde versleuteling van de meest gangbare bestanden en cryptografische binding ervan aan een netwerk mogelijk gemaakt. Dan kan het bestand dat versleuteld naar buiten is verzonden, alleen geopend worden door iemand die verbinding kan opbouwen met de verificatieserver van het bedrijf. Dat maakt het onmogelijk om bestanden te delen met mensen van andere bedrijven die niet bekend zijn op het interne netwerk en daarom het bestand niet kunnen openen. Hiervoor heeft Microsoft het aloude maar zwaar ondergewaardeerde ADFS uitgebreid, zodat de verificatieservers van ERM gefedereerd kunnen worden. Met deze federatie kunnen netwerken elkaar 'vertrouwen' en zo elkaars gebruikers bepaalde rechten toekennen. Hiermee kunnen organisaties heel fijnmazige policies definiëren; medewerkers van partnerbedrijf X kunnen bestanden me-zus-en-me-zo altijd lezen, en bestand huts-en-fluts ook nog editen waarbij de versleuteling intact blijft. Medewerkers partner Y kunnen weer hun dingen doen met andere beveiligde bestanden.

Deze ontwikkelingen zullen het werk van de beveiligingsmens ingrijpend veranderen. DLP inrichten en onderhouden is een bak werk. Veel werk is het op informatieniveau definiëren van policies die anders dan het huidige hoog abstracte beleid, ook daadwerkelijk ingrijpen. Nog meer werk is het zoeksysteem voeden dat bepaalt wat gevoelige informatie is. Beveiligers zijn niet langer mensen die dikke nota’s vol goede bedoelingen schrijven, maar mensen die computersystemen bedienen. Ik denk dat we dit werk zo snel mogelijk naar de ICT afdelingen moeten duwen.

Met dat zoeksysteem van DLP heb ik moeite. Dat heeft twee redenen. Allereerst hebben zoekmachines niet genoeg aan woordjes om mee te zoeken. Kijk naar Google, dat ondanks allerlei hoogst geavanceerde logica bij de meeste queries toch vaak een paar onzinnige flutpagina’s

[16] http://www.computable.nl/artikel/ict_topics/security/2495011/1276896/data-leakage-protection-dlp-hype-of-bittere-noodzaak.html

tevoorschijn haalt in de top tien. En dat terwijl de meeste webbouwers wel weten wat zoekmachine-optimalisatie en link-popularity is. Oftewel, er zullen een boel false positives en false negatives zijn in DLP. Vervelend, maar geen showstopper.

De tweede is erger. Het systeem inventariseert alle data op het netwerk tot in lokale mailarchieven aan toe. Daarom heeft het parsers aan boord om alle meer of minder gangbare bestandstypes en databases te kunnen lezen. Nu hebben we in anti-virusland één ding geleerd en dat is dat parsers kwetsbaar zijn voor aanvallen. Het DLP-systeem zal gegeven de rechten die het heeft om overal te kijken, zelf een belangrijk aanvalsdoel zijn. En als het als grid opgezet is, ook een omvangrijk doel met een groot aanvalsoppervlak. De parsers analyseren alles wat aangeboden wordt en een simpele overflow in een parser kan leiden tot een inbraak op het systeem. Met de historie van de antivirus-producten in gedachten is het aantal mogelijke gaten in een systeem met honderden parsers immens. Een absolute showstopper.

De impact van een ger00te DLP is veel groter dan bij een gehackte AV-appliance. Het grootste probleem voor de aanvaller is immers niet het binnenkomen op een bedrijfsnetwerk, maar het vinden van waardevolle informatie op dat netwerk. Met tientallen terabytes in een gemiddeld LAN kunnen interne medewerkers dit ook al niet. Met de zoekmogelijkheden van het DLP-grid krijg je als aanvaller veel meer kans. Zo bezien is het een hackers dream.

DLP is door de ingebouwde parsers dus zeer gevoelig voor aanvallen en storingen en zal regelmatig gepatched moeten worden. Je moet het bovendien fijnmazig voorzien van alle technische termen, intern jargon en kreten die gebruikt worden door de eigen medewerkers. Medewerkers die er bovendien op uit zijn om de bestanden toch te kunnen openen om er thuis aan verder te werken. Kortom: ga maar vast taalkundigen, beheerders en extra medewerkers voor de helpdesk werven.

Ik zou voorlopig de zoekfunctie negeren en met de rest van de DLP-propositie aan de slag gaan. Het is zeker een revolutie dat DLP de informatie centraal stelt, in plaats van het computersysteem of de gebruiker zoals we tot nu toe altijd deden. In organisaties waarin er al een zekere ervaring is met dataclassificatie, kun je met DLP een boel winst behalen. Zoals Forester al signaleerde[17], zullen dat er niet veel zijn. Maak daarbij niet de fout te veel 'policy' schermen in te zetten die melden dat iets alleen mag als je het zeker weet; je versterkt de gewoonte overal maar op ja te klikken en de gevolgen daarvan zijn bekend.

De nieuwe generatie spullenboel een levert een heleboel kansen en uitdagingen op. Ik denk dat er prima middelen bij zitten, maar de kans dat organisaties in staat zullen zijn om ze in de huidige vorm op een zinnige manier te gebruiken, acht ik bijzonder klein. Niet alleen voor nu, maar ook in de toekomst. Bij iets veel simpelers als USB-encryptie is het tenslotte ook niet goed gelukt.

[17] http://www.computable.nl/artikel/ict_topics/security/2459020/1276896/bedrijven-onbekend-met-oplossingen-tegen-dataverlies.html

Het gaat ook zo snel

vrijdag 15 mei 2009

“Ik kan het allemaal niet meer bijhouden hoor. Het gaat ook zó snel tegenwoordig. Al die details, da’s meer wat voor de jongeren”. Je hoort het al vanaf een jaar of 35, vooral van mensen met een technische of uitvoerende functie. Gaat hun geheugen echt zo spectaculair hard achteruit ineens, of hebben ze gewoon zin in een hogere salarisschaal?

Je ziet het ook in ICT Security, waar je nu zo’n tien jaar je beroep van kunt maken. In de begindagen holden we nog massaal achter technische concepten aan, zoals Firewalls, PKI, RBAC en X500. Nu verdiepen we ons massaal zich in beleid, management of ‘beveiliging als een proces’.

Feit is dat rond een jaar of twintig de aftakeling inzet. Nu ja, bij mannen dan, maar dat is in onze wereld de overgrote meerderheid. Dat wordt nog wat, gegeven de aankomende vergrijzing en ontgroening van Nederland: het aantal mensen dat de ontwikkelingen ‘niet meer kan bijhouden’ stijgt, er komen steeds minder jongeren die ‘het allemaal nog wel volgen’. Met als gevolg dat we met z’n allen meer willen besturen en minder willen uitvoeren.

Dit gedrag herken je aan het benadrukken van het belang van beleid[18]. Beleid, de panacee voor alle kwalen. Beleid is leuk: je verzint wat er moet gebeuren, zonder allerlei vervelende details, en je maakt je al helemaal niet druk om bijbehorende activiteiten als aansturing en rapportage. Krijg je ook allemaal maar stress van, dus dat moet je helemaal niet willen. Beleid maken is een prima oplossing voor de mensen die het allemaal niet meer kunnen bijhouden. Voor andere problemen is het maar afwachten of het helpt.

De achteruitgang van het geheugen is natuurlijk een zut-argument. Als je geheugen voor technische details achteruit gaat, loopt het geheugen voor andere details óók terug. Het verminderen van de ene hersenfunctie is geen reden voor een ander om het beter te gaan doen. Het is evenmin zo dat als je de details niet kent, je beter de grote lijnen ziet. Hoewel veel mensen dit wel denken, vooral die mensen die zelf de details niet kennen en nooit gekend hebben. Gaan zij beleid maken, dan krijgen dus de mensen met de minste kennis de meeste macht. Zou dat de bedoeling zijn van een kenniseconomie? Of moeten we de pensioenleeftijd maar drastisch gaan verlagen, vanwege de verminderde hersencapaciteit van 30-plussers?

Welnee. Als je na een aantal jaren in het vak erachter komt dat je niet alle details meer uit je hoofd weet, zegt dat volgens mij iets heel anders dan dat alles je te snel gaat. Het zegt juist dat je wijsheid begint te krijgen. Je beseft dat je niet alles weet, en dat het gewoon beter is om dingen op te zoeken en op te schrijven. Dit is geen goed moment om te stoppen met ‘inhoudelijke’ functies. Integendeel. Voorheen wist je óók niet alle details, maar je geloofde dat wel. Daar kwamen nu net al die ongelukken van.

Het veronderstelde causale verband tussen leeftijd en het missen van technische ontwikkelingen is een opportuun sprookje: niemand geeft graag toe iets voor het geld te doen. Geld ja. Hypotheek. Alimentatie. Van die zaken, die vanaf een jaar of 30-35 gaan spelen en die je dwingen te kiezen voor veel en zeker geld. De enige weg daarheen is ‘promotie’, waarbij specialisten beloond worden als ze generalist worden – van programmeur naar consultant, van beheerder

[18] http://www.security.nl/artikel/28790/1/Belang_beveiligingsbeleid_nog_t%C3%A9_vaak_onderschat.html

naar manager. Jammer eigenlijk, want juist als je de wijsheid krijgt dat het verstandig is om dingen op te zoeken en op te schrijven, moet je ineens aan iets heel nieuws beginnen.

Jammer ook voor Nederland, dat op deze manier een verstikkende bureaucratie dreigt te worden. Nederlandse grootbanken en multinationals opereren al vrijwel zonder uitzondering ambtelijker dan de overheid. Over een paar jaar hebben alle organisaties een overschot aan ‘architecten’, managers en adviseurs in alle soorten en maten, maar niemand voor de productie.

Natuurlijk kunnen we ons jongerendeficit nog een tijdje opvangen met het importeren van het geboorteoverschot van de derde wereld. Maar dat is wel heel erg ‘na ons de zondvloed’ en bovendien kunnen die derdewereldlanden hun eigen talenten wel heel goed zelf gebruiken.

We zullen onze carrièremodellen, beloningen en verwachtingen moeten bijstellen. En snel. Want met alleen managen en adviseren komt er geen brood op de plank.

Het stinkt hier

dinsdag 2 juni 2009

Computable heeft Ernst & Young uitgeroepen[19] tot de beste Security adviseur van 2009. De Top 7 bestaat verder uit Deloitte, Microsoft, KPN, Cap, IBM en onderaan Atos. Dit is natuurlijk drie keer slikken voor alle hooggespecialiseerde bedrijven die het beveiligingsvak bevolken; alle bedrijven in de Top 7 zijn generalist. Blijkbaar zijn generalisten ook beter in specialismen dan de specialisten. Nu heb ik wel eens uitstekend werk gezien van mensen die namens deze spelers werkten, maar het ruikt hier wel sterk naar WC-eend. En dat spul meurt.

In opdracht van Computable voerde TNS NIPO het onderzoek in februari en maart uit onder 1913 ICT-managers en 'ambitieuze ICT-professionals'. In de gids worden onder andere per topic rapportcijfers gegeven voor dienstverleners die actief zijn in dat ICT-deelgebied. Respondenten konden per topic alleen de bedrijven waarderen waarmee ze daadwerkelijk ervaring hadden opgedaan.

Enquêtes houden is een behoorlijke wetenschap, waar veel over te leren valt. Daarbij worden we overigens goed op weg geholpen door TNS NIPO zelf, die in haar confrontaties met Maurice de Hond regelmatig tal van kundige opmerkingen plaatst over hoe enquêtes uit te voeren en de gegevens te interpreteren.

In de aankondiging van het voorlaatste onderzoek uit 2007 staat te lezen: 'onderzocht TNS NIPO in opdracht van Computable alle belangrijke ICT-dienstverleners'. Om te kwalificeren als belangrijke dienstverlener en in de lijst te staan zal een bedrijf een bepaalde economische omvang moeten hebben. Daarmee valt het overgrote deel van de specialistische bedrijven af, zo niet alle. E&Y heeft in Nederland een paar honderd man op Security zitten en is daarmee zeker een hele grote, en voor zover ik weet zelfs de grootste speler. Dus het aantal mensen dat zaken heeft gedaan met E&Y zal ook groot zijn. E&Y heeft, naast beveiligingsspecialisten in allerlei smaken, veel auditoren op de loonlijst. Veel meer dan de anderen in de Top 7. Een auditor doet meer verschillende klanten per jaar aan dan bijvoorbeeld een consultant, een programmeur of een cryptograaf. En met bovengemiddeld veel auditoren zal dat oordeel vaker positief zijn dan bij alle andere soorten diensten; audits mislukken zelden. Software- en bouwprojecten daarentegen, nu ja dat weten we allemaal. Dit alles leidt tot een sterke vertekening in de statistiek. Wie de beste is zul je er niet mee kunnen vaststellen.

En waarin eigenlijk? Wat is Security eigenlijk in dit onderzoek. Auditing, het schrijven van beleid, het inrichten van processen of een firewall, forensisch onderzoek of antivirus? Vallen clustering en uitwijkvoorzieningen er ook onder? Blijkbaar is Security zodanig onderdeel van de kennis van ICT-managers en ambitieuze ICT-professionals dat het niet gespecificeerd hoefde te worden.

Als ik kijk naar de andere 'net iets minder goede' Security Adviseurs wordt duidelijk dat Computable ook dezelfde misser maakt als de meeste aanbestedende diensten en subsidieverstrekkers; het subtiele verschil tussen iets kunnen en iets kunnen leveren ontgaat ze. De grote spelers werken allemaal met onderaannemers, wanneer ze zelf de expertise niet in huis hebben. Voor vier van de zeven heb ik zelf in die hoedanigheid gewerkt en van de andere weet ik ook zeker dat ze regelmatig werken met free-lancers, allerlei smaken partners en andere sub-

[19] http://www.computable.nl/artikel/ict_services_guide/2957736/2017861/ernst--young-is-beste-securityadviseur-2009.html

contractors. Dit wordt de klant er in de regel niet bij verteld, het is vaak zelfs geheim. Dus bij deze enquete komt dat ook niet op tafel.

Kortom. Het onderzoek van TNS NIPO meet percepties rond een niet nauwkeurig afgebakende productgroep, sluit het grootste deel van het gebied uit en telt wederverkopers gewoon mee als experts. Ik kan me niet voorstellen dat de winnaar van dit onderzoek blij zal zijn met deze 'verkiezing', behalve als hij een enorme plaat voor de kop, of geen enkele integriteit heeft. TNS NIPO brengt haar geloofwaardigheid op deze manier grote schade toe. De 'business insights' waar ze zelf zo prat op gaat, ontbreken in dit onderzoek overduidelijk. Met deze onderzoeksmethode kan je ook vaststellen dat Volkswagen, Gazelle en Peugeot de beste auto's maken. Op de voet gevolgd door de Lidl, Opel en Boeing.

Ernst & Young rept overigens nergens van deze uitverkiezing. Dat pleit dan weer voor ze.

Pas toe of leg uit

maandag 22 juni 2009

In de wereld van compliance, bestuurlijke transparantie en auditing is Pas Toe Of Leg Uit het leidend principe bij uitstek. Het schrijft voor dat als je van de goede gebruiken wil afwijken, dat je uitlegt waarom je dit doet. Je mág afwijken, maar dan moet je wel een goed verhaal hebben, is het idee. Het principe vormt de hoeksteen van het governance denken, zoals bij de overheid voor het **gebruik van open source**, het EPD en in informatiebeveiliging.

Deze aanpak deugt van geen kanten. Hij steunt op een viertal problematische premissen:
1. Dat mensen niet liegen op papier;
2. Dat lezers over de verantwoording een gewogen oordeel kunnen vormen, waarvoor ze de juiste expertise hebben;
3. Dat lezers kritisch zijn en door de mooie woorden heen kunnen prikken;
4. Dat verantwoordelijken beoordeeld worden op hun resultaten.

1 Mensen liegen niet op papier
Wat je niet kunt verantwoorden, moet je laten. Liegen mag niet, immers. Dit is niet de weg van de minste weerstand; hierover zijn boeken volgeschreven. Kort gezegd: mensen liegen wél, hoewel niet altijd bewust. In tal van varianten, van opleuken, tactisch weglaten en verbloemen in managementspeak tot keihard liegen.

2 Lezers hebben de juiste expertise
De toezichthouder heeft zeer beperkte tijd en middelen om een verhaal te lezen waaraan de opstellers eindeloos kunnen schaven en een legioen van consultants voor kunnen inzetten. Het geheel is sterk asymmetrisch.

3 Lezers zijn kritisch
Mensen zien graag het positieve, ook in wat ze lezen. Kritiek is moeilijk en leidt tot een boel extra gedoe. We houden het graag gezellig.

4 Verantwoordelijken worden aangesproken
In omgevingen waarin coöptatie de norm is (zoals bij commissarissen maar ook in overheid en non-profit) is het hard aanpakken van je gelijken een riskante koers: voor je het weet val je buiten de carrousel van interessante functies. Ook kun je je ineens in een situatie bevinden waarin je iemand moet corrigeren die je zelf benoemd hebt. Daarmee stel je je eigen competentie aan de orde en dat is niet handig.

De zwakte van Pas Toe Of Leg Uit hebben we de laatste tijd een paar keer mooi kunnen zien. De auditoren van woningcorporatie Rochdale stelden vijf jaar geleden al vast dat er grote risico's gelopen werden, wat niet geleid heeft tot enige actie van de raad van commissarissen. De excessen zijn dan ook opgetreden. Zo betaalde Rochdale 46,5 miljoen voor een kantoorgebouw dat enkele maanden daarvoor voor ongeveer de helft van de prijs van eigenaar was gewisseld. Dit is een bekend trucje onder projectontwikkelaars om even wat geld te regelen. Het lijkt erop dat de directeur pas in het vizier kwam toen hij een Maserati aanschafte op kosten van de stichting en de Telegraaf er een artikel tegenaan gooide.

Sinds enkele maanden ligt bij minister Eberhard van der Laan (Wonen, Wijken en Integratie) een voorstel voor een strakker arrangement tussen overheid en corporatiebranche: het advies Meijerink. Een van de aanscherpingen die Meijerink voorstelt is de wettelijke verankering van de

sinds 2007 geldende '**Aedes governance code**' voor de hele sector. Die code is opgesteld door onder meer de jurist Jaap Winter, bekend van de 'corporate governance code' van de Commissie Tabaksblat. Deze code zal de positie van de auditor versterken en zeker meer toezicht mogelijk maken, maar laat de inherente zwaktes van Pas Toe of Leg Uit ongemoeid. Zo zie je dat een Aedeslid **doodleuk schrijft**: "We geven in het jaarverslag geen uitgebreid inzicht in de interne risicobeheersing en controlesystemen en de werking hiervan. Wij behandelen jaarlijks tijdens de bespreking van het werkplan de risiconota. Hierdoor is de Raad vroegtijdig in staat om haar controlerende functie goed te kunnen uitvoeren". In de rest van het document wordt een reeks van andere bepalingen net zo makkelijk afgeserveerd. Oftewel, we "leggen uit" dat we de hele code naast ons neer leggen, en daarmee is het klaar. Het erge is ze dat inderdaad aan de gedragscode voldoen.

Aedes, de vereniging van woningcorporaties, noemt het vertrek van de toezichthouders van Rochdale "de juiste conclusie", aldus voorzitter Willem van Leeuwen. "De inmiddels bekende informatie rechtvaardigt de conclusie dat het toezicht tekort heeft geschoten." Volgens hem wil dat nog niet zeggen "dat er reden is om te twijfelen aan de integriteit van de raad. Dat is een andere kwestie."

Het lezen van bevindingen is een vak apart en als de lezer niet doorvraagt blijft het een papieren tijger. Dat geldt zeer zeker ook in de ICT; een raad van commissarissen of een ministerie moet over een forse dosis vakkennis beschikken om een eigen oordeel te kunnen vormen. Zonder een staf van enige omvang en competentie is Pas Toe Of Leg Uit een lege huls.

Nu kunnen de verantwoordelijken zonder al te veel moeite een dergelijke staf vormen. Maar dat is er nog nooit van gekomen. De enige verklaring die ik hiervoor kan verzinnen is dat het nooit de bedoeling van Pas Toe Of Leg Uit was om méér te zijn dan een lege huls. Compleet bestuurlijk falen mag gewoon, ook uit laksheid of incompetentie. De bestuurders in kwestie mogen bovendien niet op een gebrek aan integriteit worden gewezen. Het begrip bestuurlijke aansprakelijkheid, wat al jaren een lege huls blijkt, is aangevuld met het even vrijblijvende broertje Governance. Pas Toe of Leg Uit is niet meer dan een nieuwe vorm van gedogen en als zodanig een volslagen onbruikbaar sturingsmechanisme voor informatiebeveiliging. We moeten wat anders verzinnen.

Geschikt? Ongeschikt!

donderdag 9 juli 2009

Defensie zou geen gewelddadige computergames moeten gebruiken tijdens bijeenkomsten om jongeren te werven voor het leger. Dat stelt de CDA-fractie in de Tweede Kamer. In vragen aan staatssecretaris Jack de Vries (Defensie) en minister André Rouvoet (Jeugd en Gezin) vraagt het CDA daarom een verbod op gebruik van dergelijke games. Dat zou kunnen op basis van een verbod om schadelijke afbeeldingen te verspreiden onder kinderen onder de zestien. Zij zouden immers bij de wervingsbijeenkomsten van Defensie aanwezig kunnen zijn.

Defensie gebruikt Counter Strike en Unreal Tournament. Die laatste is in Duitsland al sinds 2002 verboden, meldt het CDA. Nu is de gemiddelde 15-jarige bezig met multiplayer van Call of Duty 5. Zal hij de games van Defensie te spannend of eng vinden? Mwoah. Slap en achterhaald, eerder. Beide spellen zijn 10 jaar oud. Je zou de games van Defensie bijna willen verbieden wegens het beschadigen van het eigen imago. Maar daar is het onze christendemocraten natuurlijk niet om te doen. De games van Defensie kunnen aanzetten tot geweld, en dat willen we vijftienjarige aspirant-militairen niet aandoen, zo luidt het argument. Nee zeg, soldaten en geweld, het idee alleen al. Die jongens moeten natuurlijk niet denken dat ze iets met Geweld gaan doen als ze eenmaal hun uniform aanhebben.

En er is meer aan de hand. Ons land staat al sinds jaar en dag op een zwarte lijst van Unicef, omdat onze krijgsmacht 16- en 17-jarigen werft. Dat zijn kindsoldaten. Volgens het Internationale Recht mogen we deze leeftijdscategorie niet blootstellen aan de krijgsdienst, zonder uitzonderingen. Ten tijde van de Fitna-discussies riep onze premier andere landen nog op zich te houden aan het Internationale Recht. Maar Defensie gaat door met het werven van kinderen, want ook mét deze groep zijn er tegen de 8.000 vacatures op een totaal van ruim 46.000 militairen. Kennelijk gaat dat belang boven het Internationaal Recht, dat overigens door onze krijgsmacht zo uitstekend verdedigd wordt in de inzetgebieden.

De games die Defensie gebruikt zijn niet verboden, ook niet voor jeugd onder de 16. Daarover loopt wel een slepende discussie en er zijn al stapels beleidsstukken gewijd, maar vooralsnog is er geen zicht op een uitkomst. Volgens de minister van justitie is het onmogelijk de verkoop van spellen te verbieden. Dit bleek in 2007 ten tijde van de discussies rond Manhunt 2.

Maar, zei Hirsch Ballin, een verbod op de verkoop aan jeugd onder de 16 zou wel mogelijk zijn, hoewel hij de grens liever bij 18 jaar zou leggen. In 2008 liet het kabinet de mogelijkheden tot verbod nog een keer onderzoeken, zonder eenduidige uitkomst. De bescherming van minderjarigen tegen schadelijk beeldmateriaal is vastgelegd in art. 240a van het Wetboek van Strafrecht. Leeftijdsindicaties als 18+ en waarschuwingslabels voor geweld maken videogames echter juist aantrekkelijk voor jongeren, blijkt uit **onderzoek** van de Vrije Universiteit Amsterdam.

Als je de verkoop tegengaat, is illegaal downloaden van Usenet of met een torrent voor de gamebeluste 15-jarige het gemakkelijkste alternatief. Dat je met een illegale kopie geen toegang hebt tot een gameserver is dan hooguit vervelend; zelf een server opzetten is immers niet zo moeilijk. Verbieden stimuleert dus crimineel gedrag: illegaal downloaden van software en het opzetten van gameservers met illegale software. Dat een aardig percentage van de keygens en NO-CD fixes voor illegale spellen een trojan bevat moeten we maar voor lief nemen.

Gewoon verbieden is op praktisch niveau nog veel complexer dan het al lijkt - er zijn steeds meer ouders die zelf gamen. Mag je games voor je kinderen kopen als je zelf het geweld niet problematisch vindt? Moet je je eigen computer beveiligen tegen je kinderen zodat ze niet alle spellen kunnen starten die je zelf speelt? Ben je aansprakelijk als je dat niet goed genoeg doet? Mag een gezin afgesloten worden omdat een minderjarige online een 16+ spel speelt of spelsoftware illegaal binnenhaalt? Het is heel kenmerkend dat alle betogen over het gevaar van computerij ouders als complete digitale nitwits presenteren - spreek voor jezelf, ja!

Waar het vooral om gaat is dat de ouder/verzorger er blijkbaar op moet toezien dat het kroost geen spellen speelt die volgens het kabinet niet goed voor ze zijn. Mag de overheid in dit geval achter de voordeur ingrijpen? In principe is ingrijpen achter de voordeur alleen toegestaan als er zeer dringende redenen voor zijn. De relatie tussen gewelddadige spellen en geweldsincidenten is echter niet lineair aangetoond. Er zijn wel statische aanwijzingen dat er een correlatie is, dus de politieke druk gaat door. Met regelmaat duiken er berichten op na het plegen van een moord dat 'de dader was geïnspireerd door ...'. En dan volgt de naam van een computerspel. De daders van de moordpartij op de Columbine High School - 13 doden - speelden Doom en Quake. De dader van het bloedbad in Erfurt - 16 doden - was een fanatiek speler van Counter-strike. Wat betekent dit als je weet dat **99%** van de jeugd regelmatig computerspellen speelt en dit de populairste spellen zijn? Inderdaad, niets. De discussie speelt zich af rond opinies maar zonder feiten. Zoals kenmerkend verwoord wordt in het 'Christelijk magazine' **Terdege**: er is geen wetenschappelijk onderzoek dat bewijst dat er géén verband is tussen geweld in spellen. Ja, zo lust ik er nog wel een.

Toegeven aan de wens tot verbod opent de deur voor staatsopvoeding: is er een relatie tussen bepaalde activiteiten en strafbaar gedrag? Verbieden die hap! Als bezoekers van partyflock.nl statistisch gezien bovenmatig veel pillen slikken en over seks praten, kun je de toegang voor minderjarigen dan verbieden? Vast wel, drugsgebruik en pornificatie onder jongeren is immers een groot probleem, dat de aandacht van ons kabinet heeft. Maar als nu bezoek aan een bepaalde kerk, sport of moskee statistisch relateert aan fraude of geweld? Dan wordt het vermoedelijk ineens stil in Den Haag.

Op de CDA-politici die met het voorstel kwamen voor een verbod op games past maar één woord: ongeschikt!

Alleen maar verliezers

vrijdag 21 augustus 2009

Het illegaal downloaden is een zware slag toegebracht. Tenminste, dat stelt Stichting Brein en dat vertellen de media aan ons. De Zweedse beheerders van de Pirate Bay zijn door een Nederlandse rechtbank bij verstek gesommeerd op straffe van een forse dwangsom de site voor Nederlanders af te sluiten.

Bij verstek? Ja, de gedaagden wisten niet tijdig dat de zaak diende, zeggen ze. Stichting Brein meldt niet dat de beheerders van de site niet op kwamen dagen. Misschien wisten ze het echt niet. In civiele procedures wordt er niet altijd evenveel moeite gedaan om de gedaagde van de zitting op de hoogte te stellen. De eiser moet de gedaagde op de hoogte stellen van een rechtszaak en daarbij is opzettelijke slordigheid soms een heel handige truc. Het is een van de zwakke zaken in ons wetboek dat de 'behoorlijke oproeping' niet heel goed is vastgelegd; een gewone brief is voor de meeste civiele zaken formeel gezien genoeg. Het is bijvoorbeeld geen vereiste dat een opgeroepene bevestigt dat hij komt. Nu zegt Stichting Brein dat het gemaild, getwittert en gefacebooked heeft. En dat haar logs laten zien dat vanaf een IP-adres dat iets te maken kan hebben met de gedaagden, gekeken is op een website van Stichting Brein. Dat is kennelijk voor de Amsterdamse rechtbank voldoende.

Maar als de gedaagde de oproep niet opmerkt (spamfilters anyone?), of terzijde schuift omdat hij er niets mee te maken heeft? Dan gaat de zaak gewoon door en wint de eiser vrijwel altijd. De eiser is er dus bij gebaat dat de gedaagde niet ter zitting komt en kan dat zelf sturen. En dat is hier gebeurd.

De veroordeelden hebben aangekondigd tegen de gang van zaken in beroep te gaan, zodra ze een jurist kunnen vinden die dit gratis wil doen. De kans op succes is erg groot - het recht op hoor- en wederhoor is al in heel veel zaken voldoende geweest om vonnissen-bij-verstek te herroepen. Ook het accepteren van twitter of e-mail als instrument om een dagvaarding over te brengen zal waarschijnlijk niet op de waardering van een hogere rechter kunnen rekenen.

Maar voorlopig heeft Stichting Brein gewonnen: de burgers zijn er weer eens op gewezen dat auteursrechten niet zomaar geschonden mogen worden. En uiteindelijk is de strijd tegen 'internetpiraterij' een mediaoorlog - een uitspraak die juridisch vrijwel **geen waarde** heeft wordt als succes gepresenteerd en alle media brouwen dat gedachteloos na. Hierin past de **nepclaim** van Stichting Brein aangevallen te zijn door hackers ook prima. De Pirate Bay zal hiervan weer aangifte doen, ditmaal wegens smaad. Smaad is strafrecht en de kans dat deze zaak ontvankelijk zal zijn lijkt mij gering. De juristen van Brein zijn duidelijk gewiekster dan de beheerders van de Pirate Bay. Ze kosten een paar stuivers maar dan heb je ook wat. De Stichting Brein heeft aangetoond aan haar opdrachtgevers dat ze het geld waard zijn en kan dus weer een paar jaar verder. Dat is wel wat felicitaties waard - je zult in deze tijd maar werkloos worden.

Verder zijn er in deze zaak alleen maar verliezers.

De rechtbank heeft aanzien verloren door een uitspraak te doen die in de samenleving zeer **weinig draagvlak** heeft. Afgezien van een handvol zonderlingen zijn de enige mensen die nooit iets illegaals downloaden mensen die niets kunnen met een computer. In een democratie zal uiteindelijk de wens van de overgrote meerderheid prevaleren, zeker als de enige belangen die geschaad worden vermeende commerciële belangen zijn. Vermeende belangen? Ja, ze zijn beargumenteerd maar **niet bewezen**. Bij lange na niet.

De volgende verliezer is de politiek. Den Haag denkt nu dat het probleem een tijdje minder groot zal zijn en zal nog langer de wetsvoorstellen laten **dicteren** door de **lobbyisten** van de media-industrie. In een mediaoorlog als deze over een onderwerp dat iedereen raakt, wordt dit veel mensen duidelijk. Deze onthulling van de Haagse werkelijkheid ondergraaft het vertrouwen van de burgers in de politiek nog verder.

De rechtsstaat is door een gelegenheidsuitspraak als deze ook niet bepaald gediend. En dat op verschillende manieren. Bovenal natuurlijk de goedkeuring van dagvaarding via Twitter en e-mail door de eiser. Onbetrouwbare communicatie (naar niet-verifieerbare internetadressen) is onvoldoende voor een zaak met dergelijke consequenties. E-mailadressen die op internet gepubliceerd zijn, zijn spam-magneten, dus de kans dat ze echt in gebruik zijn is klein. En Twitter? Zouden de beheerders van de Pirate Bay followers zijn van de **Brein Twitter**? Ze hebben maar liefst twintig followers, en daar zitten onze Zweedse vrienden vast niet bij, dus ook dat is nogal een loze claim.

Een tweede verlies voor de rechtsstaat: verwijzingen (zoals de veroordeelde partij aanbiedt) vormen de essentie van Internet. Als deze uitspraak en eerdere **vergelijkbare uitspraken** overeind blijven, wordt Internet uiteindelijk zelf verboden. De uitspraak zal dus ook geen stand kunnen houden.

Ten derde: de rechtsongelijkheid. Brein richt zich op de grote overtreders en dat is vanuit hun optiek natuurlijk valide. Wat kan Stichting Brein met mensen die met wat slimmere queries in een zoekmachine open directories met mp3s, iso's en dvd-rips vinden en ze vervolgens leeglepelen? Google sommeren te stoppen met de zoekmachine misschien, of die miljarden zoekresultaten eerst verplicht laten controleren? Zo'n rechtsongelijkheid ondergraaft de essentie van de rechtsstaat, dat burgers gelijke rechten hebben, ongeacht hun SQL kennis.

Ten vierde de bewijsvoering. De claim van Brein dat van een IP-adres van de Pirate Bay gekeken zou zijn op een speciale pagina van de Stichting Brein website is door de rechter kritiekloos overgenomen als bewijs dat de gedaagden wisten van de zaak. Een IP-adres in een log - dat is in een behoorlijke forensische bewijsvoering van geen enkele waarde. Spoofing, manipulatie van het serverlog en allerlei andere zaken zouden uitgesloten moeten zijn alvorens dit argument overgenomen kan worden. De rechter toont zich ook hier van haar meest digibete kant.

De meeste schade brengt de uitspraak de samenleving toe met artikel 2.1 van het vonnis, dat stelt dat het valide is de Zweedse beheerders in Nederland voor de rechter te dagen omdat er hier gedownload kan worden. Hier botst ons beperkte nationale recht met veel grotere belangen; het betekent dat iedere aanbieder van informatie op Internet in ieder ander land aangeklaagd kan worden, als iets daar toevallig niet mag. Onze rechtbank zal dit blijkbaar honoreren en - mits er verdragen voor zijn - actief helpen de sancties uit te voeren. Dus: als de ayatollahs in Teheran vorderen van Nederlandse contentaanbieders die positief zijn over homoseksualiteit onder moslims dat ze IP-adressen uit Iran blokkeren, zal de Nederlandse rechter deze eis in principe steunen. En dit geldt mutatis mutandis voor alle content en alle mogelijke verboden in alle landen wereldwijd. Ik vermoed dat dit niet de bedoeling is van de rechtbank in Amsterdam.

De uitspraak helpt de media-industrie ook al niet: er wordt geen bit minder gedownload. Nu zal het wel tijdelijk enig rendement kunnen hebben maar de voorspelde **implosie** van het torrentverkeer zal zeker geen permanent karakter hebben. Het aanbod is immers niet verminderd - alleen een zeer vluchtig distributiekanaal is verdwenen. Er wordt uiteindelijk waarschijnlijk zelfs meer gedownload - door alle aandacht weten nog meer mensen wat torrents zijn en hoe ze ze kunnen vinden op het Internet.

Hoezo, Gezag?

maandag 7 september 2009

Beveiliging is een moeizaam vak, zeker waar het over ge- en verboden gaat. De techniek inrichten is nog tot daar aan toe. Lastig wordt het als je met de gebruikers, interne en externe medewerkers te maken krijgt. Opschrijven dat iets niet mag en iets anders zus en zo moet - kan nog net. Maar als je daar daadwerkelijk iets mee bereiken wilt - dat ze luisteren of zo - dan wordt het opeens heel moeilijk. Op dat moment treed je namelijk op als 'het gezag' binnen de organisatie. Gezag dat gerespecteerd wil worden. En daar zijn we niet goed in.

Er wordt wel eens lacherig gedaan over doorwrochte beveiligingsregels. Zoals die Linux beheerders die je in je gezicht uitlachen als je ze verplicht een virusscanner te installeren - uitermate frustrerend. Misschien kunnen we wat leren van het gezag bij uitstek, de overheid, over hoe je met ge- en verboden moet omgaan? Als uitoefenaar van gedelegeerd gezag (van het bedrijf) ben je immers in een vergelijkbare positie als de politieagent. Nu willen veel mensen in de beveiliging zich niet als politieagent zien - maar wat ben je dán? Zodra je buiten de techniek van de beveiliging gaat, ga je over beleid of over handhaving - en in de meeste organisaties over beide.

Laten we dus maar eens op les gaan. De onderwerpen gezag en haar vertegenwoordigers zijn behoorlijk populair in en rond de overheid. Wel is er duidelijk sprake van een crisis rond het gezag. Opvallend zijn de diverse voorstellen voor zwaardere sancties bij agressie tegen vertegenwoordigers van het gezag om 'respect af te dwingen'. "Respect (voor het gezag) kent een vriendelijke maar ook een strenge kant. Daar hoort het grenzen stellen en handhaven bij", stelt onze premier. Het gaat ook daar blijkbaar niet vanzelf.

Het eerste wat opvalt, is dat onze premier geen onderscheid maakt tussen verworven respect en afgedwongen respect. Toch is het een wezenlijk onderscheid, want afgedwongen respect komt neer op angst, vanwege de sancties, en dat is iets heel anders dan respect. Angst en respect sluiten elkaar zelfs uit.

De angstbenadering werkt alleen als je als overheid bereid bent hem tot het uiterste door te voeren. Met andere woorden, als een ongehoorzame burger escaleert, moet de overheid meegaan in die escalatie. Hard optreden zal sommige burgers in het gareel brengen, anderen zullen ook harder optreden, zoals we laatst op het festival in Hoek van Holland konden zien. **Opvoedkampen** voor onwenselijk gedrag en **uiteindelijk** dictatuur en doodstraf liggen in het logische verlengde van dit autoritaire pad. Dat is natuurlijk niet wat de politiek nastreeft, die wil slechts uitwassen bestrijden.

Het CDA heeft een **beschavingsoffensief** ingezet om het 'respect in de samenleving' voor het gezag terug te brengen. Goed nieuws, zou je zeggen. Onderdeel van dit beschavingsoffensief zijn verboden op growshops en kraken, ingrijpen achter de voordeur bij probleemgezinnen, en zwaardere sancties voor tal van combinaties van jeugd en **alcohol**. Premier Balkenende kondigde op het respect-congres afgelopen zomer aan dat zijn kabinet met nog scherpere plannen komt om jonge vandalen aan te pakken. Dit lijkt meer op het bijbrengen van angst dan het kweken van respect.

Het belangrijkste argument onder dit uitdijend overheidsoptreden is de toename van het aantal en de impact van wetsovertredingen. Belangrijk aan deze statistieken is dat hoe meer zaken je strafbaar stelt, hoe meer overtredingen er zullen zijn. Het aantal ge- en verboden is de laatste

jaren met een duizelingwekkend tempo toegenomen: we moeten dan ook vaststellen dat er - na correctie voor deze statistische vertekening - een forse afname van de criminaliteit is. De impact van overtredingen is een graadmeter voor de heisa rond een incident - zeer subjectieve factoren die in een normale rechtstaat geen plaats mogen hebben. Is het te rechtvaardigen dat iemand langer de bak ingaat omdat het misdrijf in de uitzending van Peter R. de Vries is geweest? Of juist korter moet zitten, omdat er ten tijde van de zaak veel voetbalnieuws was en de kamer op reces, en de zaak dus geen 'beroering' heeft kunnen veroorzaken?

Wat het respect voor het gezag niet helpt, is het grote aantal zaken dat 'verboden zou moeten worden'. Het gebruik van proefballonnetjes is in Den Haag niet met de LPF verdwenen. Zulk strooien met ge- en verboden is contraproductief, zeker omdat vervolgens onduidelijk is of ze daadwerkelijk ingevoerd worden. Het leidt op z'n best tot verwarring, maar in veel gevallen ook tot het gevoel dat 'ze' (lees de wetgever) geen idee hebben waar ze mee bezig zijn. Zomaar een paar recente berichten:

Kroegen moeten eerder de deur sluiten voor de jeugd, om ze van het drinken te weerhouden. Alcoholreclames vóór 21.00 uur worden verboden om het drankgebruik onder jongeren tegen te gaan, stelt de nieuwe mediawet. In Urk zal bier uit de supermarkt verdwijnen, omdat de supermarkten niet voldoende letten op de leeftijdsgrens. Tien- tot twaalfjarigen die 's avonds laat zonder begeleiding op straat zwerven worden strenger aangepakt. Er was al aangekondigd dat die binnenkort door het Bureau Jeugdzorg worden thuisgebracht, om de ouders aan te spreken. Balkenende zei dat na twee keer thuisbrengen de officier van justitie wordt ingeschakeld, om de ouders aansprakelijk te stellen voor de kosten en eventuele schade.

Tot je 21ste mag de jeugd niet blowen op straat of **drugs** kopen. Tweede Kamerlid Joël Voordewind van die ChristenUnie stelt dat jongeren eerst hun schoolopleiding moeten afmaken voordat ze met drugs mogen beginnen. De CU wil, eveneens om de kinderen te beschermen, het roken in de auto **verbieden**.

Jongeren tot 23 jaar moeten werken of onderwijs volgen totdat ze een 'startkwalificatie' hebben. Anders krijgen ze een boete die kan oplopen tot 2250 euro. Herinvoering van de dienstplicht is hiervoor eventueel een goed middel, aldus Balkenende.

Sinds vorig jaar zijn paddo's en 188 andere paddenstoelen verboden. Dat diverse soorten beschermde paddenstoelen ook verboden zijn, leidt tot de idiote situatie dat je bepaalde soorten moet plukken (verwijderen) en niet mag plukken (milieu).

Sinds 1 september zijn gloeilampen van 100 watt en meer verboden. Ook het lampje in de koelkast dat ongeveer een half uur per jaar aan staat zal op termijn verboden worden. Een verbod wacht ook gewelddadige computerspellen. Zij hebben immers mogelijk een slechte invloed op de jeugd.

Het kan nog erger - bij onze oosterburen mogen minderjarigen niet naar de zonnebank en wil regeringspartij CDU het motorrijden buiten de racebaan verbieden, omdat het gevaarlijk is en er andere vervoermiddelen **bestaan**. Ook wil het CDU paintballen en laserquesten verbieden omdat het te veel lijkt op oorlogvoeren. Hetzelfde staat bepaalde vechtsporten te wachten, en ook het luchtdrukgeweer zal voor minderjarigen verboden worden. Verder mogen jongeren onder de 18 wellicht niet meer in het openbaar 'genegenheid' aan een ander minderjarige tonen. Dit om de hormonen in bedwang te houden. En bij onze zuiderburen is wandelen met mp3-muziek in je oren binnenkort verboden.

Na deze opsomming zal zelfs de meest gezagsgetrouwe lezer van security.nl wel begrijpen dat een tsunami aan ge- en verboden niet helpt voor respect voor het Gezag. Zeker als je er niet bij hoort welke maatregelen uiteindelijk doorgevoerd worden en welke niet, wordt de verwarring compleet. Genoeg van bovenstaande heeft het uiteindelijk niet gehaald, blijkt als je even doorspit. Maar wat wel en wat niet? Het lijkt niet uit te maken in Den Haag - de persoon die de maatregel heeft geroeptoeterd heeft z'n mediamoment gehad. En daar gaat het kennelijk om.

Wat kunnen we nog meer leren van de overheid? Voor de geloofwaardigheid van de regels is het cruciaal dat ze 'zonder aanziens des persoons' gelden - het rechtvaardigheidsgevoel komt anders nogal in het gedrang. Burgers vinden het een vrijbrief om de wet te overtreden als 'de hoge heren' dat ook doen. De schijn dat hoge heren boven de wet staan is snel gewekt.

Dat geldt juist de pijnlijkste dossiers - zoals het tegenhouden van een Irak-onderzoek het gezag van de premier onder druk zette. Dat geldt evenzeer bureaucratische rookgordijnen, zoals de wet Openbaarheid van Bestuur niet meer van toepassing laten zijn zodra een taak 'naar de markt' gebracht is, zoals bij de OV-kaart en het EPD. Het geldt feitelijk alle zaken die als 'onderonsjes' van de old boys ervaren worden, zoals de 1 miljard teveel betaalde vergoeding aan specialisten die uit 'netheid' niet teruggevorderd wordt, van de grote steun aan banken die altijd al goed waren met Den Haag, en de minister die als bestuurder medeverantwoordelijk was voor fraude maar wegkwam met 'het niet weten', tot de omstreden huurpenningen van de burgemeester van Utrecht. Het is niet dat burgers dit alles een directe vrijbrief vinden om de wet aan hun laars te lappen, maar het draagt wel bij tot een negatieve houding naar het gezag en haar vertegenwoordigers. En de zichtbare gezagdragers, die met een uniform, merken dat het meeste.

De lessen van de landelijke politiek over respect voor het gezag voor ons als professionele beveiligers zijn zo te zien bovenal lessen van hoe het niet moet. Wat we kunnen leren is:

Een: Wees Volwassen. Als je mensen als kleuters behandelt, zullen ze zich als kleuters gedragen.

Twee: Actie is Reactie. Repressie van onwenselijke zaken door sancties leidt alleen tot de gewenste resultaten als je meer kunt escaleren dan de andere kant. Vraag je af of je dat wilt.

Drie: Alleen Raak Slaan. De geloofwaardigheid van je beleid is afhankelijk van de daadwerkelijke uitvoering van aangekondigde sancties. Als je op overtreding van beveiligingsbeleid sancties wilt zetten, heb je een beperkte set aan mogelijkheden. Naming and shaming (met naam en toenaam noemen van daders) en ontslag zijn zo ongeveer de enige juridisch houdbare sancties. En dat alleen nog na goede afspraken met de OR. En na een goede bewijsvoering, wat ook niet bepaald eenvoudig is.

Vier: Wees Rechtvaardig. Sancties zijn gelijk voor alle personen in en rond je organisatie. Ontsla je de directeur-eigenaar of die dure specialist die je net voor veel geld hebt binnengehaald? Krijgt eigen personeel een berisping waar de uitzendkracht en de ZZP-er naar huis worden gestuurd?

Vijf: Minder is Meer. De geloofwaardigheid van je gezag is afhankelijk van het draagvlak van de maatregelen. Als je een enorme waslijst van ge- en verboden hebt, is de kans groot dat je draagvlak voor het geheel van maatregelen gering is. Als vrijwel iedereen dagelijks regels overtreedt ('idiote regeltjes'), dan zal uiteindelijk geen enkele regel nageleefd worden.

Zes: Communiceer! Mensen willen je verkeerd begrijpen, het is aan jou om dat te voorkomen. Er wordt meer gehandeld naar de eigen interpretaties van al dan niet ingevoerde regels, dan naar je doorwrochte document.

Zeven: Houd Koers. Als je de indruk wekt door incidenten gedreven maatregelen uit te vaardigen die na een tijdje vanzelf weer verdwijnen, zal niemand je serieus nemen.

Het verschil tussen angst en respect voor gezag is doorslaggevend. Gezag op basis van sancties is autoritair, gezag op basis van draagvlak is het cement van een bedrijf of een samenleving. Als je weinig kan met sancties (moeilijke handhaving), dan is de weg van respect de enige weg. Nut en noodzaak, overlast en proportionaliteit van de regels moet kloppen. De conclusie is: zorg voor weinig regels, duidelijke regels, begrijpelijke regels en aanvaardbare regels.

Duizend bloemen snoeien

maandag 21 september 2009

ICT-ers zijn recht in de leer. Gelijke monniken, gelijke kappen. Alle servers moeten bestaan uit dezelfde bouwstenen en iedereen moet dezelfde muis hebben. De hele organisatie moet draaien op identieke hardware met volledig gestandaardiseerde besturingssystemen en software. En waarom? Omdat dat goedkoper is, en veiliger. Laat je duizend bloemen bloeien, dan krijg je een onbestuurbare chaos.

Dit gelijkheidsideaal neemt grootschalige proporties aan. Alle pc's moeten op hetzelfde platform draaien. Wil je naar Windows 7? Driewerf Neen, dat mag pas als we de hele firma doen en dat kan misschien al in 2014. Wil je een Mac of, godbetert, een Linux: mag niet. Twee verschillende database engines? Taboe. Iedereen moet hetzelfde draaien, anders "kan de helpdesk het niet ondersteunen." Dat is natuurlijk een kulargument - zo lang je maar een voorziening hebt om de desktop remote over te nemen, lukt het prima. De meeste helpdeskmedewerkers zijn echt niet zo volslagen debiel als we graag geloven en kunnen daadwerkelijk overweg met twee verschillende Microsoft platformen. En wat dit met servers te maken heeft snap ik al helemaal niet - bij een serverstoring bel je toch niet de eerste lijn om te vragen of ze boel remote kunnen oplossen?

Veiliger is het ook al niet: door de 'rationalisatie' draaien servers en PC's 'bouwstenen' die niet nodig, maar wél aan te vallen zijn. Omdat ze niet gebruikt worden, valt het ook niet op als er iets stuk is door een aanval. In de praktijk blijkt vervolgens ook nog dat tóch ieder stuk ijzer anders ingericht is. Het netto resultaat is dat het beheer juist duurder wordt door 'consolidatie'; je onderhoudt een fictief standaardplatform bovenop de echte servers waar meer software opstaat dan nodig is, en die dus meer storingen hebben en ook nog meer beveiliging vragen. Immers, wat er in zit, kan stuk.

Vergeet niet dat monoculturen zoals die door consolidatie ontstaan een veel groter aanvalsoppervlak vormen - de reden dat er meer virussen zijn voor Windows dan voor andere besturingssystemen is een overtuigende demonstratie van dit mechanisme. Consolidatie leidt bovendien tot een onmogelijk regressietestvraagstuk: als je een update wil testen op de bouwsteen 'standaardserver-besturingsysteem' moet je alle varianten die je uit hebt staan, testen. Dat is heel veel werk en dus heel duur. En dus laat je dat op enig moment maar zitten. Met als gevolg dat je ongeteste changes in productie uitvoert, of de updates niet installeert. Beide gevallen leiden tot een sterke toename van de onveiligheid en afname van de beschikbaarheid.

Het meest kostbare is echter opbouw en onderhoud van de bureaucratie die de dubbele taak heeft iedereen naar de standaard te dwingen en bewijzen weg te moffelen dat de standaard niet bestaat. Daar heb je wel een paar hoogbetaalde productmanagers voor nodig, geholpen door een paar ingehuurde **academische theoretici**.

Ja, maar al die verschillende software maakt het beheer zo duur. Als het bedrijfseconomisch verantwoord is om 23 verschillende tekstverwerkers te gebruiken en de IT-afdeling betaald wordt, wat maakt het dan uit? Wie betaalt, bepaalt. Ja, maar dan wordt het te móeilijk voor de mensen die het moeten beheren. Gut, dat kan natuurlijk niet - we forceren de IT-ers aapjes te worden en vervolgens minimaliseren we het aantal trucjes dat ze kunnen doen. Als je het geld dat je bespaart door niet neurotisch te standaardiseren, gebruikt om je IT-ers meer te betalen, kun je veel slimmere mensen neerzetten.

Ja maar, hoe moet het dan met updates als je allemaal verschillende sofware draait? Nou - ieder besturingssysteem en grote applicatie sinds 1998 haalt zelf z'n updates van het Internet op en dat kun je ook binnen je netwerk toestaan. Ja maar, dan kun je geen volledige garanties geven dat het systeem stabiel is, omdat je niet alle patches zelf getest hebt. Dat argument is folklore: dat kun je evenmin van de systemen die je wel centraal patcht, omdat je voor je er erg in hebt een volledig service pack achterloopt, een minor patch gemist hebt en niet doet aan regressietesten. Ja maar, hoe kun je garanderen dat de updates niet van een onbetrouwbare server gehaald worden? Welnu, als je DNS zó onbetrouwbaar is, heb je ergere problemen dan waar je patches en updates vandaan komen. Ja maar, als je al die smaken systemen hebt, hoe moeilijk wordt het dan wel niet om door de audit te komen? Dat lijkt een sterk argument. Maar in mijn boekje zijn systemen er voor de gebruikers, niet voor het gemak van de auditor. De tijd die auditoren beschikbaar hebben, bepaalt de bevindingen, niet de mate van standaardisatie. Beschouw de opmerking dat ze meer tijd nodig hebben om tot een goed oordeel te komen als een zelfverlengingsverzoek van een inhuurkracht, en je hebt het binnen de juiste proporties gebracht.

Ik denk wel eens dat al het ge-jamaar komt omdat we het onmogelijke vragen. En da's handig, dan kunnen we ons niet bezig houden met het mogelijke.

Het gelijkheidsstreven is overigens al zo oud als de ICT. Iedere organisatie van enige leeftijd heeft om de zoveel tijd weer een consolidatieproject; We gaan de Wildgroei Terugsnoeien. Zo'n project krijgt dan een krachtige naam als GRiP (maakt niet uit waar de letters voor staan), Complexiteitsreductie of BiC (Business in Control). Een naam die duidelijk maakt dat je voor eens en voor altijd in control komt. Met een uitspraak als "Betere beheersing en sturing is noodzakelijk" laat je immers iedere professioneel bestuurder soppen in zijn bureaustoel. Kostenreductie en hogere veiligheid door vereenvoudiging klinkt heel overtuigend en je hebt wel heel stevig management nodig dat hier niet in meegaat. Sterker nog - een manager die zich kan onderscheiden door zo'n project mogelijk te maken, is al vrijwel verzekerd van een promotie zodra de kredietcrisis over is. Maak als beginnend manager alleen niet de fout dat project daadwerkelijk te leiden, want gegeven het te verwachten rendement - geen - heeft dat het tegenovergestelde effect op je carrière. Je meer ervaren collega's weten dat al járen.

ICT-Security is ook overtuigd aanhanger van het gelijkheidsideaal. En minstens even goed in ja-maren. Zo roepen we dat een netwerk met al die verschillende software niet te beveiligen is. Het is toch vreselijk als er drie Officeversies naast elkaar gebruikt worden; levensgevaarlijk! Drie verschillende webservers? Oh, gruwel!

Het is inderdaad onveilig. Zo lang we ons druk maken over beleid maar ons niet wagen aan handhaving, niet beter patchen dan nu, geen idee hebben welke software er draait in ons serverpark, niet zoneren, en alleen inbound verkeer een beetje filteren, om er maar een paar te noemen, blijft dat zo. Wie kan er ingrijpen op de perimeter om bepaalde gevaarlijke content tijdelijk buiten te sluiten, als een bepaald gat in onze systemen aanwezig is? En "kan" heeft hier de dubbele dimensie: het gaat om technisch kunnen en organisatorisch kunnen. Wie kan erdoorheen krijgen dat voor onbepaalde tijd alle bestanden in PDF, Word en Excel tegengehouden worden? Standaardisatie van hard- en software is écht niet ons grootste probleem - het probleem is dat wij struikelen over de eerste drempel.

Dit gelijkheidsideaal leidt tot taferelen die dolkomisch zijn, behalve als je beseft wat het kost en hoe weinig het oplevert. Andere organisaties houden zich natuurlijk niet aan onze interne standaarden en doen het dus verkeerd. Zo moest ik ooit twee ministeries aan elkaar knopen en de eerste indrukken waren dodelijk - wederzijds. Hoewel hetzelfde formele beveiligingsniveau gold, liepen de interpretaties ver uiteen. "IK ben méér Departementaal Vertrouwelijk dan JIJ!" Deze gordiaanse knoop werd door het hoger management hardhandig doorgehakt - we voldoen allebei

aan dezelfde veiligheidseisen, dus ophouden met dat gezeur; het is veilig omdat wij dat zeggen. En strikt genomen is dat juist - niemand weet wat op dit moment veilig is, wat morgen veilig, of wat veiliger dan een ander is. Het is geen zinvolle discussie. Maar er wordt nog steeds nagesputterd. En het is inmiddels al heel wat jaren geleden.

Standaardisatie is voor beveiliging geen absolute must, maar het wordt wel zo gebracht. Dat geldt niet alleen het desktop OS, maar bijvoorbeeld ook RBAC: we stoppen gebruikersrechten in zo min mogelijk groepen en leggen iedereen op om dezelfde spullenboel op dezelfde manier (lees: "Business Roles") in te zetten. Maar je kunt best meer rollen dan gebruikers hebben - het is maar een administratieve container dus wat maakt het feitelijk nou uit? Inderdaad - het óógt minder overzichtelijk.

De valkuil is dat standaardisatie gevoelsmatig betekent dat het eenvoudiger is en dus goedkoper. Dat kan wellicht in een theoretisch geval zo zijn, maar een niet-passende standaard is niet eenvoudiger, dus ook niet goedkoper. En het is zeker geen panacee tegen alle kwalen.

Dezelfde merkwaardige toestanden zie je bij virusscanners: we willen maar één antivirusproduct voor alles. Dan moeten we dus 'de beste' scanner hebben. Tja, we zouden onderhand kunnen weten dat de één wat beter is in het vangen van virussen op de mailserver, terwijl de ander beter is in webbased trojans en de derde de meest gemiddelde mix bevat voor de desktop. Dat de Unix versie anders werkt dan de Windows variant. Een gemengde strategie is aantoonbaar beter. En ja, minder werk - bij minder infecties hoef je minder op te ruimen. Standaarden om de standaarden is kolder. Bedenk je heel goed dat consolidatie zeer gevoelig is voor de wet van de afnemende meeropbrengsten.

Het is frappant dat we nog steeds teleurgesteld zijn als onze plannetjes en normpjes door mensen buiten ons machtsbereik volkomen genegeerd worden. Dit zullen we in de toekomst nog veel meer gaan zien - we krijgen steeds meer te maken met mensen buiten onze eigen organisatie die zich niets aantrekken van onze interne standaarden. De genetwerkte economie en gesourcete ICT staan daarvoor garant.

Wat de praktijk van meer dan twintig jaar consolideren ruimschoots aantoont, is dat duizend bloemen snoeien mogelijk is, maar dat de kosten niet dalen en dat het niet veiliger wordt. Ook niet op de langere termijn. Nu kun je het nog wel harder proberen, maar als aspirine niet helpt tegen een gebroken been, moet je gaan nadenken over een ander medicijn.

Sidewikispam

zondag 18 oktober 2009

Google heeft weer een nieuwe leukigheid: de Google Toolbar biedt sinds kort sidewiki. Daarmee kun je bij een willekeurige webpagina je eigen opmerkingen plaatsen en stemmen op de opmerkingen van anderen. Dit doe je niet anoniem, maar op basis van je Google profiel. Sidewiki maakt gebruik van een algoritme en gebruikersbeoordelingen om de volgorde te bepalen van de artikelen die in de zijbalk worden weergegeven. Naast stemmen kun je ook 'misbruik melden'. Google belooft na een melding zo snel mogelijk te kijken of de melding terecht is en indien nodig maatregelen te treffen. Wil je een tekst plaatsen via sidewiki dan moet je je eerst akkoord verklaren met de gebruiksvoorwaarden.

De afgelopen week heeft een aantal mensen heel erg hun best gedaan om de eerste te zijn met opmerkingen bij de grote websites. En ja hoor, ik ook. Ik was de eerste bij nu.nl, het ministerie van Defensie, de PVV, de KLM en het CDA.

Bloggers maken zich zorgen over deze ontwikkelingen. Jeff Jarvis, auteur van "What Would Google Do?", voert de aanval op sidewiki aan met de stelling dat dit een poging van Google is blogs en Web 2.0 te monopoliseren. Hij twijfelt aan het vermogen van Google om tijdig alle zeer onwenselijke content te verwijderen. Bij microsoft.com zie je al een interessante discussie: heeft Google de oorlog verklaard aan MS?: "It seems inconceivable to me that I can place a comment against Microsoft's website and exploit all of its marketing dollars and user base"."Competitors will snipe each other's websites." Bij foxnews staat bovenaan: "Indoctrination!" Waaronder Foxnews wordt betiteld als een extremistische propagandamachine. Op twee staat het bericht dat foxnewskijkers van alle nieuwskijkers het slechtst geïnformeerd zijn. Sidewikispam is dus gearriveerd, vrijwel op hetzelfde moment als sidewiki zelf. Hoewel Google het natuurlijk verbiedt[20].

Wat kun je hier als webmaster of bedrijf tegen doen? Kun je die sitebekladders aanklagen of zo? Strikt genomen bekladden deze spammers niet je site zelf, maar een laagje ervóór. Dus de normale juridische kaders gaan je niet helpen. Ook niet als er gevoelige informatie bij je site geplaatst wordt - beursgevoelige informatie, de naam van je minnaar, of je tien grootste missers? Het heeft veel weg van domein squatting. Maar het is wellicht afwijkend genoeg om niet onder die jurisprudentie te vallen. Dus voorlopig zijn alle website eigenaren vogelvrij.

Nu zijn sidewiki postings niet anoniem - om wat te schrijven heb je een Google profiel nodig. En om zo'n profiel aan te maken heb je weer een e-mailadres nodig. Maar dat lukt prima, zo heb ik zelf vastgesteld, met obscure domeinen en willekeurige mailadressen. En als een profiel verwijderd is, blijft de entry staan. Je hebt dus Google weer nodig om te achterhalen wie je site beklad heeft, met een zeer grote kans dat je er nooit achterkomt.

Wat je bijvoorbeeld kunt doen, als webmaster, is iedereen buitensluiten die Google Toolbar gebruikt. Daar zijn al **handleidingen** voor. Maar of je dat wilt is iets anders. Hoeveel mensen ontneem je dan tegelijkertijd de toegang tot je reclame-uiting?

Wil je zien wat anderen tegen je site aanplakken, dan moet je de Google Toolbar installeren. Die is gratis, dus dat is het probleem niet. Bovendien, als je beheerder bent van een domein, kan je je

[20] http://www.google.com/support/toolbar/bin/answer.py?answer=157295

eigen sidewiki-artikelen toevoegen aan je site. Deze artikelen worden groen gemarkeerd bovenaan de sidewiki-zijbalk weergegeven, boven alle andere artikelen. Een simpele oplossing voor sidewikispam is dus een lange tekst toevoegen - de meeste mensen houden immers niet van scrollen. Een simpele oplossing. Maar wel eentje met een belangrijk nadeel. Want dan moet je wel de Google Toolbar inclusief de 'enhanced features' enablen. De enhanced feautures bevatten (natuurlijk) een uitgebreide Phone Home - Google wil immers bovenal weten waar je heen surft. Webmasters zijn een zeer belangrijke doelgroep die Google goed in de gaten wil houden.

De Google Toolbar regelt dat keurig: als je de enhanced features een keer activeert, kun je hem alleen per browsersessie uitschakelen. De volgende keer staat ie dus weer aan. Dat gedrag kenden we al van Pagerank, een andere feature voor de webmaster. De weg van de minste weerstand bij de webmaster leidt dus tot weer een heleboel zeer gerichte tracking informatie voor de adverteerder. Nu kun je natuurlijk een browser op een USB stick gebruiken die alleen voor alle Google zaken is, maar dat is extra werk en dus extra kosten. Laat je je daartoe chanteren?

Wat ik niet heb kunnen vinden is wat ik het beste zou vinden: een opt-in voor webmasters. Zelfs een opt-out mogelijkheid is er niet. Google laat weer eens zien dat ze altijd op de eerste plaats wil staan, ook bij de **schenders van Privacy**. De reactie hierop sprak ook boekdelen: **volgens** Google heeft privacyinternational.org banden met Microsoft dus zijn de beschuldigingen niet waar. Ach, zoals we vroeger in Ermelo al zeiden: zoals de waard is, stinken zijn kasten.

De Google aanpak laat zich goed samenvatten in: "gebruik onze producten, want anders ...". Nu vond een collega een briljante oplossing - eenvoudig en doeltreffend: sidewiki blijkt niet te werken op een site die https gebruikt. Nu IE bepaalde gratis certificaten vertrouwt, kan je gratis de hele site https laten praten. Dan moet je nog even alle **Google tracking adressen** blokkeren op de PC. Voor Firefox gebruikers gaat deze truc niet werken, NoScript blokkeert weliswaar de Google tracing maar begint te miepen over de gratis certificaten die het niet vertrouwt. Nu zijn deze certificaten ongetwijfeld niet allemaal even betrouwbaar, maar er zijn blijkbaar bedreigingen waartegen je je er wel mee kunt beveiligen. We zijn dus nu zo ver dat je afhankelijk bent geworden van een gat in Microsoft om je te beveiligen tegen Google.

Toekomst van het vak?

zondag 15 november 2009

De Nederlandse ICT-sector heeft al decennialang last van onvoldoende instroom van nieuw, hoogopgeleid talent. Een instroom die de laatste jaren bovendien sterk afneemt. De tekorten aan goed personeel leiden tot een dalend concurrentievermogen van onze economie, falende ICT-projecten, kostenstijgingen, achterstallig onderhoud en offshoring. Terwijl onze samenleving en economie steeds afhankelijker worden van een goede ICT, zijn we steeds minder goed in staat deze te garanderen. In analyses van dit lastige probleem komt één oorzaak telkens terug: jonge mensen kiezen niet voor een ICT-opleiding en ook niet voor een baan in de ICT. Begonnen in 1998 nog 1280 eerstejaars aan een universitaire informaticaopleiding, in 2008 waren dat er minder dan 800. Naar verwacht rondt daarvan net iets meer dan de helft de opleiding af. Over dit probleem luiden tal van clubjes - ICTRegie, IPN, PICTIO en ICT-office om er maar een paar te noemen - de noodklok. En ze hebben een schuldige: het onderwijs.

De reden voor de lage instroom zou zijn dat jongeren geen juist **beeld** hebben van wat ICT is en doet, en wat een baan in de ICT kan inhouden. De jeugd moet leren dat ICT meer is dan programmeren, zeg maar. Zo is er een actieplan, een bekende politicus (staatssecretaris De Jager) en natuurlijk een **website** met een leuk mopje muziek eronder. Op deze site worden aansprekende ICT-oplossingen getoond die de jeugd moeten inspireren.

In het Masterplan ICT, dat is opgesteld door IPN (ICT-onderzoek Platform Nederland) staat dat het informaticaonderwijs op middelbare scholen geen weerspiegeling van het vak is. "Er ligt een sterk accent op recepten voor het bedienen van computers en daarnaast - in het beste geval - op onderwerpen zoals programmeren, computerarchitectuur, databases en besturingssystemen. Dat is voor het jonge publiek niet het meest aantrekkelijke deel van ICT." Het masterplan[21] onderstreept het belang van ICT voor onze welvaart, maar benoemt helaas niet wat dan wél het meest aantrekkelijke deel van het vak is. Wel willen ze 30 miljoen euro van Den Haag.

Nu is het wel erg onterecht om het onderwijs de schuld te geven van de tegenvallende interesse. Voor zover ik het informaticaonderwijs ken, is het niveau hoog en de inzet van docenten en studenten ook. Laten we eerder kijken naar onze eigen bedrijfstak, haar imago en de realiteit, voordat we de schuld van ons af schuiven.

Werken in de ICT heeft inderdaad weinig van doen met de technische zaken die je leert in het hedendaags ICT-onderwijs. ICT-ers bij grote organisaties zijn meer bureaucraat dan techneut, bezig met het volgen van eindeloze procedures, het schrijven van managementrapportages en het invullen van checklistjes. Jongeren die ICT saai vinden kunnen maar zo gelijk[22] hebben. Changeproces coördinator bij een bank is nu niet een functie waarmee je bij het speeddaten positief opvalt, zeg maar. Jongeren hebben dat prima door en zeggen dan ook dat ICT saai is omdat het, let wel, te weinig[23] over techniek gaat.

ICT-opleidingen leiden voor het overgrote deel op voor de gespecialiseerde ICT-functies - beheerders, ontwikkelaars, architecten, consultants. Je wordt er opgeleid tot 'professional', waar de markt inderdaad om vraagt. Het onderwijs levert dus het gevraagde.

---

[21] http://www.ictonderzoek.net/3/assets/File/ICT-plan/Masterplan%20NWO%20DEF2.pdf
[22] http://tweakers.mobi/nieuws/54150
[23] http://www.loketmboict.nl/site/?mode=nieuwsdetail&rasterid=10155&nav_id=13740

Iemand die een beetje het nieuws volgt weet dat dit de groep mensen is die er bij tegenzittende markten het eerste uitvliegt[24], en die geacht wordt dagelijks enkele uren in de file te staan en overuren voor eigen rekening te nemen. En als je daar over wat te zeuren hebt, wordt je fijntjes verteld dat een Indiër jouw werk veel goedkoper en beter kan. Voorwaar geen wenkend perspectief waarmee je een getalenteerde zeventienjarige aan zult trekken.

De toon van het masterplan ICT, dat hoopt mensen te werven met de melding dat ICT meer is dan techniek, is dus helemaal verkeerd. Het onderstreept de minachting van veel ICT-management voor de 'techneut'. Wat jongeren ook niet ontgaan zal zijn, is dat technische ICT-functies een beloningsplafond kennen. De heersende besturingskaste heeft techniek onderaan de voedselketen geplaatst. Een verstandige jongere zal dus voor iets anders kiezen. Iets met management, of zo. Maar daar zijn er al genoeg van, in de ICT.

De innovatieve projecten waar allesis.it mensen mee hoopt te enthousiasmeren zijn evenzeer misplaatst. Je moet al een aantal jaren meedraaien voordat je aan dergelijke snoepjes mag komen, en ze zijn uitermate schaars. De zin van ICT in de praktijk is het uitrollen van een nieuw besturingssysteem omdat het oude ver over de datum is. Of het in de lucht houden van relikwievoorzieningen waarmee mensen naar huis kunnen mailen dat ze iets later thuis komen. Nodig? Soms. Leuk? Mwâh. Het zijn van die projecten die net zo gemakkelijk stopgezet kunnen worden, waar niemand een traan om laat. "En, zoon, heb je dit jaar nog iets nuttigs gedaan?" "Ik heb een projectplan geschreven waarin ik aantoonde dat complexiteitsreductie strikt noodzakelijk is". "Zo, da's mooi". "Maar moeder, het project is stopgezet, omdat ze het te ingewikkeld vonden". "Geeft niks hoor, ik hoorde dat de Albert Heijn nog vestigingsmanagers zocht".

De ICT is ook de bedrijfstak waar je het snelst afgedankt wordt - in welke andere bedrijfstak ben je met 35 al afgeschreven? Is dat wat ICT-office bedoeld[25] met dat "de arbeidsvoorwaarden behoren tot de meest vooruitstrevende van de Nederlandse economie?".

Er zijn al heel wat jaren veel mensen in de ICT aan het werk die in hun directe omgeving vertellen hoe het werkelijk is. Dat noodzakelijke vernieuwingen continu worden uitgesteld en knellende problemen standaard naar de toekomst worden verschoven of uitbesteed. En dat het balletje-balletje met echte incidenten op managementniveau tot grote kunst is verheven. Ik denk dat de jeugd een veel beter beeld heeft van wat de ICT is en doet, dan de digibete managers en beleidsmakers van de lobbyclubjes. En dat is nu nét de reden dat de jeugd er massaal niet voor kiest. Het daadwerkelijk echte belang van de sector voor de Nederlandse economie verdient een betere lobby dan deze. In ieder geval één die niet denkt mensen met leugens een carrière in te kunnen lokken.

[24] http://computerworld.nl/article/454/meeste-ontslagen-in-ict-sector.html
[25] http://www.ictoffice.nl/Files/TER/Samenvatting_actieplan.pdf

Kilometerheffing lijkt fraudegevoelig

vrijdag 27 november 2009

Gaan we echt rekeningrijden? Minister Eurlings verdedigt zijn voorstel, voor- en tegenstanders komen aan het woord. Opvallend was het punt van kritiek van de Raad van State. Volgens de raad ademt het voorstel een 'sfeer van onfeilbaarheid van de techniek' die niet onmiddellijk wordt gedeeld. Wellicht dat de Raad van State enige analogie ziet met andere mega-ICT projecten, zoals de OV-chipkaart die initieel eveneens als onfeilbaar gepresenteerd werd en inmiddels storingsgevoelig en lek blijkt.

Kan het kastje voor de kilometerheffing ook falen? Ik besloot tot een mini-beveiligingsonderzoekje. Vooropgesteld: ik heb zo'n kastje niet. Het is dus vooralsnog alleen een literatuuronderzoek. Enkele geïnteresseerde vakbroeders stonden mij hierbij belangeloos bij.

Relevant is het wel, vind ik. Gezien de bedragen waar veel Nederlanders voor geplaatst worden (motief) en het feit dat iedereen straks toegang heeft tot een KMH-kastje (mogelijkheid), moet een beveiliger immers oppassen. De besparing kan voor een hacker leuk oplopen. In tegenstelling tot 'gewone' hackacties kun je in dit geval heel gemakkelijk je technische vaardigheden in geld omzetten. Ik rijd elke dag over de A2 bij Utrecht, met een waarschijnlijk tarief van zo'n 17 cent per kilometer.

Dit onderzoek is bovendien leuk en leerzaam; het bouwen van fraudebestendige systemen is voor de vakidioot in beveiliging het mooiste wat er is. En als dat NXP en IBM gelukt is, wil ik heel graag de kunst afkijken. Zo niet, dan heeft minister Eurlings straks wat uit te leggen.

Op de vele online platformen wordt uitgebreid gespeculeerd hoe de financiële bijwerkingen van het rekening rijden te vermijden. Het betoog van de minister dat de meeste burgers minder gaan betalen wordt blijkbaar door lang niet iedereen geloofd. Niet zo gek overigens - diverse belangrijke financiële aspecten zijn niet belicht. Zoals het volgende: zodra de BPM wegvalt, de catalogusprijs daalt, daalt dus ook de bijtelling. Als die 520.000 leaserijders die bijtelling betalen 35% minder bijtelling hebben met ingang van hun volgende leaseauto, zal (met een gemiddelde auto van 25.000 euro en een verondersteld belastingtarief van 42%), de opbrengst van de inkomstenbelasting dalen met 1.365.000.000 per jaar. Dat zal Financiën niet leuk vinden en die zal de regels voor de bijtelling heus met een (spoed)wetje aanpassen. En ook dat (spoed)besluit zal weer een aantal mensen benadelen, die ook weer op zoek gaan naar compensatie. Nu zijn dit soort berekeningen natuurlijk ook heel lastig; dat de economie niet maakbaar is, zouden we sinds het sovjet-experiment moeten weten. Dat verkeer ook onderhavig is aan de wetten van de economie, is blijkbaar nog minder bekend.

Mochten de baten voor de burger niet het niveau halen dat de minister belooft, zal dat voor genoeg mensen gelden als een vrijbrief om te frauderen. Met de BPM was moeilijk te frauderen. Het nieuwe systeem lijkt wat meer mogelijkheden te bieden. Belastingontduiking is ondanks jaren van normen en waarden nog steeds een volkssport. De fraudekans is veel groter dan met de OV kaart - de meeste Nederlanders reizen zelden of nooit met bus of trein, en zwartreizen geldt als een zwaardere fout dan creatief omgaan met de belastingen. Als bepaalde mensen dieper gaan kijken en laten zien dat - en hoe - fraude mogelijk is en de pakkans gering, dan zal er met dit systeem grootschalig gefraudeerd worden. Het is logisch dat er een boel aandacht voor de beveiliging van het geheel is. De leveranciers zijn ook niet de minst ervaren partijen en zij hebben

veel aandacht aan de beveiliging besteed en deze ook extern laten toetsen. Zo wordt er geschermd met een Common Criteria EAL 5+ certificering en dat klopt voor minimaal één onderdeel. Maar omdat een computersysteem zo sterk is als de zwakste schakel, is het geheel maximaal EAL4+. In gewone mensentaal: behoorlijk sterk maar niet beveiligd tegen een lokale aanval. Het is hetzelfde niveau waarop Windows beveiligd is. De externe toetsing is zo te zien uitgevoerd op onderdelen van het systeem. Dat is niet hetzelfde als een toetsing van het geheel; je kunt een schakel vergeten en het kan zelfs gebeuren dat een ketting van louter sterke schakels, toch zwak is. De schakels kunnen immers verkeerd aan elkaar gekoppeld te worden.

Wat hebben we gevonden in ons minionderzoek? Hieronder een korte en theoretische beveiligingsanalyse.

We moesten eerst vaststellen hoe het ding in elkaar zit. Natuurlijk begint de analyse bij de leveranciers. Eurlings zegt dat de leiding bij NXP ligt. NXP meldt vervolgens dat het samenwerkt met het Canadese Skymeter voor rekeningrijden en met Siemens voor het kastje. De samenwerking moet zorgen voor een koppeling tussen NXP's Automotive Telematics On-board unit Platform-chipset (Atop) en Skymeters GNSS-gebaseerde afrekentechnologie. Volgens de partners zal het gezamenlijke systeem voldoen aan de grensoverschrijvende interoperabiliteitseisen zoals voor het European Electronic Tolling System (EETS). Ook bij een experiment van IBM en NXP in rekeningrijden in Leuven[26] wordt de Atop genoemd dus IBM hangt ook nog ergens in de wolk. Het zou immers niet logisch zijn dat NXP meerdere kastjes los van elkaar zou maken[27].

Gerelateerd aan het rekeningrijden is het door de overheid gesubsidieerde "Hightech Topproject" Spits (Strategic Platform for Intelligent Traffic Systems), waarvan NXP de penvoerder is. Hoofddoel van Spits is om een open hardware-upgradebaar platform te creëren voor intelligente verkeerssystemen. Behalve NXP zijn onder meer Catena, Logica, TNO Automotive en Tomtom bij het project betrokken. Dus het kastje is zeer waarschijnlijk op afstand 'hardware upgradebaar'.

Het kastje is een Atop. Atop is niet alleen bedoeld[28] voor rekeningrijden: "With its multiple interfaces ATOP allows a flexible integration in a wide variety of car architectures". Het is dus een 'open platform' met veel meer mogelijkheden. Dat maakt normaliter de beveiligingsuitdaging nog een maatje groter. Zo ondersteunt het kastje ook de E112 functie. Deze functie wordt in de stukken slechts heel zelden genoemd. Het gaat hier om een door de EU verplichte (COM 1999/539) functionaliteit, waarmee een auto automatisch een aanrijding doorgeeft aan de meldkamer, op termijn 'verrijkt' met " a Full Set of Data (FSD) such as blood type, number of passengers, car brand, etc.". Ook een interessant vraagstuk in verband met de privacy.

We lezen verder: "Using the built-in USB, CAN and UART interfaces, ATOP can be integrated into navigation / infotainment systems or connectivity boxes, allowing design teams to focus on integration of the multiple air interfaces". Da's genieten: iedere extra interface is een extra puntje van aandacht voor de beveiligingsonderzoeker. En dan: "To further ease design challenges, the solution provides an industry standard software interface based on mobile JAVA J2ME CLDC1.1 MIDP2.0 allowing safe, flexible and easy integration of customer applications". Het kastje draait blijkbaar op micro java (J2ME) met MIDlets en Thinlets. In meer detail: CLDC 1.1 (base set of application programming interfaces) en MIDP2.0 (de Java runtime environment). MIDP2.0

---

[26] http://leveninleuven.be/2009/07/13/leuven-experimenteert-met-systeem-voor-rekeningrijden/
[27] Naschrift: dit bleek achteraf wél deels het geval te zijn. De java componenten waren toch aanwezig en inderdaad kwetsbaar, zoals NXP bevestigde.
[28] http://www.nxp.com/documents/leaflet/75016563.pdf

betekent UDP/Sockets/Secure Sockets/Server Sockets en seriële poorten, naast ondersteuning voor kopieerbeveiliging voor MIDlet suites.

Nu is er niets mis met Java, al dan niet ingebakken in een kastje of een smartcard. In het smartcard geval zal het IBM JCOP[29] zijn. Java is een prima stukje code, waarmee - zoals met alle code - wel eens beveiligingsproblemen zijn. Er zijn in het verleden al kwetsbaarheden[30] in gevonden en het zou zeer onwaarschijnlijk zijn dat dat de laatsten waren. Zeker gegeven dat het een platform in ontwikkeling is. De enige bij Secunia bekende gaten zijn Highly Critical, en nooit gefixed. Gegeven dat deze in 2004 bekend zijn gemaakt[31] maakt dat het veiligheidsprofiel van J2ME knap beroerd is. Het is natuurlijk niet zeker dat dit oude gat ook speelt in het kastje voor de kilometerheffing of de smartcard. Waarschijnlijk wel, omdat de getroffen bytecode verifier functie wél gebruikt wordt voor de authenticatie van de smartcard, sterker nog, een essentieel beveiligingsmechanisme van de kaart is.

Het Atop kastje wordt dus geactiveerd met een smartcard. Of iedere bestuurder dat kaartje elke dag uit de auto moet halen, of dat de kaart in het kastje blijft zitten - al dan niet in het 'vignet' op de voorruit, roept interessante vragen op. Immers, als je je kaart kwijt bent, zal het kastje niet meer werken. Wat kan een automobilist doen met de (ontvreemde) smartcard van iemand anders? Dat is een hele nieuwe variant op identiteitsdiefstal.

Als je een systeem wilt manipuleren, dan moet je een methode hebben om het systeem te benaderen - een interface. Het ATOP kastje heeft een aantal interfaces nodig. Daarnaast heeft het kastje, omdat het ook in andere rollen inzetbaar is, interfaces die - als het goed is - niet beschikbaar zijn voor de eindgebruiker. Een beveiligingsanalyse kijkt naar al deze interfaces, de functioneel noodzakelijke eerst, om te zien waar er gemanipuleerd kan worden. Maar ook de uitgeschakelde interfaces verdienen enige aandacht, omdat 'uitschakelen' niet altijd goed gebeurt of vergeten wordt, of soms zelfs gewoon niet goed werkt. Alle interfaces moet je minimaal bekijken op in ieder geval de volgende basale beveiligingsfuncties:

1. Identificatie (wie spreekt waarvoor welke interface aan en hoe stelt het systeem vast dat dit alleen door juiste personen/systemen gebeurt)
2. Autorisatie (welke functies mogen door wie via welke interface aangesproken worden)
3. Input Validatie (welke data mag via welke interface binnenkomen en hoe sluit de interface ongewenste input uit)

Het kastje heeft in ieder geval de volgende interfaces waarop je iets zou kunnen proberen:

- Push voor verandering van routeprijzen
- Pull voor validatie bij handhavingspoort
- Push of Pull voor 'afrekening'
- Pull voor extended ritteninformatie
- USB voor de gebruiker om ritteninformatie op te halen
- UMTS/GPRS voor eGPS (downloaden van satellietinformatie)
- UMTS/GPRS voor software updates (SPITS-project)
- Contactless smartcard lezer; NFC (Near Field Communication) voor virtuele SIM-kaarten (dit kan dezelfde zijn)

[29] http://www.commoncriteriaportal.org/files/epfiles/0426_ma1b.pdf
[30] http://www.avertlabs.com/research/blog/index.php/2008/08/11/j2me-security-vulnerabilities-discovered/
[31] http://secunia.com/advisories/12945/

- E112 trigger - een fysieke koppeling naar de airbags om botsingen waar te nemen.
- eGPS - ATOP gebruikt een duaal positioneringsysteem op basis van GSM en GPS samen. Het GPS signaal wordt aangevuld met satellietgegevens via het UMTS/GPRS netwerk zodat er ook een fix te maken is in stedelijke gebieden.
- NFC interface voor RFID "vignet" (op de voorruit)

Het voert een beetje ver om in deze column de drie functies tegen iedere interface aan te houden. Duidelijk is dat de hoofdsmaken GSM, GPRS/UMTS en NAVSTAR GPS zijn.

Kort gezegd: GSM is lek. Heel erg lek. Zoals recent nog eens aangetoond[32] op Hacking At Random, maar al in 1998 door de SIM-kaart kloonactie door de Chaos Computer Club. Daar hoeven we verder geen woorden aan vuil te maken; het verkeer kan onderschept en gemanipuleerd worden.

UMTS/GPRS netwerken maken gebruik van TCP en UDP, protocollen waarvan veel mensen de beveiligingsvraagstukken kennen. De authenticatie van een device op UMTS/GPRS is beveiligd, maar niet sterk (PAP of CHAP[33]), protocollen die al gebroken zijn. Oftewel, ook dit verkeer kan onderschept en gemanipuleerd worden.

Een GPS ontvanger kan een zender normaliter niet authenticeren; de huidige standaarden voorzien niet in een authenticatiemechanisme. GPS III en Galileo zullen wel een dergelijk mechanisme[34] krijgen maar zo ver is het nog lang niet. Er zijn ook andere veelbelovende ontwikkelingen[35] op dit gebied. De huidige stand van zaken houdt echter in dat de primaire protocollen om met de interfaces te spreken op dit moment onveilig zijn, en de issues in brede kring bekend.

Dus als je kunt achterhalen hoe het systeem de informatie krijgt waarin gemeld wordt welke tarieven bij welk stuk weg en tijdstip horen, dan kun je zelf wellicht de prijzen prettig aanpassen.

Het blijkt dat er tal van vectoren zijn. De volgende hebben we nader bekeken:

Onderzoeksrichting 1: de ATOP ondersteunt contactloze en virtuele SIMs. Beide kunnen wellicht gemanipuleerd worden, maar virtuele het beste. Het doel van dergelijke SIM-spoofing zou zijn de informatie van iemand die weinig rijdt 'om te leiden' en voor je eigen veel rijdende auto te gebruiken. Een mogelijkheid is de telefoonlijst aanpassen in de virtual sim van iemand anders, of het vervangen van de fysieke sim. Daarmee kun je een permanente omleiding van de ritteninformatie maken, zodat je de rekening van iemand anders krijgt en als je eigen rittenadministratie kunt verzenden. De eigenaar van de 'gestolen' informatie zal het nooit merken, zo lang je de originele berichten ook doorstuurt. De Mifare SmartMX controller met de FameX PKI accelerator[36] is zo te zien heel goed beveiligd, en is common criteria EAL 5 gecertificeerd, dus misschien kan dit pas als je op een andere manier toegang hebt geforceerd. Het smartcard OS is echter EAL 4+, dus vergelijkbaar met MS Windows 2003, wat in het kort inhoudt dat het niet bestand hoeft te zijn tegen frontale aanvallen. Het fysieke kaartje is dus heel interessant.

---

[32] http://www.scribd.com/doc/18668509/HAR2009-Cracking-A5-GSM-Encryption
[33] http://www.rootsecure.net/content/downloads/pdf/cheating_chap.pdf
[34] http://findarticles.com/p/articles/mi_m0BPW/is_10_15/ai_n6338596/
[35] http://www.openauthentication.org/webfm_send/14
[36] http://www.nxp.com/acrobat_download2/other/identification/smartxa_security_and_pki_controllers_0.18_um_line_card.pdf

Onderzoeksrichting 2: Met een zeer significante footprint in de automotive ontstaat een nieuwe monocultuur met een zeer groot aantal identieke computersystemen. Een aantrekkelijk aanvalsdoel voor virusschrijvers. Een botnet op boordcomputers van alle auto's in Nederland is een interessante gedachte. Java-virussen zijn 11 jaar geleden al gesignaleerd. De enige vraag is welke payload het meest aanspreekt. Gegeven de mogelijkheden van Java is de keuze, reuze!

Onderzoeksrichting 3: manipuleren van het GPS signaal. Alleen GPS storen zal wellicht niet helpen - manipulatie van het ene systeem zal waarschijnlijk een alert triggeren. GPS Spoofing biedt daarentegen meer concrete kansen, mits subtiel toegepast. Er zijn wel mogelijkheden bekend om een GPS een soort intrusion detection te geven, dus het zou mogelijk moeten zijn om deze in het kastje in te bouwen[37].

Onderzoeksrichting 4: manipulatie van het update mechanisme. Het systeem zal, als het werkt zoals dit soort systemen meestal werkt, van een centraal systeem de melding krijgen dat een update beschikbaar is. Vervolgens zal deze update 'ontvangen' worden en automatisch uitgevoerd - je kunt niet de user vragen op OK te klikken, immers. De byte code verifier zal de update toetsen, eventueel nog met een controle van de digitale handtekening van de code. De uitdaging is de identiteit van het 'centrale systeem' te kapen, zodat je gericht de software kunt aanpassen. En dat kan van één kastje maar misschien ook wel van alle kastjes in Nederland.

Naast deze richtingen zijn er nog een reeks andere vectoren voorbijgekomen - zoals het gebruiken van opzettelijk corrupte PKI certificaten om de handshake te manipuleren - die verder uitgewerkt kunnen worden. Ook de logistiek om iedere auto van een gepersonaliseerde kaart met PIN-code te voorzien levert interessante vectoren om te onderzoeken op. Maar dat voert nu iets te ver.

Conclusie
De waarschuwing van de Raad van State dat de technologie onder het rekeningrijden wel eens kan falen, is zeer terecht. Het systeem is gebaseerd op technologie die niet ontworpen is om fraudebestendig te zijn. GPS en GSM kennen geen goed authenticatiemechanisme, terwijl er in het besturingssysteem een zeer kritiek gat zit dat al meer dan vijf jaar bekend is. De nodeloze technische complexiteit, mede veroorzaakt omdat de ingezette apparatuur ook andere functies moet kunnen hebben, leidt tot een groot aantal andere mogelijke aanvallen. Zo te zien is er wel veel gedaan om het geheel te beveiligen, maar omdat in ieder geval een behoorlijk aantal mensen een sterke financiële prikkel zal hebben om het systeem aan te vallen, en de kennis daarvoor niet bijzonder moeilijk te verkrijgen is, is een geslaagde aanval op enig moment meer dan hoogstwaarschijnlijk.

Zonder een echt kastje is het niet mogelijk te stellen welke van de mogelijke aanvalsvectoren succes zullen hebben. Zeker is wel dat het beveiligen van de technische voorzieningen voor het rekeningrijden een zeer grote inspanning zal vergen en zal leiden tot aanzienlijke extra operationele kosten. Omdat het ook goed uitvoerbaar lijkt om niet traceerbare fraude te plegen, zal er ook inkomstenderving voor de overheid optreden. Om van politieke schade maar niet te spreken.

Nogmaals: bovenstaand is een theoretische exercitie. Ik heb geen kastje, en ik heb oppervlakkig gekeken. Misschien kan er een leuke thematische Hackers at Large uit volgen of zo. De mogelijke aanvalsvectoren worden op dit moment vooral bepaald door de fantasie en niet door technische details van de feitelijke implementatie - er kunnen en zullen meer en andere mogelijkheden zijn.

---

[37] http://www.homelandsecurity.org/bulletin/Dual%20Benefit/warner_gps_spoofing.html

Het overgrote deel van deze onbeveiligde infrastructuur is een gegeven, en de makers van het kastje moeten het er maar mee doen. Wij straks ook.

Wij zijn allen Indianen

vrijdag 11 december 2009

In de reacties op mijn column over de fraudegevoeligheid van het kilometerheffingkastje kwam één vraag vaak terug: wat betekent dit voor voor onze privacy? Een goede vraag, want privacy is belangrijker dan een klein beetje fraude – en ook dan best veel fraude.

Volgens Staatssecretaris Heemskerk wordt het debat over privacy in Nederland gedomineerd door **indianenverhalen**: “Nu is de discussie vaak eenzijdig, domineren indianenverhalen soms het debat of blijven terechte zorgen onderbelicht”, zei hij 26 november op het jaarcongres van het Electronic Commerce Platform Nederland in Scheveningen. De indianenverhalen waar de staatssecretaris op doelt zijn "doemverhalen" dat de overheid niet het beste voor heeft met de burger met de kilometerheffing, het EPD, de OV-chipkaart en de slimme energiemeter, zoals Heemskerk stelt. Als hij gelijk heeft, is er reden tot zorg. Dit punt verdient een nadere analyse.

Een rondgang over internetforums en wetenschappelijke documenten leert dat veel burgers de overheid **onbetrouwbaar** vinden, zeker als het gaat om privacy, terwijl politici en bestuurders zichzelf juist heel betrouwbaar achten en bij privacyproblemen vooral denken aan bedrijven die telefonisch hun rommel proberen te slijten.

De hoofdvraag is natuurlijk of het wel indianenverhalen zijn - de essentie van indianenverhalen is dat ze niet waar zijn. Het door de indianen veronderstelde patroon is dat de overheid iedere keer terugkomt op de beloofde waarborgen van de privacy.

Ik wil hier niet ingaan op de vraag of de overheid überhaupt wel het beste voorheeft met de burger. Deze vraagstelling veronderstelt een overheid die optreedt met een doelgerichtheid, effectiviteit en eenheid die zonder precedent is in de geschiedenis. Laten we uitgaan van goede bedoelingen bij het gros van onze bestuurders. De vraag is dan of de overheid daadwerkelijk achteraf de ‘spelregels’ verandert. En de tweede vraag is waarom veel burgers de overheid niet vertrouwen met gevoelige informatie. Het antwoord op deze vragen beantwoordt de vraag waarom er zo veel indianenverhalen worden verteld - en geloofd.

Breekt de overheid haar beloften over privacy? Nee. Alleen spreken burgers en overheid een verschillende taal. De burger hoort iets anders dan de overheid zegt. In het bestuurlijk-juridisch jargon staat privacy namelijk gelijk aan de zorgvuldige omgang met persoonsgegevens, terwijl burgers er veel meer onder verstaan. De burger ziet zichzelf als wezen van vlees en bloed in een samenleving van mensen. De bestuurder ziet de burger als een administratieve abstractie met zorgvuldig te registreren en te onderhouden kenmerken; herkenbaar aan het BSN, woonachtig in een bestuurlijke regio – een subject in een bureaucratische biotoop. En de beloftes over privacy houden dus in dat de informatie in principe voor alle belangstellende overheidsdiensten beschikbaar kan zijn. Maar, let wel: zorgvuldig.

Dit verschil in perceptie is levensgroot. Het verklaart ook waarom de burger het College Bescherming Persoonsgegevens (CBP) een tandeloze tijger vindt, terwijl de politiek er op vertrouwt. De expliciete opdracht van het **CBP** is namelijk het waarborgen van de Wet Bescherming Persoonsgegevens. Niet het handhaven of uitvoeren ervan, welnee, maar een stukje adviseren en een beetje toetsen.

Dit verschil in beleving van waar privacy in de kern over gaat is goed te zien in de Nota “**gewoon doen**” van de commissie Brouwer. Deze commissie schreef in de titel van de nota dat “het gaat

over bescherming van de veiligheid en de persoonlijke levenssfeer” en gaat vervolgens alleen maar over persoonsgegevens in de overheidscontext. Hiermee toont de commissie zich in al haar bestuurlijke glorie. Het rapport maakt zonneklaar dat de overheid meer gegevens zal opslaan en uitwisselen. Dat burgers “erop mogen rekenen” dat overheidsinstanties waar nodig onderling informatie delen. Niemand wil immers dat boeven vrijuit gaan omdat "de instanties" even niet communiceerden. De commissie ziet er vooral op toe dat dit ‘zorgvuldig en transparant’ gebeurt, niet óf dit überhaupt gebeurt. Volgens de commissie staat bovenaan dat burgers mogen weten wat er met hun persoonsgegevens gebeurt, dat er ‘zo min mogelijk informatie’ wordt vastgelegd en dat burgers onjuistheden mogen corrigeren. Evenzeer staat voor de commissie als een paal boven water dat gegevens tussen instanties gedeeld moeten en zullen worden, als het over veiligheid gaat.

Deze nota toont zonneklaar het verschil in paradigma tussen burgers en overheid. Wat impliciet besloten ligt in de nota "gewoon doen", is dat niet geregistreerd worden geen optie is. Dat is blijkbaar zo evident dat het niet eens uitgesproken hoeft te worden. Burgers willen echter niet dat informatie vastgelegd wordt. En al helemaal niet dat die informatie gedeeld wordt. In ieder geval niet die van henzelf, natuurlijk wel die van de buurman die zwart werkt/hennep kweekt/sjachert in hypotheken of vul maar in.

Bestuurders willen de vastgelegde informatie juist efficiënt delen en willen dat op een nette manier doen. Als burger mag je van de bestuurders ook bijdragen aan de datakwaliteit – graag zelfs - en krijg je te horen wie er toegang tot de gegevens heeft gehad. Dat laatste gebeurt natuurlijk alleen achteraf, en mits dat in de protocollen is vastgelegd. En je krijgt te horen met welk doel je gegevens bewaard worden. Mits dat in de werkinstructies staat. En natuurlijk als de uitvoerende instanties zich aan de regels houden, wat **zelden** het geval is. Maar dat zijn bedrijfsongevalletjes waar je niet zo zwaar aan mag tillen. Waar gehakt wordt, vallen **spaanders**. Toch?

Het gros van de burgers wil echter helemaal niet gevolgd worden, ook niet op een nette en zorgvuldige manier door aardige ambtenaren die met een tien geslaagd zijn voor de cursus integriteit. Vrijheid is ook de vrijheid om soms onzichtbaar te zijn, om soms niet mee te doen, om de regels een beetje te buigen – geen geld in de meter bij vijf minuten parkeren, of het grof ’s avonds vast op de stoep zetten, in plaats van tussen 07:00 en 07:30, zoals de lokale politieverordening voorschrijft. Dan staan we namelijk in de file, ja!

Dus nee, mensen willen niet gevolgd worden óók omdat ze zich wel eens niet 100% aan álle regels willen houden. Voor normale mensen zijn niet al die regels even belangrijk of uitvoerbaar, iets wat de bestuurder tegen de borst stuit, omdat de ontkenning van één regel de ontkenning van de regelgever impliceert. Dan is het aanzien van het gezag in het geding. Het naleven van alle duizenden regeltjes heeft niet bij iedere burger de hoogste prioriteit. Zeker omdat de perceptie bestaat dat de ‘hoge heren’ zich ook niet aan de regels hoeven te houden; de meeste gewone mensen vinden dat een ‘hoge dame’ van Buitenlandse Zaken te veel ontvangen geld per ommegaande moet terugsturen - net als zijzelf - en dat een Procureur-Generaal die op tijd op z’n werk moet zijn gewoon op tijd moet vertrekken en niet met zwaailichten aan langs de file over de vluchtstrook mag rijden. Dergelijke anekdotes van een hypocriete overheid zijn immens populair, zeker op allerhande internetfora. Het bevoogdend toontje dat sinds onze huidige premier 'bon ton' is in het Haagse, wordt daarmee zeer effectief ondergraven. En als laatste overweging telt dat niet alle regels even zinvol of uitvoerbaar zijn, hoe goed ze ook bedoeld mogen zijn.

Nog een wezenlijk aspect is de dimensie waarlangs privacy speelt. In de bestuurlijke visie gaat privacy over het spanningsveld tussen burgers en bedrijven. Daarbij moet de overheid de burger beschermen tegen al te opdringerige commercie. De overheid is 'van de burgers' en kan dus nooit

de privacy van de burgers bedreigen. Dit semantische hoogstandje is afkomstig van de bij onze bestuurlijke elite zo populaire gedachtespinsels van **Etzioni** waarover ik al eerder schreef. Deze redenering lijkt als twee druppels water op wat de communistische leiders van de DDR de burgers tot 1989 voorhielden; wij zijn het volk en als je tegen ons ingaat, ben je tegen het volk. En dat mag niet. Waarop de burgers van Berlijn uiteindelijk de apparatsjiks eruit gooiden onder de strijdkreet: "**Wir sind das Volk!**". Waarvan Akte.

De burger maakt echter geen onderscheid tussen bedrijven of overheid als het over privacy gaat. Laat me met rust - daar gaat het om. Als burgers dan toch onderscheid maken tussen bedrijven of overheid, zien ze de overheid juist als een grotere bedreiging voor de privacy dan bedrijven, omdat je de overheid niet kunt boycotten. Voor de bestuurder is dat onbestaanbaar, die is immers overtuigd van zijn eigen goede bedoelingen.

De kloof zie je ook terug in het taalgebruik. Burgers spreken over de **Wet op de Privacy**, bestuurders over de Wet op de Persoonsgegevens. Dat zijn twee heel verschillende werelden. De grondwet definieert het als volgt in artikel 10, lid 1: "Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer". Dat lijkt zowaar een Wet op de Privacy. Echter, de volgende twee artikelen vernauwen het begrip tot de administratieve registratie: lid 2. "De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens". En lid 3: "De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens". Noteer dus even: er is geen wet op de privacy! Er is een lappendeken van regeltjes waar iedere niet-jurist in verdwaalt. En menig bestuurder.

De tweede vraag is waarom burgers de overheid niet vertrouwen met de privacy. Nou, dat is eigenlijk niet zo'n moeilijke. Bovenal heeft de overheid een heel negatief imago dat regelmatig in allerlei onderzoeken bevestigd wordt– als regentesk, **hufterig**, kil en **onverschillig**, hoogmoedig en **overambitieus**, onoordeelkundig en **incompetent**. Dat was lekker zeg, schelden met bronvermelding. De meeste burgers horen bovendien alleen wat van de overheid als ze moeten **betalen**. Dat is geen beste uitgangspositie als je het hebt over vertrouwen. Het vertrouwen in de overheid daalt sinds een plotse **omslag in 2002**, **structureel**. Dat verhoudt zich slecht met een overheid die zich op steeds meer terreinen begeeft, inclusief achter de voordeur.

De overheid versterkt het wantrouwen, juist op het gebied van de privacy, door toe te geven zelf niet te weten wat het allemaal verzamelt of waarom, noch wat wel en niet mag. Dat is te lezen in het onthutsende rapport Data voor **daadkracht** dat de minister van Binnenlandse Zaken in augustus 2007 met zichtbare tegenzin prijsgaf aan de openbaarheid. Het rapport concludeert: 'Aan de normen van maatschappelijke zorgvuldigheid wordt niet voldaan'. En " Aan de eisen van effectiviteit wordt niet voldaan". Daarbij is het 'niet mogelijk inzicht te verkrijgen in de consistentie en de samenhang van die wet- en regelgeving'. Het rapport is door de Minister van Binnenlandse Zaken vervolgens in de **prullenbak** gegooid.

Wat ook niet helpt is dat alle kritische vragen over nieuwe registraties iedere keer terzijde als irrelevante indianenverhalen geschoven worden, of deze nu komt van de Raad van State, de Eerste Kamer of het **College Bescherming Persoonsgegevens**.

Een ander voorbeeld van incompetentie rond privacy dat nogal wat mensen aanspreekt zijn de staatsgeheimen die met een vaste regelmaat precies daar belanden waar ze niet mogen komen. Het adres van Erik O. op de site van **Defensie**, laptops vol gegevens of **straat** of dossiers van verdachte moslimextremisten in de **brievenbus** van hun imam.

Recent hebben we meegemaakt hoe dat gaat met door AIVD-ers aan de Telegraaf gelekte **gevoelige informatie**. Volgens minister Ter Horst is daarmee principieel het staatsbelang geschonden, ongeacht welke informatie er gelekt is. Wat geheim werd gehouden was het falen van het inlichtingenapparaat, waardoor Nederland in een slepende oorlog is betrokken waarvan het prijskaartje en het aantal burgerslachtoffers ook al (staats-)geheim is. Allemaal zaken die voor de burger – als kiezer de baas van de overheid immers - van essentieel belang zijn om te weten. Als het in het landsbelang is de kiezer dergelijke informatie te onthouden is er toch iets heel vreemds aan de hand. En wat zien we vervolgens? Een minister die mokkend de uitspraak van de rechter - die de Telegraaf in het gelijk stelde - ontvangt met **'ik heb toch gelijk'**. Vervolgens meldt een 'toezichtscommissie' de kamer nog formeel dat de minister gelijk had en de rechter dus **fout zat**. Je zou maar zo de indruk krijgen dat de overheid er structureel alles doet om haar eigen falen onder de pet te houden. Dat wekt op z'n minst de schijn dat we alleen het topje van de ijsberg te zien krijgen.

Even zo dodelijk zijn de verhalen over de rampzalige "G**rote ICT projecten**" bij de overheid. De storm daarover onder de Haagse stolp is weer gaan liggen, maar de trackrecord van de overheids-ICT projecten is zeker **niet beter** geworden. In alle discussie rond de registratiedrift is dit een cruciaal element - er is bar weinig vertrouwen bij de gemiddelde burger in de kunde van onze bestuurlijke lagen om een ICT-project groter dan een upgrade van winzip succesvol uit te voeren. Vergeet niet, iedereen kent wel een ICT-er die bij een overheid werkt of gewerkt heeft en die verhalen zijn niet mals. Dus de verwachting is dat de systemen zullen **falen**.

Al met al gelooft menig burger niet dat de overheid in staat is goed om te gaan met gevoelige informatie en dat de bestuurders hun eigen belang boven dat van de burger stellen. Dat geloof blijft, zelfs al zouden het patiëntendossier, het kinddossier, het biometrische paspoort, de OV reisinformatie en de kilometerheffing wél technisch veilig gebouwd kunnen worden. Zelfs al zou een echte Wet op de Privacy op de agenda belanden en het CBP gepromoveerd worden tot een Privacy Autoriteit. Immers, de bestuurlijke overtuiging is en blijft dat informatie-uitwisseling een plicht is. De informatie in de genoemde systemen zal dan ook, op een 'betrouwbare' en 'transparante' manier weliswaar, voor andere doelen ingezet worden. Betrouwbaarheid en transparantie leiden vervolgens via procedure en bureaucratie naar nieuwe bedrijfsongevallen. De indianen kunnen de komende jaren dan ook op een groeiende belangstelling rekenen.

Waar een wil is, staat een hek

maandag 4 januari 2010

De lobbyisten van de media-industrie blijven maar doorgaan met het agenderen van ‘illegaal downloaden’ in politiek **Den Haag**. Ik zet de term tussen aanhalingstekens, want ik vind het een manipulatieve term – downloaden is namelijk NIET illegaal. We trappen er alleen wel allemaal in. Het herrezen **Bits of Freedom** en collega Security.nl auteur Arnoud Engelfriet verrijken de discussie. Zij stellen dat het downloadverbod de meerderheid van de bevolking zal criminaliseren en dat dat niet goed is. Dat ben ik op zich met ze eens. Al vraag ik mij af hoe sterk dit argument feitelijk is – de hele bevolking is immers al lang crimineel: we nemen pennen van de zaak mee naar huis, we geven geen richting aan op een rotonde en we draaien een studenteneditie van MS Office terwijl we niet studeren. Heus, dat mág allemaal niet!

En verder schenden we dus kennelijk het intellectueel eigendom door het downloaden van muziek en films. Wat vooral ontbreekt in deze discussie is het meest essentiële punt: het 'redelijk belang'. Wat dat is? Dat is het belang dat je wilt beschermen. Een belang waarvoor je, om het te beschermen, een vermindering van rechten van anderen acceptabel acht. De staat zet een hoog hek om wat ze belangrijk vindt, en een lager hek om wat ze minder belangrijk vindt. Rond het auteursrecht staan hoge hekken, en de trend is deze nog een stuk hoger te maken, waardoor de mensen nog meer overlast zullen hebben. De nu voorgestelde stap om downloaden strafbaar te maken leidt ertoe dat niemand meer onbespied op Internet kan. En dat omwille van het belang van de rechthebbenden op muziek en films, onder de noemer van bescherming van het intellectuele eigendom.

Ik ben op zich niet zo tegen hekken. De omgang met intellectuele eigendommen moet goed geregeld worden. Maar dan moeten de hekken wel op de goede plaats worden gezet, en enigszins met elkaar in verhouding staan. Dat gaat nu helemaal mis. De muziekhekken zijn veel te hoog.

Een voorbeeld uit een heel andere industrie. Stel, een briljante jonge onderzoekster, in loondienst van een jong en fris farmaceutisch bedrijf, ontdekt het medicijn tegen kanker. Wat zijn haar rechten op het rendement daarvan? Geen enkel. Ze is immers in loondienst. Het bedrijf bepaalt of ze wat krijgt, wat ze krijgt, en hoe lang ze dat krijgt. In de regel zal het best goed geregeld worden - de onderzoekster kan immers nog wel het medicijn tegen AIDS ontdekken. Die moet je binden. Dat is marktwerking.

Het intellectueel eigendom is van het bedrijf, dat bepaalt de wet. Het bedrijf zal het medicijn patenteren, en kan daar dan maximaal twintig jaar economisch rendement van trekken. Patenteren is een ingewikkelde procedure die per land of per groepje landen moet, en het lukt niet altijd. Voor de eigenaren van het bedrijf is de snelste en minst riskante manier om het economisch rendement te incasseren, de rechten zo snel mogelijk te verkopen aan de meestbiedende. Dat zal in deze case een enorm bedrag zijn – zeg een paar honderd miljoen. De partij die de rechten koopt, gaat vervolgens het medicijn uitontwikkelen, testen en op de markt brengen. Na twintig jaar is het alleenrecht op het intellectuele eigendom over, en kunnen de concurrenten een identiek medicijn gaan maken.

Vergelijk de briljante jonge onderzoekster nu eens met een briljant, jong bandje. Om groter te worden dan een regionale doorbraak, gaat de band in zee met een grote, hippe platenmaatschappij. Hoewel er geen sprake is van loondienst, gaat het intellectueel eigendom direct en volledig over naar de platenmaatschappij. Dat staat in de standaardcontracten. Tijdens de onderhandelingen is het bandje de zwakkere partij, dus in de praktijk geeft het de

auteursrechten en de naburige rechten op voorhand op. Het eerstvolgende plaatje knalt wereldwijd naar de eerste plaats en wordt de jaren daarna zo af en toe opnieuw een hit – door reclames, films, noem maar op. Ook volgen er nog een paar succesvolle opvolgers. Kassa!

Muziek valt niet onder het patentrecht, maar onder het auteursrecht en de naburige rechten. Om deze rechten uit te oefenen hoef je niets te registreren of te doen - dat gaat helemaal vanzelf. Organisaties als Buma/Stemra en Sena regelen de geldstroom grotendeels voor je en het enige dat je moet doen is lid van worden, voor een klein bedrag. Deze comfortabele situatie duurt tot 70 jaar na het overlijden van de componist. Daarna houdt het geld op. Of moet je als rechtenhouder gaan lobbyen om de termijn nog wat te rekken. In het overgrote deel van de gevallen gaan deze opbrengsten naar de platenmaatschappijen, en ontvangen de muzikanten maar een schijntje. En anders dan bij een arbeidscontract waar je relatief gemakkelijk vanaf kunt, zoals de onderzoekster hiervoor, zit de band voor jaren vast aan een contract.

Er is daarbij het onderscheid tussen ‘auteursrechten’ en ‘naburige rechten’. Bij muziek is het auteursrecht van muziekauteurs (componisten en tekstdichters) en -uitgevers. Ook bewerkers, arrangeurs en vertalers kunnen auteursrecht hebben. Naburige rechten zijn de rechten van producenten van cd's en andere geluidsdragers (meestal de muziekuitgevers) en van de uitvoerende artiesten. Een dergelijk onderscheid is er bij patenten niet; dergelijke 'uitbatersrechten' zijn uniek voor muziek.

Tot 1995 verviel het auteursrecht vijftig jaar na de dood van de auteur. De Europese Unie heeft daar toen 70 van gemaakt, en in 2008 is de termijn verlengd tot maar liefst 95 jaar. Ik moet het ze nageven - ze hebben zeer kundige lobbygroepen daar in Brussel. Ik denk dat iedere artiest het met me eens is dat een medicijn tegen kanker belangrijker is dan om het even welk muziekje dan ook. De looptijd van 95 jaar voor muziek tegen maximaal 20 jaar voor andere vormen intellectueel eigendom maakt echter duidelijk dat de wetgever andere prioriteiten stelt. De wetgever vindt blijkbaar ieder willekeurig deuntje muziek belangrijker dan een medicijn tegen kanker. Natuurlijk is het waar dat de concurrentie na 20 jaar ook zo’n medicijn kan maken – zodat de levensreddende medicijnen goedkoper worden, in het algemeen belang. Maar dat de uitvinder zo veel minder beschermd wordt dan de muziekmaker, gaat mij veel te ver.

En er is nog meer.

Op overtreden van het auteursrecht staan gevangenisstraffen, overtreders van het patentrecht kunnen hooguit een dwangsom tegemoet zien via een civiele procedure. De wetgever vindt muziek blijkbaar zó belangrijk, dat auteursrechten automatisch zijn, waar patenten pas na een uitgebreide en kostbare procedure geregeld zijn. De bewijslast voor het liedje is daarbij omgekeerd – een maker van medicijnen moet aantonen vernieuwend te zijn, waar de rechtenhouder op muziek zonder enige inspanning automatisch wereldwijd de rechten heeft. Hooguit ontstaan er problemen als het deuntje te veel lijkt op een ander deuntje, of als er al te vrijelijk gesampled is. Dat is blijkbaar minder belangrijk, want dat hoeft niet vooraf aangetoond te worden.

Willen we de zaken terugbrengen naar maatschappelijk te verantwoorden proporties, dan moeten we dus niet soebatten over downloaden, sampling of het live spelen op een bruiloft. We moeten het intellectueel eigendom als één vraagstuk bekijken, in plaats van per juridisch haargekloven deelgebied en per gevestigd belang er wat omheen pappen en nathouden. We moeten intellectueel eigendom in de breedte benaderen. Dan kunnen we conclusies trekken.

Het eerste dat aangepast moet worden is de looptijd. De verlenging van de looptijd van auteursrechten naar 95 jaar zoals vorig jaar door de EU is **bepaald**, moet direct van tafel. Wat een

aperte kolder. Als ik mijn werk goed doe, word ik per uur betaald. Ik krijg niet achteraf nog wat geld als mijn spamfilters of firewalls langer meegaan dan vooraf overeengekomen. En mijn dochter hoeft al helemaal nergens op te rekenen, tegen de tijd dat ze hoogbejaard is. Netzomin moet ik achteraf betalen aan Hitachi omdat mijn versterker het na dertig jaar nog steeds doet, in plaats van de redelijk te verwachten tien jaar. In de normale wereld word je betaald voor het werk, niet voor de opbrengst van dat werk. En dat het in 'de Kunst' anders is, daar kan ik en ieder weldenkend mens wel een stukje in meegaan. Hoewel je ook prima kunt beargumenteren dat een formule speelfilm of een lopende band RnB deuntje gewoon een commercieel product is en dus helemaal geen wettelijke uitzonderingspositie verdient.

De gedachte achter auteurs- en octrooirecht is dat mensen dingen maken om het gewin. Artiesten hebben - gegeven de verschillende invulling - daarvoor blijkbaar meer hulp van de staat nodig dan uitvinders en wetenschappers. Deze moderne vorm van mecenaat maakt duidelijk dat de specifieke wetgeving expliciet niet bedoeld is voor de uitbaters, maar voor de makers van Creatieve Werken. Een galerie is geen Kunst, net zomin als een platenmaatschappij dat is – die horen bij de normale wereld en verdienen geen extra bescherming. Een galerie krijgt die ook niet, maar een platenmaatschappij wel.

Dat het ooit zo gegroeid is, wil niet zeggen dat het tot in alle eeuwigheid zo moet blijven. Natuurlijk is het voor de rechtenhebbenden economisch een drama dat de opnames van de Beatles ooit rechtenvrij worden. Maar wie zijn die rechtenhebbenden? De kinderen en kleinkinderen van Julian Lennon en Beatrice Milly McCartney krijgen geen cent. De rechten zijn van Sony en de erfgenamen van …. **Michael Jackson**. Dit gaat toch helemaal nergens over. Wie denken ze wel dat ze zijn – de Belastingdienst of zo? Dus rechten op muziek of films? Vijf jaar misschien. Tien, hooguit. Maar dat is eigenlijk al te veel als je het vergelijkt met bescherming van ander, maatschappelijk veel relevanter intellectueel eigendom.

Het tweede dat aangepast moet worden, is de overdraagbaarheid van de rechten. Artiesten zijn zelden gehaaide zakenlieden, en de praktijk is dat ze, zo lang ze nog niet heel groot zijn, hun rechten verspelen aan de media-industrie. Waarom denk je dat Paul McCartney niet de rechten heeft op de Beatles liedjes - hij is toch best vaak de auteur. De auteurswetgeving is er toch voor de artiest? Welnu, dat is de wet in de huidige vorm bepaald niet. Follow the Money, en je weet genoeg. Een eenvoudige verbetering van de regels kan zijn dat de rechten alleen tijdelijk overgedragen kunnen worden, voor zeg maximaal één jaar. Wellicht zou het auteursrecht de auteur dan daadwerkelijk helpen.

De discussie moet dan ook niet gaan over welk middel proportioneel is bij de handhaving van de huidige auteurswet, maar over de wet zelf. Die moet uit het strafrecht en met normale termijnen en procedures. Als het geheel tot redelijke proporties is teruggebracht is, kunnen we gaan praten over handhaving.

Hoe lost mijn voorstel het 'illegaal downloaden' op? Nou, als het merendeel van de muziek niet tot in alle eeuwigheid (en laten we wel wezen, 95 jaar komt een eind in de richting van de eeuwigheid) van 'iemand' is, dan is er weinig reden om wel beschermde muziek te downloaden. Het leeuwendeel van het totale aanbod is dan immers rechtenvrij. Wil je dan nog wat verdienen aan de verkoop van opgenomen muziek, dan moet de prijs dalen – fors. Er is immers zo veel gratis goede muziek. Dan moet je concurreren op kwaliteit, net als in de gewone wereld. Zo introduceer je marktwerking in een bedrijfstak die nu één groot door de staat beschermd kartel vormt. Een kartel? Zeker. Waarom denk je dat een cd overal hetzelfde kost? Nee, Neelie had haar karwei nog lang niet af.

Maar hoe moeten muzikanten dan hun geld verdienen? Nou, net zoals nu; met optreden, dat is nu ook al de belangrijkste bron van inkomsten. Zo krimpt het vraagstuk tot haar werkelijke, triviale proporties. Dan kan de overheid haar kostbare tijd besteden aan zaken die wel relevant zijn. Of zo.

De utopie van de maakbare veiligheid

zaterdag 23 januari 2010

Nederland heeft weer een nieuwe volksziekte, vindt D66-er Menno van der Land. Hij doopte de aandoening privacyfundamentalisme. Met deze dooddoener serveert hij de bezwaren tegen nieuwe naaktscanners op Schiphol af. Opmerkelijk, vooral omdat zijn partijgenoten Pechtold en In 't Veld juist pleiten voor meer privacybescherming.

Van der Land zelf vertoont hiermee symptomen van een andere, iets eerder ontdekte aandoening: veiligheidsutopisme. Deze kwaal is **ontdekt** door de criminoloog Hans Boutellier, directeur van het Verwey-Jonker Instituut: "het onhaalbare verlangen naar het samenvallen van maximale vrijheid en maximale veiligheid". De denkfout van het veiligheidsutopisme is het geloof in een maakbare veiligheid.

Het mantra van dit geloof is dat je alles moet doen wat mogelijk is om problemen te voorkomen. Doe je niet alles, dan ben je schuldig als het misgaat. Preventie boven alles, is het motto van de veiligheidutopist, en de eerstverantwoordelijke is de overheid. Ook van der Land toont zich in zijn artikel aanhanger van dit dictum. Waartegen Boutellier waarschuwt: "Veiligheid is een onverzadigbare behoefte en het najagen daarvan kan een obsessie worden".

Op jaarbasis een paar miljard uitgeven om misschien drie levens te redden is voor de veiligheidsutopist een volkomen valide en zelfs onvermijdelijke maatregel. Alle kinderen 24x7 volgen en alle ouders onder staatstoezicht stellen om een kindermoord te voorkomen, ook.

Of ik daar iets op tegen heb? Ik ben toch niet tegen veiligheid? Nou, het is dat je het vraagt want ik zie toch een paar lastige probleempjes.

Allereerst en bovenal is er het probleem de maakbaarheid zélf. Werkt de voorgestelde maatregel überhaupt wel? Helpt het Elektronisch Kinddossier tegen kindermoord? Helpt het EPD tegen medische fouten? Helpt de identificatieplicht tegen geweld op straat? Leidt de legitimatieplicht in ziekenhuizen tot minder medische fouten? (Ja, dat wordt echt serieus **beweerd**). Helpen meer bevoegdheden voor justitie en politie tegen terrorisme? Helpt de inval in Irak tegen de spanningen in het Midden Oosten? Helpen de aangeschafte naakstcanners op Schiphol tegen **bomaanslagen**?. Helpt het Internationaal recht tegen oorlog? Het antwoord is dan: soms, of misschien. Maar meestal is het antwoord: we kunnen niet vaststellen of het helpt. Maar we hopen het wel. Waar vervolgens bij nader inzien maar al te vaak blijkt dat de **maatregel** helemaal niet helpt.

Beveiliging is in de praktijk knap lastig, er is maar al te vaak een groot verschil tussen het doel en het effect van de maatregel. Dus als je privacy inlevert voor meer veiligheid, raak je iets kwijt waar je al dan niet aan hecht, maar de kans dat je er daadwerkelijk meer veiligheid voor terugkrijgt is bijzonder klein.

Het tweede probleem is veel banaler: geld. Beveiligen kost geld – veel geld. Je moet afwegen of het redden van een mensenleven in een vliegtuig meer geld waard is dan het redden van een mensenleven in een thuissituatie, een ziekenhuis of in het verkeer. Je budget is immers beperkt. Meer veiligheid is dus maar afwachten, minder geld is een zekerheid.

Het derde probleem is bijwerkingen. Baat het niet, dan schaadt het niet? Dat gaat bij beveiliging maar zelden op. Iedere maatregel heeft bijwerkingen, die je niet kunt vermijden. De beveiliging

van de één is per definitie de overlast of onveiligheid van de ander. Zo zijn de onderzoeken naar mogelijke bijwerkingen van 'naaktscanners' nog niet afgerond, en zijn er signalen dat er mogelijk een verhoogde kans op **kanker** zou zijn. Los van dit soort directe bijwerkingen: of je vliegtuig nu met jou er nog in terugvliegt **omdat** er een raar pakketje of een verdachte reiziger aan boord is, of dat je drie uur extra moet wachten op een trein, het is overlast. Dat je meer tijd op een vliegveld doorbrengt dan dat je in het vliegtuig zelf zit, met dank aan allerlei voorzorgsmaatregelen, is ook overlast. En als je op ieder vliegveld apart wordt genomen voor extra onderzoek en te maken krijgt met de bijpassende verdachtmakingen en intimidatie, is dat heel veel **overlast**. Je zou het maar zo als onveiligheid kunnen ervaren. Als blanke burger tref je het dan nog, want dan word je niet zo snel gezien als verdachte van terrorisme. Tot de IJslanders aanslagen gaan plegen op Britse en Nederlandse vliegtuigen, in verband met de herstelbetalingen voor Icesave. Het wordt dus nooit voor iedereen veilig.

Het vierde probleem is dat veiligheid voor de een iets anders betekent dan voor de ander. Er zijn verschillende agenda's en verschillende belangen. Zo moet je niet denken dat het bij de luchtvaart alleen gaat om het redden van mensenlevens; de luchtvaart heeft als sector te maken met een grote gevoeligheid voor angst – als mensen bang zijn om te vliegen, dan vliegen ze niet. Geen passagiers is dodelijk voor de luchtvaart. Af en toe een kaping niet.

Een vijfde probleem dat een grote rol peelt is de klassieke **veiligheidsparadox**: hoe meer veiligheid we hebben, hoe erger we een inbreuk daarop ervaren. Dat zie je goed terug in de onderzoeken in ons land – mensen die minder met criminaliteit te maken hebben, voelen zich minder veilig. Dus hoe veiliger we de boel maken, hoe onveiliger we het gaan vinden. En hoe harder we schreeuwen om meer maatregelen. Zo wordt veiligheid een obsessie. En je portemonnee steeds leger.

Het zesde probleem is dat van de afnemende meeropbrengsten. Dit effect zie je goed in het autoverkeer – de invoering van de veiligheidsgordel en de valhelm scheelde enorm veel mensenlevens. Maar de opeenvolgende maatregelen zoals het derde remlicht, voorlichtingscampagnes en opeenvolgende snelheidsbeperkingen hebben steeds minder resultaat, tot er een restcategorie verkeersslachtoffers overblijft die je maar niet weg krijgt, al laat je iedereen in een tank rondrijden. Dat is normaal – er zal altijd een onbereikbare restcategorie overblijven. Toeval blijft immers bestaan, hoe graag je dat ook weg wilt reguleren. En menselijke stupiditeit natuurlijk, dat blijft ook bestaan. Je kunt de menselijke factor in het verkeer zo veel mogelijk reduceren – door technologie. Een hele vette computer met een boel sensoren in iedere auto en geleidende systemen langs iedere weg. Kost ook een lieve duit. Maar onfeilbare technologie zullen ze nooit gaan leveren. Verkeersslachtoffers blijven.

Het zevende probleem is de realiteit van beveiligingsmaatregelen. Je doet wat je kunt. De meeste veiligheidsmaatregelen lossen problemen niet helemaal op, maar maken de kans op problemen kleiner en de gevolgen minder erg. Dit maakt beveiligingsmaatregelen bijzonder gevoelig voor kritiek – ze roeien het probleem immers niet met wortel en tak uit. Een goed voorbeeld hiervan is het Nederlandse drugsbeleid. Critici kunnen altijd roepen dat het gedogen niet helpt – er worden immers nog steeds drugs gebruikt. Het gedoogbeleid heeft tot doel het probleem te verkleinen, omdat volledig uitbannen gewoonweg niet lukte. Om vervolgens te stellen dat dit gedoogbeleid faalde, omdat het drugsgebruik niet volledig uitgebannen is, is erg gemakkelijk scoren. Een even goed voorbeeld is het vuurwerkdossier – ondanks alle beperkende maatregelen begon 2010 met minder ogen en minder vingers. Dan maar helemaal verbieden? De ieder jaar **grotere** hoeveelheid illegaal vuurwerk maakt overduidelijk dat dat niet zal helpen, toch is een pleidooi voor een **totaalverbod** een even vast **Nieuwjaarsritueel** als het schanssprin gen in Garmisch Partenkirchen. Ook hier is Rupsje Nooitgenoeg aan het werk.

Als laatste probleem zie ik de enorme uitbreiding van het taakgebied van de overheid. Waakte Bromsnor vroeger alleen tegen criminaliteit, en was vooral reactief, tegenwoordig moet Oom Agent samen met een groeiend aantal toezichthouders en gespecialiseerde autoriteiten overal tegelijk zijn en alles maar zien te voorkomen. Daarvoor wordt hij voorzien van steeds meer bevoegdheden en technologie. Zo ontstaat een grote en machtige overheid. En ook een heel kostbare. Maar resultaten zijn daarmee nog steeds niet verzekerd. Grote organisaties zijn zoals bekend zelden effectief.

Terug naar de luchtvaart. De bereidheid om met grote bedragen bij te dragen aan de veiligheid van het luchtverkeer is op de keper beschouwd vooral ondersteuning van de economische belangen van de sector. En deze belangen zijn blijkbaar heel erg veel waard, zodanig dat andermans **geld en privacy** geen rol spelen. Vergeet niet dat we de vingerafdrukkendatabase en ons nieuwe paspoort óók omwille van de veiligheid van de luchtvaart hebben gekregen, in het kader van het **ICAO**.

Ja, hoor je dan, terroristen hebben toch een sterke voorkeur voor de luchtvaart en daarom moeten we daar de boel beter beveiligen? Nou, kijk, het ligt wat genuanceerder. De terroristen achter de aanslagen van de afgelopen jaren hadden wel een lichte voorkeur voor vliegtuigen en vliegvelden, maar inmiddels zijn ook ambassades, synagogen, hotels, **oorlogsschepen**, **cruiseschepen**, discotheken (Bali en Berlijn), treinen (Madrid, de Punt), bussen (Londen) en zelfs hele stadswijken (Mumbai) het doelwit geweest. Maar zijn er voorstellen gedaan scanpoortjes te plaatsen op alle perrons, bushaltes en stranden? Niet dus, natuurlijk niet. Omdat de reacties op aanslagen op de luchtvaart veel groter zijn, is dat voor terroristen een reden te meer om dat als doelwit te nemen – het doel van terrorisme is immers niet zoveel mogelijk te doden, maar zoveel mogelijk aandacht voor het politieke doel te krijgen.

Zo gaat inmiddels het grootste deel van de prijs van een passagiersvliegtuig op aan veiligheidsvoorzieningen, en ook de kosten van alle vormen van beveiliging op en rond het vliegen zelf en het vliegveld zijn torenhoog. Het gevolg is dat je nergens zo veilig bent als in een vliegtuig. Wil je een vergelijkbare veiligheid realiseren in bijvoorbeeld een ziekenhuis of in het wegverkeer, dan zou het EPD niet – zoals nu – voor een grijpstuiver in elkaar **geknutseld** moeten worden en zou de maximumsnelheid in de bebouwde kom naar 15 km per uur gaan, op snelwegen naar 35.

Evenzeer asymmetrisch is dat we voor een marginale veiligheidsverbetering in de luchtvaart moeiteloos miljoenen uitgeven waar we dat voor andere, veel beter aantoonbare veiligheid, zoals voedselveiligheid, ziekteveiligheid, milieuveiligheid of oorlogsveiligheid niet doen. Al helemaal niet als dat over dit soort veiligheid in andere landen gaat. Nee, dan soebatten we er liever over of die stuiver niet voor de helft verkeerd wordt uitgegeven of stellen botweg dat je de derde wereld gewoon hun **oorlogen** moet laten voeren omdat dat goed voor ze is.

Deze asymmetrie maakt duidelijk dat het veiligheidsutopisme alleen een paar stokpaardjes berijdt en helemaal niet gedegen met onze veiligheid omgaat. Dat de luchtvaartsector in deze debatten haar eigen belangen behartigt, is logisch. Alleen, dat politici en burgers daar kritiekloos intrappen is onthutsend. Het moment van de veiligheidsobsessie, waar Boutellier voor waarschuwt, is al aangebroken.

Hoe irrationeel dit denken is, zie je ook aan onze eigen Defensie; voor een paar stuivers minder dan het **halve minimum** moet ons land veiliggesteld worden van de ultieme ramp, oorlog. En vervolgens wordt dat geld weggegooid in missies die als primair doel hebben het aanzien van onze vergadertijgers in internationale gremia op **peil te houden** en de **smet van Srebrenica** op de morele superioriteit van Nederland Gidsland te wissen. Om van de voorgenomen aanschaf van

Amerikaanse prestigejagers om maar ‘Atlantisch loyaal’ te zijn niet te spreken. Deze excessen zijn een rechtstreeks gevolg van het gemakzuchtig uit de weg gaan van het relevante veiligheidsdebat door burgers en politiek, zodat minuscule belangen – de status en carrière van een paar kopstukken – de echte belangen kunnen verdringen. Wie weet is ons hele defensiebudget wel weggegooid geld, omdat we ons niet verdedigen tegen wat ons bedreigt. Of omdat we ons niet kunnen verdedigen. Of niet hoeven - maar deze vragen stellen we nooit; uitgaan van een paar bejaarde ‘**hoekstenen voor het beleid**’ zonder er verder over na te denken, is veel gemakkelijker.

Veiligheid is het bewust kiezen voor de best haalbare opties op basis van beperkte financiële middelen en uitvoerbare maatregelen, hoe vervelend en hoe onsmakelijk dat soms ook is. Deze keuzes uit de weg gaan en onze veiligheid overlaten aan belangenclubjes en politieke avonturiers, is levensgevaarlijk. De prijs voor ons vluchtgedrag zullen we op een keer alsnog moeten betalen, en van dat vooruitzicht word ik niet vrolijk. Daarom moeten we zo snel mogelijk afstappen van de veiligheidsutopie en ons afvragen wat we nu eigenlijk het allerbelangrijkste vinden en daar onze aandacht en inspanningen op richten. En dan niet alleen preventief graag, maar pragmatisch en realistisch. Waarbij onlosmakelijk hoort dat we bepaalde risico’s accepteren en maatregelen die niet blijken te werken, intrekken. Vanwege de bijwerkingen en de geldverspilling.

Het speelkwartier is over

zondag 7 februari 2010

Het zal vrijwel iedereen ontgaan zijn: de eerste echte cyberwar is geweest en de Amerikanen hebben gewonnen. En wij ook.

U zegt?
Het gaat mij niet om **Georgië**, **Kirgizië** of **Estland**. Dat waren geen oorlogen. Hooguit hier of daar een lullig conflictje om een paar border routers en een webserver. Het gaat me ook niet om de dagelijkse digitale aanvallen vanuit China op kopstukken uit het internationale zakenleven. Ik heb het over een echte oorlog, met echte doden en veel bloed: de oorlog in Irak.

Ik heb het dan heel specifiek over the **Surge**, het Amerikaanse offensief dat in 2007 de ruggengraat van meerdere strijdende partijen heeft gebroken. Door grootschalige infiltratie en manipulatie van computers en telefoons – de Command en Control van de tegenstanders - bleken de Amerikanen in staat om de voornaamste strijdende partijen uit te schakelen. Niet met kruisraketten en andere high-tech precisie snuffen, die in de praktijk niet precies blijken, maar gewoon met de infanterie. Boots on the ground, die wisten hoe de tegenstanders opereerden, wie het waren en waar ze op een bepaald moment waren of zouden zijn. Ze hebben ook vijandelijke strijders in de val gelokt met nepberichten. Dat geeft phishing een hele nieuwe dimensie. Dit alles met dank aan een stelletje **militaire hackers**. Ziedaar het nieuwe gezicht van Oorlog. Ook de tegenstander is afhankelijk van de moderne technologie, en in plaats van de tegenstander het gebruik van deze middelen te ontzeggen, gebruik je die middelen tegen hem, zo legde **Generaal Petraeus** uit aan het Amerikaanse congres.

Nu kun je objectief vaststellen dat het sinds de Surge nog lang geen vrede is in Irak. Maar het is wel al bijna drie jaar veel rustiger en het aantal slachtoffers is **sterk gedaald**. En dat is al heel wat.

Hoe hebben wij dan gewonnen? ‘Onze jongens’ waren immers al een jaar eerder vertrokken uit Irak. Nou, dat is eenvoudig: als Irak na ons vertrek in chaos ten onder was gegaan, hadden we Srebrenica 2.0 gehad – en zouden ‘wij’ politieke schuld dragen. Met als gevolg dat de reflex om maar door te blijven gaan met moeizame missies nog sterker zou zijn dan die nu al is. Deze reflex

is op dit moment zelfs de voornaamste drijfveer om nog een tijdje in Afghanistan te willen blijven – de overtuiging is dat we niet **mogen verliezen**. Sinds Clausewitz weten we echter dat we – en waarom we – een oorlog die we niet winnen uiteindelijk **altijd verliezen**. Maar goed, het blijkt dat ons land tal van **militairen**, **politici** en **veiligheidsspecialisten** rijk is die het beter menen te weten dan de vader van de **krijgswetenschap**.

De Surge heeft ons een tweede Srebrenica bespaard en dat mag je van mij winnen noemen. Nou beweer ik niet dat onze troepen betrokken zijn geweest bij de Surge of de cyberwar die daarin een doorslaggevende rol speelde, deze capaciteit heeft Nederland (volgens gezaghebbende **bronnen**) immers niet, anders dan een groeiend aantal **andere landen**, met de **VS op kop**. Daarom is de FBI ook al begonnen met het registreren van **IT Security specialisten**. De mobilisatie van onze vakbroeders wordt dus al voorbereid.

Dat cyberwar realiteit geworden is, heeft de grote pers dus niet gehaald. Het verhaal is achteraf in stukjes een beetje naar buiten gekomen. Er zijn ook geen mooie plaatjes van. En, natuurlijk, is zo'n beetje alles geheim. In vakkringen is er echter wel aandacht voor – ook in ons land: **project 2020**, de studie naar de toekomst van de Nederlandse krijgsmacht, opende met een beschrijving van een digitale overval op Nederland in 2020, waarvan de Commandant der Strijdkrachten Fatima Agrid verslag deed. Dit opmerkelijk stukje regie mag er wezen. Defensie heeft het onderwerp ook op de **Strategische Kennisagenda** geplaatst. Ook hebben kopstukken rond oorlog en vrede, zoals professor Ko Colijn, zich gemeld op het gebied van Cyberwar. Maar het is nog allemaal erg pril, en de traditionele wereld is erg sterk. Generaals hebben normaliter meer met tanks en commandostructuren dan met kleddertjes bytes die door glas of de lucht gaan. Ze hebben nog wat tijd nodig om te wennen. Maar als ze gewend zijn - en sommigen zijn het al - komt het moment dat ze met IT beveiligingsmensen willen praten. Die hebben er verstand van, zouden ze kunnen denken.

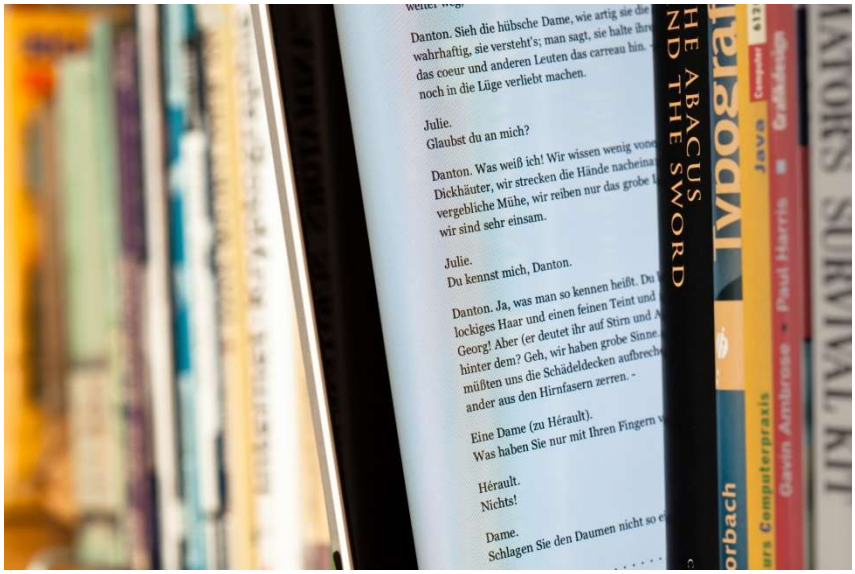
Het cyberwar-vraagstuk is bezig met een doorbraak op de hoofdforums van de internationale politiek: de VN roerde bij monde van Hamadoun Toure op het World Economic Forum in **Davos** één van de meest relevante vragen aan: wanneer is cyberwar een **casus belli**, een aanleiding voor een echte oorlog? Daarbij riep Toure op tot een verdrag, met het expliciete doel escalatie te voorkomen. In dit verdrag moeten landen beloven niet als eerste een "cyber strike" tegen een ander land uit te voeren. John Negroponte, oud-directeur van de Amerikaanse inlichtingendiensten gaf al aan dat zo'n verdrag er niet komt: "intelligence agencies in the major powers would be the first to 'express reservations' about such an accord".

Ook IT specialisten kwamen in Davos aan het woord – zo greep Craig Mundie, chief research strategy officer van Microsoft, de gelegenheid om te pleiten voor een Internet rijbewijs én een Internet APK. "If you want to drive a car you have to have a license to say that you are capable of driving a car, the car has to pass a test to say it is fit to drive and you have to have insurance".

Wat hebben thuiscomputers met niet-gepatchede software en knullige gebruikers in vredesnaam met cyberwar te maken? Duidelijker dan dit had Mundie niet kunnen maken dat hij er geen biet van snapt. De Surge toont aan dat de nieuwe slagvelden mobiele netwerken en slimme telefoons zijn. Dan moet je niet beginnen over rijbewijzen en APK's. Dat is alsof een Security Manager aan tafel bij de CEO, na een miljardenfraude á la Kerviel, over virusscanners begint. Het optreden van Mundie in Davos toont aan dat veel IT-beveiligers nog lang niet klaar zijn voor een plaats in de schijnwerpers. En denk niet dat Mundie, omdat hij van Microsoft is, niets van beveiliging snapt – deze reflex hebben vrijwel alle ICT-ers. Zoals de generaals hechten aan hun tanks en hun vertrouwde werkelijkheid, hangen wij aan onze knusse maar voorbije wereld van virusscanners en patchdinsdagen. Als we niet snel bijspijkeren wordt het een legendarische afgang wanneer we met de generaals aan tafel gaan.

E-readersuïcide

maandag 22 februari 2010



Volgens de stichting CPNB (Collectieve Propaganda voor het Nederlandse Boek) is het gedaan met traditionele boek. Uitgeverijen staan in de rij om met e-books en sexy e-readers de markt te bestormen. Er zijn wel wat kritische noten maar de algemene teneur is dat de digitale toekomst van het boek toch niet tegen te houden is, en dat uitgevers dan maar zo snel mogelijk mee moeten doen.

Laat ik maar met de deur in huis vallen: dat wordt een drama voor de uitgevers. Het is zelfs een suïcidaal idee.

We beginnen bij het begin. E-readers zouden kunnen helpen nieuwe markten aan te boren; die van mensen die het gesleep met dikke stapels papier zat zijn. Vaak wordt hierbij gewezen op het probleem van de ontlezing – wie leest er tegenwoordig nog eens een goed boek?

Nou, dat blijken heel veel mensen[38] te zijn. We lezen meer dan ooit te voren. Het medium papier vormt daarbij kennelijk geen belemmering.

Dat maakt het plan om zo snel mogelijk mee te gaan doen met e-books en e-readers op zijn minst weggegooid geld. Suïcidaal wordt het vanwege de business en de beveiliging, twee zaken die bij digitale content onlosmakelijk met elkaar verbonden zijn.

Eerst maar eens de business. Uitgevers doen twee dingen, selectie en distributie. Ze selecteren welk werk het uitgeven waard is, en brengen dat vervolgens op de markt. Uitgevers zorgen ervoor dat boekhandels regelmatig leuke nieuwe titels hebben.

Als lezen verandert door de voorziene e-reader revolutie, veranderen beide uitgeefprocessen volledig. Uitgevers moeten een volledig nieuwe business ontwikkelen. Nu geeft het feit dat iets op papier wordt uitgebracht, de consument een zekere indicatie dat het geen absolute pulp is – iemand heeft immers een financieel risico genomen om er een uitgave van te maken – redactie, vormgeving, drukken. Online gaat dat radicaal anders. Iedereen die een PDF-je of ePub kan **genereren** kan een boek digitaal uitgeven. Het 'merk' dat een uitgever nu vooral impliciet is, zal

[38] http://www.nrc.nl/W2/Lab/Profiel/Lezen/ontlezing.html

dus expliciet moeten worden. Een uitgever moet een sterk merk worden, met bijbehorend marketingbudget.

Ook de distributie wordt anders. In plaats van met de boekhandel op de hoek, doen uitgevers voortaan **zaken** met Amazon, Sony en Bol. Dat zijn veel grotere partijen, waarmee het moeilijker kersen eten is. De **acties** van Google geven al een voorschotje op deze nieuwe werkelijkheid.

En dan de hamvraag: hoe gaan de uitgevers op hun nieuwe digitale pad geld verdienen? Het commercieel maken van digitale content is tot nu toe nog niemand gelukt – de enigen die er na bijna twintig jaar Internet geld aan verdienen zijn advertentieboeren en juristen.

Advertentieboeren worden niet betaald door de afnemers, maar door de adverteerders die hopen dat de advertenties effect hebben. De juristen verdienen evenzeer een stevige boterham, door rechtszaken te voeren tegen de afnemers, en worden betaald uit de opbrengsten van de rechtszaken. Stichting Brein heeft haar diensten al **aangeboden** aan de uitgevers. Logisch, deze aasgieren werken op provisie – en de verwachting van Brein dat de auteursrechten bij e-books zwaar in het geding komen, is volkomen terecht. Maar rechtstreeks verdienen aan digitale content is lastig. Waarom? Omdat dezelfde content al snel genoeg gratis te krijgen is. Tenzij het goed beveiligd is.

En zo komen we van de business bij de beveiliging. Hoe moet dat, digitale boeken beveiligen? Kraken mag niet, maar gebeurt natuurlijk toch. En dan? Gaan de uitgevers net als de muziekindustrie op voet van oorlog met hun klanten staan? Dat zal niet veel helpen - boeken zijn nu niet direct een eerste levensbehoefte. Kijk naar de muziekindustrie: vroeger kwam het geld vanzelf binnen, nu niet meer.

Andere vragen die opkomen bij de hamvraag over geld roepen ook al associaties op met de muziekindustrie. Voor een deel zijn het dezelfde vragen, die bij het downloaden van muziek ook nog niet opgelost zijn – een omineus teken:

Wat koopt de consument ? Een gebruikersrecht? Verdwijnt dat recht dan met het verdwijnen van de drager, zoals bij muziek CD's, of gaat de uitgever bijhouden wie allemaal rechten op welke boeken heeft? Is een gebruiker een boek kwijt als de e-reader gestolen wordt? Als je als uitgever bijhoudt wie je boeken heeft (en dat gaat vrijwel vanzelf met online transacties) hoe ga je dan om met de privacy van lezers? 'Nee mijnheer de AIVD-er, wij kunnen u écht niet vertellen wie er bij ons het Handboek Terrorisme van O. Bin Laden heeft gekocht.' Ik noem maar wat hoor.

Mag ik een gekocht e-book kopiëren naar een ander apparaat? En, als dat kan, kan dat dan ook naar het apparaat van iemand anders? De standaard van DRM op ePub anticipeert hier al op.

E-readers zijn als verkapte computers ook nog eens erg **beveiligingsgevoelig**: hoe meer snuffen en verbindingen, hoe meer er beveiligd moet worden. En hoe meer beveiliging in tweede instantie niet blijkt te voldoen.

De huidige generatie e-readers is vanuit beveiligingsperspectief heel helder. De beveiliging beschermt de leverancier tegen de gebruiker. Het lijkt vooral op de Trusted Computer (zie **Wikipedia** voor een zeer goede beschrijving) : de gebruiker kan geen dingen doen die niet mogen van de leveranciers. Dat klinkt heel aantrekkelijk, maar ondanks enorme investeringen is Trusted Computing in de praktijk nog steeds een fiasco.

Omdat de e-reader conform 'trusted computing' principes werkt, is het een apparaat dat snel in de kast belandt zodra er een alternatief is met meer mogelijkheden. En dat zal ieder apparaat zijn waar de gebruiker zelf de baas over is. Waarom zou je meer betalen voor iets dat **minder** kan?

Een andere goede beschrijving van de e-reader is: "**met DRM geïnfecteerde Tablet PC**". DRM staat voor Digital Rights Management - kopieerbeveiliging. De niet geïnfecteerde variant zal het uiteindelijk altijd gaan winnen van het zeer beperkte elektronisch hebbedingetje dat toch wel meer dan een paar stuivers kost. En als je er zelf een bestand op wil zetten, kost dat ook weer geld. De Kindle DX heeft een PDF-reader, maar als je jezelf een document van 10MB wilt mailen, kost je dat anderhalve dollar (Amazon rekent 15 cent per megabyte). Dat houdt geen stand. Net zomin als een reader die maar één winkel ondersteunt – anders moet ik straks drie e-readers kopen als ik drie verschillende kranten wil lezen. Ik wil gewoon zelf data erop kunnen zetten - via mijn eigen netwerk of via Internet. Zonder absurde kosten. Het apparaat dat dat kan, dat komt er. Daar kun je vergif op innemen.

De verhalen over de **sterke beveiliging** met DRM worden met veel overtuiging gebracht. De les van IT beveiliging is echter dat iedere lokale beveiliging op enig moment **gekraakt** wordt. En naarmate hetgeen beschermd wordt aantrekkelijker is voor de massa, gebeurt dat sneller. Dat is de voornaamste les van WRM (de media variant van Microsoft DRM) en CSS – de beveiliging van films op DVD. En dat het kraken ervan zwaar verboden wordt, heeft geen biet geholpen.

De beperkingen van de huidige generatie e-readers zijn wel tijdelijk. De leveranciers zijn bezig de e-readers in complete PC's te veranderen: internettoegang, e-mail, films. Als je een cloud-tekstverwerker neemt, ben je helemaal compleet.

Als de huidige minuscule footprint in de markt onverhoopt wordt wat de fabrikanten hopen, krijg je de hele mikmak aan vraagstukken: identiteitsdiefstal, virussen, botnets en dus patches, firewalls en antivirus – you name it.

De geleerde lessen van de PC's worden echter hoogst zelden toegepast. Ook hier niet. Een goed voorbeeld: als je e-reader van een niet noemenswaardig merk gestolen wordt, dan heeft de dief niet alleen je gadget, maar ook meteen je creditcardgegevens en je accountgegevens van de e-bookhandel. Er zit immers helemaal geen lokale beveiliging op. Beetje dom.

De e-reader lijkt al met al niet veel meer dan een gewone IT-hype van het niveau netcomputer en settop box, die over de volgende nietsvermoedende doelgroep is uitgestort.

Wat moeten uitgevers dan wél doen? Gewoon, waar ze goed in zijn; boeken uitgeven. Op papier. Vreselijk ouderwets, ja vast wel. Maar besef dat de belangrijkste beveiliging van de broodwinning van uitgevers bestaat uit het feit dat een boek van papier is. Een boek scannen gaat niet echt snel of zo. Als de audio-CD er niet was geweest, zou de muziekindustrie ook veel minder grote problemen hebben. Ga maar eens een LP digitaliseren en vergelijk dat met het rippen van een CD, dan weet je wel wat ik bedoel. Als de uitgevers nu zelf deze barrière slechten, dan graven ze hun eigen graf. Dan zijn ze nog dommer dan de muziekindustrie.

Stop ACTA

zaterdag 6 maart 2010

ACTA wordt een nieuw handelsverdrag met het doel de regels rond intellectueel eigendom wereldwijd te harmoniseren. De onderhandelingen vinden in het geheim plaats. Uit **gelekte stukken** van het overleg blijkt dat Internet providers in de toekomst verantwoordelijk en financieel aansprakelijk zullen zijn voor alles wat de gebruikers doen. Nederland doet niet mee aan het ACTA-overleg, maar de EU wel. Als de EU akkoord gaat, zal ons land aan dit verdrag gebonden worden. De middelen die ISP's in moeten zetten om hun nieuwe taak uit te voeren zal onder meer deep packet inspection omvatten. Naast dit voorstel zet het verdrag sterk in op de kopieerbeveiliging **Digital Rights Management** en worden sancties geplaatst op het verwijderen ervan. Ook andere middelen om beveiliging te omzeilen, zoals de R4 kaart voor de Nintendo DS, zullen **verboden worden**.

Het stokpaardje van **Brein** is ook weer van de partij: het afsluiten van overtreders van een downloadverbod na drie overtredingen. Dat dit een disproportionele maatregel is, probeer maar eens te e-mailen zonder internet, of je in te schrijven bij het UWV is blijkbaar nog steeds irrelevant.

De maatregelen van ACTA gaan niet helpen. Burgers zullen **cryptografie** of steganografie inzetten om toch aan de DVDRip van Avatar te komen – die screener is inderdaad niet om aan te zien. ISP's zullen de cryptografie moeten breken, willen ze hun verplichtingen nakomen. Bovendien zullen ze het verkeer moeten reconstrueren en analyseren – iets dat zelfs de NSA al **sinds 1999** met al haar rekenkracht en storage **niet** meer voor elkaar krijgt.

Dat versleuteling alle ISP filtering buitenspel zet, weet de media-industrie ongetwijfeld, maar dat maakt ze niet uit. Het zal vast wel een paar jaar hun business model overeind houden. En die paar jaar is blijkbaar al die bijwerkingen waard; failliete ISP's, structureel hogere kosten voor internetgebruik, grotere onveiligheid voor iedereen. Kan niet bommen dat de samenleving instort, als ze hun royalty's maar krijgen.

Samenleving instorten – nou, nou Peter, zo'n vaart zal dat toch niet lopen? Het is toch gewoon de zoveelste zinloze maatregel zoals we de hele tijd zien, die hooguit de privacy van mensen raakt. En dat vinden mensen nu eenmaal niet belangrijk.

Nou nee. Ik heb het niet over privacy; de gewone gebruiker staan genoeg middelen ter beschikking om daar zelf voor te zorgen. Vrijwel iedereen heeft inmiddels voldoende processorcapaciteit, en moeilijk is het gebruik van **cryptografie** nu al niet. Bovendien zullen genoeg proggers dit aanbod van gebruikersvriendelijke middelen gaan uitbreiden, zodat we naar een situatie gaan waarin het leeuwendeel van het internetverkeer **versleuteld** zal worden. En daar zit nu net het probleem.

Al die extra processorcapaciteit kost nogal wat stroom en dat heeft weer invloed op het klimaat. Dat is jammer voor de ijsberen. Om van al het extra ijzer bij de ISP's om het verkeer te bekijken maar niet te spreken.

En het is ook jammer voor allerlei andere beveiliging – je kunt geen virus of spam onderscheppen in versleuteld verkeer. Het internet wordt er onveiliger op.

En het is ook erg vervelend voor de opsporingsdiensten – ze kunnen nu al geen pedofielen, terroristen of criminelen afluisteren als deze lieden crypto inzetten. Op dit moment is versleuteld verkeer relatief gemakkelijk te herkennen, omdat het zich niet laat comprimeren, en het meeste verkeer gewoon leesbaar is. Maar als heel veel mensen crypto inzetten, kun je daar geen verdachten meer aan herkennen.

En tenslotte, maar niet het onbelangrijkste, is dat de ACTA regels weer een boel handhaving oplegt aan de politie die het komende jaren toch al met minder geld moet doen. Omdat er geen mogelijkheid is tot automatische bekeuringen zoals bij flitskasten is de keus wellicht straks om achter een illegale downloader aan te gaan, dan wel op treden bij lichte vormen van mishandeling. Waarschijnlijk werpt de stichting Brein zich dan op als **vrijwillige politie**, dan kunnen ze nog meer lawaai maken.

De samenleving zal niet dus niet direct instorten oké, ik overdrijf dus toch een beetje, maar zeker minder veilig worden.

Nu kunnen overheden proberen terug te gaan naar de tijd van het Wassenaarverdrag, door sterke cryptografie zonder overheidsachterdeur te verbieden. Maar die geest is al jaren uit de fles – dat zal niet lukken. Bovendien wordt cybercrime zonder cryptografie een stuk eenvoudiger: Telebankieren met zwakke cryptografie is echt geen aanrader.

Zodra blijkt dat de ISP als politieagent door de versleuteling kansloos is, heeft de RIAA ook hier al weer een oplossing. Dan moet de PC van de gebruiker maar filteren. Dit idee is in 2008 al door de RIAA baas Sherman geopperd[39]. Omdat mensen dit niet vrijwillig gaan doen, moeten besturingssystemen het maar doen. Dus als de ISP's als politieagent falen, moet Microsoft dit maar doen.

En zo komen we weer uit bij Trusted Computing en DRM. De computerindustrie heeft nu niet bepaald de schouders onder dit concept gezet – logisch ook; als Windows 8 iets niet kan wat in alle oudere versies wel mogelijk is, dan nemen mensen geen Windows 8. Dus Microsoft kijkt wel beter uit. En als net als nu door de EU afgedwongen voor de browsers DRM ook in al uitgerolde versies gestopt wordt, dan wordt het nog interessanter om een niet ondersteund besturingssysteem te blijven draaien. XP? Windows 98?

Ja maar, Linux dan – het hoeft toch niet altijd Windows te zijn? Linux moet verboden worden – je zou immers zelf een distro zonder DRM troep kunnen bakken. En dat mag niet.

Zo zal XP nog veel meer jaren bij ons blijven. Als een nieuwe auto je niet naar je bestemming brengt, maar een 50 jaar oude[40] wel, dan koop je toch die oldtimer. Dat je dan wellicht wat virussen oploopt en je machine in tien botnets tegelijk hangt – zo lang je je films en muziek maar hebt maakt dat toch niet uit? Bandbreedte genoeg.

De politiek en onze ambtenaren laten zich in dit dossier ringeloren. Zo **zeggen** ze notabene bezig te zijn met innovatie en kennisbescherming . Minister van der Hoeven meldde in 2008 aan de kamer dat het "een fenomeen van internationale omvang met ernstige gevolgen op economisch vlak, maar ook op het gebied van de consumentenbescherming, de volksgezondheid en de openbare veiligheid" betreft. Nu moge dit de intentie zijn, feitelijk doet ACTA het tegenovergestelde: het maakt de consument vogelvrij en bedreigt de openbare veiligheid.

---

[39] http://arstechnica.com/old/content/2008/02/riaa-boss-spyware-could-solve-the-encryption-problem.ars
[40] http://security.nl/artikel/32587/1/Microsoft%3A_Windows_XP_is_50_jaar_oude_auto.html

De semantische truc die wordt gebruikt om octrooi-inbreuk, merkenfraude vervalsing en piraterij op één hoop "Intellectual Property[41]" te gooien gaat feitelijk over legale monopolies, waarbij wetgevers over de hele wereld een grote complexiteit van regels hebben gemaakt. Nu is het voor IP-uitbaters veel overzichtelijker om gewoon één regel te maken. Maar dat gaat voorbij aan het waarom van al die verschillende regels. In de rechtstheorie leer je dat wetten gemaakt worden om bepaalde uitwassen die zich daadwerkelijk voordoen tegen te gaan. Dit gaat ook op voor deze regelgeving; er zijn immers grote risico's verbonden aan monopolies, en er zijn grote problemen geweest. Om al deze geleerde lessen omwille van de 'harmonisatie' en de 'globale economie' onder druk van een industriële lobby overboord te gooien, is hoogst riskant.

Ik vind het ook echt een vreemde ontwikkeling; in een tijd waarin we net weer de gigantische risico's van monopolisten dagelijks aan den lijve ervaren (kredietcrisis, systeembanken) zouden we dan weer nieuwe giganten creëren? Hoogst merkwaardig.

De belangen die voor de industrie op het spel staan, zijn natuurlijk enorm; het is erop of eronder. De bestaande bedrijven hebben alle belang bij het in stand houden van de status quo. De economie is echter vooral gebaat bij nieuwe initiatieven; in economenvaktaal creative destruction[42]. Daar is de gevestigde orde natuurlijk niet voor te porren.

De discussie over IP gaat echter helemaal uit van de gevestigde orde. En dat is nooit goed. Stel je eens voor dat Xerox in 1973 de PC, de muis, de laserprinter en het LAN voor 75 jaar gepatenteerd zou hebben. Of dat IBM in hetzelfde jaar het Disk Operating System **gepatenteerd** had – dan zaten we nu nog met groene schermen en zou het Internet SNA draaien. Of – veel waarschijnlijker – alleen een paar universiteiten met elkaar verbinden. Te veel ruimte voor IP is echt catastrofaal voor innovatie.

Het Europese en ons nationale parlement zijn door de ACTA-werkgroep vooralsnog buitenspel gezet. Binnen de politiek bestaat op dit dossier gelukkig nog wel enige **waakzaamheid**. Groen Links heeft het onderwerp **opgepikt** en ook de VVD stoort zich aan de geheimzinnigheid. Het EP vind echter dat het onderwerp haar toebehoort, niet de nationale parlementen. Dat kan gunstig zijn, zoals we laatst zagen met het tegenhouden van de beschikbaarstelling van **SWIFT-gegevens** aan de VS. Je zou er pro-Europa van worden.

Kunnen we dan zelf nog iets doen om de media-industrie op meer realistische gedachten te brengen? Ik denk van wel. Uiteindelijk is de consument de baas; ook het machtige Shell ging bij de **Brent Spar** door de knieën. Maar de media-industrie is wel veel machtiger dan Shell. Stichting Brein en de RIAA zijn daarbij maar organen, niet de kern. Daar moet je je niet op richten.

Hoewel het natuurlijk wel weer leuk is om de Reclame Code Commissie in te schakelen tegen de misleidende reclamecampagnes van Brein, als ze weer eens uit hun nek beuzelen over **virussen** of de jeugd intimideren en **misleiden**. Ze hebben overigens nog een flinke bak geld om de emotionele schade te vergoeden. De toezichthouders hebben al meermalen hun zorgen geuit over het mogelijk op **onduidelijke gronden** verkregen **geld**, wat in de **honderden miljoenen** schijnt te lopen.

Bits of Freedom is – natuurlijk - al **bezig** met ACTA en die kunnen nog wel wat steun **gebruiken**. Niet alleen met geld – ook met daden. Het enige legale dat er voor ons gewone burgers op zit is een totale boycot van alle producten van bedrijven die aangesloten zijn bij of kritiekloos meedoen

[41] http://www.wipo.int/about-ip/en/.%20Intellectual%20Property
[42] http://www.mckinsey.com/ideas/books/creativedestruction/index.asp

met de media-industrie. Geen muziek meer kopen, ook niet online, geen DVD's en niet meer naar de bioscoop.

De industrie zelf is een onoverzichtelijke coalitie met meer en minder **grote spelers** – dat lijkt een moeilijk doelwit. Ze zullen ook niet allemaal even fout zijn en helemaal dezelfde overtuigingen en belangen hebben. Een boycot moet als strategisch doel hebben deze coalitie te breken. Je wilt eigenlijk bereiken dat partijen zich expliciet gaan afscheiden. Breek het front; koop alleen bij partijen die niet meedoen of weer zodra ze zich distantiëren.

Een "Boycot Brein Week" bekt prima, en kan een krachtig signaal zijn. Ik zie al een soort campagne voor me, en uitgestorven platenzaken. Laten we alle maatschappijen en artiesten die afstand nemen van ACTA, de RIAA en Brein voortaan aanduiden als "Verantwoorde Artiesten", en alleen dat nog maar kopen. Misschien kan BoF een keurmerk of zoiets instellen?

Dit zal echter niet genoeg zijn. Via de omroepen en commerciële zenders heeft de media-industrie nog een stevige greep op onze portemonnee. Omroepen zijn echter verenigingen, geen commerciële partijen. Leden kunnen het bestuur dwingen om alleen muziek te draaien van Verantwoorde Artiesten. De publieke media zijn immers van 'ons', niet van de media-industrie. Een beetje tumult hoort daar wel bij. Dus neem contact op met je favoriete DJ. Mail Giel Beelen. Bel Gerard Ekdom. SMS Paul Rabbering – en hun collega's. Tegen de lawaaimachine van Brein is tegenlawaai vereist, en wie zijn daar beter in dan de Jocks van Radio 3?

Misschien draaf ik een beetje door. Maar het is van wezenlijk belang dat ACTA er niet komt, en de tijd dringt. Actievoeren klinkt anno 2010 een beetje kansloos. Als je met een spandoek in de regen op het Malieveld gaat staan, helpt dat inderdaad geen moer. Maar een kopersstaking is een machtig wapen. Onderschat dat nooit.

Tussen spionage en veiligheid

maandag 29 maart 2010

Werkgevers kunnen hun personeel op veel manieren controleren. En dat doen ze ook. Ze willen weten of we niet zitten te lanterfanten, te frauderen of iets anders aan het doen zijn dat niet in het bedrijfsbelang is. Er zijn werkgevers die álles willen weten, om zeker te zijn dat iedere minuut aan productie besteed wordt.

Slavendrijvers uit vroeger eeuwen? Niet meer van deze tijd? Of gebeurt dit alleen bij achterlijke bedrijven zoals de Lidl[43], Deutsche Telekom[44] en de Duitse spoorwegen[45]? Deze drie kwamen in opspraak omdat ze verregaande maatregelen troffen om het eigen personeel te bespioneren. De Duitse rechter achtte het plaatsten van camera's door Lidl "in höchstem Maße skandalös", omdat het over toezicht op het gedrag van het personeel op de werkvloer gaat, niet over toezicht op het werk. Alleen toezicht op het werk is volgens deze rechter toegestaan. Ook beide andere bedrijven zijn teruggefloten. In 2009 ging de Lidl opnieuw in de fout[46], met het bijhouden van geheime medische dossiers van haar personeel. Deutsche Bahn tenslotte heeft toegegeven e-mails van driekwart van haar werknemers, 173.000 man, te hebben gelezen om erachter te komen of er onoorbare praktijken plaatsvonden tussen het personeel en leveranciers van materialen. Eventuele bijvangsten zijn niet gemeld. Die Bahn bevestigde dat het in 2005 personeelsgegevens had vergeleken met die van klanten, om te onderzoeken of er geen omkoping was gebeurd. In februari 2009 leidde dit schandaal tot het aftreden van topman Hartmut Mehdorn.

Helaas, dit soort idiotie bestaat niet alleen in Duitsland. Hoewel er strenge regels zijn, gaat ook hier van alles mis. 'Wij verkopen tussen de vier en tien keer per week spionagesoftware' voor op mobiele telefoons, zegt een medewerker van het Utrechtse filiaal van de Spy Web Shop. Je kunt de telefoon van degene die je wilt volgen bij de winkel inleveren, die de dan de software voor je installeert. Ook verkoopt de Spy Web Shop kant-en-klare spionage toestellen, meestal een Nokia. De medewerker[47]: 'Dan zegt de baas: kijk eens, een toestel van de zaak, alsjeblieft'. Op het toestel heeft de winkel dan de benodigde software gezet. Eén keer een sms'je sturen vanaf je eigen toestel naar het toestel van je werknemer en de twee toestellen zijn aan elkaar gekoppeld. Het activerings-sms'je is onzichtbaar voor degene die wordt afgeluisterd.

En het gaat niet alleen om spionage met telefoons. Zo wilde het UWV een medewerkster ontslaan[48] omdat ze een mailtje wilde rondsturen dat ze geen slingers op haar verjaardag wilde. Na een gerechtelijke uitspraak mocht de medewerkster toch blijven. Dat ze dat überhaupt nog wilde, schetst de kwetsbaarheid van werknemers: ze was vast liever weggegaan, maar elders een baan vinden is geen vanzelfsprekendheid. Je bent als personeelslid bij lange na geen gelijke in dergelijke situaties.

---

[43] http://www.stern.de/wirtschaft/news/unternehmen/ueberwachungsskandal-lidl-gibt-bespitzelung-zu-615031.html?eid=614772

[44] http://www.tijd.be/nieuws/ondernemingen_diensten/Deutsche_Telekom_en_Deutsche_Bahn_bespioneren_personeel.8139494-431.art

[45] http://www.zibb.nl/10259222/Personeelszaken/Personeelszaken-nieuws/Personeelszaken-nieuwsbericht/Boete-voor-bespioneren-personeel.htm

[46] http://www.distrifood.nl/web/Nieuws/Buitenland/Buitenland-artikel/132468/Lidl-weer-schuldig-aan-spionage.htm

[47] http://www.depers.nl/binnenland/355746/Doe-het-zelfspion-rukt-op.html

[48] http://www.intermediairpw.nl/artikel.jsp?id=1392750

Werkgevers mogen hun personeel niet zomaar overal op controleren. Ze mogen bijvoorbeeld niet hun computergebruik registreren, tenzij er een gegrond vermoeden van misbruik is. Bovendien moeten controlemaatregelen van tevoren worden overlegd met de OR, en de werknemers moeten ervan op de hoogte worden gesteld. Als de UWV- medewerkster het bericht over haar verjaardagsslingers gewoon had rondgestuurd, was er waarschijnlijk minder aan de hand geweest.

Tegelijkertijd neemt het aantal middelen dat controle voor werkgevers mogelijk maakt, snel toe. De kans dat ze ingezet worden dus ook. De grens tussen wat wel en niet kan, staat door de nieuwe mogelijkheden ernstig onder druk. Er is een grijs gebied waar angst, reële en minder reële veiligheidsbelangen, managerial machogedrag en nieuwe technologie elkaar ontmoeten. Dat is een mix waar het goed geld verdienen is. Een greep uit het nieuwe aanbod:

1: Bewaking van rijgedrag. Met de nieuwste boordcomputers kan de eigenaar van de auto het rijgedrag van de berijder achteraf analyseren. Dat geldt dus ook de leaserijder, via het leasecontract. De analyse geeft meer informatie dan alleen waar je in het weekend uithangt: "Zooooo, Berend, vorige maand was je drie keer te laat op je werk!" In de voorstellen rond de voorlopig begraven kilometerheffing bleef dit aspect[49] buiten beeld. Dat toont maar weer aan dat zaken eerst mis moeten gaan voor we er aan denken.

2: Camera's op de werkvloer. Populair onder bezorgde ouders is de **nanny-cam**, uiteraard om drama's met kwetsbare kleintjes te voorkomen. De nanny-cam biedt **onzichtbaar toezicht**. Begrijpelijk? Mja, vooruit, enigszins. Bovendien hangt de nanny-cam in je eigen huis. Aan de andere kant: voor de oppas is dat toch gewoon haar werkplek. Zij is ook kwetsbaar: als zij bezwaar maakt tegen de camera's, wekt ze de indruk van kwade wil te zijn: wat heeft ze te verbergen? Zoals Arnout Engelfriet al eens **liet zien**, mag een verborgen camera in je eigen huis niet, maar dan soms toch opeens weer wel. Je bent in ieder geval safe als je het duidelijk aankondigt. Maar als je de nanny-cam onder bepaalde omstandigheden wel vindt kunnen, moet je ook niet klagen als er op je eigen werkplek een camera komt te hangen. En dat mag jouw werkgever doen, als hij een goed verhaal heeft.

3: Proxy monitoring. **Hiermee** kun je zien of medewerkers wel naar zakelijk relevante internetsites gaan. En dat biedt een plethora aan mogelijkheden: zo kun je met speciale alerts op banensites op je personeelsomvang sturen. Er zijn wel regels voor, maar overtreding leidt in de praktijk niet bepaald tot zware sancties. En ook hier geldt dat er omstandigheden zijn waarin een werkgever een redelijk belang kan aanvoeren dat het nodig is; als je personeel veel tijd op sociale netwerksites doorbrengt, kan dat tot schade in het bedrijfsaanzien leiden, zoals de Engelse gemeente Portsmouth merkte[50]. Even doorgerekend: deze ambtenaren zaten gemiddeld 12 minuten per maand op Facebook – schokkend hoor.

4: E-mail monitoring. Ook dit kan vele nieuwe inzichten opleveren. Uit de interne communicatie kun je de officieuze hiërarchie in kaart brengen ('wie neemt er nu echt de beslissingen') en extern kun je zien of er niet voor eigen rekening zaken worden gedaan.

[49] http://www.nu.nl/politiek/2207698/cda-stapt-af-van-kilometerheffing.html
[50] http://carriere.blog.nl/actualiteit-wereldwijd/2009/09/02/luie-ambenaartjes-572-uur-op-facebook-in-een-maand

5: PC monitoring. Hiermee is het mogelijk om te kijken wat een kantoormedewerker verder zoal doet – patience is immers het meest gespeelde[51] computerspel. De webcam en de microfoon geven PC monitoring nog een extra dimensie; een **boss-screen** helpt dus echt niet meer.

6: Bedrijfsrecherche. Een groeiende bedrijfstak, met het 'in de gaten houden' van de medewerkers als core business. Met een meer pessimistisch economisch verwachtingspatroon is de neiging achter interne zaken aan te gaan groter, **stelt** de directeur van Hoffman, de bekendste aanbieder van dit soort diensten. De groei van deze bedrijfstak illustreert dat de grenzen afgetast worden.

7: De mobiele telefoon. Het nieuwste snufje: de Japanse telefoniegigant KDDI **biedt** technologie aan die alle fysieke bewegingen van mensen volgt via een telefoon. De bedoeling hiervan is dat je de productiviteit van het personeel bewaakt. Met de analytische software kan bijvoorbeeld vastgesteld worden of een schoonmaker aan het zwabberen of aan het stoffen is. Of iets heel anders aan het doen is. Stiekem koffiedrinken bijvoorbeeld – je ziet het meteen, en kan zelfs automatisch een SMS-je sturen ("Werken, kreng!"). De software gebruikt de metingen van de accelerometers, die in steeds meer toestellen zit.

Hiroyuki Yokoyama, hoofd van de onderzoeksafdeling bij telefoonfabrikant KKDI: "Er moet natuurlijk nagedacht worden over privacyvraagstukken en er moet aangedrongen worden op overeenkomsten tussen werknemers en werkgevers hierover." Het nadenken is echter overduidelijk nog niet afgerond, 'overeenkomsten' met het personeel zijn immers dingen die je alleen hebt bij grote bedrijven – het merendeel van de economie speelt zich af bij kleine bedrijven waar dit dus geen bruikbare aanpak is. Geen ondernemingsraad, dus geen centrale afspraken. Zo zijn we uiteindelijk dus overgeleverd aan de grillen van de werkgever. En dat gaat lang **niet altijd goed**.

Alle ervaringen met soort middelen om de productiviteit te verhogen wijzen uit dat zij averechts werken. Een hogere productiviteit bereik je juist met vertrouwen in, en vrijheid voor de medewerkers, in combinatie met inspirerend leiderschap. Toch zullen bedrijven dit soort technologie inzetten. Inspirerend leiderschap vind je nu eenmaal niet overal, en een cultuur waar vertrouwen de boventoon voert ook al niet. Vrijheid is in veel bedrijven ook ver te zoeken: de wantrouwende en ongeïnspireerde leiders menen doorgaans dat eigen initiatief nergens voor nodig is. Volg gewoon de Heilige Procedure en dan komt het helemaal goed.

Zo lang de werkgever kan beargumenteren dat het om toezicht op het werk gaat of het tegengaan van criminaliteit, is er een heleboel geoorloofd. Veiligheid gaat immers **boven** privacy. En er is ook best vaak wat voor te zeggen. Het is bijvoorbeeld niet zo vreemd als Defensie kijkt of medewerkers op Facebook gerubriceerde informatie zetten. En ja, dan zien ze ook meteen of die medewerkers in hun vrije tijd zuipende en snuivende feestbeesten van de eerste orde zijn, wat ook formeel **gevoelig ligt**. Volgens de gedragscode van Defensie is het personeel ook buiten werktijd personeel, en hebben ze zich dus ook onder privétijd te gedragen.

Ook het bewaken of iemand daadwerkelijk ziek is die zich ziek gemeld heeft, is zo'n grijs gebied. Mag je je Facebook bijwerken als je ziek thuis zit? Een Zwitserse werkgever vond van niet en **ontsloeg** hierom een medewerkster.

Er zijn nog veel meer grijstinten te verzinnen. Baas Henk: "Ik wil precies weten wat je de hele dag aan het doen bent. Er verdwijnen de laatste tijd veel laptops en ik heb op TV gezien dat er in onze sector veel gefraudeerd wordt." Medewerker Gert-Jan: "Henk, ik vertik het te vertellen wat ik

[51] http://www.slate.com/id/2191295/

precies allemaal doe onder werktijd, als mijn werk maar op tijd af is, is het toch goed!" Baas Henk: "Nee. En anders ga je maar permanent buitenspelen!"

Baas Gijs: "in onze sector leef je in een glazen huis. Wat je in je eigen tijd doet kan hele negatieve impact hebben op de geloofwaardigheid van ons bedrijf. Ik wil dat je per direct stopt met dat blog over de geneugten van nederwiet!" Medewerkster Inge: "Wat ik in mijn eigen tijd onder mijn eigen naam doe, is mijn zaak". Gijs: "Dat ben ik niet met je eens – voor onze klanten ben jij een vertrouwenspersoon. Dan moeten we maar afscheid van elkaar nemen."

Baas Jan: "Ons bedrijf moet moreel hoogstaand zijn, omdat onze klanten dat belangrijk vinden. Daarbij past geen bezoek aan een naturistencamping. Stel je voor dat je daar een klant tegenkomt." Medewerker Hans: "Die klant is dan toch ook naakt?" Jan: "Het gaat hier om onze professionele uitstraling, wat de klant doet moet -ie zelf weten. Ik wil dat je niet meer naar die blote billentoestand gaat."

Baas Erik: "Je meldt je te vaak ziek omdat je zoontje niet naar school wil. Hij heeft ADHD, dus ik wil dat je hem Ritalin geeft." ZZP-er Raymond: "Die beslissing nemen mijn vrouw en ik samen met de dokter," Erik: "Nou dan huur ik wel een ander in."

Baas Ron: "Ons bedrijf is afhankelijk van een sportieve uitstraling. En je bent veel te dik. Ik eis dat je gaat sporten en gezonder gaat eten!" Uitzendkracht Jan-Willem: "Maar ik kan er niets aan doen, ik heb een hormonale afwijking." Ron: "Niets mee te maken."

In welke van deze scenario's de werknemer uiteindelijk verwijtbaar werkloos is, is niet duidelijk. Ik vrees in de meeste gevallen.

Het waarom van deze praktijken ligt vrijwel altijd op het gebied van de veiligheid – zoals bij de Deutsche Bahn waar het personeel doorgelicht werd om omkoping te vinden. Dit soort onderzoek strekt zich noodzakelijkerwijs uit tot de privétijd van het personeel. Daarmee zijn we wel een kritische grens over: het toezicht heeft de privétijd en het privégedrag van de medewerker bereikt.

En dit gebeurt niet alleen in het autoritaire Duitsland of in het nog gekkere Japan. In Nederland is de juridische situatie helemaal niet zo duidelijk, zeker niet waar het gaat over nieuwe ontwikkelingen. Dat ten eerste. Ten tweede krijgen we meer en meer te maken met bedrijven die in buitenlandse handen zijn. Zij houden in de corporate policies niet allemaal rekening met lokale wetgeving, zeker waar de handhaving zwak of zelfs afwezig is, zoals in Nederland. Ten derde is de fascinatie voor directief leiderschap nog steeds stijgende; de polder is helemaal uit de mode. Met de uitwassen van het procesdenken zijn initiatief en vrijheid voor de medewerker passé. En, last but not least, in de huidige angstcultuur zullen bedrijven proberen alles wat mogelijk schadelijk is, te verbieden. Dus ook in het gedrag van het eigen personeel. Veiligheid is immers een oneindig rekbaar begrip, zeker als het om imago gaat; er hoeft maar iemand lange tenen te hebben en het imago is in gevaar. En lange tenen zijn nu helaas juist wel in de mode.

Toch is de stap van Defensie heel begrijpelijk, vooral nadat in de pers telkens verhalen opdoken over militairen die weer eens een café hadden verbouwd. Ook justitie moest ingrijpen na herhaalde berichten over drugsuitspattingen van politiemensen in hun eigen tijd. En het gaat niet alleen om drugs - als een politieagent een **moordenaar** blijkt te zijn vinden we dat extra erg: blijkbaar stellen we de politie toch min of meer verantwoordelijk voor wat het personeel doet in de eigen tijd. De politie onderzoekt dan ook of de **screening** wel goed genoeg is geweest. Deze kandidaat had natuurlijk nooit agent had mogen worden. Maar als je dat denkt, bedoel je volgens mij eigenlijk gewoon dat de moord op Milly Boele nooit had mogen gebeuren. Wat ik bedoel is:

de buurman heeft het meisje heus niet vermoord OMDAT hij politieagent was. Met het leggen van een verband tussen een gruwelijke moord en het feit dat de dader politieagent was, maken we de politie medeschuldig. En dat is niet terecht. Zo veel kan een screening nu ook weer niet bereiken: het voorspelt niet wat iemand over vijf of meer jaren zou kunnen doen. Als een screening dat wel zou kunnen, dan kunnen we beter de hele bevolking screenen en iedereen opsluiten met een duidelijk risicoprofiel. En die kant[52] denken sommige mensen al een beetje op.

Ook begrijpelijk, en juridisch acceptabel, is het om medewerkers te verbieden als privépersoon te beleggen, als ze op hun werk in aanraking kunnen komen met beursgevoelige informatie. Ook is het niet zo'n vreemd idee als Stichting Brein medewerkers wil ontslaan die veel 'illegaal' downloaden.

Er zijn dus situaties waarin het begrijpelijk en geaccepteerd is dat een werkgever de grens tussen werk en privé opheft. Er zijn valide redenen. Het is ook gewoon echt waar dat het privégedrag van een werknemer grote schade kan aanrichten aan het bedrijf of de organisatie, met name door de publiciteit en de 'guilt by association'. Organisaties zijn overgeleverd aan de grillen van de publieke opinie en de lange tenen van (mogelijke) klanten. En werknemers zijn weer overgeleverd aan hoe de werkgevers daarmee omgaan.

Als een bedrijf vermoedt dat het gedrag van een medewerker de belangen van het bedrijf kan schaden, zal ze dat moeten tegengaan, ongeacht waar en wanneer dat gedrag plaatsvindt. Als bij privégedrag de werkkring van de medewerker betrokken raakt, heeft dit grote consequenties voor ieders privacy. Dus het kan maar zo zijn dat de Lidl niet achterlijk, maar juist voorlijk is.

Dit leidt tot een cultuur van zelfcensuur; bedrijven zullen geen hoge tolerantie hebben voor mogelijk omstreden gedrag – ook zaken die volstrekt legaal zijn kunnen immers onwenselijk zijn. Ik verwacht dan ook meer en meer verboden. En zoals wij in Securityland heel goed weten, is een verbod zonder handhaving (dus zonder toezicht en sancties) zinloos. Dus bedrijven zullen gaan handhaven, ook buiten werktijd en buiten de bedrijfspanden. Camera's op de werkvloer en toezicht op internetgebruik zijn écht nog maar het begin.

[52] http://www.waarden.org/actueel/achtergronden/criminele_aanleg.html

EPD: het blijft Nee

dinsdag 20 april 2010

Een genante vertoning van het ministerie van VWS rond een beveiligingsonderzoek naar het EPD: onderzoeker Guido van 't Noordende van de Universiteit van Amsterdam onderwierp het huidige EPD aan een nader onderzoek en kwam met een aantal bevindingen die er niet om liegen, die vervolgens door het ministerie onder de tafel werden weggeschoffeld. Van 't Noordende werd weggezet als oppervlakkig en ondeskundig.

Volgens onderzoeker Van 't Noordende kan iedereen met een UZI pas (de toegangspas voor alle medewerkers in de zorg) uiteindelijk bij alle patiëntgegevens, door een intrinsiek zwak ontwerp rond de delegatie van rechten. Ook de afwezigheid van technische middelen in de communicatie draagt aan dit probleem bij. "AORTA (het landelijke EPD) fully relies on security of the GBZ (Goed Beheerd Zorgsysteem) systems delegation tables, and, if required, on inspection of LSP (Landelijk SchakelPunt) audit logs after the fact". De kern van dit **probleem** is dat het Landelijk Schakelpunt LSP feitelijk geen middelen heeft om een mandatering door een arts – de formele vereiste voor toegang – te verifiëren, maar wél de toegang tot de patiëntendossiers verschaft. Dus controle vóóraf is niet mogelijk en achteraf alleen als er een aanleiding toe is – en het kost een boel moeite. Dat is intrinsiek een zwakke aanpak; je zult niet structureel alle logentries bekijken. Dat is duur. Er zullen altijd financiële afwegingen meespelen als er het idee is dat een event in het EPD nader bekeken moet worden. Forensisch onderzoek is immers nog duurder. En dat idee moet ook nog eens ergens vandaan komen.

Minstens even dodelijk zijn de keuzes die gemaakt zijn in de toepassing van HL7 (het **communicatieprotocol** voor uitwisseling van patiëntgegevens). "An important assumption of the trust model that underlies authorization in the EPD, is that one can always address the responsible physician (overseer) when something goes wrong. However, our analysis of the internal protocols shows that this assumption does not hold, because any overseer can be filled in in a HL7v3 message without involving the physician". "Employee UZI passes can be used to sign tokens on behalf of arbitrary overseers. In fact, the overseer field is not even included in the token, so it could be tampered with by anyone without the signer's knowledge – a fact which could allow an employee who conspired with an attacker to deny involvement with the attack in court". De "system delegation tables", de kern van de toegangsbeveiliging, zijn hiermee irrelevant.

Omdat er geen end-to-end authenticatie bij het opvragen van patiëntgegevens gebruikt wordt, kan een aanvaller ook nog ongezien zijn werk doen. "The attack may be particularly powerful because delegation can also be used to claim a treatment relationship, as far as the LSP is concerned". In de AORTA specificaties zijn wel oplossingen hiervoor opgenomen: "XML headers to support end-to-end authentication protocols and (payload) encryption" maar blijkbaar worden dit soort basale beveiligingsstappen op dit moment niet uitgevoerd.

De intrinsieke zwaktes van het EPD zijn dus de afgelopen jaren overeind gebleven en daarbovenop zijn zwakke implementaties gestapeld. Het systeem is uiteindelijk gebouwd op de veronderstelling dat de gebruikers betrouwbaar zijn en dat alle deelnemende partijen hun 'Goed Beheerde Zorgsystemen' 100% dichtgetimmerd houden. Een beveiliging die van dit soort veronderstellingen uitgaat, is geen beveiliging maar wat Bruce Schneier zo treffend aanduidt als 'Security Theater'.

Het ministerie van VWS verwijst de kritiek echter naar de prullenbak en stelt dat het onderzoek slecht onderbouwd is en verkeerde conclusies trekt. "Voor het LSP gelden strenge

beveiligingseisen voor ontwikkeling, implementatie en beheer die jaarlijks door onafhankelijke derden worden getoetst door middel van audits en indringerstesten. De testen die tot op heden werden uitgevoerd, onder andere door gespecialiseerde hackers, hebben aangetoond dat de genomen maatregelen adequaat zijn". Helaas maakt dit pijnlijk duidelijk dat het ministerie van Volksgezondheid weinig kaas heeft gegeten van de waarde van penetratietesten en audits. Een penetratietest kan namelijk alleen bewijzen dat er op een specifiek moment een gat in de beveiliging zit, nooit dat er géén gaten zijn. Als er geen gat wordt gevonden kan de tester hooguit aangeven welke gaten er – op het moment van de toetsing - niet zijn, wat echt iets heel anders is dan dat er geen gaten zijn. En dat laatste is nu net wat VWS wél veronderstelt.

Van 't Noordende: "Bovengenoemde toetsmethoden geven geen enkele garantie voor de veiligheid van het systeem. Als het EPD waterdicht zou zijn, zou dit het eerste systeem ter wereld zijn. Het punt is dat wanneer er een inbraak in het systeem plaatsvindt, de beveiligingsarchitectuur van het EPD de mogelijke schade moet kunnen beperken. Dit is in het huidige ontwerp niet het geval".

Ook de kritiek dat de controle op door artsen gemandateerde medewerkers onvoldoende is, veegt het ministerie van tafel. De huidige, decentrale, registratie van mandatering is een bewuste keuze geweest, juist omwille van de veiligheid, schrijft het ministerie.

Informaticus Van 't Noordende kan zich terecht niet vinden in de kritiek van het ministerie. Hij beraadt zich op een reactie waarin hij de stellingname van het ministerie zal weerleggen. Opvallend in de hele affaire is dat de Nictiz, het landelijke expertisecentrum dat ontwikkeling van ICT in de zorg faciliteert en dat vanaf het prille begin betrokken is bij de technische realisatie van het EPD, het onderzoek in NRC Handelsblad juist "**zeer zorgvuldig**" noemt.

Het ministerie stelt verder dat doorvoeren van de end-to-end authenticatie (wat Van 't Noordende bepleit) zal leiden tot een "significante toename van de complexiteit van de implementatie GBZen met mogelijke nieuwe implementatie-, beheer- en beveiligingsrisico's." Met andere woorden zeggen ze dat ze niet kundig genoeg zijn om een standaardbeveiligingsfunctie aan te zetten. We hoeven dus ook niet te rekenen op end-to-end versleuteling, wat blijkbaar op dit moment ook niet nodig – of te moeilijk - wordt gevonden.

Nu wil de nieuwste loot in ons politieke landschap, de piratenpartij, van het hele EPD af. Begrijpelijk, als je deze vertoning ziet. Daarmee zou het EPD dat andere prestigeproject, de kilometerheffing, volgen. In Engeland is het landelijk EPD al begraven, omdat het de **macht** van de bouwers te boven ging. Dat risico lopen we hier te lande ook, gezien de keuzes om 'moeilijke' beveiliging maar achterwege te laten. Echter, niet alleen de beveiliging is lastig – in een groot systeem als het EPD zijn er wel meer moeilijke dossiers. Hieruit concludeer ik dat een compleet projectfalen niet uit te sluiten is.

Dat moeten we hier niet willen. Het is immers niet dat een landelijk EPD geen goed plan is, het is dat het huidige EPD niet goed is. Het moet op een aantal kritieke punten keihard op de schop, onder meer rond de toegangsbeveiliging. En als dat te moeilijk is voor de mensen die het nu moeten regelen, dan moeten er maar andere, meer competente mensen op gezet worden.

Van de **opmerkingen** van beveiligingsgoeroe van der Staaij in het **NRC** over het EPD moeten we het in ieder geval niet hebben. Hij **stelt** dat het allemaal best wel meevalt met het EPD, en heeft zulks ongetwijfeld ook in de Kamercommissie **gemeld**: "Stel, een corrupte ziekenhuismedewerker is uit op de medische gegevens van een bekende Nederlander. Wat zou die persoon moeten doen om die gegevens te achterhalen? Allereerst zou hij een UZI-pas van iemand moeten zien te bemachtigen, de pas waarmee toegang tot het EPD kan worden verkregen". "Dan zijn er echter

ook nog het loggingmechanisme van het EPD en een keur aan forensische technieken, waarmee achteraf kan worden nagegaan wie wanneer welke gegevens heeft benaderd". Van der Staaij veronderstelt dat de corrupte medewerker blijkbaar zelf geen pasje heeft, dat de auditoren helderziend zijn en dus weten wanneer en waar ze moeten onderzoeken dat er iets mis is gegaan. Bovendien wordt de corrupteling geacht technisch een onbenul te zijn. Een indrukwekkend aantal aannames.

Bovendien, stelt Van der Staaij, is er in de praktijk weinig echte dreiging, omdat hem weinig gevallen bekend zijn van diefstal van medische gegevens. "Op dit moment – nu er nog geen EPD is – is het namelijk veel gemakkelijker om aan vertrouwelijke patiëntgegevens te komen. Papieren dossiers liggen letterlijk voor het opscheppen, veel pc's in zorginstellingen voldoen nog lang niet aan de moderne beveiligingseisen en het risicobewustzijn bij zorgverleners, zoals al eerder is aangehaald, is laag".

Ik zie alleen niet hoe het EPD dit zal veranderen. Het risicobewustzijn van medewerkers in de zorg zal met het EPD niet spontaan stijgen, en de pc's in zorginstellingen zullen niet structureel veilig worden – daar zorgt het EPD niet voor. Het GBZ gaat immers over servers in het koppelvlak naar het **EPD**, en helemaal niet over pc's of de rest van het netwerk. Het betoog van Van der Staaij snijdt dus geen hout.

Ik zal mijzelf nog eens herhalen: papier is in alle gevallen oneindig veel veiliger dan digitaal, zelfs als iedereen altijd alles laat slingeren – inclusief USB-sticks en op pc's die wijd **openstaan**. Wil een aanvaller een papieren dossier stelen, dan zal hij het eerst moeten vinden en er fysiek de hand op moeten leggen om het te kopiëren of te ontvreemden. Digitalisering maakt het geheel veel kwetsbaarder, omdat kopiëren simpeler wordt. Het probleem dat overblijft is het vinden van de digitale data, een probleem dat de verwijsindex van het landelijk EPD echter keurig oplost. De aanvaller hoeft dus alleen een netwerkverbinding en enige technische skills te hebben – waar de informatie is, is duidelijk.

Als je op dit moment een enkel medisch dossier op papier of uit een slecht beveiligd systeem wilt stelen, zal het nog wel lukken, maar alle dossiers van alle Nederlanders krijg je niet bij elkaar. In het EPD-tijdperk werkt het anders: als je er één hebt, kun je ze maar zo allemaal hebben. De UZI-pas met pincode is overigens alleen nodig als je via de voordeur aan wilt vallen. De praktijk van 30 jaar hacken is dat de meeste mensen het raam wel weten te vinden.

In plaats van een persoon die het pand binnenloopt of er al werkt, zijn er bij een digitaal systeem twee miljard mogelijke aanvallers die met z'n allen technisch veel meer kunnen dan welke set pentesters dan ook. Het gaat ook niet alleen om technisch begaafde hackers. In plaats van enkele tientallen personen die een papieren of USB-variant kunnen laten slingeren, zijn er immers enkele honderdduizenden die slordig met hun sleutels kunnen zijn, sleutels die toegang geven tot alle patiëntendossiers, in plaats van tot een beperkte set. Daarom moet centraal bewaarde gedigitaliseerde informatie per definitie heel veel beter bewaakt worden dan dezelfde informatie op papier of in decentrale vorm. Hiervoor is een beetje klassiek autorisatiebeheer voor systemen waar de informatie op zou moeten staan, zoals in het huidige EPD, zelfs in de beste vorm al een erg magere aanpak.

En eigenlijk missen we het grootste probleem; de beveiligers kijken maar naar een beperkt aantal scenario's. Diefstal van informatie is heus niet het enige aanvalsscenario waar je bij de beveiliging van het EPD rekening mee moet houden. Met het weghalen van een allergie voor pinda's uit iemands medisch dossier kun je een perfecte moord plegen. En er is ongetwijfeld meer te verzinnen. Maar dat licht is zo te zien nog niet gaan branden bij de goegemeente die zich over het EPD heeft gebogen.

Als klap op de vuurpijl stelt Van der Staaij in het NRC: “tegen corrupte medewerkers is vrijwel geen enkel informatiesysteem bestand”, waarmee hij impliceert dat je daar dan ook maar niet al te veel moeite voor moet doen. Het is met een systeem met uiteindelijk een paar honderdduizend gebruikers – zoals het EPD – dan ook een feitelijk advies om de beveiligingsillusie maar helemaal op te geven. Als dat echt zo is, dan kun je de hele EPD exercitie maar beter begraven, samen de digitale belastingaangifte en alle bancaire systemen voor betalingen.

Nu zul je dergelijke complexe systemen inderdaad nooit 100% waterdicht krijgen, maar je kunt een heel eind komen. Het is in ieder geval geen reden standaard zaken achterwege te laten. Er bestaat een hele categorie van systemen die niet alleen geacht worden tegen de gebruikers bestand te zijn, maar zelfs tegen de beheerders. Dit is wat wel aangeduid wordt als Military Grade Security. Zo ver hoef je wellicht niet te gaan, maar reken maar dat je de huidige inherent zwakke en indirecte beveiliging van het EPD een stuk beter kan krijgen.

Van ‘t Noordende doet hiervoor een aantal zeer waardevolle aanbevelingen, onder meer:

1. Zorg voor 'end-to-end' authenticatie van berichten, zodat het informatiesysteem dat een verzoek om een dossier ontvangt kan controleren of dit verzoek daadwerkelijk van een zorgverlener afkomstig is. Dit teneinde aanvallen vanuit het LSP voorkomen.
2. Versleutel deze berichten end-to-end.
3. Gebruik vooraf door de arts ondertekende -beperkt geldige- mandateringscertificaten als bewijs van autorisatie, voordat medewerkers toegang wordt verleend tot het EPD.
4. Bevestig behandelrelaties expliciet, (eventueel achteraf middels het klantenloket), ten behoeve van effectiever toezicht.
5. Ook kan na bevestiging bepaalde privacygevoelige loginformatie uit het LSP worden verwijderd of versleuteld.
6. Voer een smartcard voor patiënten in die veilig inloggen mogelijk maakt, en die ook het versleutelen van gevoelige patiëntgegevens in het LSP mogelijk maakt.

Vooral met het vierde punt slaat Van ’t Noordende de spijker op zijn kop. De keuze om centraal te autoriseren op basis van informatie die centraal niet beschikbaar is, is wellicht een aardige weergave van de politieke realiteit in de zorg, maar een gruwel vanuit beveiligingsoogpunt. Met de toevoeging ‘eventueel achteraf’ toont Van ’t Noordende zich veel te mild – dat werkt niet en het hoeft niet.

Wat je moet doen is de behandelrelaties herleiden uit andere systemen. Immers, als organisatie heb je je informatiehuishouding op orde en houd je bij wat je mensen zoal doen. Op basis hiervan zouden dan dynamisch autorisaties toegekend (‘geprovisioned’) moeten worden. Voor de hand liggend is aan te sluiten op **DOT 2010**, de opvolger van het DBC-systeem (Diagnose-Behandel-Combinatie) dat in het kader van de “**prestatiebekostiging**” ingevoerd wordt. Als je daarin vastlegt welk behandelteam – of zelfs maar welke afdeling – bij een patiënt (lees BSN+DOT-code) betrokken is en van wanneer tot wanneer, dan heb je voldoende broninformatie voor dynamische autorisaties. Als je je informatiehuishouding hiervoor niet voldoende op orde hebt, is een geavanceerd systeem als een lokaal EPD al niet te verantwoorden.

Een goede technische methode zou zijn om een Claims Based aanpak te plaatsen **bovenop** het bestaande statische rollenmodel, waarbij het landelijk schakelpunt alleen valideert (met een token) of een aanvrager op dat moment een behandelrelatie met de patiënt heeft, alvorens toegang te geven. Daarmee houdt het ziekenhuis nog steeds grip op de data. Het gaat wat ver om hier Claims Based Autorisation uit te leggen, voor degenen die er nooit van gehoord hebben, maar het biedt een hele zwik mogelijkheden die ten tijde van het bedenken van het EPD (in **2003**) nog niet ‘bewezen’ waren, maar inmiddels wel. En ruimschoots.

Op dit moment vragen de beveiligingseisen voor het EPD niet om een dynamische autorisatie op basis van actuele gegevens. Bij deze oorspronkelijke eisen ligt uiteindelijk de oorzaak van het zich verder ontvouwende EPD beveiligingsdrama: om te beginnen zijn er vanaf het begin lage beveiligingseisen gesteld. Deze zijn bepaald naar het belang van de gebruikers van het systeem in plaats van naar het belang van de informatie in het systeem. In deze discussie hebben de zorginstellingen zich als informatie-eigenaren opgesteld, terwijl de echte informatie-eigenaren – de patiënten – niets gevraagd werd. Vervolgens is er te weinig kennis, terughoudendheid bij zaken die 'moeilijk' klinken, te weinig budget en tijd, zodat er steeds meer zaken 'uitgesteld' zijn naar 'een volgende release' dan wel openlijk geschrapt. Het EPD lijdt sterk onder de klassieke projectdynamiek waarbij alles wat ingewikkeld of moeilijk is omwille van het champagnemoment (de deadline) overboord gaat. Er is immers een minister bij betrokken, en die wil resultaten zien. In deze lijn past het afserveren van een degelijke analyse, zoals die van Van 't Noordende, naadloos.

Met andere woorden: eerst is een beveiligingsniveau gekozen dat ver onder het minimum ligt, waar dan met de kaasschaaf nog wat vanaf werd bezuinigd. Vervolgens zijn er tijdens de daadwerkelijke implementatie nog hele stukken beveiliging vervallen omdat het niet op tijd lukte. Door de looptijd is de beveiligingsarchitectuur intussen ook nog zwaar verouderd en irrelevant geworden. Alle alarmbellen zijn vakkundig genegeerd. Het resultaat van dit alles is om ziek van te worden. Niet te ziek hoop ik, want dan kom je in het EPD, en dat kan ik je voorlopig dringend afraden.

Het schijndebat

zondag 9 mei 2010

Security gaat altijd boven privacy **roept de een**. Nee, het één kan juist niet zonder het ander, roept de ander. Zo draaien we al een paar jaar rondjes rond onze uitgangsstellingen. Het lijkt een discussie zonder einde.

Op de keper beschouwd is er helemaal géén tegenstelling tussen privacy en veiligheid, dus je kunt niet het één inleveren om het ander te krijgen. Het zijn sterk overlappende begrippen. In Orwell's "**1984**", dat synoniem geworden is met het verlies van privacy, zie je dat heel goed. Het boek heeft als onderwerp het verlies van waarheid, vrijheid en veiligheid in de totale dictatuur van 'Big Brother'. Eén van de machtsmiddelen die Big Brother inzet is spionage tegen de eigen burgers. Het is echter bij lange na niet het belangrijkste middel van Big Brother: dat is de manipulatie door de taal, newspeak. En zoals het boek zeer duidelijk maakt; daar is geen ontsnappen aan. De hoofdpersoon houdt uiteindelijk van Big Brother. De burgers uit 1984 hebben helemaal geen behoefte aan privacy, ze hebben niets te verbergen omdat ze gehersenspoeld zijn. De schijntegenstelling tussen privacy en security is zélf een goed voorbeeld van Orwell's hoofdthema; het besturen van de geest en het gedrag beïnvloeden door manipulatie met de taal.

Verdachtmakingen als van de ex-leefbare en tegenwoordige **VVD-coryfee Teeven** ("alleen slechteriken willen dingen in het geniep doen") en ex-PvdA minister **Ter Horst** met de schijnkeuze tussen privacy en security zijn hier een goed voorbeeld van. Deze daadkrachtverslaafde politici willen hun beleid erdoor hebben en tegenspraak moet van tafel, koste wat het kost. Het is een manipulatie waar we massaal in trappen – van **Bruce Schneier** tot **Bits of Freedom**. We zijn dus in goed gezelschap. Het gaat dit soort politici echter helemaal niet om veiligheid óf privacy; ze willen gewoon hun geurvlag zetten en hun zin doordrijven.

De enig terechte reactie op deze Haagse fratsen zou homerisch gelach zijn, maar dat is slechts weinigen gegeven. Daarvoor is deze **mindfuck** te effectief. Om te ontsnappen moeten we het verhaal helemaal duidelijk en helder hebben, en dan maar helemaal uit de doeken doen.

Veiligheid is een gevoel. Je voelt je veilig, of je voelt je niet veilig – dan voel je je bedreigd. Er is vast wel een correlatie met 'objectieve' veiligheid - de afwezigheid van een daadwerkelijke bedreiging - maar de mogelijkheid tot objectiviteit is niet hoog. Als er veel aandacht is voor een bepaald gevaar, dan zullen meer mensen bang zijn dan voor een gevaar waar niemand het over heeft. En gevaar waar je aan gewend raakt, zul je niet meer als zodanig ervaren. Suggestie en gewenning dus. Dat maakt het een ingewikkeld veld.

Nu is de één gevoeliger voor suggestie dan de ander, we zijn niet allemaal **hypochonder**. Dat kun je voor jezelf testen; lees een aantal artikelen over een bepaalde wazige ziekte, en je voelt je gelijk een stuk minder **senang**. Of begin op een verjaardagsfeestje over hoofdluis, en voor je het weet zitten diverse mensen op hun hoofd te krabben. En jij zelf ook. Bedenk dit de volgende keer als je ergens bang voor bent; relativeer en objectiveer. Veiligheid is immers van nature een zeer subjectief begrip, en daardoor ben je extra gevoelig voor manipulatie.

Privacy is volgens Wikipedia een '**afweerrecht**', een recht om dingen niet te tonen of mee te maken. Privacy gaat daarom meestal over angst; zoals in de discussies rond de kilometerkastjes of slimme meters goed te lezen is: mensen denken dat wanneer de vastgelegde gegevens niet kloppen ze bestraft zullen worden voor iets wat ze feitelijk niet gedaan hebben. De suggestie van mogelijke fraude is daarom een **zeer effectief propagandamiddel**. O jee, voor je het weet betaal je te veel! Angst is niet objectief, en privacy dus ook niet. Zo wil je niet dat je baas weet wat je in je

slaapkamer doet of in je wilde jeugd gedaan hebt. Daarbij maakt het weinig uit wat de baas er van vindt. Privacy is op de keper beschouwd de verzameling grenzen die je veiligheid moeten waarborgen.

De angst waar privacy over gaat, hangt samen met schaamte; het verborgen houden van gedrag of gedachten omdat het niet veilig voelt dat anderen weten dat je het doet of denkt. Je zou er immers mee geconfronteerd kunnen worden, dat iemand het niet accepteert en je er vervolgens op aanspreekt. Of erger. In die zin is privacy een beschermingsmechanisme tegen de normen en waarden van anderen (die zich kunnen uiten in geroddel of openlijke afkeuring). Dit betekent dat de behoefte aan privacy samenhangt met de overheersende normen en waarden; als er meer zaken 'niet kunnen', zal er meer behoefte zijn aan privacy – om ze toch te kunnen doen. Dat is de directe relatie tussen privacy en vrijheid.

De vrijheid die door privacy mogelijk gemaakt wordt, is onmisbaar voor het anders denken en het anders zijn. Afwijken van de heersende normen en waarden is randvoorwaardelijk voor de ontwikkeling van de maatschappij; zonder privacy stagneert de samenleving, zoals TNO-er Dr. Hoepman **terecht vaststelt**.

In de relatie van burger tot burger gaat het vooral over schaamte. In de discussie over overheid en privacy komt er een dimensie bij: macht. Een complicerende factor. Je houdt dingen stil omdat je bang bent voor de gevolgen, feitelijk voor de macht van de overheid. Nu gooien best veel mensen allerlei privézaken vrijelijk op internet – het populairste argument van de anti-privacy kruisvaarders – maar er zijn weinig mensen die op Facebook melden hoe en voor hoeveel ze de belasting getild hebben. De belastingdienst heeft immers macht en gebruikt die ook.

Als de overheid op meer gebieden haar macht doet gelden, zal de burger meer zaken in het verborgene houden. Als de dreiging is dat de overheid je uit het ouderlijk gezag zet omdat je een aso bent, dan zul je zaken die met asociaal gedrag geassocieerd zouden kunnen worden, voortaan maar stiekem doen. Je weet immers nooit hoe een anonieme beslissingsambtenaar denkt; het zou maar zo een superburgerlijke moralist kunnen zijn. Daarom zien sommigen het Elektronisch Kinddossier als zo'n grote bedreiging voor de veiligheid van het gezin; je weet immers niet welke **consequenties** er aan verbonden zijn als er ingevuld wordt dat je wel eens een sigaretje in de woonkamer hebt gerookt, computergames speelt of geen sociaal netwerk hebt.

Nu de overheid zich op de normen en waarden heeft gestort en dus openlijk zedenmeestert, is het einde zoek. Dit verklaart de gevoeligheid van het onderwerp; uit angst en kwetsbaarheid (voor misbruik en incompetentie) neemt de burger uit voorzorg ruime veiligheidmarges, en waar die ruime marges kruisen met plannen van bestuurders en politici leidt dit tot irritatie en frustratie. Zoals recent goed te zien bij VVD-er Teeven: "Overheidsdienaren moeten altijd en overal bij mensen naar binnen kunnen lopen. Zo maak ik hoogstpersoonlijk van Nederland een veilig land. En wie dit niet leuk vindt, moet maar emigreren of springt voor de trein". **Hier spreekt de frustratie**, naar ik mag hopen. Want als hij dit serieus meent, en mij dus vertelt dat ik moet oplazeren uit mijn land, moet hij toch wat meer meenemen dan die grote bek.

Schaamte en macht zijn voor privacy dus heel belangrijk, zeker aangaande zaken die cultureel gezien taboe zijn verklaard. Hier hebben we te maken met de traditionele normen en waarden; vraag een gemiddelde Nederlander naar zijn banksaldo of slaapkamervoorkeuren, en het antwoord zal iets zijn in de trant van 'flikker op'. Nu had ons land ooit een schuldcultuur, waarin geheimhouden niets hielp tegen het alziend Opperwezen, dat is inmiddels meer een **schaamtecultuur** geworden. Oftewel, schaamte stuurt ons gedrag en zeker nu de overheid weer de zedenmeester uithangt, willen we extra bescherming tegen normen en waarden die we niet onderschrijven. De overheid zet dan ook, zeer consequent, schaamte ('**naming and shaming**') in om het gedrag van burgers te beïnvloeden.

Er zijn ook mensen die deze angst niet lijken te hebben. Een hacker die voor de bragging rights gaat, zal alleen maar blij zijn met de extra aandacht door naming and shaming. De schaamteloze 'generatie exhibitionist' gooit zelf allerlei zaken op het internet die anderen privacygevoelig achten. Dit is géén uiting van categorisch minder behoefte aan privacy, zoals bij hoog en bij laag beweerd wordt, maar eerder een uiting van de behoefte aan andere normen en waarden. Een homo die uit de kast is gekomen, heeft een deel van zijn seksuele gedrag publiek gemaakt, maar dat betekent helemaal niet dat hij geen behoefte heeft aan privacy. Wat hij doet is duidelijk maken dat hij vindt dat homoseksualiteit niet iets is om je voor te schamen, en dus bekend mag zijn. Oftewel, het is een uiting van andere normen, niet meer dan dat. En je ziet ook dat 'uit de kast komen' andere mensen ertoe aanzet om dat ook te doen.

Als je weet dat heel veel mensen doen wat jij zou willen doen, dan zul je het eerder doen – meer informatie leidt tot ruimdenkendheid en daarom tot minder behoefte aan privacy. Je zult mensen niet snel over je aambeien vertellen, tot je merkt dat vrijwel iedereen ze wel eens heeft. Onder invloed van Internet zullen er nog de nodige taboes sneuvelen, deze eeuw. De kleinburgerlijke normen en waarden die onze premier wil versterken, zullen in het informatietijdperk geen stand houden.

Met het terugtreden van de huidige generatie machthebbers zal het belang van schaamte in de privacydiscussie dus afnemen. Daardoor neemt het soortelijk gewicht van het veiligheidscomponent van privacy toe, een aspect dat ook autonoom al wint aan belang. Dat zie je bij de discussie over de slimme elektriciteitsmeters: inbrekers kunnen zien dat je op vakantie bent en je TV stelen. Op dit soort scenario's zijn vooral mensen alert die al redelijk gewend zijn aan de informatiemaatschappij en de kwetsbaarheden kennen. Dat zie je ook terug op security.nl – het zijn juist de IT-ers die de boel niet vertrouwen, of het nu een EPD, een kilometerkastje of een slimme meter betreft. Natuurlijk zijn de scenario's soms erg vergezocht, de zorg en de emotie zijn echter wel heel reëel.

Privacy is in deze gedachtegang een afweer tegen diefstal, waarbij identiteitsdiefstal steeds belangrijker wordt; zeker gezien het probleem van identiteit in de digitale werkelijkheid. Op Internet besta je immers alleen halfslachtig en indirect, via je IP-adres, via je e-mail adres (je feitelijke identiteit op dit moment), een paar pseudoniemen en avatars en meer en meer via je sociale profielen op allerlei sites, in de wereld van Web 2.0 en Identity 2.0. Omdat deze identiteit op een wankele basis rust, is deze zeer kwetsbaar. Daarom is online privacy extra belangrijk.

Een door de overheid opgelegde digitale identiteit kan deze wankele basis niet verstevigen. Het maakt hem juist wankeler. Bedenk maar eens wat je over een paar jaar met de DigID of de digitale handtekening van iemand anders kunt doen. Want dat gebeurt nu; de overheid legt je een digitale identiteit op, die rechtsgeldig kan handelen. En als het daarmee fout gaat, dan is dat per definitie jouw eigen schuld en draai jij op voor alle mogelijke gevolgen totdat jij onomstotelijk bewezen hebt dat het niet zo is. Waarschijnlijk nog langer, omdat bewijs nog vaak niet tot correctie van de fout leidt. Dit omkeren van de bewijslast lijkt wel standaard te worden bij digitale zaken.

We zijn op dit moment nog zoekende naar de nieuwe normen en waarden, passende bij het informatietijdperk. In deze onzekerheid is niet zo goed te zien wie je kunt vertrouwen; je kunt wél zien wie niet te vertrouwen is en dat zijn mensen en partijen die overduidelijk aantonen er geen barst van te begrijpen. Die kunnen we onze veiligheid in ieder geval niet toevertrouwen. En in deze lijst staat de politiek, vrijwel zonder uitzondering, bovenaan.

Tweedehands angst

Dinsdag 15 juni 2010

4 mei 2010, de dodenherdenking op de Dam. Een zonderling schreeuwt iets onverstaanbaars. Iemand anders ziet een koffer en roept: “Bom”. Gevolg: 63 gewonden door paniek in de massa, omdat veel mensen direct aan het drama in Apeldoorn dachten op Koninginnedag vorig jaar.

6 mei 2010, Wall Street. Het handelshuis Wadell verkoopt per ongeluk massa’s e-mini contracten. Wereldwijd verdampt 1.000 miljard na **paniekverkopen**.

Ook de verkiezingen stonden in het teken van de angst: we moeten vooral vrezen voor de economie, dus de voorstellen voor de zwaarst mogelijke maatregelen buitelden over elkaar heen. Samen met die andere angst, die voor de islamisering, bleek dit genoeg om een politieke aardverschuiving te veroorzaken.

In ons land is dat een nieuw fenomeen; een maatschappij met een angststoornis. Het weefsel van vertrouwen is stuk en de hysterie ligt dicht onder de oppervlakte. Geert Mak **schetst** overtuigend de overeenkomsten met de jaren 50 in de VS toen de schaduw van McCarthy de samenleving overheerste. Deze situatie is ernstig, omdat vertrouwen het belangrijkste bindmiddel is van de samenleving en tevens de belangrijkste bescherming ervan. Bezwijkt onze samenleving onder de stress van terrorisme en de economische crisis?

Daar is een simpel antwoord op: nee.

Wat nou, nee?

Ik zal het even uitleggen.

Terrorisme is op dit moment zeer beperkt. De laatste jaren zijn juist zeer rustig geweest. Wanneer was de laatste **aanslag** ook alweer in Nederland? Juist, in **2004**. Ook internationaal gezien lijkt het rustiger, behalve dan in de landen waar het al jaren gedonder is.

Ook de economische crisis is geen logische oorzaak; het diepste dal is al geweest en een groot deel van de bevolking – zeker in ons land - is minder geraakt dan in 2003 of 1982. Dus als we bang zijn, is dat niet voor iets wat veel erger is dan voorheen. Pak een willekeurig geschiedenisboek en je zult zien dat we niet in een bijzondere tijd leven. Terrorisme is van alle tijden en economische crises zijn dat ook.

De huidige angststoornis kan ook niet komen door de televisie of andere media, die bestaan daar echt al veel te lang voor. Voor wie het meegemaakt heeft – de beelden van de Vietnam-oorlog kwamen ruw en ongefilterd iedere woonkamer binnen, ook in ons land, maar daar werd Nederland niet en masse bang van. En dat terwijl toen nog een groot deel van de bevolking zelf herinneringen had aan echte oorlog.

Wat is er dan wel aan de hand – vanwaar deze extra angst en hysterie?

Het antwoord zal je niet verrassen; angst verkoopt dus angst wordt gekweekt. Angst is goed voor de kijkcijfers, de krantenoplages, de verkoop van bewakingsspullen en de handel in politieke producten.

Zoals de twee incidenten begin vorige maand aantoonden is angst zélf gevaarlijk. Achteloos strooien met angst is daarom onverantwoord.

De meeste negatieve connotaties van angst hebben te maken met groepsangst. Het bekende beeld is een 'stampede', een hysterische horde die alles verwoest. Dit is de angst die zichzelf voedt en versterkt. Een individu kan zich wapenen tegen angst, een groep kan dat niet. Als de groep echter te klein wordt, kan de angst zichzelf niet meer voeden. Daarom is het essentieel dat we ons individueel wapenen tegen deze manipulatie en de groep de kritische massa ontnemen.

Verkleutering
In navolging van de Jip en Janneke taaldiscussie is er een taboe gekomen op complexe zinnen en in het verlengde daarvan op ingewikkelde verhalen. Door deze verkleutering verdwijnen alle nuances. Bij gevaar ontneemt dat de mogelijkheden tot nuance en analyse. In plaats van extra alert te worden, komt alleen de hysterie dichterbij; het meest angstwekkende is immers te weten dat je bedreigd wordt, maar niet te weten waardoor. De terrorismemonitor[53] van de coördinator terrorismebestrijding is hiervan een kenmerkend voorbeeld; er staat hoe bang je moet zijn, maar waar is de informatie?

Ieder wat ingewikkelder verhaal moet blijkbaar in kleutertaal uitgedrukt worden – iets wat alleen zeer getalenteerde schrijvers kunnen zonder de essentie te verliezen. De essentie van een verhaal blijft dus bijna altijd achterwege. Hóe bedreigt de Griekse crisis onze welvaart? Wordt het door de klimaatverandering nu warmer of kouder? Is Al Qaida nog steeds gevaarlijk, of niet meer, als je al dat gestuntel met die aanslagen ziet? Was het vroeger veiliger in Nederland, of niet? Wil je het gevaar duiden, dan moet je er zelf de informatie bij zoeken. Doe dat!

Spinning
Uit de VS komen de begrippen '**framing**' en '**spinning**', waarbij de laatste via 'spindoctors' de meeste bekendheid heeft gekregen. Spinning is professionele manipulatie door taal. Je leert een spin herkennen door te bekijken hoe en waar ze toegepast zijn. Daarom een kort overzicht uit de recente, Nederlandse geschiedenis.

We begonnen deze eeuw met het Y2k probleem. Omarmd door commercie spinden religieuze laatste-dagenfanaten als **Gary North** een wereldwijde hype. Y2K zette een dikke streep door het optimisme van de jaren 90 en eindigde de overwinningsroes van het eind van de Koude Oorlog. Y2k liep met een sisser af; ook niet gefixte systemen bleken het gewoon te blijven doen.

9/11 was de volgende klapper. Wat er op volgde was een periode van wapengekletter en cultuur van angst, met tijdsbeelden als de moorden op Van Gogh en Fortuyn. Met die angst hebben de neo-conservatieven en hun Nederlandse volgelingen hun oeroude wensdromen ingevoerd; een wereld vol regels en camera's. Het is dat politie en rechtspraak weigerden mee te doen, anders leefden we in een politiestaat.

In deze periode werd de eerste Nederlandse spindoctor bekend, Jack de Vries. Dat deze spindoctor struikelde over een affaire met een ondergeschikte in plaats van over het lekken van ministerraadstukken, die volgens onze premier maar zo **Staatsgeheim** kunnen zijn, is veelzeggend. Het schouderklopje[54] van de Majesteit maakt duidelijk dat spin niet meer weggaat uit onze politiek.

---

[53] http://www.nctb.nl/onderwerpen/Alerteringssysteem/actuele_situatie.aspx
[54] http://www.nu.nl/binnenland/2249675/koningin-ontslaat-en-bedankt-jack-vries.html

Vervolgens zijn we de euro 'ingespinned'. De euro zou monetaire crises zoals in de jaren 30 uitsluiten, onze financiële sector versterken en een grote groei mogelijk maken, is ons beloofd. Wat zien we anno 2010? Mét de euro zitten we in de grootste monetaire crisis sinds de jaren 30. In 2008 brak de kredietcrisis uit, een crisis waar de euro ons tegen zou beschermen, zo **stelden** althans de politici. Dat blijkt in 2010 óók al niet waar te zijn, zo leert de Griekse crisis. De euro geeft de crisis juist extra venijn. Zonder de euro zou Griekenland veel eerder, en daardoor veel minder heftig, door de markt gecorrigeerd zijn. De euro is eerder de oorzaak van de huidige crisis dan de beloofde dam ertegen.

We zijn op dezelfde manier de EU ingespinned. Weet je nog; volgens Balkenende zouden de buurlanden ons straffen bij een tegenstem op het **Referendum**. Volgens VVD-kamerlid Van Baalen zouden ze zelfs met 'een muur om Nederland onze economie kapotmaken'. Pure spin; het aanzien van een land is alleen van belang voor de carrièrekansen van politici en markten trekken zich niets aan van politiek geneuzel. De **overtreffende spin** kwam van CDA-minister Donner: als we niet meedoen met de EU komt er oorlog. We stemden massaal tegen maar er kwam geen oorlog en ook geen muur.

Uiteindelijk kregen we geen 'grondwettelijk verdrag' maar een 'gewoon verdrag'. Dit Lissabonverdrag zou geen grondwet zijn en dus geen raadgevend referendum nodig hebben, omdat er geen vlag en volkslied in stonden. Welnu, die staan in de Nederlandse grondwet ook niet en dat is toch heus een **grondwet**.

Met hetzelfde gemak zijn we een postkoloniale oorlog ingespinned, in eerste aanleg om de kernwapens van Saddam uit handen van Al Qaida te houden. Toen die redenering ontmaskerd was bij gebrek aan kernwapens, verlengden we keer op keer de missies om ons internationale aanzien te behouden; alles in het landsbelang!

Herken je de spin?
De Hoop Scheffer **meldde** in februari 2010 in een interview met het NRC dat Nederland bij een terugtrekking uit Uruzgan gepasseerd zou worden voor hoge functies in de NAVO. Deze spin bevat een nogal Verontrustende Boodschap. Het belang dat De Hoop Scheffer en vele kenners met hem hechten aan de nationaliteit van de poppetjes, maakt overduidelijk dat kwalificaties anders dan nationaliteit voor die posten blijkbaar niet zo relevant zijn. Het maakt mij geen biet uit of er een Spaanse of Nederlandse generaal zit – ik wil gewoon dat de beste generaal daar zit.

Een volgende spin is de argumentatie over de Nederlandse plek bij de G20 die we zouden verspelen met het vertrek uit Afghanistan. De **G20** zijn de 19 grootste economieën plus de Europese Unie. Nederland is via de EU vast deelnemer aan de G20 en kan er dus helemaal niet 'uit' gezet worden. In Den Haag is onder eigen naam meedoen echter een wens die van links tot rechts leeft, wederom om het 'internationale aanzien'. Onder deze spin zit een nóg venijniger veronderstelling, namelijk de implicatie dat bij de EU onze economische belangen niet goed gewaarborgd zijn.

De overtreffende trap van spinning is de 'War on'-taal. War on Terror, War on Drugs, **War on Ideas**. In de VS is deze hyperbool al jaren gemeengoed, hier slaat deze woordkeuze wat minder aan, maar we springen wél in het gelid. Voor de War on Terror verstoken we een miljard per jaar om een **inktvlek** te beschermen in Verweggistan en voor de War on Drugs bouwen we ons gedoogbeleid af, tot grote vreugde van crimineel Nederland.

De term 'War' is overtrokken. Je kunt geen pantserdivisies op ideeën, terroristische cellen of straatdealers afsturen. Door de emotionele lading van het begrip oorlog eraan te geven, maak je tegenstanders tot verraders: als je niet voor ons bent, ben je tegen ons. Dat is een frame.

Framing is een **NLP** techniek, die spinning veel effectiever maakt. Mooi is het voorbeeld dat als je een getuige vraagt: 'Heb je de auto gezien?', je vaker een ja-antwoord krijgt dan wanneer je vraagt: 'Heb je een auto gezien? Framing is in ons land nog niet zo bekend, maar door het **voorbeeldige gebruik** ervan door Geert Wilders, zal het veel navolging krijgen.

Zoals de recente geschiedenis leert is veiligheid favoriet bij spinning en framing. Je moet immers verkopen, en **angst verkoopt** nu eenmaal het best. Het nadeel van angst is dat het niet erg meetbaar en niet bestuurbaar is. De juiste dosering is niet te voorspellen. De sluimerende hysterie die vorige maand zichtbaar werd op de Dam, op Wall Street en in het stemgedrag, heeft dan ook velen verrast. Het bewijst dat de angst zeker zo gevaarlijk is als datgene waar we bang voor zijn. Dat inzicht is niet nieuw, Roosevelt zei in de donkerste dagen van de crisis van de jaren 30 al: "There is Nothing to Fear, But Fear Itself[55]".

Onbewust voelen de meeste mensen echter wel aan wanneer ze genaaid worden en dan gaat de angst na een tijdje vanzelf over. Onze overlevingsinstincten zijn uiteindelijk sterker dan alle spin bij elkaar opgeteld. Dat zie je goed in de nieuwe media – op Internetforums wordt nog steeds gedebatteerd over al die onderwerpen die in Den Haag en de traditionele media als gesloten dossiers gelden; de euro, Irak, 9/11, de IRT, noem ze maar op. Dit zijn essentiële uitlaatkleppen: angstige situaties worden geëvalueerd en verwerkt. De dossiers zijn voor de deelnemers niet gesloten omdat de gevolgen er nog zijn en de verantwoordelijken nog op het pluche zitten.

Wat we moeten bestrijden is uiteindelijk niet alleen de crisis of de terreur, maar vooral ook de angst daarvoor. Als genoeg mensen weten hoe het wel zit, en niet in paniek raken, ontstaat er geen kritische massa voor massahysterie. Het middel bij uitstek tegen angst is grip op de zaak. Als je gevaar kunt duiden, krijg je er grip op. Daarmee is het wapen tegen spin en frame kennis en een zelfstandig kritisch vermogen.

Op Internet ontstaat een nieuw collectief geheugen, zeker met dank aan Google dat je regelmatig trakteert op een onbedoelde geschiedenisles door oude pagina's van zeer wisselende kwaliteit als relevante zoekresultaten te tonen. Dan leer je vanzelf dat je niet alles moet geloven wat je leest of hoort. Er is dan ook licht aan het eind van deze lange tunnel.

[55] http://historymatters.gmu.edu/d/5057/

ACTA door de achterdeur

Zaterdag 3 juli 2010

Het aanstaande ACTA handelsverdrag over intellectueel eigendom (“IP”) staat ter consultatie online. ACTA beoogt de bescherming van intellectuele eigendom wereldwijd te harmoniseren. Tot nu toe waren de onderhandelingen en voorstellen geheim. De consultatie vindt plaats binnen het streven van de minister van Economische Zaken om de onderhandelingen alsnog transparant te laten verlopen, waarvoor hulde. Het staat een ieder vrij aan deze consultatie deel te nemen; je hoeft niet met je DigID aan te loggen om je verhaal te doen.

EZ kan echter niet vertellen wat ze zal doen met de inbreng van de burgers. “Op een later tijdstip wordt op de centrale website een verslag op hoofdlijnen geplaatst. In dit verslag staan de resultaten van de internetconsultatie op hoofdlijnen en wordt aangegeven hoe wij met deze resultaten zijn omgegaan. Wanneer dat precies zal zijn, is nog niet te zeggen” citeert **Webwereld** EZ.

Internetconsultaties als deze zijn nog experimenteel. De site meldt de overheid dat je inbreng wel kan gebruiken ‘voor het eventueel verbeteren van het voorstel’. Duidelijk en transparant nietwaar; zo weet je precies waar je aan toe bent. Ik doe mijn plasje over dit onderwerp dan maar gewoon op mijn vertrouwde platform bij Security.nl. Er gebeurt dan ook niets mee, maar daar wordt het tenminste nog gelezen.

Vooropgesteld moet worden dat iedere mogelijk ACTA-regelgeving in ons land best mild kan uitpakken, het opportuniteitsbeginsel maakt dat justitie er maar zo – bijvoorbeeld vanwege hogere prioriteiten – weinig aandacht aan zal besteden. Den Haag kan wel wat bedenken, maar de praktijk blijkt vaak heel anders uit te pakken. Iets dergelijks zien we bijvoorbeeld ook met de anti-kraakwet.

Het is echter moeilijk voorspelbaar, het gaat hier over civiel recht en dat is een heel andere wereld dan het strafrecht. Dat er na invoering van ACTA meer zaken dan nu zullen zijn, ligt wel voor de hand. Hoe een sterk toegenomen werkdruk uitpakt op justitie lijkt duidelijk – zoals de commissie Deetman in 2006 al vaststelde is de kwaliteit van de rechtspraak en daarmee de rechtsstaat in het geding. Al in 2005 luidde de hoge raad de noodklok over het aantal zaken en het daarmee samenhangend kwaliteitsverlies. De gevolgen daarvan halen de laatste jaren met grote regelmaat de pers.

Het ACTA-gebeuren is een opvolger van het **Trips verdrag**, en veel van de bepalingen zijn niet nieuw. Van Trips heeft de burger geen last gehad – behalve dan mensen in de derde wereld die bepaalde dure medicijnen tegen AIDS niet konden betalen en nu dood zijn. ACTA zal ons allemaal, hoe dan ook, wel raken; de bestaande milde jurisprudentie zal door de nieuwe regelgeving geen stand houden. Een nieuw verdrag is een nieuwe situatie zodat er nieuwe afwegingen zullen gelden. Laten we een paar punten uit het conceptverdrag daarom eens nader bekijken.

Aansprakelijkheid
“Parties [may] shall also ensure that right holders are in a position to apply for an injunction against [infringing] intermediaries whose services are used by a third party to infringe an intellectual property right”. Onder deze bepaling kunnen bijvoorbeeld ISP’s en torrent hosters aansprakelijk gesteld worden voor de schade die de uitbater van intellectuele eigendomsrechten zouden lopen. Maar zoekmachines die hun zoekresultaten niet filteren, bouwers van software en

zelfs leveranciers van internet koppelvlakken als de AMS-IX kunnen in theorie aansprakelijk gesteld worden. ‘Intermediary services’ is immers een heel breed begrip.

Nu biedt het verdrag deelnemende landen ruime mogelijkheid de aansprakelijkheid van ‘intermediaires’ te beperken. De eerste uitzonderingsgrond zou kunnen zijn dat het gaat om “automatic technical processes”, zoals de zoekbots van Google. De tweede mogelijkheid is wanneer het gaat om handelingen van gebruikers zonder opdracht en medeweten van die gebruikers: “the actions of the provider’s users that are not directed or initiated by that provider and when the provider does not select the material”. De laatste uitzondering betreft “the provider referring or linking users to an online location”. Op grond van deze bepaling kunnen landen dus een uitzondering maken, waardoor zelfs The Pirate Bay legaal zou kunnen blijven. Voorwaarde is wel dat providers als TPB verwijzingen naar verdacht materiaal “without undue delay” verwijderen. In dat ‘undue’ zit nog een interessant punt: een service provider moet het illegale materiaal verwijderen na melding maar mag dit pas doen als er geen “legally sufficient response from the relevant subscriber of the online service provider indicating that the notice was the result of mistake or misidentification” is. ACTA geeft de aangeklaagde het recht op weerwoord. Dat mag een positief resultaat heten. Natuurlijk kan dit ‘due delay’ ook gebruikt worden als vertragingstactiek om de links nog een paar dagen of weken online te laten, je zult immers per overtreding tot verwijdering gesommeerd moeten worden en per overtreding een antwoord kunnen geven. Dat zullen de IP-uitbaters niet leuk vinden.

Schadeberekening
Zeer relevant is de hoeveelheid schade die IP-uitbaters kunnen claimen; in een civiele procedure is de omvang van de claim eigenlijk het belangrijkste. “in determining the amount” kunnen IP-uitbaters “the lost profits, the value of the infringed good or service, measured by the market price, the suggested retail price” eisen.

ACTA stelt dus doodleuk dat de adviesprijs vergoed moet worden door de overtreder. Dat dit losstaat van de feitelijke schade of de gederfde inkomsten is blijkbaar te moeilijk. Hoe vaak worden goederen tegen de adviesprijs verkocht? Nooit. Van/voor staat al voorgedrukt op ieder prijskaartje maar betekent in het economisch verkeer niets.

Maar ook de feitelijke verkoopprijs is niet belangrijk. Zou iedereen met een nep-rolex van 80 euro ook een echte gekocht hebben, zelfs als deze afgeprijsd is? Zou iemand met twee Terabyte aan mp3’s (wat toch wel een eurootje of honderd gekost heeft) anders 30.000 cd’s gekocht hebben voor een ton of zeven of acht? Tuurlijk niet. Toch worden dergelijke fictieve schadeclaims door ACTA op voorhand gehonoreerd.

Wat moet nog meer betaald worden?
Illegale content moet per direct verwijderd worden, op kosten van overtreder. “each Party shall provide that in civil judicial proceedings, at the right holder’s request, its judicial authorities shall have the authority to order that such goods be [recalled, definitively removed from the channel of commerce, or] destroyed, without undue delay and without compensation of any sort at the expense of the infringer”.

Dat klinkt niet zo vreemd, als je over een website hebt. Alleen het is geen 1996 meer. Hoe vertaal je dit naar de wereld van torrents? Draait de aanbieder van een tracker op voor de kosten van de verwijdering van alle seeders en leechers wereldwijd? Leuk; dan huur je de duurste wereldwijde IT toko in om dat te regelen en legt de rekening bij de overtreder. Dat zal aardig in de papieren lopen en het lijkt mij dat ook dit kostenaspect de toets van de redelijkheid en proportionaliteit niet kan doorstaan. De voorstellen zijn op dit punt wel heel ver verwijderd van de realiteit.

Rechtbanken staan in de regel dichterbij de werkelijkheid en zullen dit punt niet zomaar honoreren.

Spreek- en klikplicht
De aangeklaagde wordt door ACTA verplicht "[for the purpose of collecting evidence] any [relevant] information [information on the origin and distribution network of the infringing goods or services][in the form as prescribed in its applicable laws and regulations] that the infringer possesses or controls" te overhandigendigen aan de IP-uitbater of de rechtbank. Je bent dus verplicht je wachtwoorden in te leveren en te vertellen waar je allemaal materiaal hebt staan. "Such information may include information regarding any person or persons involved in any aspect of the infringement and regarding the means of production or distribution channel of such goods or services, including the identification of third persons involved in the production and distribution of the infringing goods or services or in their channels of distribution". Je moet dus ook je medeplichtigen met naam en toenaam noemen.

De aangeklaagde wordt door ACTA verplicht om belastend bewijs te leveren tegen zichzelf en bovendien verplicht tot het aangeven van medeplichtigen. De overheden zullen vervolgens alle betrokkenen uitleveren aan de advocaten van de IP-uitbaters zodat deze ook aangeklaagd kunnen worden. Fijntjes stelt ACTA dan dat " this provision does not apply to the extent that it would conflict with common law or statutory privileges, such as legal professional privilege". Advocaten vallen dus buiten deze verplichting.

De onderhandelaars hebben blijkbaar nooit gehoord van "Nemo Tenetur", waarbij mensen niet verplicht kunnen worden aan het bijdragen tot de eigen veroordeling. Dit zwijgrecht is een van de meest belangrijke rechtsbeginselen. Een dergelijke verplichting kan wel als bepaling in een verdrag terechtkomen, maar – zoals te doen gebruikelijk in Internationaal recht – treedt dit pas in werking als de nationale wetgeving er iets mee doet. En dat zal in weinig landen lukken; in de meeste beschaafde landen moeten wetten in overeenstemming zijn met de grondwet en de rechtsbeginselen en zal een dergelijke uitzondering geen stand houden bij de hogere rechtbanken. In Nederland is het echter nog afwachten, wij kennen een dergelijke toetsing niet.

DRM
De concepttekst zet – zoals verwacht – zwaar in op Digital Rights Management technologie: het breken ervan moet verboden worden, evenals de middelen daarvoor. Fijn voor de IT industrie die graag DRM-spul wil slijten, maar gegeven dat de bulk van de nu bestaande illegale kopieën voorlopig nog wel online staat is dit hooguit relevant voor nieuwe muziek en films. Daarbij is het technologieverbod behoorlijk vaag; als ik cd's rip over de analoge uitgang van de dvd-speler in mijn computer, breek ik de beveiliging niet maar passeer deze gewoon. Vrijwel iedere wat oudere speler heeft een dergelijke uitgang – is die dan verboden?

ACTA stelt dat je zou kunnen weten dat je daarmee een bescherming passeert en dus strafbaar bent. Welnu, dat is prima. Dan moet er wel op ieder doosje duidelijk komen te staan dat een dergelijke beveiliging aanwezig is – een herhaling van een onzichtbare beveiliging die vervolgens de computer sloopt of op heel veel apparaten niet werkt, zoals we al hebben meegemaakt, moet vermeden worden. Hier voorziet ACTA niet in, en dat is wel een echte tekortkoming. Als er met koeienletters op de hoesjes staat dat de media beveiligd is, kan ik zelf beslissen of ik deze koop en het risico van een systeemcrash of een andere miskoop neem. Hier schiet de bescherming van de consument tekort.

Zal een verbod op het kraken van DRM uiteindelijk zal helpen? Voor het kraken van beveiligde software zijn cracks overal te vinden, en er wordt nooit tegen opgetreden. Het enige gevolg is dat

er een extra vector is om virussen en andere zut te verspreiden. Dit zal voor DRM-cracks niet anders zijn.

Grenscontroles
Aan het optreden aan de grenzen wijdt het verdrag een speciaal hoofdstuk. Hierin wordt ruimte geschapen om 'kleine overtreders' te ontzien: "Parties may exclude from the application of this Section small quantities of goods of a non-commercial nature contained in travelers' personal luggage". Dat is prettig. Minder prettig is dat de douane de gegevens van de mogelijke overtreder, met tal van details mag doorgeven aan de IP-uitbater. Zo wordt de douane een onbezoldigd verlengstuk van de IP-boer. Ik weet niet of ik daar wel belasting voor wil betalen; laat de douane eerst gewoon smokkelaars en terroristen vangen. Maar als minister van Financiën De Jager een factuur kan sturen voor dit opsporingswerk, kan ik er misschien vrede mee hebben.

Het ACTA verdrag wekt met deze douaneregels de indruk aardig compleet te zijn, maar dat is niet zo. Interessante dilemma's in het juridisch domein komen in het geheel niet aan de orde. Zoals de bewijsvoering: als ik 50 GB aan MP3's op mijn harde schijf blijk te hebben bij een grenscontrole, moet ik dan bewijzen dat ik in ze Nederland legaal verkregen heb? Of moet de 'IP-houder' bewijzen dat ik het illegaal heb verkregen? Ik kan er dan fijntjes op wijzen dat ik de 50 gieg aan deuntjes heb gedownload vóórdat dat verboden werd.

Moet ik dat kunnen bewijzen? Prima, dan maak ik vanavond een hash met een timestamp en doe daar een digitale handtekening op; et voila, rechtsgeldig bewijs. Waar kan ik dit bewijs inleveren om te voorkomen dat ik later in Boekiwoekistan aansprakelijk wordt gesteld voor gedrag dat op dat moment legaal was? Zo'n meldpunt is er niet, zodat ik op voorhand weet dat ik niet kan bewijzen de wet niet te overtreden. Evenmin kan de aanklager bewijzen dat ik de wet overtreden heb met het bezit van een hoop mp3's waar ik geen bijpassende cd's of lp's van heb. Bewijs is er pas met een 'heterdaadje', bij de daad van het downloaden zelf. Daar heeft de douane geen zicht op. Het douane artikel is dan ook nogal zinloos.

Gegeven de spelers zal het ACTA verdrag er op enig moment toch komen. Dus ren snel even naar de ijzerboer om een paar schijven van twee Terabyte te halen en trek de komende maanden alle muziek, series en films die je kunt vinden naar binnen. Gewoon alles, inclusief de complete As The World Turns. Dus ook wat je niet leuk vindt – je smaak kan immers veranderen. Wat je binnen hebt gehaald onder de huidige regelgeving, is immers per definitie legaal en ik vermoed dat je de rest van je leven wel toe kunt met alleen muziek en films van vóór 2011. Iedereen wordt een dagje ouder en op enig moment hoeft dat moderne gedoe niet meer, schijnt het.

Maar dan. Mag je deze legaal verworven collectie ook aan je dochter laten horen? Mag je je liedjes op de thuisserver zetten zodat je huisgenoten ernaar kunnen luisteren? Mag je ze op de harde schijf van de laptop van je zoon zetten? En mag hij, als hij uit huis gaat, deze collectie op zijn laptop dan meenemen? Is het 'gebruiksrecht' dat je zou hebben op de muziek en films overdraagbaar? Is dit 'recht' gekoppeld aan een persoon of aan een huishouden?

Als je bestaande collectie door het verbieden de facto gelegaliseerd is, dan mag je die mp3's legaal gaan verkopen, net als dat je nu cd's en dvd's doorverkoopt. Dus als je nu snel alles binnenhaalt wat je kunt vinden, is dat een goede investering voor later. Maar als je je mp3's mag verkopen, hoe zal dan vastgesteld worden dat je niet toch nog een kopietje op een back-up medium hebt staan? Wie controleert dat? Krijgt de stichting Brein toegang tot al je datadragers, ook die niet gemount zijn? Dat is pas een interessante technische uitdaging.

Je gelegaliseerde muziekcollectie zal op enig moment ook deel uitmaken van de erfenis. Tien Terabyte aan muziek heeft volgens de IP-uitbaters een immense waarde, dus daar moeten we niet

lichtvoetig mee omgaan. Moeten je erfgenamen daar successierechten over afdragen? En hoe gaat het bij echtscheidingen?

Vragen, vragen en nog meer vragen, waar ook de laatste ‘reparatiewet’ op de Auteurswet uit 1912 geen antwoord op geeft. En als dit ACTA verdrag leidt tot de volgende reparatiewet, komt dat antwoord er ook niet. Pandora’s doos bevat nog een boel verrassingen.

Kortom. Het ACTA verdrag is een weinig samenhangend, incompleet en vrijblijvend geheel en lost met al haar spierballenvertoon de vraagstukken rond muziekpiraterij in het geheel niet op. Het helpt consument noch IP-boer. Alleen juristen en DRM fabrikanten kunnen hier wat aan hebben. ACTA is in haar huidige koers verspilde moeite. Als de overheid dan toch zo nodig moet bezuinigen op het ambtenarenapparaat, laat ze dan ophouden met het meedoen met dit soort kansloze regelgeving.

Daarbij is deze Internet-raadpleging een staaltje briljante timing in het juridisch schimmenspel rond intellectueel eigendom; een warrig proces vlak voor de zomervakantie, tijdens het WK voetbal en Wimbledon. Zo wordt het besluitvormingsproces wel heel erg **transparant**, zo doorzichtig dat het onzichtbaar wordt.

Ministerie van Veiligheid

Zaterdag 28 augustus 2010

Komt er een Ministerie van Veiligheid? De PVV is groot voorstander, en ook het CDA heeft zich hier al eens sterk voor gemaakt. Het is al sinds de jaren tachtig een terugkerend dossier, bijna een ritueel dat maar niet overgaat. Deze bewegingen zijn al eens treffend getypeerd als 'Stratego op het Binnenhof'.

Het Ministerie van Veiligheid dat er nu wellicht komt, wordt een samenvoeging van grote delen van Binnenlandse Zaken en Justitie. Daarmee heb je natuurlijk nog maar een deel van het veiligheidsgebeuren onder één dak. Wat denk je van Defensie? Nu ja, die moet er ook bij – de PVV wil toch al de KMar probleemwijken in kunnen **sturen**. De douane zal ook moeten verhuizen, van Financiën naar Veiligheid, willen we bommen en illegalen aan de grens kunnen tegenhouden. Hetzelfde geldt voor de gespecialiseerde opsporingsdiensten van andere ministeries. Er komt dus een forse reorganisatie aan, met als resultaat een superdepartement, dat waarschijnlijk in de wandeling MinVeilig gaat heten.

Op zich is de wens voor een reorganisatie wel begrijpelijk. Partijen die roepen om keihard optreden op een heel specifiek dossier lopen telkens vast in de huidige structuur, waarbij burgemeesters uiteindelijk de baas zijn. Zo is het hard bevochten kraakverbod feitelijk van tafel, omdat andere zaken een hogere prioriteit krijgen van de korpscommandanten. Hetzelfde zie je rond softdrugs: de landelijke politiek kan hoog of laag springen, maar heeft uiteindelijk heel weinig te vertellen. De politiek zoekt nu grip op de uitvoering van de criminaliteitsbestrijding en wil daarom centraliseren – politie en justitie op één grote hoop en dat dan in Den Haag.

Er zijn voors en tegens. De huidige ingewikkelde structuur is opzettelijk zo ingericht. Zij creëert bewust afstand tot "Den Haag", om te voorkomen dat de politiek – de wetgever – te veel directe invloed op rechterlijke en uitvoerende macht heeft. Die drie afzonderlijke machten, de Trias Politica, daar is de hele beweging tot centralisatie nu juist tegen gericht.

De Trias Politica heeft het in Nederland al jaren zwaar. De uitvoerende macht, het kabinet, maakt de wetten, waar de wetgevende macht, het parlement, dit zou moeten doen. Nu doet de uitvoerende macht ook nog eens een greep naar de rechterlijke macht. Het openbaar Ministerie heeft steeds meer rechterlijke macht; tal van zaken worden zonder rechter afgehandeld, omdat dat doelmatiger is. Zorgvuldigheid is immers maar lastig en bovendien kostbaar. Weet je wat ook goedkoop en doelmatig is? De hele rechtsgang afschaffen. Komt ook nog vast wel een keer.

Eén groot Ministerie voor Veiligheid is omstreden. Mensen vrezen dat het zal leiden tot te grote machtsconcentratie en dat het een voorbode is van een autoritaire dictatuur. Alle macht centraal in Den Haag is hen een gruwel. Nou deel ik die angst niet; grotere organisaties leiden steevast tot grotere mislukkingen – kasten vol beleid en uitvoerenden die hun eigen gang gaan door de interne afstanden. Chaos en anarchie dus, niks dictatuur. Of het zou een dictatuur van het onvermogen moeten zijn.

Het **COT**, een ongrijpbaar instituut voor veiligheids- en crisismanagement pleit juist wel luid voor een dergelijke centralisatie: "Nederland heeft slecht gereageerd op de grote incidenten en crises van 2009 en moet daarom een Ministerie van Veiligheid krijgen". Het COT kwam tot deze conclusie na **analyse** van de reactie van de overheid op onder andere de Q-Koorts, de rellen bij Hoek van Holland en het Koninginnedagdrama in Apeldoorn. Blijkbaar moet dit Haagse

Ministerie van Veiligheid ook belast worden met volksgezondheid en lokale evenementen? Het wordt steeds groter.

Afgelopen zaterdag **pleitte** OM-topman Harm Brouwer in het NRC voor één landelijke politie. Hij liet in het midden of dit onder dit nieuwe ministerie moet vallen, maar gegeven de timing in de formatie is het duidelijk dat de stellingen binnen het politie- en justitielandschap ingenomen worden. Er zijn natuurlijk ook nogal wat bestuurlijke baantjes te vergeven.

Volgens Brouwer moet de politie op dit moment tachtig procent van de georganiseerde bendes die zich bezighouden met drugs- en mensenhandel laten lopen, wegens capaciteitsgebrek. De korpsbeheerders laten vaak andere zaken voor gaan, zoals evenementen. Zonder capaciteitsgroei (en die is met de begroting van Rutte I niet te verwachten) is de interessante vraag dus, hoe de schaalvergroting van de fusie tot de doelmatigheidswinst leidt, die zoveel capaciteit vrij maakt dat de grote boeven nu wel gepakt gaan worden. Terwijl ook de evenementen en andere prioriteiten bediend worden natuurlijk. Waar komen de synergievoordelen vandaan? Er is immers al een hoop samengevoegd in overheidsland. Korpsoverschrijdende werkzaamheden liggen bij de landelijke politiediensten verenigd in de KLPD. Die paraplu is er al meer dan tien jaar. Als die niet goed functioneert, dan is het toch beter om dat te repareren dan een grootschalige hervorming te beginnen, met alle problemen van dien. Maar daar gaat het ook niet om: het OM wil grip op de politie krijgen om haar eigen prioriteiten te stellen en verwacht dit via een Nationale Politie te kunnen doen. Er zullen in de toekomst nog wel meer evenementen niet doorgaan omdat de politie geen capaciteit heeft om ze te beveiligen. Hoe het dan met het **WK in Nederland** moet weet ik ook niet.

De Vereniging van Gemeenten (VNG) en het Nederlandse Genootschap van Burgemeesters willen juist geen gecentraliseerde nationale politie. Hun argument is dat het merendeel van de criminaliteit en dus van de politie-inzet lokaal of regionaal is. Dit betekent dat de 80% niet aangepakte misdadigers waar Brouwer naar verwijst het grootste deel van maar een heel klein stukje van de totale criminaliteit is. Volgens de WODC, het wetenschappelijk instituut van de rechtbanken, is de omvang van de 'georganiseerde criminaliteit' **niet te meten** dus het gaat over 80% van iets niet meetbaars. Daar heb je wat aan.

Het CBS lijkt de burgemeesters **gelijk te geven**; het overgrote deel van de misdrijven is duidelijk niet georganiseerd en dus lokaal. Nu kun je de ernst van een delict meewegen, maar dat is al snel niet meer objectief. Moord en geweldsdelicten zijn nog wel duidelijk, maar drugs? Sommige mensen beschouwen grotere wietkwekers als zware criminelen terwijl bijvoorbeeld de wietrokers dat héél anders zien. Zelfs Bolkestein is nu voor **decriminalisering** van softdrugs en dus kan de VVD kwekers moeilijk als zware criminelen neerzetten.

De VNG is bang dat met een nationale politie de grip op de wijken verloren gaat. "Hoe moet je vanachter een bureau in Den Haag bepalen waar politie-inzet nodig is?" Ze vrezen traagheid en afstandelijkheid, wat niet onlogisch is – grote organisaties hebben zelden slagkracht, iets dat bij de overheid toch al een aandachtspuntje mag heten. Volgens deze betrokkenen zal de voorgestelde oplossing de problemen juist verergeren.

Eric Nordholt, oud-korpschef van de politie Amsterdam zegt: "Het veiligheidsvraagstuk in Nederland is terug te voeren op een ernstige leiderschapscrisis op dat gebied. Met het samenvoegen van twee ministeries verandert slechts de structuur, daarmee los je het probleem niet op". Ook voormalig procureur-generaal prof. De Wijckersloot **noemt** het "een verkeerd antwoord op de verkeerde vraag".

De tegenstanders hebben een punt. Bestaande lokale en regionale samenwerkingsverbanden van gemeenten, brandweer, politie, GGD'en en andere diensten die in crisissituaties worden ingezet, dat zijn de partijen die het allemaal moeten doen. Het veranderen van de topstructuur zal niet bijdragen aan het verbeteren van de 'output & outcome' van die regionale en **lokale veiligheidsketens**.

Het superministerie zal zich als grote organisatie van nature richten op grootschalige oplossingen. Bovenaan komen de nieuwe en dus nog niet geclaimde dossiers die het goed doen in politiek Den Haag. Deze hebben meestal maar weinig te maken met de alledaagse banaliteit van veiligheid en ze mijden de weerspannige achterban binnen de veiligheidssector. Het Ministerie van Veiligheid zal daarom als vanzelf ontaarden in een Ministerie van Internet- en Cameratoezicht.

En wie wordt de baas op dit superdepartement? **Volgens** de Telegraaf: Fred Teeven, de barokke Officier van Justitie die nog even fractievoorzitter van Leefbaar Nederland was. Over Teeven valt veel te vertellen. Ik noem slechts een paar dingen. Hij heeft veel ervaring met het doorbreken van allerlei bureaucratische lagen en dat is een vaardigheid die op het aanstaande fusiedepartement hard nodig is. En nu Fred van **privacybestrijder**, opeens **privacybeschermer** is geworden zouden we blij moeten zijn.

Wel een beetje jammer is dat Teeven niet altijd even veel ontzag heeft voor de gevestigde rechtsstaat; hij zoekt naar eigen zeggen graag de grenzen van de regeltjes op. Dat hij daarbij jarenlang op heel veel **tenen** is gaan staan, helpt niet. Teeven zelf stelt dat het als 'Crime-Fighter' nu eenmaal onvermijdelijk is dat hij wel eens een **klein beetje** over **de grens van het toegestane** is gegaan.

Een klein beetje over de grens? Teeven geldt als de uitvinder van het '**begeleid doorvoeren**' in het Delta Onderzoek (IRT affaire), waarbij tonnen cocaïne en honderden tonnen softdrugs op de Nederlandse en Belgische markt kwamen. Teeven hoopte in die periode bewijzen rond te krijgen van zeer omvangrijke corruptie aan de top van Justitie, en sloot hiervoor ook een **deal** met Mink K. De in 1994 voor wapenbezit tot zes jaar veroordeelde Mink K. kan zich sindsdien weer **vrij bewegen** in ons land en zijn carrière voortzetten. Hij kwam de deal echter niet na (opmerkelijk, nietwaar) en ringeloorde Teeven: de corruptiezaak kwam nooit van de grond. Op grond van welke bevoegdheid een Officier van Justitie een gerechtelijke veroordeling tot celstraf kan omzetten in een boete vertellen de stukken niet.

Grenzen van regeltjes opzoeken? Een Officier van Justitie is geen rechter en de 'begeleide doorvoer' met infiltranten was op dat moment **expliciet verboden**. Tegenover de parlementaire commissie Van Traa stelde Teeven niet van de details van de begeleide doorvoer te weten en alleen formeel een beetje verantwoordelijk te zijn, wat Van Traa overnam in het eindrapport. Politiechef Van der Putten verklaarde echter **onder ede** dat Teeven wel op de hoogte was. De rijksrecherche bevestigt dit in **haar onderzoek** naar de RCID Kennemerland. Het lijkt er veel op dat hij tegen de parlementaire commissie heeft gelogen. Onder ede.

Neuh, dit gaat niet over "een klein beetje over grenzen van de wet heengaan, omwille van het grotere belang". Deze leugen diende alleen zijn eigen belang. De beoogde minister is op z'n best een bestuurlijke draaikont voor wie maar één ding telt – zijn eigen positie. Dat voorspelt voor het aanstaande ministerie van Veiligheid, een fusiedepartement met onwillige partners, weinig goeds. Weinig medewerkers zullen staan te popelen om zo'n baas. Bij Justitie lopen nu eenmaal bovengemiddeld veel mensen rond die regels wél belangrijk vinden. Geen goede uitgangspositie voor zo'n zware baan.

Maar is er nog hoop. Want hoewel de vorming van een superministerie en een nationale politie al jaren op de agenda staat, is het er nog nooit van gekomen. Hopelijk loopt het ook deze keer weer met een sisser af. Bedenk dat beide beoogde coalitiepartners het dossier veiligheid uit electorale overwegingen niet aan de ander kunnen overlaten. Bovendien beschouwt het CDA justitie als haar eigen terrein; deze partij heeft het sinds 1989 (Lubbers II) bij justitie voor het zeggen gehad, met als enige onderbreking de twee paarse kabinetten en na het struikelen van Hirsch Ballin over de IRT affaire in 1994. Rutte zal Verhagen dan ook veel moeten bieden om het superministerie aan Teeven te laten, en Verhagen is vakman genoeg om deze troefkaart maximaal te benutten. Rutte is bovendien ook vast nog niet vergeten dat Teeven meer voor **Verdonk koos**, dan voor hem. Met twee ministeries echter, komt elke partij aan zijn trekken en dat is wel een veel gemakkelijker uitweg in een formatie.

Mijn advies: hou nu maar eens op over een ministerie van Veiligheid. Samenvoegen, splitsen, ijken, herijken – het zijn rookgordijnen voor slechte resultaten. Iedereen die wel eens in een groot bedrijf heeft rondgehangen, herkent dit plan als een reorganisatie die alleen bedoeld is als bezigheidstherapie voor het management; bordjes omhangen in het beleidsgebouw maar niets veranderen in de productie. De aandeelhouders denken dat het goed komt, het personeel weet wel beter. Deze rondedans van veiligheidsbestuurders toont aan dat ze verstand hebben van bestuurlijke bezigheidstherapie en uitstelstrategie, maar niet van veiligheid. Dit ministerie zal niets bijdragen tot meer veiligheid in Nederland. De ene lappendeken wordt vervangen door een andere, gemaakt van dezelfde stukjes stof. Of erger: door de complexiteit van de fusie zullen de betrokken diensten langdurig minder aandacht voor hun taken hebben, zodat de criminaliteit goede tijden tegemoet gaat. Wat natuurlijk wel weer leidt tot een luidere roep om meer veiligheid. Zucht.

Donkere wolken

Maandag 13 september 2010

Noem het maar een managementuitdaging. Want dat is dat hele cloudgedoe, uiteindelijk. Geen technisch probleem, maar een besturingsprobleem. Om het juiste buzz-word te gebruiken: cloud computing is een governanceprobleem en een hele grote.

Vraag een IT manager: “Doen Jullie Al Aan de Cloud?”, dan is het antwoord meestal iets van “we kijken er naar”, of “op dit moment niet, wellicht later”. 68% van de CIO’s zegt dit, **meldt** de Automatiseringsgids. Het argument bij uitstek van de IT-manager is de twijfel over de veiligheid van de cloud en over de volwassenheid van de technologie. Zo, voorlopig zijn we klaar; het is niet veilig en het is niet goed.

Maar neem je de moeite om verder te kijken in de organisatie, dan zie je waarschijnlijk een heel ander verhaal. Bij steeds meer organisaties kopen mensen van ‘de business’ diensten uit de cloud in, zonder het aan IT te vertellen. HR doet een paar eHRM applicaties, sales gebruikt Salesforce, bij de boekhouding hebben ze een stukje Twinfield en ga zo maar door.

Gartner **stelt** dat één op de vijf organisaties over twee jaar geen IT spullen meer heeft, en alles in de cloud doet. Dit is wel een memorabele misser van Gartner; geen enkele organisatie zal zijn bestaande spullenboel versneld afschrijven en binnen twee jaar alles kunnen migreren.

Toch is dit bericht, voor de IT-ers die Gartner geloven, zeer zorgelijk. Als het waar is wat ze zeggen, ook als het iets langzamer gaat, dan betekent dat voor de meeste IT-ers ontslag, feitelijk. Het is dan ook logisch dat de IT niet staat te popelen om in de cloud te duiken; als een kalkoen die over het kerstdiner adviseert. Het IT management zit met de kop of met de hakken in het zand.

Dat is nergens voor nodig.

De cloud brengt ons terug naar de eilandautomatisering zoals we die in de jaren ’90 kenden. Voor wie dat niet meegemaakt heeft: bij eilandautomatisering heeft iedere afdeling in de organisatie allerlei eigen spulletjes, die ze zelf hebben gekocht. Had je software nodig, dan kocht je dat en installeerde het op je pc. Of je leende het van een familielid of een vriend bij een ander bedrijf.

De nadelen van eilandautomatisering spelen bij de cloud ook. De productselectie geeft alleen aandacht aan gebruikersbeleving en negeert zo’n beetje alle andere ‘kwaliteitsattributen’ die we in de IT kennen, zoals schaalbaarheid, migreerbaarheid en veiligheid. De business denkt vooral na over hoe je de cloud in gaat, maar hoe je er ooit weer uit komt is niet aan de orde. Dan ga je niet de cloud maar de mist in, uiteindelijk.

De business mist de kennis en ervaring om de kwaliteit te beoordelen. Nu zijn er cloud aanbieders die van alles goed doen. Dat benadrukken ze ook in glimmende folders: goede beveiliging op de servers, maandelijkse pentests, sterke crypto en Intrusion Prevention, allemaal zaken die de meeste organisaties zelf niet op orde hebben, zitten volgens de marketing in het pakket. Dus, is de redenatie van de business, zij kunnen het wel, en onze eigen IT niet.

Daar is nogal wat op af te dingen. Ten eerste vergelijk je een folder van een leverancier met de dagelijkse realiteit van je eigen IT. Dat is al een lastige. En wat is ‘van alles’, is dat hetzelfde als ‘alles’? Om dat te kunnen beoordelen moet je het geheel kunnen overzien, en weten wanneer de beveiligingsarchitectuur compleet is. Sterke crypto heeft bijvoorbeeld weinig zin als er een groot

gat in de applicatie zit. De benodigde kennis daarvoor is in de IT al schaars, en het is vrijwel uitgesloten dat de mensen die voor hun eigen eilandje iets kopen, dit kunnen overzien. Kortom, hier komen ongelukken van. Je ziet de post-its met wachtwoorden van cloudapplicaties al weer verschijnen op de hoeken van de beeldschermen. Er is ook al een term voor aangeschafte cloudapplicaties die toch maar niet gebruikt worden: Shelfware as a Service.

Maar waarom doet de business dit dan toch? Wij IT-ers hebben verdorie de afgelopen tien jaar al die wildgroei teruggeduwd en nu doen ze het weer!

De cloud is goedkoop, dat is waar. Maar dat is niet de voornaamste drijfveer om maar van alles voor je eigen eilandje te gaan kopen. De voornaamste 'business driver' is 'agility'. Ik druk het even uit in de geheimtaal van het management, ja. Agility wil zeggen dat je sneller over nieuwe spullen kunt beschikken, ook over spullen die niet in de schaalgrootte van de organisatie passen. Als je met twee boekhouders bent, dan kun je misschien na veel gedoe een simpel pakketje aanschaffen, maar dat zal wel een kale bedoening worden. Voor iets luxueuzers is al snel een hele server nodig en dan wordt het te moeilijk en te begrotelijk en dan mag het niet.

Dit speelt ook in grotere organisaties. De IT is onder druk van bezuinigingen met allerlei consolidatie en standaardisatie gaan uitblinken in eenheidsworst: het hele bedrijf mag maar één boekhoudpakket gebruiken. Terwijl er vaak toch meerdere soorten boekhouding zijn, maar de interne IT is zelden groot genoeg om specialisten in twee verschillende CRM-applicaties zinvol aan het werk te houden. Nou ja, of ze willen dat gewoon niet betalen. Het gaat dus ook om de kwaliteit van de beschikbare specialisten. Agility was een van de voornaamste drivers voor de outsourcingsmode van een paar jaar terug. Outsourcing is het niet geworden, vooral omdat blijkt dat je dan niet één, maar verschillende ivoren torens hebt, die onderling lopen te soebatten waardoor alles nog erger wordt.

De ivoren toren van de jaren 70 is na 2000 weer in ere hersteld: de IT is ongenaakbaar, autoritair en onnoemelijk traag. Bij de ABN/AMRO duurde het heel **veel langer** om Internet Explorer 5.5 of XPSP2 uitgefaseerd te krijgen dan om de bank te koop te zetten, te verkopen, te splitsen, failliet te laten gaan en te nationaliseren.

Security is gekaapt om de nering en het werkcomfort van de IT veilig te stellen, meer dan de veiligheid van de organisatie. Omwille van de security mogen gebruikers niets meer lokaal installeren, wat ook afgedwongen wordt door het besturingssysteem, dus als business heb je maar te slikken wat IT doet. En bovenal, niet doet. Want de installatie van een nieuwe browser is afhankelijk van een nieuw service pack. Nou, en dat is dus onveilig. De IT doet niets omdat iets repareren wat nu al stuk is, misschien iets anders stuk zou kunnen maken, maar ze weten niet wat. En voor dat niets doen en niet weten willen ze ook nog salaris.

De business ziet dat je in de cloud zonder gedoe en gezeur twee verschillende boekhoudpakketten kunt gebruiken en dat IT daar niets tegen kan doen. En doet het dan ook.

De CIO die zegt dat er geen cloudapplicaties worden gebruikt omdat ze nog niet veilig en volwassen zijn, is de kruidenier die stelt dat de concurrerende supermarkt slechtere waren verkoopt. Nu is het uitstekend dat de kruidenier gelooft in zijn eigen winkel. Maar als zijn klanten steeds vaker naar de supermarkt gaan, moet de kruidenier toch eens heel erg goed gaan nadenken.

De IT kan de cloud computing-hype ook negeren. Gewoon wachten tot het overgaat. De outsourcingshype ging ook over. Uiteindelijk zullen de ontwikkelingen wel weer bij elkaar komen en zullen bedrijven naar een hybride model gaan. Sommige dingen zullen in de cloud

terechtkomen, andere in India en ook nog van alles in het eigen rekencentrum. De interne IT zal de regie hebben en de kwaliteit bewaken. De IT afdeling zal dan wel anders moeten zijn dan we nu gewend zijn, en beveiliging ook.

De ontwikkeling daarnaartoe kan maar zo tien jaar duren, net als de eilandautomatisering die begon met Windows for Workgroups en eindigde min of meer met Windows XP. Dat waren tropenjaren. In plaats van de klanten beter te bedienen gingen we ze bestrijden, met als gevolg veel stress en kwaaie koppen. Het netto resultaat is dat de meeste gebruikers anno 2010 vrijwel dezelfde IT-functionaliteit hebben als in 1996.

De uitdaging voor IT op dit moment is om de regie, feitelijk de makelaarsrol, naar zich toe te trekken. Gebruik de regie nu al om de balans tussen agility en kwaliteit te vinden, niet om de deur voor de concurrentie dicht te houden. Anders raak je de controle snel weer kwijt. Bepaal waaraan cloud applicaties moeten voldoen om goed genoeg te zijn, help de business kiezen of zoek ze zelf, en zorg voor migreerbaarheid, integratie en beveiliging.

De cloud systemen zelf worden door de leverancier beveiligd, dan vraag je om de testrapporten en auditorsverklaringen. Beveiliging van de cloud applicatie is echter niet hetzelfde als beveiliging van jouw informatie, al staat-ie daar. Security krijgt de uitdaging om de cloud, interne en externe leveranciers in één virtuele perimeter te vangen, zodat de eigen middelen daadwerkelijk voor eigen gebruik alleen zijn. De grote beveiligingslast komt op het stuk tussen de applicatie buiten de deur en de eigen systemen. Dit stuk is complex en je moet het zelf doen. Je bent er nog lang niet met een SSL-VPN. Contracten en procedures helpen ook niet; stukken papier vangen geen bad guys.

Het gaat bij de cloud om webapplicaties waarbij iedereen aan de voordeur kan rammelen, dus het aanloggen wordt veel belangrijker dan bij interne systemen. Wil je cloud applicaties beveiligen, dan zul je als vanzelf uitkomen op sterke authenticatie. En omdat je het hebt over meerdere cloud applicaties, dan praat je automatisch over federatie – je kunt moeilijk gebruikers voor iedere cloud applicatie een nieuw pasje geven, toch? Single Sign On naar de cloud is bovendien wel zo kosteneffectief. Ook zul je waarschijnlijk een soort ‘Cloud Portal’ opstellen, als een gezamenlijke presentatielaag. Je wil niet dat iedereen de cloud-URL’s gewoon op de desktop zet, en zelf verandert als je – heel Agile – van cloudleverancier wisselt? En zodra je cloud applicaties gaat integreren met eigen applicaties of met elkaar, moet je deze web services beveiligen. Ze zitten in tal van https-domeinen, dus je zult diep in de WS-Security en OAuth moeten duiken om hier de juiste antwoorden voor te vinden.

Last but not least zul je de security monitoring ergens moeten integreren; de enige plek waar je de bewaking kunt bedienen, is vanuit de eigen organisatie. Natuurlijk wil je de applicaties zelf ook weer in de cloud kunnen draaien (SIEM as a Service?), en de datastroom naar buiten kunnen richten in plaats van naar binnen. Het werk blijft echter hoe dan ook binnen. IT en Security hebben dus andere kennis en een andere inrichting nodig dan nu. Dat kost tijd, en anders héél veel geld. Je snapt wellicht dat de cloud niet gratis zal zijn in de praktijk. Voor niets gaat immers alleen de zon op. Het kan wel behoorlijk wat goedkoper zijn dan sommige interne IT clubs. Er zijn er die 60.000 euro per jaar rekenen voor een eenvoudige bladeserver zonder stroom, netwerktouwtje of besturingssysteem. Tja, dan gaan je klanten wel lopen.

Ik wist niet dat ik het ooit nog eens serieus ging opschrijven, maar Gartner heeft op **één punt** wel gelijk. Gartner stelt namelijk dat het tijd is om als IT een strategie op te stellen voor cloud gebruik en de hakken uit het zand te halen. Het IT-management kan zich een aantal zware jaren besparen, door nu al de regie te nemen. Bedenk daarbij dat hoewel de cloud hype vast wel weer overwaait,

de klant ontevreden blijft als we de cloud net zo klantonvriendelijk verpakken als we met de rest van de IT hebben gedaan.

De veiligheid voorbij (1)

Vrijdag 1 oktober 2010

Het rommelt bij Justitie. Lege kas, hoge werkdruk, ICT-gedonder en fout op fout in rechtszaken. Over het ICT-gedonder in deel twee meer. Nu eerst iets over de rechters, de burgers, de bezuinigingen en de kwaliteit van onze rechtspraak. Om het gerommel te verbeteren is Justitie op zoek naar geld, en gebruikt steeds meer het 'profijtbeginsel'; hogere boetes, meer plukze, meer boetes in plaats van andere straffen. De hoogte voor een snelheidsboete wordt niet meer bepaald door de ernst van de zaak, maar door financiële nood bij Justitie.

Een ambtelijke commissie moest april dit jaar al een **bezuiniging** van 2 miljard op een begroting van 10,3 miljard vinden. "Het is de werkgroep gebleken dat een algemene bezuiniging zonder daarin nadere keuzes te maken (overal 20% af) het risico oplevert dat het niveau van de veiligheidszorg dat bereikt is met de extra inzet over een langere periode al snel teniet wordt gedaan". Om toch de doelen te bereiken stelde de commissie onder meer voor om vrijwilligers in te schakelen op lokaal niveau. Bijvoorbeeld als onderdeel van een sociale dienstplicht. Ook is gekeken of de Koninklijke Marechaussee voor opsporingstaken ingezet zou kunnen worden, en waar er taken naar gemeentes en particuliere instellingen 'overgeheveld' konden worden.

Overhevelen is niet hetzelfde als bezuinigen. De kosten komen dan immers alleen uit een ander potje. En ook dat andere potje moet door dezelfde burgers gevuld worden. Ook de inzet van 'sociaal dienstplichtigen' als gratis personeel is een uitvlucht; een dergelijk programma bestaat niet, en het is nogal de vraag of jongelui zonder startkwalificatie op de arbeidsmarkt wel voldoende kwaliteit in huis hebben om Justitie te helpen. Natuurlijk rouleren er voorstellen om sociale dienstplicht in te voeren voor álle jongeren. Maar daar staan de werkgevers dan weer niet zo om te springen denk ik. De toestroom aan jongeren op de arbeidsmarkt wordt toch al steeds **dunner**.

De vergezochtheid van de voorstellen laat zien dat de commissie er gewoon niet uit kwam. Dat is helemaal geen schande. Justitie is de afgelopen jaren al behoorlijk uitgekleed door een bombardement van extra taken en minder geld. Het niveau is op dit moment dan ook zeer bedenkelijk .

De situatie is bar en boos. Vonnissen worden voor de zaak alvast **geschreven** door de griffier, de rechter krijgt een uurtje om een dossier van **1000 pagina's** te lezen, en in meervoudige kamers verdelen de rechters **onderling** de zaken, waardoor het doel van de meervoudige kamer vervalt. Daarnaast zijn er al tal van taken en bevoegdheden omlaag overgedragen, zodat politierechters zwaardere zaken mogen behandelen en lichtere zaken door het OM afgehandeld worden. Nu is het OM geen rechter, en omdat zij rechtstreeks onder de verantwoordelijkheid van de minister valt **géén onafhankelijk orgaan**. In het ergste geval kan de minister middels een aanwijzing het OM een bepaalde straf laten opleggen. Een vooruitzicht waar ik met de politieke geldingsdrang die het veiligheidsdossier bepaald, niet vrolijk van word. De partijen in een rechtszaak krijgen steeds minder kans om gehoord te worden, waarmee de uitspraak een loterij wordt. In deze organisatie, die al jaren onder zware druk staat, moet nu nog een keer heel veel veranderen.

De gouden driehoek geldt ook de overheid; als de hoeveelheid taken niet afneemt maar het budget wél, daalt de kwaliteit. En als er dan nóg meer taken bij komen, gaat de kwaliteit nog verder omlaag. Misstanden en dwalingen van onze rechterlijke macht worden nu nog als

“incident” afgedaan, en zo mogelijk met de mantel der liefde bedekt. Het gaat echter om structurele bedrijfsongevallen met een banale oorzaak: een overbelaste organisatie.

Op dit moment hangt de rechtstaat af van de onbezoldigde inzet in privétijd van justitiepersoneel; als er iets goed gaat is het bijzonderder dan als er iets fout gaat. De komende jaren gaat bovengemiddeld veel van het rechtbankpersoneel met pensioen en vervanging met vergelijkbare kwaliteit is nu al een schier onmogelijke opgave. Met de kaasschaaf die nu over salaris en pensioenrechten heengaat, wordt het vooruitzicht zo mogelijk nog somberder. Een mogelijke uitwijk door de inzet van externen wordt bestuurlijk afgesneden, maar zal er in de praktijk toch van komen. Straks komen ook de rechters van een detacheerder.

Een minister is in feite een soort directeur, en we hebben hier een directie die de BV Rijksoverheid met steeds nieuwe taken en aandachtsgebieden blijft opzadelen, zonder zich af te vragen wat dit met de productiecapaciteit doet. Bovendien regent het nieuwe regels uit Brussel. Wat er bij onze directie maar niet in wil is de ijzeren wet: nieuwe wetgeving = nieuwe taken. En de eerste afgeleide: minder geld = minder taken. Zo niet: dan minder kwaliteit.

Nieuwe taken zonder nieuwe uitvoeringscapaciteit leidt tot lagere kwaliteit. Nu kun je wel heel gemakkelijk zeggen ‘dat die ambtenaren dan maar harder moeten werken’, maar dat is een flauwe. Ten eerste: welk inspirerend leiderschap zal ze daartoe brengen? Ten tweede: sommigen ambtenaren zullen er nog wel een schepje bovenop kunnen doen, maar harder werken is zelden hetzelfde als beter werken. Na een uurtje of 50, 60 per week ga je toch significant meer fouten maken. En bij de rechtbank betekent dit: foute uitspraken. Justitie gaat dus nog verder het hellend vlak op. De maatschappij eist een foutloze rechtspraak, de overheid levert dit bij lange na niet en haalt de schouders op bij het volgende ‘incident’.

De snelste manier om het vertrouwen in de overheid te verliezen, is het aanspannen van een rechtszaak. Gegeven dat er tegen de twee miljoen zaken per jaar zijn, is de kans voor iedere burger om geconfronteerd te worden met een gerechtelijke dwaling behoorlijk groot. 95% van die twee miljoen zaken zijn civiel, en juist in deze lopendebandzaken gebeuren de meeste ongelukken. Het zijn kleine zaken, vanuit Justitie bezien, maar belangrijk voor de betrokkenen. De grote drama’s zijn dus niet zo snel te vinden in vrijspraak voor schuldigen, zitten voor onschuldigen, en andere publicitaire rampen, zoals proefverlof voor de verkeerde TBS-er, maar de ervaring bij gewone burgers dat hun rechten niet gewaarborgd worden door de overheid. En laat dat nu net de bestaansgrond van de overheid zijn, het beschermen van de burger.

De veiligheid voorbij (2)

Maandag 11 oktober 2010

De dagelijkse werkelijkheid bij de rechtbank belooft weinig goeds voor de aanhoudende reeks oprispingen van juridische daadkracht, zoals het recente wetsvoorstel computercriminaliteit. In dit voorstel zou het Openbaar Ministerie de bevoegdheid krijgen om ‘strafbare’ informatie van internet te laten verwijderen zonder tussenkomst van een **rechter**. Het verzet hiertegen werd geleid door het onvolprezen Bits Of Freedom en een aantal internet publicisten als **Bert Brussen**. Een meerderheid in de kamer **floot** minister Hirsch Ballin op dit punt terug. CDA en PVV waren blijkbaar voor.

deze column is het vervolg op De veiligheid voorbij (1)

Het voorstel is feitelijk een voorbode op het ACTA verdrag, hoewel dat er niet bij verteld wordt. Door de verwijdering van illegale content van websites een hamerstuk voor het OM te maken,

kan de minister de rechtbanken vrijwaren van de extra werkdruk. Het OM kan zonder vervelend geneuzel als het horen van de aangeklaagde en andere waarborgen van de rechtstaat nu eenmaal veel efficiënter werken. En, geef nou toe, voor ieder MP3-tje op een Hyves-pagina de rechtbank inzetten leidt inderdaad tot een belachelijke werkdruk.

Dit voorstel was geen persoonlijke hobby van de vorige minister maar een uiting van het denken van de beleidsfabriek bij justitie. Wetgeving en flankerend beleid worden voorgesteld door de beleidsambtenaren, niet door de politiek. Een minister is vanuit het departement gezien toch vooral een goedkope interim manager. Dus dit voorstel zal zonder veel veranderingen gewoon terugkeren, maar dan vanuit een missionair kabinet zodat de VVD niet dwars kan liggen, zoals nu gebeurd is. Zeker nu het Europees Parlement in een motie heeft gestemd voor een strenge ACTA, is een terugkeer van dit voorstel in de één of andere vorm hoogstwaarschijnlijk. Het nieuwe kabinet zal zeker geen radicale breuk met het vorige zijn. Juich dus niet te vroeg.

Het grootste probleem met het voorstel is niet dat het een vorm van censuur introduceert, terwijl we nu geen censuur zouden hebben. Het leidt tot censuur, dat wel. We hebben ook nu al allerlei vormen van censuur, zoals het verbod op godslastering, NSB-kranten en haatzaaien illustreert. Deze verboden worden alleen in de praktijk zelden toegepast, omdat vervolging zeer arbeidsintensief is, met een lage kans op een veroordeling.

Het grootste probleem is ook niet dat de bevoegdheid bij het Openbare Ministerie wordt neergelegd, zodat je alleen achteraf kunt protesteren tegen het verwijderen van bepaalde content. In plaats van klagen kun je de gegevens immers op een server in het buitenland zetten. Het is hooguit vervelend voor Nederlandse ISP's.

Het allergrootste probleem is ook niet dat webpublicaties anders behandeld worden dan andere media. Als het OM vergelijkbare bevoegdheden zou krijgen over kranten en televisie zou de wereld te klein zijn om alle kritiek te bevatten. Dit verklaart waarom de traditionele media weinig aandacht besteden aan de internetcensuur, omdat het over hun concurrenten gaat, en ook voor journalisten geldt dat het hemd nader is dan de rok.

Ook niet het allergrootste probleem in het voorstel is dat iedere censuurmaatregel te allen tijde een zorgvuldige afweging vraagt, en dat de kans daarop – gegeven de stand van zaken bij justitie – oneindig klein is. Hoeveel minuten zullen de richtlijnen toestaan om te beoordelen of content 'strafbaar' is?

Wat is dan wél het grootste probleem?

ACTA gooit alle intellectuele eigendomsrechten op één grote hoop. Om het verdrag erdoor te krijgen moet er immers een breder belang in het spel zijn dan alleen dat van de mediaindustrie. Een vertaling naar lokale wetgeving moet dit uitgangspunt volgen, en dat is precies wat Hirsch Ballin heeft gedaan. Daarom wilde de minister het publiceren van "niet openbare gegevens zonder toestemming" via het OM strafbaar stellen. ACTA dendert als een losgeslagen trein op ons af, en Justitie zet zich schrap voor de extra werkdruk. Hirsch Ballin staat daar en hij kan niet anders.

Laat het volgende even door je hoofd spelen. In de strijd tegen de illegale mp3 wordt het publiceren van niet openbare gegevens zonder toestemming strafbaar.

Wat is dat eigenlijk, niet openbaar? De wet vertelt het niet. Vanuit een ambtelijke werkelijkheid is dat waarschijnlijk simpel; openbaar is alles dat bewust openbaar is gemaakt, dus via een publicatie en als het echt niet anders kan, via een **WOB**. Al het andere is niet openbaar. Het feit dat gegevens

al ergens gepubliceerd zijn maakt ze niet automatisch openbaar, zoals journalisten ondervonden toen ze uit gelekte staatsgeheimen citeerden. Zo geldt het verbod dus alle gegevens die niet via de afdeling Communicatie naar buiten zijn gebracht. Zo tekent zich een onbegrijpelijk en onbestuurbaar geheel af; de meeste bedrijven hebben geen formele publicatieprocessen en burgers al helemaal niet. Als je de link legt naar ACTA wordt het echter opeens wel duidelijk; vervang niet openbaar door 'van een auteursrechthouder' en het het verhaal wordt opeens wel concreet.

Ook het onderdeel 'zonder toestemming' is problematisch. Je kunt gegevens dus uitsluitend publiceren als je toestemming hebt van de eigenaar. Als je niet weet wie de eigenaar is, kun je geen toestemming krijgen, en bega je met publicatie blijkbaar een strafbaar feit. De eigenaar zoeken is dus verplicht. Wie de eigenaar is van een bepaald gegeven kan nogal een zoektocht worden. Door publicatie van een gegeven wordt iemand daar immers niet automatisch 'eigenaar' van. Als je informatie ergens online of in een papieren uitgave vindt, weet je dus niet of het daar met toestemming van de eigenaar staat. Met het overnemen ervan kun je ook in de problemen komen. Nu kan er wel onder een gegeven op Internet staan dat er toestemming door de eigenaar is gegeven, maar moet je dit dan verifiëren of kun je gewoon ouderwets claimen 'te goeder trouw' te zijn? Bij een film of een stuk muziek kun je de rechthebber gewoon opzoeken; ook hier is de link met ACTA zeer verhelderend.

Even doorredenerend: als ik mijn eigen vakantiefoto's op Flickr zet, mag dat? Strikt genomen heb ik toestemming nodig van de mensen die ergens in een hoekje herkenbaar in beeld zijn of de eigenaren van objecten die herkenbaar in beeld komen. Die mensen kunnen nu naar de rechter stappen en eisen dat ik de foto verwijder. In de nieuwe situatie wordt dit een strafrechtelijk gebeuren: de politie moet blijkbaar overtredingen gaan zoeken en het OM moet dit maar gaan vervolgen. Dus agenten gaan de Privé lezen en verifiëren of ieder gegeven dat ze aantreffen openbaar is, en zo niet, of de eigenaren toestemming hebben gegeven tot publicatie. Gelukkig geldt dit alleen de online wereld, en hoeft de politie alleen naar alle sites te kijken die onder de Nederlandse jurisdictie vallen. Jammer genoeg is alleen dat laatste al een fors probleem; een .nl domein kan op een server in de VS staan, een .tv gewoon hier: hosting op **Tuvalu** is nog niet zo goed geregeld. Maar vallen mijn vakantiefoto's op **Flickr** onder de Nederlandse jurisdictie? Ik heb geen idee, en Flickr blijkbaar ook niet. Ik denk dat de 3.000 man extra politie die Rutte I ons in het vooruitzicht stelt, alleen al voor deze wet ruim onvoldoende is. Bovendien; extra capaciteit bij de rechtbanken is naar verluid geen deel van het programma van ons aanstaande kabinet.

Dit voorstel is een onbeheersbaar juridisch gedrocht, omdat het voortkomt uit dat andere juridische drama, ACTA. Van poep komt alleen maar meer poep. Dát is het allergrootste probleem.

Wat hier gebeurt is een goede illustratie waarom de rechtbank en in het verlengde onze rechtstaat naar de bliksem is gegaan; er is niet nagedacht over uitvoerbaarheid van de wet en de impact daarvan op **politie en justitie**. De minister wil blijkbaar gratis meer handhaving van slecht doordachte wetgeving door zijn uitgemergelde organisatie. Hij kan geen nee zeggen tegen ACTA en de daarachter opererende mediamaffia, en dan blijft er alleen maar juridisch broddelwerk over.

Bedrijven kunnen de kwaliteit van hun producten niet onder een bepaald niveau laten zakken, omdat de klanten anders weglopen. Justitie kan dat wel. Klanten van Justitie kunnen niet weglopen, dan komt Oom Agent achter ze aan. Maar uiteindelijk zijn alle burgers klant van Justitie, en die kunnen wel weglopen van de overheid, de baas van Justitie. Dat heeft de partij van Hirsch Ballin bij de laatste verkiezingen aan den lijve ondervonden. Ik ben benieuwd op welke nieuwe held we bij de volgende verkiezingen zullen stemmen, nu Wilders zich zo te zien laat

inkapselen door het systeem.

Wat er hier gebeurt, is niet links of rechts, maar gewoon dom. Justitie is jaren geleden al door het ijs gezakt, dat is niet iets van de laatste minister. Wat kun je op dit moment doen? Om te beginnen kun je Bits Of Freedom **sponsoren**. En verder geldt: we kunnen de rechtstaat alleen beschermen tegen de 'daadkracht' van onze politiek door het verminderen van het aantal ge- en verboden. Dat is nogal een ommezwaai die begint bij onszelf. Alleen met minder regels is een kleinere en capabele overheid mogelijk. Iedere keer als we om een verbod van het een of het ander vragen, vragen we feitelijk om een belastingverhoging. We moeten dus in elk geval ophouden met voor ieder wissewasje een verbod te eisen.

Op grond van de ontvangen reacties blijkt het verhaal nog een hoogst interessante dimensie te hebben. Hier ga ik in deel drie op in.

De veiligheid voorbij (3)

Maandag 22 november 2010

In het eerste deel van dit drieluik stelde ik dat de werkdruk van de rechtspraak zich in de gevarenzone bevindt. Ik nam aan dat het stellen van nieuwe, complexe regels vragen om ellende is, vanwege geldgebrek bij justitie. Uit een interessante reactie bleek dat de veiligheidssector als geheel geen geldgebrek zou moeten hebben; de hele veiligheidsketen heeft de laatste jaren juist veel meer geld gekregen. Waar we met z'n allen in 2002 nog 7,5 miljard euro uitgaven aan veiligheidszorg, was dat in 2008 al opgelopen tot 10,8 miljard euro. Volgens het CBS[56] zijn in die zes jaar de uitgaven aan veiligheidszorg gemiddeld met ruim 6 procent per jaar gegroeid, bijna anderhalf keer zo snel als de gemiddelde groei van het bruto binnenlands product.

In tien jaar tijd stegen de kosten voor rechtspraak met **47 procent** (na inflatiecorrectie). In de **sector strafrecht** valt vooral op dat het aantal strafzaken bij het OM sterk is afgenomen: in 15 jaar een halvering. De enige groei bij het strafrecht is te zien bij de **Muldertjes**, de welbekende verkeersboetes. Het aantal misdrijven in ons land vertoont sinds 2003 een langzame maar structurele daling. Deze daling sluit aan bij de daling van het aantal rechtszaken. Nu wordt bij dalingen in de misdaadstatistieken nog al eens gewezen op de vertekenende werking van de **aangiftebereidheid** met de suggestie dat de criminaliteit helemaal niet daalt. Dat is theoretisch mogelijk, als dat de aangiftebereidheid daalt. Wat gezien alle online mogelijkheden (**zoals meld misdaad anoniem**) onwaarschijnlijk is. Het percentage misdrijven waarvan aangifte gedaan is kan dus net zo goed gestegen zijn. Het **CBS** toont een aanhoudend dalende trend in de criminaliteitscijfers, al vanaf de jaren '90. Dat de cijfers van justitie pas later dalen, wijst er eerder op dat de aangiftebereidheid toegenomen is, dan gedaald.

Bij civiele zaken is overigens een heel ander beeld zichtbaar. Daar verdubbelde het aantal zaken in de afgelopen tien jaar. De werkdruk zal daar dan ook zeker gestegen zijn, en de klachten vanuit de rechtspraak zullen hiermee te maken hebben. Maar in de roep om meer geld wordt het veiligheidsargument gebruikt.

De vraag die zich hier opwerpt is: waar blijft het extra geld dat we uitgeven aan onze veiligheid? De grootste post in de uitgaven, preventie, is met meer dan 40% van de totale bestedingen relatief constant. We zijn relatief meer gaan besteden aan tenuitvoerlegging en relatief minder aan opsporing en berechting. Veel geld gaat dus op aan het gevangeniswezen. Dat heeft te maken het

[56] http://www.cbs.nl/nl-NL/menu/themas/veiligheid-recht/publicaties/artikelen/archief/2010/2010-3024-wm.htm

langer zitten van veroordeelden; maar het is doorgeschoten, zodat we nu een cellenoverschot hebben.

De uitgaven door Binnenlandse Zaken en Justitie zijn de laatste tien jaar ondanks een relatieve afname fors **gegroeid**. In 1998 telde ons land bijna **40.000 agenten**, in 2010 zijn dat er ruim **55.000**. De productiegroei van Justitie bij de verkeersovertredingen komt voor een groot deel door automatisering– van flitskast tot incasso, alles is volledig geautomatiseerd. Maar de aantallen andere zaken dalen. Justitie levert dus met meer mensen minder productie, en dat speelt vooral bij het Openbaar Ministerie. Dat verklaart waarom het OM steeds meer taken, zoals de vervolging van rechtenschendingen bij het downloaden van muziek en films, naar zich toe trekt. Dan hebben ze tenminste weer wat te doen. Ook de politie spoort minder op met meer mensen. In het gevangeniswezen is er het cellenoverschot, en ook de rest van de veiligheidsketen kampt met overcapaciteit.

Als je goed kijkt zie je drie trends. De eerste is dat er een sterke afname is in de getalsmatige doelmatigheid van de veiligheidssector. Er is met de daling van de criminaliteit gewoon minder te doen. De tweede trend is dat de veiligheidssector in Nederland zich is gaan richten op nichemarkten als terrorisme, zware criminaliteit en cybercrime. De derde trend is een grote hoeveelheid bestuurlijke aandacht voor veiligheid. Rond veiligheid is immers een ongelimiteerde hoeveelheid advies-, inspectie- en bestuurswerk te bedenken. Dat leidt tot een enorme bestuurlijke drukte. Op en tussen alle bestuurslagen, in Brussel, landelijk, provincie, regio en gemeente, is een tsunami van organen ingericht over veiligheid. Een centraal overzicht van de organen, projecten, programma's, instellingen en commissies die zich met het veiligheidsdossier bezighouden is niet te vinden. Er is duidelijk ook geen centrale regie.

Nu zou je kunnen denken dat een dergelijke centrale regie in deze barre en gevaarlijke tijden er wel zou komen, maar dan ken je de Haagse realiteit niet. Zo is in februari dit jaar de **Stuurgroep Nationale Veiligheid** bij wet ingesteld, een overlegorgaan dat moet coördineren, waken en schakelen tussen alle departementen, de AIVD en NCTb. Ver van Den Haag komt dit orgaan dan ook niet. Wat deze stuurgroep nou eigenlijk stuurt, wordt nergens duidelijk gemaakt. Ook het eerdere Project Nationale Veiligheid heeft een dergelijke centrale regietaak nooit ondernomen, laten de stukken op **bigwobber** overduidelijk zien. Overlapping en dubbelingen zijn zeer waarschijnlijk en zullen voorlopig ook niet verdwijnen.

Een voorbeeld. Het CBP, het College Bescherming Persoonsgegevens, houdt toezicht op de naleving en toepassing van de Wet bescherming persoonsgegevens (Wbp), de Wet politiegegevens (Wpg) en de Wet gemeentelijke basisadministratie (Wet GBA). Maar er is ook nog een "Adviescommissie Veiligheid en Persoonlijke Levenssfeer". **Deze commissie** had "tot taak te adviseren over regulering van, voorlichting over, werkwijzen bij en indien nodig protocollisering van de omgang met persoonsgegevens, zodat deze de veiligheid van personen bevorderen". Dat hier een fikse overlapping met het CBP is, moge duidelijk zijn.

Eigenlijk moet ik het ontbreken van overzicht ('een veiligheidstopografie') en regie niet laten zien. Want om dit langs elkaar werken van overlappende clubs te beheersen, zul je net zien dat er nog meer coördinerende organen komen. Om 'bestuurlijke samenwerking te borgen'of zo. En helaas kosten bestuurders meer dan uitvoerenden, met voorspelbare gevolgen voor het budget.

Zo zien we in de veiligheidssector de wet van de afnemende meeropbrengsten in volle glorie; meer capaciteit leidt tot steeds minder extra productie. We zien dat om dit te compenseren 'hippe' onveiligheid steeds meer capaciteit krijgt. Bij **cybercrime** bijvoorbeeld, (2) dat volgens de KLPD '**exponentieel groeit**'. En de veiligheidspendant groeit mee. Elk regioparket heeft zijn eigen **cybercrime officier**. Dat zijn er dus 25. Daar bovenop bestaat nog een **kenniscentrum** en een

gespecialiseerd team bij het Landelijk Parket van het Openbaar Ministerie . Op een verjaardag vertellen dat je 'achter hackers aanzit' is inderdaad een beter verhaal dan dat je wildplassers opspoort.

Nu is cybercrime niet onbelangrijk, zeker niet, maar in aantallen te **verwaarlozen**. In 2008 waren er 901 geregistreerde misdrijven; dit omvat niet alleen spam, hacken en identiteitsdiefstal maar ook grensgevallen als online smaad, **creditcardfraude** en **kinderporno** waarbij de digitale dimensie wel aanwezig is, maar feitelijk onbelangrijk. Al die gespecialiseerde organen hebben nooit een formele afbakening van de categorie cybercrime gemaakt. Tot hoeveel veroordeelden dit alles leidt is ook nergens te vinden. Veel zullen het er niet zijn. In haar eerste **trendrapport cybercrime** geeft Govcert expliciet toe dat er geen harde cijfers zijn. Er zijn dus ook geen meetbare ontwikkelingen. Ik concludeer dat ons land meer 'bevoegd gezag' in Cyberspace heeft dan cybercriminelen.

We zien iets vergelijkbaars bij de **georganiseerde criminaliteit**. Zo zouden we volgens het OM op dit moment maar 20% aanpakken. Als je op zoek gaat naar de omvang van deze georganiseerde criminaliteit en hoeveel boeven dus nu buiten schot blijven (hoeveel is 80%?), dan blijkt dat cijfers niet bestaan. Oftewel, we roepen maar wat.

Ook het dossier terrorisme vertoont vergelijkbare taferelen; een boel **overlegkaders**, instituten en uitvoerders met kasten vol beleid en flankerend beleid, terwijl er in velden noch wegen een terrorist te bekennen is.

En dan nog een moeilijke vraag: wat is het rendement van al deze inspanningen? Daalt de criminaliteit door meer aandacht voor veiligheid? Als dat zo is, zijn we op de goede weg en moeten we vooral zo doorgaan. Maar het lijkt daar niet op. Als je de wetenschappers van justitie (het WODC) vraagt naar het waarom van de criminaliteitsdaling, dan leggen zij de oorzaak niet bij maatregelen van de overheid, maar bij de demografie – meer specifiek de **afname** van het aantal jonge mannen. En dat is een inzicht dat criminologen wereldwijd onderschrijven. Dankzij de vergrijzing daalt de criminaliteit. Dat gaat vanzelf.

Terrorisme dan: hebben we zo weinig terrorisme in Nederland omdat er 200.000 mensen **tegen strijden** of omdat er **geen terroristen** zijn die ons de moeite waard vinden? De cijfers van **Europol** en de **verslagen** van de coördinator terrorismedreiging onderstrepen een daling naar nul; er is de afgelopen jaren helemaal niets gebeurd. Waarom het dreigingsniveau terrorisme desondanks op 'beperkt' blijft staan terwijl er ook een niveau '**minimaal**' bestaat? Nou, stel dat er toch eens iets gebeurt. Dan hebben ze het mis gehad met hun dreigingsniveau. Het zal dan ook nooit minimaal worden.

De veiligheidssector stelt vooral zijn eigen werkgelegenheid veilig. Roep gewoon af en toe dat een bepaalde dreiging uit de klauwen loopt, en Den Haag springt in het gelid met hoger budget en meer mandaat. Hier zien we dus een perverse prikkel; instellingen die er zijn om onze veiligheid te verbeteren, verminderen ons veiligheidsgevoel en daarmee onze veiligheid, omwille van de eigen werkgelegenheid. Ik wens onze nieuwe minister van Veiligheid veel wijsheid om dit ten goede te keren.

Blame The Victim

Vrijdag 17 december 2010

Begin in een van de vele Wikileaks-discussies eens over de verantwoordelijkheden van het Amerikaanse leger voor het slecht beveiligen van diplomatieke stukken. Dan krijg je vaak het "Don't Blame The Victim"-argument terug: je mag het slachtoffer niet de schuld geven. De dader heeft het immers gedaan, niet het slachtoffer. Tja, spreek dat maar eens tegen. En dat doet dan ook niemand. Toch is het daar tijd voor.

Het Department of Defense (DoD) is namelijk niet het slachtoffer en Wikileaks niet de dader. Iemand die toegang heeft tot de berichten heeft op z'n gemakkie de boel gekopieerd. Dat is een lek in de beveiliging, hoe je het ook wendt of keert. Wikileaks is slechts het platform, of het kopieerapparaat zoals Arjen Kamphuis op **sargasso** haarfijn en zeer overtuigend uit de doeken doet. De gelekte documenten hadden net zo goed naar de sectie Stiekum in Moskou of van de Taliban kunnen gaan en dan had niemand geweten van het lek. De dader is een Amerikaanse militair, het slachtoffer het Amerikaanse State Department. Zo eenvoudig is het. De rest is een rookgordijn, om de discussie over de inhoud van de gelekte berichten te overstemmen.

Laten we dit rookgordijn opheffen. Dat is eigenlijk heel simpel.

Het DoD heeft de taak de boel te bewaken; de VS inclusief de stukken van een ander department. Het State Department is hier het primaire slachtoffer, haar interne bedrijfscommunicatie ligt op straat en het DoD heeft als ingehuurde bewaker gefaald. Verschuil je je achter het moralistische Don't Blame The Victim, dan pleit je de bewaker vrij. Dat is misleidend en contraproductief. Beveiliging gaat niet over moralisme, maar over professionaliteit. En die is tekort geschoten.

Dit moralisme wordt wel bijzonder cynisch als je ziet dat een groot deel van de ITSec industrie de US Army te hulp schiet (of haar mond houdt) uit commerciële overwegingen. De US Army zal, met haar nieuwe taken rond cyberwar, de inlichtingendienst opvolgen als grootse afnemer van consultancyuren en -producten. Zo ontstaat het beeld dat de belangrijkste spelers in de beveiligingsindustrie ('de specialisten') tegen Wikileaks zijn, en de mensen die voor Wikileaks pleiten een stelletje wereldvreemde scriptkiddies. Wat ze natuurlijk, uitzonderingen daargelaten, niet zijn.

Het DoD heeft gefaald in één van haar primaire taken, het beschermen van de VS, in een gebied waarin ze torenhoge ambities heeft, het digitale domein. En dat is bijzonder ernstig. Deze blunder goedpraten maakt de kans dat het Amerikaanse leger van de gemaakte fouten leert een stuk kleiner. Straks wordt het Internet bewaakt en gereguleerd door een partij die nu toont de essentiële zaken niet te begrijpen, bijgestaan door deskundologen die geen enkele moraal hebben en op afroep komen liegen. Als ze zich niet bewust zijn dat ze liegen, zijn ze niet deskundig. Beseffen ze wel dat ze liegen, dan zijn ze niet betrouwbaar. Het ziet er dan ook naar uit dat OpenLeaks, de aangekondigde opvolger van Wikileaks, en Cryptome, de nog steeds actieve voorloper, ook de komende jaren de beschikking zullen hebben over bendes interessant leesvoer.

Privacy Made in Brussels

Maandag 3 januari 2011

Het wordt een spannend jaar. De EU belooft namelijk met een opvolger van de huidige "**privacy-richtlijn**" te komen. De **huidige richtlijn 95/46/EG** stelt regels en kaders over de verwerking van persoonsgegevens in geautomatiseerde systemen. De richtlijn is alleen van toepassing op verwerkingen van gegevens "als zij geautomatiseerd zijn of als de betrokken gegevens zijn opgeslagen of zullen worden opgeslagen in een bestand dat gestructureerd is volgens specifieke persoonscriteria teneinde een gemakkelijke toegang tot de betrokken persoonsgegevens mogelijk te maken". De benaming "privacyrichtlijn", die ook door het College Bescherming Persoonsgegevens (CBP) voor 95/46 wordt gebruikt, maakt de onderliggende visie op privacy duidelijk – privacy is het waarborgen van de zorgvuldige omgang met persoonsgegevens in de geautomatiseerde administratieve werkelijkheid van bedrijven. Het gaat dus niet over privacy zoals de meeste mensen dat in het verlengde van **Van Dale** en **Wikipedia** bedoelen, zoals het recht om zo min mogelijk lastig gevallen en bespioneerd te worden.

Afgezien van een paar academisch ingestelde Security Officers, heeft in het bedrijfsleven niemand ooit van de EU privacy-richtlijn 95/46 gehoord. En zoals te verwachten valt, hebben er nog minder bedrijven naar gehandeld – de "privacyrichtlijn" is alleen met heel veel moeite en nog meer goede wil als een succes te beschouwen. Vraag maar eens conform artikel 11 aan de telefonische colporteur om "een recht op toegang tot" de "eigen persoonsgegevens en op rectificatie van deze gegevens". Of vraag of de registratie van de persoonsgegevens aangemeld is bij het **CBP**. Heb ik een keer gedaan bij een jongeman die namens de Nederlandse Energie Maatschappij belde – het zou genieten zijn, als het niet zo triest was. De manager van de NEM wist mij in een aansluitende mailwisseling te melden dat ze legaal over mijn telefoonnummer beschikten, omdat ze het van een legaal bedrijf gekocht hebben. En dan mag het, **natuurlijk**. Legale bedrijven doen immers nooit illegale dingen, daar staat de KvK toch borg voor? Of zoiets?

Wat je er in zo'n gesprekje niet bij moet vertellen zijn de uitzonderingen die de richtlijn vermeldt. Vooral de bepaling "tenzij zulks onmogelijk blijkt of onevenredig veel moeite kost" is erg leuk. Moet je eens voor de rechter proberen: "Nee, edelachtbare, ik hoef niet aan de wet te voldoen, want dat kost onevenredig veel moeite". Ik zou het bijzonder waarderen als deze verfijning in het wegenverkeersreglement zou staan, maar helaas, blijkbaar geldt een vrijstelling voor luiheid en incompetentie alleen bij wetgeving rond privacy. Deze achterdeuren zijn niet het gevolg van onnadenkendheid van de opstellers, maar expliciet zo bedoeld.

De huidige richtlijn stelt hierdoor dus vrijwel niets voor. En dan te bedenken dat er maar liefst 15 jaar aan gewerkt is. De nieuwe richtlijn heeft nog veel meer uitdagingen, nu zaken als Internet, social networks en offshoring een grote rol zijn gaan spelen – dat bestond allemaal nog niet in 1995 in de Brusselse werkelijkheid. Ik ben dan ook heel benieuwd of de EU bij de vernieuwing van deze regelgeving er dit keer wel echte regels van weet te maken, zonder levensgrote achterdeuren.

De grootste achterdeur in 95/46 is er voor de overheid. Artikel 13 stelt expliciet dat "activiteiten met betrekking tot openbare veiligheid, defensie, staatsveiligheid en de activiteiten van de Staat op strafrechtelijk gebied niet onder de toepassingssfeer van het Gemeenschapsrecht vallen", noch "de voor de economie van een Staat noodzakelijke verwerking van persoonsgegevens", "indien deze verwerking verband houdt met de Staatsveiligheid". In al die gevallen geldt de richtlijn niet. Je kunt feitelijk zo ongeveer alles aan 'openbare veiligheid' of 'staatsveiligheid' ophangen in Europa, zonder dat Brussel of Straatsburg daar iets aan kan - of wil - doen. Dat zien we in

Hongarije, waar algemene censuur is ingevoerd, omdat de pers wel eens de stabiliteit van de regering zou kunnen schaden. En passant zijn ook de rechtbanken en de centrale bank hun zelfstandigheid kwijtgeraakt. We zien het al veel langer in Italië, waar de wet al jaren de regering en de commerciële belangen van maffiapremier Berlusconi dient. Nu is de passiviteit van Brussel in deze dossiers niet heel vreemd – de regerende partijen in Hongarije en Italië zijn in het Europees parlement lid van Christen Democratische EVP-fractie, net als Barroso, Buzek en van Rompuy, de drie presidenten van **Europa**. En je laat je partijgenoten niet vallen, want voor je het weet ben je niet meer de grootste partij, en dan kost dat je je baan. Natuurlijk is dit niet de officiële verklaring, die mompelt iets over de autonomie in de binnenlandse zaken van de lidstaten. Als Fidesz in Hongarije nog verder doorslaat en iets als het goulashcommunisme van Kádár of het fascisme van **Horthy** herinvoert, zal Brussel dus hooguit 'Foei' zeggen, en dan ook nog op een toon die niemand kan horen. De EU kan aan lidstaten immers alleen eisen stellen bij toetreding, daarna is Europa een tandeloze tijger. Noem het een weeffoutje van de projectgroep Goede Bedoelingen in Brussel. Maakt Brussel hier zich druk over? Welnee, Hongarije is 1 januari 2011 gewoon **voorzitter** van de EU geworden, en vanaf 3 januari gaat de EU gewoon verder met regels, richtlijnen en beleid maken.

Helaas is de aanleiding voor de Brusselse herziening van de richtlijn niet een analyse van de effectiviteit van 95/46, maar de ontwikkeling van **Cybercrime en Web 2.0** . De aanpak is dus dezelfde als bij de vorige regelgeving: we gaan achter de feiten aanlopen en na jaren en jaren concluderen dat we ze niet ingehaald hebben. Met de altijd verder evoluerende technologie kan dat natuurlijk ook helemaal niet. Dat is geen kwestie van gebrek aan capaciteit maar van een verkeerde aanpak. Er komt dus een richtlijn, wellicht al in 2011 maar het kan net zo goed 2021 worden, die bedrijven tot een beetje inspanning verplicht, maar - gegeven de niet verbeterde constellatie in Brussel - niet verplicht tot resultaten. Nou, joepie, hoor.

Daar gaan we weer

Vrijdag 28 januari 2011

Vannacht viel het besluit met een riante Kamermeerderheid van 76 zetels over een nieuwe missie naar Afghanistan. **We gaan weer**. De discussie daaraan voorafgaand spitste zich toe op de kosten, het risico, of er niet te veel geschoten en te weinig opgebouwd zal worden en andere operationele vragen. De vraag die alleen zijdelings gesteld werd, en niet beantwoord, is of en zo ja hoe onze krijgsmacht met deze missie de veiligheid van Nederland verhoogt. En, ook weer zo ja, of dit het hoogst haalbare rendement is voor deze pakweg half miljard euro? Ik ben daar eigenlijk wel erg benieuwd naar.

Rutte zegt: “De nieuwe missie is gericht op de opbouw van de rechtsstaat in Afghanistan en heeft een strikt opleidings- en trainingskarakter. Geen van de onderdelen van deze missie zal worden ingezet voor offensieve militaire activiteiten.” We gaan de politie trainen en heus niet vechten. Als de term niet zo besmet zou zijn, zou de politiemissie een **politionele actie** heten.

In het debat stelden de meeste deelnemers centraal dat er opgebouwd moet worden, en dat er niet **gevochten** mág worden – de door ons opgeleide agenten mogen alleen terugschieten. De steun van de doorslaggevende Kamerfracties **hing op dit punt**. Sommigen denken iets verder en vragen zich af of het geheel wel **kans van slagen** heeft, of de politie niet stiekem paramilitairen zijn en of onze jongens niet te veel gevaar lopen.

Deze vragen zijn terecht en begrijpelijk, maar de belangrijkste vraag zit er niet bij. Stel dat de missie volledig slaagt, en Afghanistan een democratische rechtstaat naar westerse snit is geworden, hoe draagt dat dan bij tot meer veiligheid voor Nederland? Immers, als we er echt veel veiliger van worden, dan moeten we gaan en zijn slachtoffers te rechtvaardigen. Of moeten we om veiliger te worden aansluitend eerst nog naar Pakistan, Iran, Tsjetsjenië, Soedan, Jemen, Israël en wie weet waar nog meer naartoe?

De minister van Buitenlandse Zaken geeft als een van de weinigen in dit debat een antwoord op deze vraag. **Volgens** Rosenthal is de "opbouwmissie" een "zinvolle bijdrage aan stabiliteit en veiligheid" in Afghanistan. Stabiliteit in de regio, met buurlanden als Pakistan en Iran, is ook van groot belang, aldus de bewindsman. Hij wijst er, met name in de richting van pseudoregeringspartij PVV, op dat de terroristische dreiging voor Nederland voor een belangrijk deel uit dit gebied komt. Daarmee impliceert hij dat deze missie deze dreiging kan en zal verminderen.

Met deze stellingname draait Rosenthal oorzaak en gevolg om; zijn wij daar om een bestaande bedreiging op te ruimen of komt de dreiging uit ‘die regio’ omdat wij daar militair aanwezig zijn? Dat klinkt misschien semantisch, maar is wel cruciaal. De geschiedenis geeft het antwoord: Al Qaeda heeft Nederland nooit aangevallen, hooguit de Nederlandse troepen in Afghanistan. Al Qaeda strijdt tegen het westen omdat de militaire aanwezigheid van de VS in de Arabische wereld, in het bijzonder in Saoedi Arabië waar alle belangrijke heiligdommen zijn, voor strenge panislamieten niet acceptabel is. En omdat de VS daarmee een zeer corrupt en repressief regime in het zadel houden. Het regime dat wij in Kaboel overeind houden is onbetrouwbaar en zeker zo corrupt, en we weten dat al lang, zoals blijkt uit **WikiLeaks**. Het contractueel willen vastleggen van garanties met Karzai is dan ook uitzonderlijk naïef. Kunnen die garanties überhaupt iets voorstellen?

De strijd van Al Qaeda richt zich **bovenal** tegen dit soort corrupte en repressieve regimes, met Riyad in het bijzonder. Vijftien van de negentien 9/11-kapers kwamen uit Saoedi-Arabië, net zoals de meeste Arabische strijders in Afghanistan en Guantánamo. En Osama bin Laden, de meest gezochte terrorist ter wereld en leider van Al Qaida, is ook al een **Saoedi**. De relatie met de Taliban is nog vergezochter, die hebben buiten de eigen regio nog nooit ambities getoond – sterker nog, ze willen het liefst geen buitenland. Door onze voortdurende interventies – we zijn er al sinds 2002 - in de regio neemt de terroristische dreiging bij ons eerder toe dan af, zeker omdat we er maar niet in slagen de terroristen te pakken.

Het antwoord van Rosenthal klopt dus niet. Deze missie heeft nauwelijks iets met onze veiligheid te maken en hoort niet onder het kopje defensie. Dit is een soort ontwikkelingshulp in een eeuwenoude traditie; wij gaan de wereld met het pistool in de vuist beschaving brengen, en voor je er erg in hebt is er weer een democratie bij. Alleen het kerstenen ontbreekt nog.

De huidige discussie is een herhaling van de zetten die we bij de eerdere missies konden zien. WikiLeaks geeft ons steeds meer inzicht in hoe we de Uruzgan missie en de opeenvolgende **ingerommeld** zijn. Dit kan ons helpen om de huidige debatten te duiden. Daarbij vallen drie zaken op:

1. Defensie geeft stelselmatig en bewust een onvolledig en soms onjuist beeld van zaken (zie het papieren **NRC** van 17 januari), net als in andere dossiers, zoals Irak en de **JSF**. Hierbij speelt een sterke geldingsdrang mee, omdat Defensie wil laten zien dat ze in staat is een moeilijke missie uit te voeren en de grote crises als Srebrenica en de herstructureringen na het einde van de Koude Oorlog te boven is.
2. Rapporten van de inlichtingendiensten worden geherformuleerd als ze politiek niet goed uitkomen. Dit was ook al gesignaleerd door de commissie Davids rond de missie in Irak.
3. De voornaamste reden om mee te gaan is het meegaan zelf; we gaan omdat de NAVO gaat en de NAVO is het anker van **onze veiligheid**. Als we niet meegaan dan schaadt dat ons internationale aanzien. Het internationale aanzien van Nederland is gedefinieerd als het mogen aanschuiven bij grote gremia als de G20 en de carrièrekansen voor Nederlandse individuen. Zo werd minister Bos **gewaarschuwd** dat hij een internationale carrière wel kon vergeten als hij bleef tegenstribbelen. Dit thema keert al jaren terug; als je niet meedoet, kunnen Nederlanders hun internationale carrière wel vergeten.

Dus wat er ook gebeurde of gezegd werd, we gingen en gaan weer. WikiLeaks en Davids leren ons dat daarbij voor de gevestigde orde het doel de middelen heiligt. Er is al heel wat afgelogen, er zijn tal van loze beloftes gedaan en er werd zonder enige schaamte cruciale informatie weggemoffeld.

De vraag of, en zo ja op welke manier deelname aan een nieuw Aziatisch avontuur bijdraagt tot de Nederlandse veiligheid mag dus slechts binnenskamers gesteld worden en het echte antwoord is staatsgeheim. Daarom is WikiLeaks zo vervelend. En zo nodig.

Dus: waarom gaan we? Daarom. Zoals altijd. We gaan omdat anderen gaan. We doen mee om het meedoen. Deelname aan het bestaande internationale machtsspel is blijkbaar het doel en niet het middel; wij willen internationaal op de kaart staan om internationaal op de kaart te staan. Wat we daar dan vervolgens gaan doen, weten we eigenlijk niet. Daar hebben we geen strategie voor. Onze enige strategie is de Amerikanen helpen. Welnu, die kunnen prima voor zichzelf zorgen.

Het internationale veiligheidslandschap waarin we de op kaart willen staan, wordt daarbij als een feit aangenomen. Terwijl het volop aan het veranderen is. Die ontwikkelingen worden volstrekt genegeerd. We gaan voorbij aan gigantische veranderingen bij de NAVO, de VS, de EU en China

en we houden vast aan de Atlantische reflex van de jaren '50, waarin trouw aan de VS de maat aller dingen is.

Laten we beginnen bij de NAVO. Die werd ooit opgericht 'tegen de Russen', maar evenzeer om de Amerikanen aan Europa te binden en om Duitsland onder controle te houden. Sinds het einde van de Koude Oorlog is de NAVO een oplossing op zoek naar een probleem. De Russen hebben hun handen vol aan hun eigen chaos en de Duitsers blijken écht hun lesje geleerd te hebben.

Na het demarche van het Warschaupact is de focus van de wereld niet langer de West-Duitse laagvlakte, wat het meest wordt getoond door de opkomst van Japan en vervolgens die van China. De Amerikanen zijn nog maar matig geïnteresseerd in de NAVO, het is een sideshow geworden en Europa een 'backwater'. Dat is ook te zien in de dagelijkse operaties in Afghanistan, waar de NAVO missie veelal door de Amerikanen genegeerd wordt en gekwalificeerd als een **vijfde wiel** aan de wagen. Als de bondgenoten niet doen wat Washington wil, dan kan de NAVO beter ophouden te bestaan, **dreigde** minister Gates in 2008 al.

De VS is een grootmacht in verval, die per dag meer geld leent dan het uitgeeft aan het in stand houden van het militair overwicht. De hulptroepen van de Europese bondgenoten zijn voor Washington zeer prettig om deze boven de eigen stand levende hypermacht in het zadel te houden. Maar dan moeten de hulptroepen wel doen wat er gezegd wordt, en niet van die rare dingen doen als een eigen aanpak kiezen.

In de jaren '50 stroomde het geld van de VS naar Europa in het kader van de Marshall hulpt en wie betaalt, bepaalt. Nu stroomt het geld al jaren de andere kant op, de bodemloze put in van Amerikaanse hypotheekbanken en creditcard consumenten. Wij betalen maar beseffen nog niet dat we dus kunnen bepalen. De EU begint nog maar net te ontwaken in deze nieuwe realiteit.

De krediet en de aansluitende eurocrisis dwingen Brussel om de economische macht te onderbouwen met politieke macht, binnen Europa en ook daarbuiten. Met een steeds machtiger bestuurslaag in Brussel wordt Den Haag meer een soort provinciale staten, die steeds harder moeten roeptoeteren om relevant te lijken. Daarom moet en zal Den Haag autonoom op het wereldtoneel acteren. Dat zie je aan de behoefte om zélf mensen naar de G20 te sturen; dat hoeft helemaal niet, we zitten daar via de EU allang bij. De realiteit is dat de EU een economische wereldmacht is, volgens het IMF overzicht van 2011 meer dan 10% groter dan de VS en drie keer zo groot als **China**. En Nederland is een provincie van de EU. Met de invoering van de Euro is het 'point of no return' gepasseerd.

Zoals de geschiedenis van de oorlogen in de laatste twee eeuwen ons leert, geeft industriële kracht uiteindelijk de doorslag. In beide wereldoorlogen was de VS in het begin economisch een reus maar militair een dwerg, in beide gevallen duurde het heel kort voor ze ook militair een reus werd. Nu is de EU de industriële reus. De VS is wel groot, maar de economie drijft op de dienstensector: banken, consultancy en software. Ik zie McKinsey, Goldman Sachs of Microsoft niet zo snel omschakelen op de productie van tanks of vliegdekschepen.

Als laatste is er de machtsverschuiving richting China. Dit land heeft zich ontwikkeld tot de derde industriële wereldmacht en groeit nog heel snel. China heeft dan ook een gigantisch machtspotentieel. Ook China is in militair opzicht verre de mindere van de VS, maar laat zich niet door Washington sturen zoals de EU. En ook China financiert de VS en is daartoe evenmin verplicht.

Beide nieuwe grootmachten, de EU en China, betreden onzeker en terughoudend het wereldtoneel. China omdat ze nog relatief klein is en nog moet wennen aan de nieuwe statuur, de

EU omdat ze haar gewicht ontkent en omdat de provinciale regeringen de schijn van autonomie willen ophouden en daarvoor diplomatieke spelletjes spelen via Washington tegen Brussel. Dit is voor beide landen van voorbijgaande aard. Wij zullen deze nieuwe realiteit onder ogen moeten zien, en dat kunnen we beter zo snel mogelijk doen.

Terug naar de vraag waarom we toch weer naar Afghanistan gaan. Samenvattend: we gaan om de NAVO overeind te houden, een lange neus te maken naar Brussel en om de internationale carrière van Nederlandse politici en specialisten te helpen. Waarom houden we NAVO overeind? Omdat we daarmee een sterkere EU overheid kunnen vertragen en de dromen van autonomie en het belang van ons provinciaal bestuur in Den Haag overeind kunnen houden. En daarbij speelt nationalisme een rol, maar zeker ook het aanzien en gezag, en in het verlengde daarvan wederom de poppetjes en baantjes. Ook de NAVO zelf biedt natuurlijk nog de nodige carrièrekansen.

Het is wel heel erg cynisch om naar de wisselkoers te vragen. Maar ik doe het toch. Hoeveel soldaten moeten we sturen voor hoeveel hoge posities? Hoeveel dode soldaten is een voorzitterschap van de NAVO of een commissariaat in Washington of Irak ons uiteindelijk waard?

Een ongezond plan

Zondag 27 februari 2011

Een wereldwijd Elektronisch Patiënten Dossier (EPD). Dat hebben we nodig, vindt de EU, onder aanvoering van Neelie Kroes. Het staat op de **agenda** voor uitbreiding van de digitale dienstverlening. Hiervoor tekenden Kroes en de Amerikaanse Secretary of Health and Human Services Kathleen Sebelius in december een akkoord. De bedoeling is dat uitwisseling van medische gegevens mogelijk wordt tussen de VS en de landen van de EU. Beide bewindsvrouwen zeiden dat dit van groot belang is voor bedrijven die actief zijn of willen worden in de e-health sector, en ook voor de patiënten. “Nothing makes more of a difference to people's lives than good health,” aldus Kroes. Daar heeft ze natuurlijk een punt.

Volgens de EU zal “the deployment of eHealth technologies in Europe” “improve the quality of care, reduce medical costs and foster independent living, including in remote places”, dit alles in navolging van het eHealth **Lead Market Initiative** (LMI). Ook daar kan ik me nog wat bij voorstellen. Dit LMI is één van de zes gebieden waarop de Europese industrie zich in steun vanuit de EU kan verheugen. In het **oprichtingsrapport** staan lovende woorden voor de mogelijkheden. Heel mooi is ook dat security in het document wordt benoemd als een speciaal aandachtsgebied.

Nu ben ik er niet per definitie op uit om een domper op al deze blijheid plaatsen, maar het zal toch moeten. Het hoofdstuk security wordt afgedaan met de opmerking dat het onderwerp onder een ander Europees aandachtsgebied valt, namelijk het innovatie-stimuleringsprogramma FP7, ook wel KP7 genoemd (voluit: Framework Programme of Kaderprogramma 7). In **FP7** wordt e-health inderdaad genoemd maar je moet wel erg van goede wil zijn wil je beweren dat daar iets substantieels gebeurt voor de **elektronische beveiliging** van de zorg. Het is eigenlijk vooral een verwijzing naar weer een ander bestuurlijk kader, waar vervolgens vooral leegte te vinden is.

Hou deze gedachte even vast: het doel is de softwarebedrijven te verlossen van de landsgrenzen die nu belemmerend zouden werken, zodat de burger betere zorg kan krijgen. En daarom moet er dus uitwisseling komen tussen EPD’s wereldwijd. Klopt deze redenering wel?

De zorg heeft al jaren internationale standaarden voor patiëntgegevens, zoals **HL7**, die vrijwel algemeen toegepast worden. Zorginstellingen kunnen dus al jaren gegevens uitwisselen. Maar, zoals het nog steeds niet bijster landelijke EPD bewijst, dat willen ze niet! Het gaat om concurrentieoverwegingen. De grootse bedreiging van de privacy van het landelijk EPD is niet dat de psychiatrische dossiers van bekende Nederlanders lekken naar RTL Boulevard. De grootste bedreiging is dat iedereen die weet hoe je een SQL query bakt, precies kan zien hoe goed en hoe kosteneffectief welke zorginstelling of medicus is. Met marktwerking in zicht voorwaar geen prettig idee. De deelnemers aan het EPD willen dan ook helemaal niet deelnemen, dat mogen ze alleen niet vertellen want dat is politiek niet opportuun. Concurrenten willen gewoon niet samenwerken, ook niet als het moet vanwege een computersysteem.

Goed, ze willen niet en de security stelt niets voor. Maar daarom kan een wereldomspannend EPD op zich nog wel een goed idee zijn. Voor wie? Me dunkt voor de mensen die veel in het buitenland verkeren. Hoeveel mensen zijn dat eigenlijk? Hoeveel procent van de tijd zijn Europese burgers in een ander land? Twee procent? Vier? Meer zal het niet zijn. Maar dat is zeker nog geen twee procent van de patiënten. De mensen die het meest van zorg afhankelijk zijn, zijn het minst mobiel: de ouderen. Alle overwinteringen ten spijt; zodra de zorgbehoefte stijgt, is het adios Costa del Sol en terug naar Voorthuizen.

Mensen die wel veel in het buitenland zijn, zoals expats en studenten, zijn bovengemiddeld gezond. Zelfs al zou de Europese burger gemiddeld tien procent van de tijd over de grens zijn, dan rechtvaardigt de zorgbehoefte over de grens een wereldwijd EPD zonder zeer doortimmerde beveiliging zeker niet. En de wereld buiten de EU is ook nog best wel groot. Hoeveel procent van die landen waar we overwinteren of onze vakantie doorbrengen is zo geavanceerd dat daar een aansluiting op een wereldwijd EPD zinvol is? Bedenk, er is een wereld van verschil tussen Thailand en Finland; er gaan veel meer Nederlanders naar Thailand dan naar Finland. In Finland zal ieder ziekenhuis een EPD hebben, maar in Thailand, Egypte, Belize? Neuh. Oftewel, om wellicht één promille van alle medische cases te dekken, wordt een wereldwijd ICT project opgetuigd. En, zoals het blijkbaar hoort bij ICT en zorg, dat moet dan op een koopje.

Onder het mom van betere zorg voor van de 'wereldburger' worden EPD's wereldwijd met een gigantische impact op de privacy en veiligheid genormaliseerd en gekoppeld. Gigantische impact? Ja, best wel. De lokale dienstkloppers, de chanteurs, de loverboys en de secties Stiekem Wereldwijd krijgen toegang tot je patiëntgegevens als ze maar genoeg aandringen. Voor je het weet word je aan de grens van je favoriete vakantieland geweigerd omdat je huisarts geregistreerd heeft dat je maar niet van het roken af komt. Of wordt je dochter opgewacht door een paar gladde types met gouden kettinkjes omdat haar psychiater in het dossier schreef dat ze gemakkelijk te beïnvloeden is. Een groot systeem is nu eenmaal per definitie kwetsbaarder dan een klein systeem. Het aanvalsoppervlak en de bedreiging (het rendement van een gerichte aanval) groeit exponentieel wanneer de omvang lineair groeit. En de beveiligingskosten groeien evenzeer exponentieel. De enige bestuurlijke oplossing voor dat probleem is – zoals altijd - de veiligheidsmaatregelen weg te laten en het gat te vullen met loze praatjes. Zet dat maar niet in de folder, nee.

Het verbeteren van de zorg voor de patiënt middels wereldwijde e-health voorzieningen is dus een loos verkooppraatje. Het echte verhaal is veel banaler: de EU wil Europese bedrijven in de e-health sector ondersteunen. Dat is nodig, omdat Microsoft en Google zich op de materie gestort hebben, en de Europese bedrijven niet tegen deze giganten op kunnen. De vraag is echter of ze dit met een beetje industriepolitiek vanuit Brussel wel zullen kunnen. Het is je wellicht nog niet opgevallen, maar het taboe op industriepolitiek is helemaal weg. Een taboe dat ontstaan is in de jaren tachtig toen bij de parlementaire enquête naar **RSV** en de bauxietschraper voor Suriname bleek dat industriepolitiek een onverantwoordelijke bestuurlijke hobby is. De overheid schoot kwakkelende bedrijven te hulp in moeilijke economische tijden. Deze industriepolitiek hield een aantal grote, oude en ongezonde bedrijven iets langer weg bij de curator, waarmee gezonde bedrijven oneigenlijk beconcurreerd werden. En waarmee de burger met een onbetaalde rekening van miljarden achterbleef. Geld dat de burgers in de economisch sombere jaren '80 liever in de portemonnee hadden gehad. Geld dat voor een deel afkomstig was uit de pensioenfondsen die ons straks niet zullen uitbetalen.

Industriepolitiek werkt niet – een goede ondernemer met een goed plan werkt wel. Een goede ondernemer kan altijd wel aan geld komen, zelfs als de rente 12% is, zoals bleek in diezelfde jaren '80. Alleen slechte ondernemers met een mager plan hebben subsidie nodig. Helaas is het gemakkelijker om subsidie van Brussel of Den Haag te krijgen dan om een goed ondernemer met een goed plan te zijn.

Industriepolitiek is het belangrijkste speerpunt van ons kabinet en ook bij de EU zijn ze er wel van; de overheid strooit anno 2011 lustig met subsidies voor bevriende grote bedrijven. Ik mag natuurlijk niet opschrijven dat dit helpt om straks een leuk commissariaatje te scoren, maar de gedachte gaat wel door mijn hoofd. Dat is het meest opvallend bij het innovatiedossier - de geldstromen worden weggehaald bij TNO en de universiteiten en gaan naar grote bedrijven die

natuurlijk eigenlijk helemaal geen subsidie nodig zouden hebben. Dom? Zeker. Maar de RSV-enquête is al weer meer dan 25 jaar geleden is en wie weet dat nu nog?

In het geval van de internationale standaardisatie van het EPD is dit dan ook de echte reden; Europese softwarebedrijven krijgen een duwtje in de rug en daar is ongetwijfeld stevig voor gelobbyd. Dat dit twee kanten op werkt, ontgaat de Europese commissie blijkbaar ten enen male: buitenlandse bedrijven krijgen door deze insteek natuurlijk ook meer toegang tot de Europese markt.

Met dit beetje industriepolitiek zullen de Europese e-health bedrijven de wereldmarkt heus niet veroveren; de steun moet heel substantieel zijn, wil het helpen om Google en Microsoft te verslaan. Maar dat is te duur voor Brussel en Den Haag. Dus dan lijkt een gratis maatregel als een verdrag om het EPD technisch te standaardiseren een mooie daad.

De kernvraag is wat de Europese burger aan deze industriepolitiek heeft. Dat iets van Microsoft of Google is, is niet het beste voorteken voor veiligheid en privacy, maar waarom zou de Europese concurrentie zo veel beter zijn dat ze de markt kunnen veroveren op de twee machtigste ICT-bedrijven ter wereld? De privacy en de veiligheid van de burger wordt hier onnadenkend opgeofferd aan een beetje symbolische industriepolitiek. En goedkoper wordt het vast ook niet.

De blinde wapenwedloop

Vrijdag 1 april 2011

Op het cyberfront is een wapenwedloop op gang gekomen, waarbij Stuxnet vrijwel alle weifelaars over de streep heeft getrokken. Volgens de Amerikaanse DNI James Clapper is het aantal Chinese cybercommando's een 'enorme zorg'. Zelfs het zeer degelijke Duitsland is overstag en heeft een divisie van ruim 6000 cyberreservisten toegevoegd aan de Bundeswehr onder een heuse brigadegeneraal. Ook ons land doet mee. We hebben sinds kort een Nationale Cyber Strategie en bij Defensie heeft een werkgroep cyberoperations een overkoepelende visie opgesteld. Nog meer? Formeel niet.

Bij nader inzien loopt Nederland een beetje achter. Wat kunnen we ook, tegen dergelijke cybergrootmachten? We zijn maar een klein land en Nederland (nu ja, onze **HDIO** dan) ambieert ook helemaal geen leidende rol op het cyberfront voor onze krijgsmacht. In Libië moeten we het immers ook doen met zes bejaarde straaljagers en één zevenentwintig jaar oude mijnenjager. We moeten voor menskracht en meer geld dan ook vooral samenwerken met onze traditionele bondgenoten. En die zijn huppekee in een wapenwedloop gesprongen.

Traditioneel gezien win je een wapenwedloop alleen door outspending. Dat werkt zo: je koopt meer spullen dan je tegenstander, die dan nog meer koopt en jij dan nog meer, tot het moment dat één van de partijen moet afhaken omdat het geld op is. Deze strategie werkt natuurlijk alleen als jij rijker bent. Maar goed, wij zijn het rijke westen, en hullie niet. Dit was de strategie van de 20e eeuw.

In de eeuw van cyberoorlog klopt hier echter geen moer meer van. Exploits en firewalls zijn geen slagschepen of atoomraketten. Materieel overwicht is in de cyberdimensie van nul en generlei waarde; met één exploit op een zeer gangbaar stuk ICT krijg je je tegenstander op de knieën. De levensduur van wapentuig is daarbij zeer onvoorspelbaar en wellicht beperkt; zodra je een exploit gebruikt, weet de tegenstander ervan en kan hem ook tegen jou inzetten. En wellicht onschadelijk maken. Afstand nemen van het verouderde wapenwedloopparadigma is echter duidelijk nog niet gelukt.

Nederland loopt op het cyberwarfront weliswaar achter, maar eigenlijk is dat achterlopen niet zo'n probleem. Wél een probleem is dat onze bondgenoten blijkbaar niet helemaal door hebben waar het om draait en wij - zoals altijd - afwachtend aan tafel zitten tot we gevraagd worden mee te doen, op hun manier en op hun voorwaarden. Ook dat is een diepgewortelde gewoonte: wij bouwen onze defensie zo dat hij zo veel mogelijk aansluit op die van onze verwachte bondgenoten. Dat deden we al vóór de NAVO en zelfs lang voor de Tweede Wereldoorlog, terwijl we officieel nog helemaal geen bondgenoten hadden. Zelfstandig nadenken over hoe je oorlog moet voeren is feitelijk sinds de vestingwet van 1874[57] in ons land niet meer vertoond.

Het is erg jammer dat de Nederlandse ambities op het cyberfront door Defensie op voorhand op een heel laag niveau worden geplaatst. Het is een nieuw operatiegebied voor de NATO, en iedereen is zoekende. Het beleid is nu dat we even wachten tot het iedereen duidelijk is wat er moet gebeuren. Dit lijkt mij een beleidsbeslissing die niet aan een hoger ambtenaar van een uitvoeringsministerie als Defensie is, maar aan de politiek. Daarbij zou ook naar de bredere belangen gekeken moeten worden, onder meer dat er een geheel nieuwe wapenindustrie te ontwikkelen is. Reken maar dat daar ook goed geld mee te verdienen is.

[57] http://nl.wikipedia.org/wiki/Vestingwet

Cyberwar staat nog in de kinderschoenen. Dat wordt snel duidelijk als je de discussies en de programma's nader bekijkt. Laten we beginnen bij de aanleiding, Stuxnet, het computervirus dat het Iranese kernprogramma onderuit geschoffeld heeft. Stuxnet leidde tot een whodunnit in de beste tradities van de BBC detective.

Stuxnet gebruikt maar liefst **4 zero day gaten** in Windows, is dus zeer complex en zeer verfijnd, en moet dan ook gemaakt zijn door een grote groep met **significante hulpbronnen**. De enige partijen die een dergelijke capaciteit in huis hebben, zijn China, de VS en Israël. En omdat China niets heeft tegen Iran, hebben dus de Israëli's óf de Amerikanen het gedaan. En omdat die twee altijd samen optrekken, zullen ze het wel samen gedaan hebben, volgens gezaghebbende deskundigen althans. Deze analyse is – zonder de landnamen weliswaar – opgenomen in de Nederlandse Cyber Security strategie. Niet gek, want op het eerste gezicht is het best overtuigend.

Maar de analyse is bij nadere beschouwing afhankelijk van een aantal forse aannames. Aannames die aantoonbaar onjuist zijn.

De belangrijkste verkeerde aanname is die over de benodigde hulpbronnen. Lees hiervoor het historische voorbeeld van **L0pht**, zoals beschreven in het onvolprezen boek 'Beautiful Security[58]'. Daarin beschrijft Mudge de '**confirmation trap**' (in goed Nederlands: tunnelvisie) aan de hand van zijn persoonlijke ervaringen rond L0pthcrack. Deze geschiedenis vertoont verontrustend veel overeenkomsten met het hele Stuxnet-verhaal. Volgens Mudge stelde een NSA-agent dat L0phtcrack "not possible" zou zijn "without nation-state-type funding". En dat terwijl L0pht niet meer was dan een paar techneuten zonder geld, maar met tijd, kennis en vooral slimme ideeën. Voor zero days heb je blijkbaar geen digitaal regiment met een budget van een paar miljoen per maand nodig. Wat je nodig hebt is een paar slimme mensen met een paar doorsnee computers. Een klein groep researchers bewees dat dit anno 2011 nog steeds geldt, door in korte tijd 34 nieuwe **exploits** voor SCADA te onthullen.

De analyses van Stuxnet tonen naast deze cruciale confirmation trap nog meer kritieke denkfouten. Deze zitten in een verkeerde perceptie van het vulnerability management. Vulnerability management is het beheer van gaten in je systemen en het fixen (patchen is maar één manier) ervan. Vulnerabilities zijn de basis voor de meeste offensieve digitale 'wapens' en de fixes de belangrijkste operationele defensieve wapens.

Een goed beeld van hoe de wereld van vulnerabilities in elkaar zit is essentieel voor hoe we ons voorbereiden op de toekomst met onze nationale cyberstrategie en militair georganiseerde cyberlegers. Als we niet weten welk slagveld we betreden en wat de wapens en de realiteiten daar zijn, is onze overlevingskans gelijk aan nul. En daar heeft het alle schijn van. Voor deze fouten zullen we op enig moment stevig moeten bloeden.

De meest opvallende fout is de inschatting dat 4 zero days heel bijzonder is. Dit is een categorische denkfout over hoe de wereld van vulnerabilities en exploits in elkaar zit. Overigens is dit een fout die vrijwel iedereen in de beveiligingsindustrie maakt. Hoe zit dat?

Om te beginnen is het inzicht dat de wereld van security mondiaal is, geheel afwezig. De security industrie wordt – net als de hele ICT - gedomineerd door Amerikaanse bedrijven en gaat volledig uit van het Anglo-Amerikaanse wereldbeeld en de Engelse taal. Als een niet-westerse onderzoeker een gat aanmeldt in een westers product, zal dat vrijwel altijd in het Engels moeten. Als de onderzoeker die taal niet beheerst, of het te veel moeite vindt om het uit te zoeken, dan wordt de

[58] http://oreilly.com/catalog/9780596527488

vulnerability niet gemeld. Zeker als de leverancier niet zit te wachten op een kritische melding over een product, is de receptie en bijbehorende afhandeling van een melding al niet erg behulpzaam, zeg maar ronduit irritant. En laten we wel wezen, de meeste leveranciers zitten er inderdaad niet op te wachten. Bedenk vervolgens dat meer dan de helft van de internetgebruikers (en dus computergebruikers) geen Engels kan lezen of schrijven. Het resultaat is dat het gat niet gemeld en dus niet gefixed wordt.

Als de goedwillende Azerbeidzjaan, Egyptenaar of Pakistani dan maar op Full Disclosure of een ander forum in krakkemikkig Engels de bevinding meldt, is een welwillend oor zeer ongebruikelijk. In de regel wordt zo iemand volledig weggeflamed. Ook securitymensen zijn xenofoob. Dat doet de niet-westerse persoon in de regel dus ook maar één keer. Met als netto resultaat: de bevindingen raken hier niet bekend en worden niet gerepareerd. Het aantal gaten dat hier een zero day is, maar in de rest van de wereld niet, is waarschijnlijk niet gering en zal zonder ingrijpende veranderingen in hoe wij security bedrijven, alleen maar veel groter worden.

Er schuilt nog een kritieke fout in de disclosure wereld. Dit beeld ken ik uit eigen observatie – in projecten bij klanten kun je tegen zaken aanlopen, die je niet mag melden aan de leverancier omdat dan op enig moment formeel bekend zal worden wat het gat is en de klant dan juist kwetsbaar wordt. Dit speelt vooral bij grote klanten met verstand van beveiliging; zij weten dat het verschijnen van een patch via reverse engineering leidt tot exploitatie in het wild, terwijl ze ook weten dat de patch niet zo één-twee-drie over alle systemen uit te rollen is. Deze 'no-disclosure' policy heeft zeer verregaande gevolgen. Het zal immers meer voorkomen bij typische Enterprise software dan bij een populair appje voor thuis. Gaten worden dus eerder bekend gemaakt van populaire maar minder belangrijke applicaties, dan van de kritieke infrastructuur van grote bedrijven en overheden. Dat zie je ook heel goed aan de statistieken van bekendgemaakte vulnerabilities: de bulk van de gemelde gaten betreft veelgebruikte desktop- en webserversoftware. Je zou haast concluderen dat Acrobat veel meer fouten bevat dan SAP Netweaver. Dat is natuurlijk hoogst onwaarschijnlijk; grote, samengestelde en normaliter gecustomiseerde producten zijn veel complexer en veel moeilijker te beveiligen. Zij bevatten per definitie veel meer fouten dan kleine producten. Dat bewijzen Stuxnet en de recente vondsten in SCADA ook weer.

Grote en complexe producten worden gemaakt door grote en complexe bedrijven. Die zijn van nature gevoeliger voor tunnelvisie dan kleinere en jonge bedrijven. De kans dat een gat in de software of de systemen niet gezien wordt, is bij de gevestigde orde dan ook veel groter. Dit is recent nog eens te zien geweest bij de hack van **RSA**, één van de grootste gespecialiseerde spelers in security.

Nu kun je denken dat de ontbrekende kennis over vulnerabilities dan wel aangevuld zou worden uit analyse van de aanvallen die in het wild voorkomen. Nou, dan moet ik je toch teleurstellen. Wat er in het wild met exploits gebeurt, geeft juist een zeer onvolledig beeld. Bij de meeste organisaties worden kapotte zaken hersteld, maar ontbreekt de technische kennis en vaak ook de interesse om vast te stellen of er ingebroken is, dan wel of er een storing is geweest. Wat organisaties volgens het boekje moeten doen is vaststellen wat de gebruikte methode is en verifiëren of deze al bekend is. Als de methode niet bekend is, dan is het een zero day en moet er aan de bel getrokken worden. Als dit gehele moeizame traject doorlopen wordt – wat vrijwel nergens ooit gebeurt - geldt vervolgens hetzelfde als bij disclosure: willen ze het melden, mogen ze het melden en kunnen ze het melden, gegeven de taal? We moeten er van uitgaan dat het overgrote deel van de aanvallen die in het wild voorkomen, niet in de wijde wereld bekend wordt.

De conclusie van dit lange betoog: het geheel aan bekende exploits is hoogstwaarschijnlijk niet representatief voor de gaten die er zijn. Het gebruik van 4 zero days in Stuxnet is dus helemaal

niet bijzonder en er hoeft helemaal geen grote organisatie met een megabudget achter te zitten. Dat betekent overigens niet dat cyberwar niet bestaat. Maar het bewijst wel dat de invloedrijkste ICT-security experts lijden aan tunnelvisie en dat zij essentiële zaken over het hoofd zien.

Voor de actieplannen die de NAVO-militaire-denkhoofden samen met deze leidende ICT-security experts opstellen doet dit het ergste vrezen. Dit gaat niet leiden tot veel resultaat. Wel leidt het tot een groeiende berg publiek-private samenwerkingsovereenkomsten. Zo'n praat- en processenfabriek is heel fijn voor de security markt, maar niet voor het beoogde resultaat. Dus mocht Nederland ooit gevraagd – of gedwongen - worden mee te doen, dan zullen onze cyberlegers net zo hard de verkeerde kant op marcheren als die van onze bondgenoten.

We doen het zelf

Vrijdag 22 april 2011

De grootste bedreiging voor onze privacy is niet de overheid of het bedrijfsleven, dat zijn we zelf. En dan nog niet eens op de manier zoals Den Haag ons wil doen geloven, dat 'iedereen' zijn hele hebben en houen op Hyves en Facebook flikkert. Nee, de bedreiging is dat we massaal in de veiligheidsutopie geloven.

Dat is weer goed te zien in de afwikkeling van de schietpartij in het winkelcentrum van Alphen. In de discussies daarover vraagt men zich vooral af hoe het in godsnaam mogelijk is dat een zwaar gestoorde godsdienstwaanzinnige aan een **wapenvergunning** kan komen.

Tja. Alsof het dáár om gaat. Dat iemand het misschien had kunnen voorkomen. Die moet hangen. Er moet een zondebok zijn, en omdat de schutter zichzelf voor de kop geschoten heeft is er geen.

De eerst aangewezen zondebok was Call Of Duty MW2; de schutter zou dit gespeeld hebben en inspiratie opgedaan kunnen hebben in het roemruchte **vliegveldlevel**. Nu is dit nou net het enige saaie level van MW2, dus wat daar inspirerend aan is? Maar goed, er wordt dus wat gesputterd om dit soort spellen te verbieden, maar dat blijft bij gesputter. Het verbieden van de verkoop zou ook weinig helpen; CoD 6 is nu al het **meest illegaal gedownloade spel**. Wil je het spelen van dit spel voorkomen, dan moet je op iedere PC 'een stukje toezicht' aanbrengen – een beetje overheidsspyware, zeg maar. Daar wil niemand aan. Op dit moment, dan. Wat niet is, kan nog komen natuurlijk.

Dan maar de wapenwet. En de politie en de schietclubs. Er is immers duidelijk iets mis gegaan in de handhaving; de schutter had een wapenvergunning. Deze moet jaarlijks worden verlengd en daarbij moet gekeken worden of de vergunninghouder niet in aanraking is geweest met de politie. Bovendien is de politie in Nederland verplicht vuurwapenbezitters elk jaar minstens een keer te controleren. Die huisbezoeken worden lang niet altijd uitgevoerd, zo bleek uit onderzoek van de **GPD-kranten in 2008**. In de kamer gaan stemmen op om deze controle uit te breiden tot 'psychische stabiliteit' met een **controle** naar psychische stabiliteit van de wapenbezitter.

We gaan dus wellicht extra maatregelen krijgen die psychisch instabiele mensen uitsluiten van een wapenvergunning. Een voor de hand liggende optie is een psychologisch onderzoek bij de jaarlijkse verlenging van de wapenvergunning. Klinkt goed, nietwaar?

De kans dat iemand op zo'n keuring eerlijk meewerkt aan het psychologisch onderzoek is echter een stuk kleiner dan bij een normaal onderzoek; de wapenbezitter wil immers goedgekeurd worden. Bovendien weet hij dat de politie de gegevens van dit onderzoek te zien krijgt; wie weet wat voor consequenties het allemaal zal hebben als er in je dossier staat dat je labiel bent en van schieten houdt. Daarbij weten we al jaren dat mensen met psychische stoornissen best goed zijn in het misleiden van hulpverleners. Zo'n extra toets gaat dus waarschijnlijk niet veel helpen.

Aansluiten op de normale zorg dan maar? Ja, dat gaat helpen: als je lid van een schietclub bent en je een beetje down voelt, denk je voortaan wel twee keer na voordat je naar de huisarts gaat. Kun je je hobby door kwijtraken. Zo bezien levert zo'n maatregel wel een bezuiniging op in de zorg en dat is dan weer fijn voor Rutte, maar de bezuiniging zal niet opwegen tegen het toenemend risico van schietpartijen à la Alphen. Een depressievelling onder behandeling is immers een kleiner gevaar dan een depressievelling zónder behandeling.

Los daarvan, wie moet er dan gemonitord worden? Volgens het GGZ heeft 43,5% van alle volwassen Nederlanders op enig moment **psychische problemen**. Het overgrote deel hiervan is alleen bij de huisartsen geregistreerd. Naast deze mensen die in beeld zijn bij de GGZ zijn er ook nog mensen die nooit zorg zoeken. Vooral mannen mijden de zorg, en vooral mannen hebben 'iets' met wapens. Dus, voor alle zekerheid zou het maar het beste zijn als zeker de helft van alle Nederlandse burgers nooit en te nimmer een wapenvergunning zou mogen hebben. Nou kan ik daar persoonlijk niet mee zitten want ik houd niet van schieten, maar ik zie het niet gebeuren. Niet eens zozeer vanwege de traditie van sportschutters die je daarmee om zeep helpt, en die op zich toch ook wel wat waard is. Er bestaat ook nog zoiets als de jagerslobby. Een volledig wapenverbod heeft het eerder ook al nooit gehaald. Dus er zullen wel aanvullende maatregelen rond de vergunning komen.

Deze maatregelen zullen hoe dan ook impact hebben op de privacy – hoe zie je het anders voor je om mensen met een labiele geest een wapenvergunning te onthouden? Nu is het verlies van enige privacy best nog te verdedigen, als het werkt. Maar of het werkt, dat is nogal de vraag. Het probleem is namelijk – zoals altijd – de uitvoering. Of zo je wilt, de handhaving. Krijgt de politie inzage in alle medische dossiers van ieder lid van een schietvereniging? Makkelijker gezegd dan gedaan. Gegeven de decentrale aard van medische dossiers en het sneven van het landelijk dossier houdt dit in dat de politie toegang moet krijgen tot alle decentrale zorgsystemen; er is immers sinds de dood van het landelijk EPD geen verwijsindex waarin op te zoeken is bij welke zorgverlener iemand allemaal bekend is.

Wat ook kan, is dat de zorg meldplicht krijgt. Klinkt lekker daadkrachtig, maar het betekent – zoals wel vaker – helemaal niets. De zorg weet immers niet of iemand een wapenvergunning heeft of zou willen hebben. Dus moet je de zorg naar eventuele wapenvergunningen laten vragen en dit registreren in de zorgsystemen. En dan maar hopen dat de patiënt eerlijk antwoord geeft.

Hmm. Vast niet.

Dan moet de zorg maar iedereen 'aangeven' waarbij twijfel is of de persoon nu of in de toekomst stabiel genoeg is om een wapen te bezitten. Om er zeker van te zijn dat niemand erdoorheen glipt, zal dat vrijwel iedereen zijn die zich meldt met psychische problemen. Hoe zich dit verhoudt tot het medisch beroepsgeheim en de ethiek van de gemiddelde zorgverlener is duidelijk; de medicus werkt tegen. Maar stel nou, voor het gemak, dat de zorgverleners mee zouden werken. Dan heeft de politie een dossier tegen ongeveer de helft van de Nederlandse bevolking. Dat houden we juridisch niet droog: één simpele procedure richting het Europese Hof voor de mensenrechten op grond van de proportionaliteitsregel en de maatregel wordt teruggedraaid.

Zowel bij inzage in medische systemen als bij meldplicht gaan we heel veel privacy inleveren. Met de beste bedoelingen, daar niet van. Het gaat erom een drama als in Alphen te voorkomen. Maar het risico op zo'n drama zal hierdoor juist groeien omdat mensen met een bepaalde depressieve inslag de zorg gaan mijden, omdat de zorg dan als verlengstuk van de politie gezien kan worden. Wat ze dan overigens ook is.

Hmmm. Ook al niet.

Er zijn in deze gewoon te veel onzekerheden om het goed te doen. En er is een grote kans om alleen maar verkeerde dingen te doen. Zwartepieten en daadkracht eisen van politie en politiek is dus het laatste wat we moeten doen; van ondoordachte acties komen over het algemeen alleen maar nog grotere ongelukken. En die zullen er komen: de beleidsfabriek in Den Haag kan deze reuring immers niet negeren, dus er komen maatregelen, bevoegdheden, overlegstructuren en

flankerend beleid. En dat alles ongeacht de effectiviteit – er moet iets gedaan worden, ook als evident is dat het niet helpt; Den Haag wil immers echt wel naar de burgers luisteren.

De waarheid is dat er voor drama's als deze geen preventie mogelijk is - hoe graag we dat ook zouden willen. Volledige veiligheid is een utopie; we zullen als samenleving dan ook een andere manier dan dit geroeptoeter moeten vinden om met het verdriet en onze onmacht om te gaan.

Schengen 2.0

Maandag 9 mei 2011

De strijd tegen Cybercrime heeft weer alle aandacht. In Den Haag, maar nog meer bij de EU. Op de bijeenkomst van Enfopol en Enfocustom in februari onthulde de LEWP (Law Enforment Working Party) haar plannen: we leggen een digitale grens aan rond het Europese deel van het internet. Een “single secure European cyberspace with a certain virtual Schengen border and virtual access points”. De ISP’s zullen “illicit contents” blokkeren op basis van de "**black-list**".

Wow. Een ‘secure European cyberspace’, dat klinkt pas goed. Virussen, hackers en spam worden voortaan als ongewenste vreemdelingen aan de poort geweigerd, en overtreders zonder pardon over het metershoge virtuele hek gesmeten. Zo krijgen we binnen deze Eurozone een veilig internet. Bedrijven en burgers weten zich beschermd door een waakzame en kundige overheid.

Tot zo ver de illusie. In de echte wereld is dit namelijk je reinste kolder. Het zou misschien kunnen, als virussen, hackers en spam alleen buiten de EU ontstaan en zich vervolgens alleen maar verspreiden via het internet. En als je door het blokkeren van bepaalde content op de lijn, een secure zone kan creëren. Iedere firewallbeheerder weet dat dit een kansloze aanpak is, zelfs met deep packet inspection en oneindig veel rekenkracht. Er blijven immers genoeg andere vectoren, zoals corporate WAN’s, USB sticks, smartphones en laptops die overal maar onbeschermd in netwerken worden geprikt en wie weet zelfs nog diskettes, om er maar een paar te noemen. Om maar niet te spreken over de problematiek van de detectie van zeker vier nieuwe virussen **per minuut**.

Het voorstel gaat dan ook eigenlijk helemaal niet over onze veiligheid. Die indruk wordt alleen maar gewekt, door het gebruik van het woord Security. Waar gaat het dan wel over? Het weggevertje in deze is de term ‘Illicit Contents’. En dat is een heel breed begrip. Het wordt gebruikt over de volle breedte voor zaken waar mensen tegen zijn, van het voorkomen dat tieners onbedoeld met porno in aanraking komen tot smaad, opruiende geschriften en illegale mp3’s.

Als dit voorstel wordt uitgevoerd, dan wordt Europa ontkoppeld van het Internet. Wat we dan krijgen is een soort Internet Light, met alleen goedgekeurde content; dus content waar voor betaald wordt en waar niemand anderszins bezwaar tegen heeft gemaakt of zou kunnen maken. De gezamenlijke Europese opsporingsdiensten besteden hun tijd aan het inrichten van dit gedrocht ondanks het censuurverbod in de **Nederlandse grondwet** . Je kunt natuurlijk beargumenteren dat dit niet zomaar kan, omdat opsporingsambtenaren uitvoerders van de wet zijn, en niet op kosten van de belastingbetaler de rechtsstaat mogen ondermijnen. Je zou ook kunnen beargumenteren dat het plan vanwege het censuurverbod in de grondwet toch niet doorgaat.

Jammer, maar helaas.

Het censuurverbod heeft namelijk de toevoeging ‘behoudens ieders verantwoordelijkheid volgens de wet’, en dat is oneindig rekbaar. En reken er maar op dat de dames en heren van de Europese politiemachten veel meer zicht op de ontwikkelingen hebben dan wij gewone burgers. Internet Light komt er.

Het plan voor wat een soort virtueel Schengen moet worden, is niet meer dan weer een maniertje om een filter op mp3s en geripte dvd’s te zetten, en ondertussen even moralistische, politieke en vooral **commerciële censuur** naar **Amerikaanse snit** in te voeren. En dan natuurlijk nog beter.

Tja, ze geven niet snel op. Internetcensuur is een typisch geval van een bestuurlijke Betuwelijn; niemand is er echt voor, maar omdat de machine in gang is gezet, is hij kennelijk niet meer bij te sturen.

Gaat het dan om een variant op het **ACTA-monster**? Volgens Brein beloopt de economische schade van het downloaden van films en muziek in Nederland intussen al **315 miljoen euro** per jaar. Zeggen ze. Het Schengen 2.0 plan heeft inderdaad met ACTA te maken, maar dan met een verfijnde nuance: de misgelopen indirecte belastingen – hoe anders de rol van de douane te duiden? Als de industrie per jaar 315 miljoen euro verliest, dan verliest de overheid 19% btw daarvan en die 60 miljoen kan Den Haag vast wel gebruiken om de kraters in de begroting te dichten. Nee nee mijnheertje, belasting ontduiken, dat gaat zomaar niet!

In 2000 concludeerde de Nederlandse regering dat het innen van btw in de digitale wereld geen doen was, en besloot tot een **nultarief**. Toenmalig minister Zalm van Financiën zag geen **praktische mogelijkheden** om deze belasting te innen. Deze pragmatische gedachte hield echter niet lang stand, en vanaf 2003 werd alsnog btw **ingevoerd** op digitale producten. Het innen daarvan bleef echter, met het uitblijven van een grootschalige digitale economie, wel problematisch; het overgrote deel van de digitale handel is nog steeds het downloaden uit illegale bron. Geen btw op te heffen dus.

Om de stijgende kosten van de gezamenlijke opsporingsdiensten in al haar bestuurlijke gelaagdheid te financieren worden nu de ISP's aangewezen als digitale tolpoortjes. Met de door de vergrijzing onomkeerbaar teruglopende criminaliteit moet er toch nieuw werk geschapen worden - het jagen op downloaders mag sommige politici een slecht idee lijken, de opsporingsdiensten zien er blijkens dit voorstel best wel brood in. De term cybercrime triggert de belangrijkste bestuurlijke reflex bij regeringen; het probleem aanpakken. Deze reflex is snedig samengevat door Sir Humprey Appleby: "We must do something. This is something. Therefore we must do it![59]". En dat levert banen op.

Om deze kronkel te verkopen wordt de burger belazerd met beloftes over een veiliger Internet en wordt de politiek belazerd met beloftes over inbare belastingen. Laten we hier niet intrappen. Laten we voor ogen houden over wiens veiligheid we het hier nu uiteindelijk hebben; we hebben het hier over de baanveiligheid van de opsporingsdiensten en we hebben het over de omzetveiligheid van de media-industrie. Van dit plan wordt verder geen enkele burger in Europa beter.

[59] http://www.jonathanlynn.com/tv/yes_minister_series/yes_minister_episode_quotes.htm

Proven technology

Vrijdag 27 mei 2011

Vroeger was informatiebeveiliging goed te doen. Je had binnen, daar stonden je servers en daar zaten je gebruikers. En je had buiten, daar zaten je klanten. Dat waren subjecten in een informatiesysteem, waar alleen je eigen gebruikers bij konden. Beveiligen was zorgen dat er alleen mensen binnen konden die je vertrouwde. De erfenis hiervan zie je nog in de vorm van wachtposten aan de deur en screening van personeel. Nu zijn de wachtposten bij de deur er alleen nog om je tegen fysieke diefstal te beveiligen, vroeger was het een belangrijke (vaak zelfs de belangrijkste en ook de enige) voorziening van informatiebeveiliging. Dat noemen we het kokosnootmodel, hard van buiten en zonder structuur van binnen. Iedere organisatie wist zich veilig verschanst achter de fysieke muren.

Je mag het eigenlijk niet zeggen, maar vroeger was beveiliging dus echt slechter. Toen ik midden jaren '90 in dit vak begon was de voornaamste taak van de beveiligingsafdeling van de bank het geheimhouden van het telefoonnummer van de modempool. En als dat nummer uitlekte, dan, eh, ja, wat dan eigenlijk? We zouden een inbraak waarschijnlijk pas gemerkt hebben als de telefoonrekening absurd hoog werd. Stel dat we naar de rekeningen hadden gekeken.

Dat was vroeger, en het inzicht dat dit achterhaald is, is gemeengoed; waarom zou je daar een column aan wijden? De case is immers toch duidelijk gemaakt met het **Jericho project** rond 2006. Een goed gevonden beeld; de fysieke muren zijn inderdaad omgevallen. Het punt is echter dat dit niet het einde van deze geschiedenis is. Wat komt er ná het vallen van de muren? In 2006 hadden we nog geen Bring Your Own Device (BYOD), de Cloud moest nog uitgevonden worden en over de Smartphone gingen alleen nog maar geruchten. Dit zijn allemaal zaken die ons sindsdien vanuit de business overvallen hebben, en die we niet kunnen negeren, hoe graag we dat ook willen. Moeten we nu het wiel met bloedspoed gaan uitvinden?

Ja, dat moet.

Gelukkig zijn er waardevolle bouwstenen beschikbaar, de meesten al jaren. De grootste schatten zitten verstopt in het Claims Based gebeuren, de WS-Security hoek en bij **XRML**. Deze laatste kennen de meesten van ons wellicht beter als WRM, het MS Office broertje van Digital Rights Management.

Helaas zijn deze middelen onder het hoogst irritante adagium 'proven technology' vrijwel overal buiten de deur gehouden. En nu kunnen we er niets mee omdat we de kennis er niet voor hebben. De grootste gotspe van de Security is wel dat proven technology hier óók als valide argument wordt beschouwd.

Voor de mensen die het niet kennen: proven technology wil zeggen dat we dingen pas inzetten als ze zich een paar jaar bewezen hebben bij anderen. In de praktijk is proven technology vooral een eufemisme voor ouwe troep. Een excuus voor conservatisme, van mensen die de veranderingen bijhouden blijkbaar te veel moeite vinden. Het principe is vooral populair bij IT-managers in grote organisaties, banken en ministeries voorop.

Met de eis voor proven technology zeg je dat het nieuwe nog niet bewezen is. Dat is natuurlijk ook zo. Maar je impliceert ook dat het oude zich wél bewezen heeft. Dat is in de ICT Security hoogst zelden het geval. Maar al te vaak is proven technology een excuus om iets niet te doen;

immers als je iets doet, dan krijg je weer van die ICT projecten. En die mislukken. Vandaar deze reflex bij IT managers. Begrijpelijk, maar verkeerd.

De mens is van nature geneigd om te stellen dat het vroeger beter was. Dat hebben we allemaal; ook auditoren kijken minder kritisch naar proven technology dan naar onbekende zaken. Dat bleek overduidelijk bij het **Deepwater Horizon olielek van BP**. Deze tunnelvisie is zeer bepalend van onze waardering van beveiliging. Het begrip proven technology is dus het perfecte voorbeeld van hoe contraproductief een **selectief geheugen** werkt. Vroeger was het niet beter, we hadden alleen minder zicht op hoe slecht het allemaal was; dat is de prijs van meer kennis en inzicht.

Een kleine vertaling naar de dagelijkse IT-werkelijkheid. Wat is de levensduur van computersystemen? Vijf jaar. Wanneer is iets proven technology? Na drie jaar elders in gebruik. Hoe snel kunnen we iets nieuws invoeren? In ongeveer twee jaar, en omdat vrijwel iedereen eerst op iedereen zit te wachten beginnen de eerste implementaties na vier jaar, en is de grote massa na negen jaar in productie. Inderdaad: Windows XP.

En dan nog een kleine vertaling naar best practices. Waar ontstaan best practices? Bij grote organisaties. Hoe voorop lopen die? Niet bijster, meestal lopen ze een paar jaar achter op cutting edge. Zeg vijf jaar. Hoe lang duurt het voor een best practice vertaald is naar een bestaand normenkader? Drie jaar? Hoe lang doen we er over om een nieuwe versie van een normenkader in te voeren? Vijf jaar? Door de lengte van deze keten is de gemiddelde 'best practice' een oplossing van een 13 jaar oud vraagstuk. Inderdaad: ITIL v3.

Organisaties die kiezen voor proven technology, kiezen dus gewoon voor slechter.

Het concept proven technology komt uit de bouw. In die wereld is het een prima concept: zwaartekracht, torsie, baksteen en beton veranderen niet, en wat er verandert in materialen gaat meestal langzaam. Maar wat in het ene domein een wet van Meden en Perzen is, hoeft dat in een heel ander domein niet te zijn. Zo heeft IT beveiliging meer overeenkomsten met het militaire bedrijf (je wordt aangevallen) dan met de constructie van huizen (het regent).

In het militaire bedrijf is bewezen dat unproven technology soms onmisbaar is; onderzeeboten tot 1950 waren onbetrouwbare doodskisten, vliegtuigen tot 1940 ook – en toch bepaalden ze de uitkomst van de Tweede Wereldoorlog. Als slotakkoord van die oorlog had je dan nog de ultieme unproven technology: de atoombom.

Een goed beginpunt voor hoe militairen denken over proven technology zijn de **Technology Readiness Levels** waarmee de inzetbaarheid van technologie wordt geclassificeerd. Daar kunnen wij een boel van leren. Zelfs het hoogste niveau, 9, is veel eerder bereikt dan het ongrijpbare 'proven technology' zoals wij dat dagelijks gebruiken. Een dergelijke formalisering van wat 'proven' dan wel 'unproven' is had er in de IT Security al lang moeten zijn. Maar dit soort volwassenheid hebben we na ruim 25 jaar professionele beveiliging blijkbaar nog steeds niet bereikt.

Hackers in het groen

Vrijdag 8 juli 2011

Wereldwijd hebben overheden de conclusie getrokken dat het tijd wordt de traditionele defensieapparaten uit te breiden met Cyberlegers. Zo ook ons land, dat in een tijd van zeer forse ingrepen in de krijgsmacht, 50 miljoen euro gaat uitgeven aan 'cyber defense'. Nederland zet de laatste Leopard 2 tanks bij het schroot en gaat cyberen. Wat ik me afvraag is wat we dan eigenlijk gaan doen met die 50 miljoen. Komen er nu aanbestedingen voor zero days? Krijgen de ICT beveiligers van defensie meer geheugen in hun PC en mogen ze een ander OS gaan draaien dan het toch wel wat belegen Windows XP van de standaard MULAN omgeving? Of – zouden er opslagen in het vat zitten voor de schaarse IT security specialisten?

Ik denk het niet. Het zal als vanouds een Hollandse oplossing zijn als het kopen van wat doosjes bij gerenommeerde leveranciers maar vooral het instellen van een studiegroep. En eigenlijk is een studiegroep helemaal geen slecht idee, want hoe een cyberleger er in het echt uit ziet, is ondanks tal van boeken en legio congressen, nog nauwelijks beschreven. De evangelisatiefase is namelijk nog volop bezig; alle tijd en energie gaat zitten in roeptoeteren hoe hard een cyberleger nodig is. Nu blijkt dat de enigen die er over nagedacht hebben wat een cyberleger dan zoal nodig heeft, leveranciers van 'solutions' zijn, die - logisch - hun eigen 'solutions' adviseren. Dat is op voorhand een kansloze aanpak.

Hoe dan wel? Een cyberleger is natuurlijk iets heel anders dan een traditioneel leger; het uniform zal wel anders moeten, het wapentuig zal heel anders zijn en ook de organisatie zal niet langs de lijnen van een infanterieregiment zijn. Maar een cyberleger omvat wel degelijk de normale componenten van troepen, wapens en organisatie. Laten we de grootste vragen eens op een rijtje zetten.

De Troepen
Een rondgang langs de internationale online discussiefora over cyberwar laat zich best samenvatten als één grote litanie over het probleem van het vinden en behouden van cyberwarriors. Een cyberwarrior is de klassieke factum totem die aanvallen kan uitvoeren, kan verkennen en kan verdedigen. Dat dergelijke technische alleskunners niet uit hun bed komen voor de loonschalen der overheden leidt tot een verlamming van de discussie. De VS **stelt** dat ze 20 tot 30.000 van deze mensen nodig heeft, en er 1.000 heeft. Het kan heel wel zijn dat die 30.000 er überhaupt op de hele wereld bij elkaar niet zijn. Dit heeft al geleid tot leuren met green cards, waarmee briljante techneuten uit andere landen verleidt worden om dienst te nemen bij het Amerikaanse leger. Ook heeft de FBI de druk opgevoerd op hackers uit eigen land, die voor de keuze worden gesteld om of de bak in te gaan, of voor de overheid te gaan werken.

Nu leidt ronselen zelden tot goede troepen, en of de import uit andere landen tot de gewenste resultaten gaat leiden is ook nogal de vraag. Waar liggen de loyaliteiten van deze beide categorieën? Het lijkt vooral op een noodgreep. Nu biedt het wel leuke carrièrekansen voor Nederlandse supertechneuten, maar dan houden we hier te lande alleen proceduretijgers en procesboeren over voor ons cyberleger en daar win je geen oorlog mee. Dan kunnen we ons maar beter gelijk overgeven.

De Wapens
Een cyberarsenaal opzetten en aanhouden is ook geen simpele zaak. Wat moet daar dan zoal inzitten? Wat hebben we nodig en wat willen we hebben? Wat moeten we kopen en wat hebben we al?

Wapens vallen normaliter uiteen in twee hoofddtypes, offensief en defensief. Daarnaast heb je in de regel nog wat aanvullende zaken, zoals verkennning en verzorging. Laten we beginnen bij defensieve wapens. Als computerbeveiliging voortaan cyberdefence heet hebben we die namelijk al. Misschien wat beter of misschien wat slechter, of je je systemen beveiligd tegen de een of tegen de ander, de wapens zullen op hoofdlijnen hetzelfde zijn.

Bij offensieve wapens wordt het opeens snel erg ingewikkeld. De eerste vraag is of offensieve digitale wapens wel de morele toets der politiek kunnen doorstaan. Mag je computervirussen bouwen of inbreken op systemen van anderen? In een defensiecontext klinken deze vragen nogal debiel, gegeven dat veel defensiematerieel erop gericht is mensen te doden of liever nog, ernstig te verminken. Een gewonde vraagt immers meer zorg dan een dode. Da's toch beduidend serieuzer dan het inbreken op een switch.

Toch zijn deze vragen al gesteld en dit is de grootse bedreiging voor een zinvol cyberleger. De politiek heeft een lange traditie om de specialisten nooit zelf de middelen te laten kiezen. Als het voorspelbare en onvermijdelijke falen dan komt, schuift de politiek vrolijk de schuld door naar dezelfde specialisten. **Van de politiek** mochten er geen zware wapens als tanks en anti-tank raketten mee naar Srebrenica omdat de Serviërs daar waarschijnlijk op tegen waren. Toen Mladic met een paar antieke T*55* tanks aankwam, stonden onze jongens met lege handen en konden alleen wegrennen. Bij de recente uitspraak dat Nederland **schuld draagt** aan de massamoorden die daarop volgden wordt de schuld door de politiek en de media doodleuk bij Defensie neergelegd, terwijl de beperkingen door de politiek waren opgelegd. Als klap op de vuurpijl beslist de politiek dat we in de toekomst prima zonder tanks kunnen, omdat missies daar niets aan zouden hebben. Von Clausewitz is duidelijk geen verplichte kost op de bestuursacademie.

Maar goed, onneembaar als deze horde lijkt, is dit niet de enige die genomen moet worden. Offensieve wapens in de cyberdimensie maken vaak gebruik van zwaktes in de systemen van de tegenstander. En dat leidt tot lastige situaties. Als de tegenstander weet welke zwaktes jij in zijn systemen kent en weet hoe deze te misbruiken, zal hij zijn maatregelen treffen en jou daarmee ontwapenen. Dus als je een cyberwapen gebruikt of het bestaan ervan uitlekt, weet de tegenstander ervan en ben je ontwapend.

Als de inzet van een wapen het onbruikbaar maakt, dan moet je nauwkeurig het beste moment van inzet kiezen. Bij iedere situatie moet je je afvragen of het doel het waard is jezelf te ontwapenen. De kans is dus groot dat je het wapen niet op het juiste moment tegen het juiste doel inzet. De waarde van je arsenaal is dus heel moeilijk voorspelbaar.

Dit is erg. Heel erg. Onder specialisten is dit punt al uitvoerig besproken. Maar dit is nog niet het ergste.

Dat komt zo: Je moet je wapens geheim houden. Ze zullen wellicht het grootste geheim zijn dat een cyberleger hebt. De geheimhouding zal dus zeer strikt zijn. Als je je offensieve wapens geheim wilt houden, zul je je collega's aan de defensieve kant er dus niet van op de hoogte stellen. En de leverancier ervan al helemaal niet. Immers, als jij de gaten dicht, kan de tegenpartij er maar zo lucht van krijgen. Als de leverancier de gaten dicht, is je tegenstander ook geholpen. Om je tegenstander te kunnen treffen zul je jezelf bewust kwetsbaar houden. Er zal in de toekomst meer gezocht worden naar gaten in systemen en er zullen dus meer gaten gevonden worden, en er zullen meer redenen zijn om ze open te laten. Daar worden we uiteindelijk allemaal onveiliger van.

Dat leidt tot een volgend interessant punt: het escalatiemechanisme. Omdat je nooit precies kunt voorspellen wat een cyberwapen precies voor resultaat zal opleveren zul je goed bekijken wát je

er precies mee aanvalt. Ga je voor de maximale schade omdat je wellicht maar één kans krijgt, of hou je je in? De kans is groot dat je een aanval te groot maakt omdat je wegwerpwapens gebruikt en daarna zwakker bent. De tegenstander heeft hetzelfde probleem. Cyberconflicten zullen dus vanzelf escaleren. Dat is heel slecht nieuws.

En als je dan uiteindelijk toch je wapen inzet, dan kopieert je tegenstander het snel of laat zien dat hij het al lang had maar net zo heeft afgewacht als jij. Je collega's die de aanval van de tegenstander moeten opvangen, kunnen wellicht een voorsprong hebben door met je te praten, maar ze weten waarschijnlijk niet eens dat je bestaat. En dat is aan de andere kant net zo. Het klassieke Need to Know leidt dus tot maximale schade.

Nog lastiger is dat er op internet meer dan twee partijen zijn. Als jij een wapen gebruikt of lekt, kan het zijn dat de tegenstander het niet door heeft, maar één of andere slimme crimineel of een ander land wel, dat vervolgens elders in de aanval gaat. Door cyberwapens te hebben kun je onbedoeld anderen bewapenen, terwijl je jezelf bewust kwetsbaar houdt.

Wat het wapenarsenaal zal bevatten en hoe doelmatig het zal zijn is dus nog lang geen uitgemaakte zaak.

De Organisatie
De grote vraag is altijd bij een nieuwe krijgsmachttaak: welk bestaand onderdeel krijgt de buit? Valt cyber onder de landmacht, de marine of hoort het toch bij de luchtmacht? De historische voorbeelden voorspellen weinig goeds - ieder voor zich is ook bij Defensie het motto. Nederland heeft een luchtmacht sinds 1953, na 40 jaar militaire luchtvaart. Tot die tijd werd er weliswaar gevlogen en waar nodig de vijand bestreden, maar over doelmatigheid en effectiviteit valt wel het een en ander minder positiefs te melden. Voor een cyberleger is er ook geen evidente kandidaat, omdat het zo nieuw is. De IT club van Defensie is overigens geen kandidaat, omdat het een dom uitvoeringsbedrijf moet zijn. Bovendien werken daar vooral heel veel burgers waarop bezuinigd moet worden en bovendien is het geen krijgsmacht. De strijd is dus voorlopig niet beslecht.

Deze grote vraag overschaduwt de vraag hoe het cyberbedrijf er uit moet zien. Dit zal – mits niet de kop ingedrukt - hetzelfde effect hebben op ons militair vermogen in de lucht tussen 1913 en 1953, als op ons cyberapparaat in de komende jaren. Je zou verwachten dat tenminste onze luchtmacht voldoende historisch besef heeft om niet uit alle macht aan het cyberdingetje te trekken bij Minister Hillen. Maar in tijd van nood, en dat is onder de huidige bezuinigingen zeker aan orde, verdwijnt historisch besef echter als sneeuw voor de zon en we kunnen in de burelen op en rond het Ministerie van Defensie nog wel het nodige getouwtrek tegemoet zien. Nu ja, wij zullen niets zien - Defensie staat immers niet bekend om haar openheid - maar de militair historicus van de 22e eeuw zal z'n lol op kunnen.

Voorlopig zullen we niet de juiste organisatie hebben.

De Vijand
De lastigste vraag van allemaal hebben we nu nog niet gehad, maar dit is zeker een heel wezenlijke bij defensie-onderwerpen; de vijand. Het maakt namelijk nogal wat uit of je rekening houdt met een oorlog tegen je buurlanden of tegen een niet nader benoemd Verweggistan.

In het eerste geval weet je goed waar je aan toe bent, en heb je behoorlijk veel troepen en redelijk weinig logistiek. Zoals het tot 1989 was, dus. In het tweede geval heb je veel onzekerheid, heel veel logistiek en navenant veel meer overhead, en dus **minder troepen** voor hetzelfde geld. Daarom lijkt ons huidige leger zo vreemd; voor iedere Jan Soldaat zijn er bij de Materieel Organisatie DMO 70 officieren en al jaren kost dit krijgsmachtonderdeel veel meer dan bijvoorbeeld de

landmacht en de marine samen. Toch klopt het: een wereldwijd bereik heb je niet voor een paar stuivers.

Dit is het gevolg van een politieke keuze. Sinds 1991 heeft onze krijgsmacht namelijk als eerste hoofdtaak het wereldwijd een bijdrage leveren aan vrede, veiligheid en stabiliteit. Als er één ding duidelijk is, is dat dit een zeer ambitieuze en in al haar breedte schier onuitvoerbare taak is. Ons land heeft onder deze doctrine sindsdien aan tal van missies deelgenomen, en het eind is alleen in zicht omdat het geld opraakt; zo zullen we Libië niet bombarderen, behoudens dan nog eventuele financiële meevallers voor Rutte. Dit geldt overigens niet alleen bij ons: niemand zal ingrijpen in Syrië. Dat is te duur.

Een wereldwijde ambitie leidt vanzelf tot wat Paul Kennedy zo treffend **Imperial Overstretch** noemt. Je kunt immers niet overal tegelijk zijn. Met de internationale rechtsorde gaat het dan ook steeds slechter: de NATO en de EU zijn aan het desintegreren, de VS staat er financieel net zo voor als Griekenland en het aantal en de ernst van de conflicten neemt toe. De kans dat een oorlog ook ons zal raken wordt dus steeds groter. We moeten dus wat doen.

Het inrichten van cyberwar met een vergelijkbaar wereldwijd bereik is op het eerste gezicht minder moeilijk; de fysieke plaats van een tegenstander is immers slechts bij een beperkt aantal scenario's relevant. Belangrijker is of je in het gehele geweldsspectrum wilt kunnen optreden tegen alle mogelijke tegenstanders, of dat je je doelen kleiner maakt door ze te benoemen. Zeg maar of je in staat wil zijn de Syrische hackers van anti-assad sites te bestrijden, of wil je ook het vermogen hebben om het Amerikaanse satellietnetwerk naar je eigen hand te zetten. Nu is het onder de Atlantische Reflex ondenkbaar dat ons land ooit tegen de VS zal komen te staan , maar dat is meer omdat we er niet over wíllen denken dan dat we er niet over zouden móeten denken. Afgezien van in het hoofd van onze politieke en militaire top is de Twintigste Eeuw namelijk al lang voorbij.

Maar goed, stel dat we een cyberarmy inrichten om binnen NAVO verband samen te werken. Gegeven dat eenieder zijn wapens geheim moet houden, hoe ziet 'samenwerken' er dan uit? Waar moeten we ons dan in specialiseren? Spreken we af met Washington dat wij Sun Solaris doen, Italië Cisco IOS doet, Noorwegen Android en doet de VS dan Windows? Onwaarschijnlijk. Dus iedereen doet van alles een beetje.

Zonder heldere keuzes kunnen er op z'n best breedte-investeringen gedaan worden. Het effect is voorspelbaar en al de dagelijkse realiteit in rest van de krijgsmacht: we hebben van alles een beetje, en dus van het goede te weinig. Hoe fijn vijftig miljoen ook is voor de vaderlandse cyberveiligheid, zonder antwoord op bovengenoemde en nog andere lastige vragen is de kans levensgroot dat het allemaal opgaat aan defensieve middelen die we eigenlijk al lang hebben. En een studiegroep hoeft echt geen vijftig miljoen te kosten, zelfs niet als je ze allemaal inhuurt. Dan kunnen we dat geld veel beter besteden om in ieder geval een paar Leopard 2 tanks te behouden. Voor in Kunduz.

Blauw Online

Vrijdag 19 augustus 2011

Engeland is in Europa het land met het minste privacy voor de burger. Het heeft ook de meeste controlemaatregelen, zoals het alomtegenwoordige cameratoezicht. De vriendelijke ongewapende bobby is niet meer dan een zorgvuldig gecultiveerde mythe. Midsomer Murders beschrijft de Idylle van een verloren gegaan landelijk paradijs – de dagelijkse realiteit is juist snoeihard, zeker in de grote steden. Engeland strijdt vooral tegen 'vandalen' en hooligans, de onderklasse van de traditionele klassenmaatschappij die Engeland nog steeds is. Het hard aanpakken van die onderklasse is overigens ook een eeuwenoude traditie. Met als gevolg dat deze **omvangrijke klasse** het wettelijk gezag alleen kent als een repressieve en intimiderende instelling. Zij eist nu de aandacht op, met de omvangrijkste zomerrellen ooit. Een verdere uitbreiding van de toch al zeer strenge Britse regels ligt in het verschiet.

De Britse overheid noemt het tuig **yobs**, vergelijkbaar met ons begrip hangjongere, relschoppers, bendeleden, criminelen, van alles. Maar niet: een politieke beweging. Iemand die een tv uit een winkel steelt is immers gewoon een dief, een 'common criminal'.

Er bestaat echter wel een politieke laag onder de rellen. Wat we zien is een opstand van de stedelijke onderklasse, in de financiële hoofdstad van de wereld waar het flitskapitaal en de bankiersbonussen letterlijk zichtbaar zijn in het straatbeeld. Arm zijn is erg, arm zijn waar velen uitbundig en uitdagend rijk zijn, is heel veel erger. Tel daarbij op dat die Britse bovenlaag de laatste maanden zeer slecht in het nieuws kwam. Met de ophef rond Murdoch die de politiek bepaalde en de politie betaalde. Met nog doorstijgende bonussen voor de financiële elite. Met een overheid die op grote schaal en zeer openlijk intiem is met het grote geld. Met een vast patroon van **excessief politiegeweld** dat met de mantel der liefde bedekt word. Voor onaangepast tuig is er niets anders dan de knoet, voor het aangepaste tuig van de News of the World en de banken is blijkbaar een vermanend vingertje genoeg.

De conclusie van de Britse overheid dat het 'gewoon' straattuig is dat loopt te rellen, zonder enige politieke achtergrond, is gebaseerd op het gegeven dat er geen eisen geformuleerd zouden zijn. Deze conclusie is hier te lande voetstoots overgenomen. De rellen begonnen met een protest tegen het **structurele excessieve politiegeweld**. Dat is blijkbaar geen acceptabele politieke eis, dus als je dat eist ben je een gewone boef. De 'common criminals' zullen dan ook primair justitieel worden aangepakt. Zonder handschoenen. Dirty Harry, in de vorm van de gewezen New Yorkse politiebaas Bill Bratton, is al ingevlogen.

Het gaat niet helpen.

Zo gaat het in Engeland al jaren: zonder handschoenen. Zero tolerance is default. De onderklasse krijgt de overheid op zijn dak en achter de voordeur. Terwijl de huidige geweldsexplosie juist overduidelijk aantoont dat deze keiharde aanpak faalt. Maar de logische koers is kennelijk om dan maar nog harder te gaan: dreigen met het leger en met rubberen kogels. Dat is wat er nu **gebeurt**. En als de rubberen kogels niet helpen, dan volgen gewone kogels, zoals in Noord-Ierland. En dan? Dan zal,

net als daar, de bevolking uiteindelijk terugschieten.

Dat met scherp schieten zal de politie overigens moeten doen. Het overgrote deel van het voetvolk van het Britse leger komt uit dezelfde sociale klasse als de relschoppers. Sterker nog, veel Britse militairen zijn ooit voor de keuze gesteld: dienst of jeugdgevangenis. De inzet van hen tegen de eigen bevolking is dus niet erg slim. Dat is het nooit, zoals ook Assad en Khadaffi door massale desertie ondervonden, maar in Engeland zelfs verbijsterend dom. Maar geef toe, dreigen met het leger klinkt natuurlijk wel lekker daadkrachtig.

De Engelse geschiedenis levert zelf het overtuigende bewijs dat zero tolerance geen oplossing is. Engeland had vroeger de zwaarste straffen ter wereld, van honderd zweepslagen voor roken via levenslange verbanning naar een strafkolonie voor Ieren en broodstelers tot de doodstraf voor zowat alles wat erger was. Dit superstrenge regime heeft nooit geholpen. Er is niet minder om gestroopt, er werd niet minder gerookt en Ierland werd toch onafhankelijk. Sterker nog, Groot-Brittannië is van oudsher één van de meest criminele landen van Europa, met een grote onderklasse die geen ander leven kent dan de misdaad. Deze groep staat volledig buiten de maatschappelijke orde en de wet. Deze outlaws bestaan al eeuwen – hun geschiedenis gaat zelfs terug tot aan Robin Hood in de twaalfde eeuw.

Maar nu. Wat kan de Britse overheid anders doen dan hard harder hardst optreden? Ik zeg: afkopen dat schorriemorrie. Geef ze net genoeg geld dat ze niet de boel afbreken. Geef ze een jeugdhonk zodat ze niet alleen maar rondhangen. Afkopen is goedkoper dan alle waardevolle spullen voorzien van bewakers, camera's en wat dies meer zij. En het is vooral veel veiliger, zo zonder rondvliegende stenen en molotovcocktails.

Dat je op deze manier mensen beloont voor asociaal gedrag is moreel bezien wellicht verwerpelijk, maar het is de enige methode die werkt. En alle andere methoden hebben bewezen niet te werken.

Maar premier Cameron wil straffen, geen werkende oplossing. De politiek wil optreden, niet oplossen.

Net als bij de opstanden in de Arabische wereld speelt ook in Londen de moderne technologie een significante rol. De beknotting van de internetvrijheid in Egypte leidde tot **verontwaardiging** van Europese leiders en de VN betitelde Internettoegang als mensenrecht. Nu stelt de Britse regering voor om een avondklok in te stellen op de BlackBerry Messenger service en ook andere sociale media te beperken, omdat de relschoppers **deze gebruiken**. Dit leverde instemmende reacties van onze leiders op, terwijl Cameron precies hetzelfde doet als Mubarak en Assad. Bedenk dat in de ogen van de Syrische en Libische leiding de opstandelingen ook gewoon **vandalen zijn**. Dus? Zijn sommigen dieren dan toch meer gelijk dan andere dieren?

De firma RIM, de maker van de BlackBerry, heeft inmiddels beloofd de Britse politie te helpen. Ze twitterde onder meer: 'We zullen de overheid zoveel mogelijk helpen.' Hackers hebben daarop een blog van BlackBerry **aangevallen**. De Londense politie meldt extra veel cybercops te zullen **inzetten** om de uitvoerders van deze trivialiteit voor het gerecht te brengen.

Ook zet de Britse politie de relschoppers **online**, onder meer met foto's van Facebook van personen die **online toegeven** mee te doen. Facebook blijkt maar weer een prima plek om boeven te vangen: voor door niemand opgevolgde oproepen tot rellen op Facebook worden straffen van **jaren cel** opgelegd. Daarbij geldt dat de uiting op Internet staat als een verzwarende omstandigheid. Het lijkt er veel op dat de politie online beter controleert dan op straat. Nu ja, met dit weer is een kantoor natuurlijk ook wel zo gerieflijk. Op straat is het maar koud en nat,

nietwaar. Maar het jagen op dit soort 'criminelen' is als een verkeerscontrole op een bospad achterin Siberië: met meer dan **50 miljard webpagina's** is het bereik van iets online per definitie extreem beperkt en weinig belangrijk.

Nu er veroordelingen zijn kunnen we verwachten dat de politieaanwezigheid op Internet blijvend zal groeien. Privacy en mensenrechten zijn kennelijk heel leuk en aardig, maar niet als het om de macht van de eigen staat gaat. Dit signaal is ook in Nederland opgepikt, waar de PvdA-coryfee **Diederik Samson** pleit voor het alvast uitbreiden van de politiebevoegdheden op Internet voor het geval van rellen. Na kritiek in NRC Next **krabbelde** hij weliswaar een klein **beetje terug**, maar Minister Opstelten, toch altijd al een voorstander van meer bevoegdheden voor de politie, zal hier ongetwijfeld wel voor voelen. Dit soort rellen komt immers voor in alle landen, ook bij ons. Dat heb ik als inwoner van Utrecht in ons eigenste Ondiep **van heel dichtbij** mogen zien. En Opstelten, ex-burgemeester van Utrecht, is een man van het grote gebaar, vooral als het niets kost. Meer bevoegdheden zijn gratis, en dat is veel beter dan de politie bijpassende middelen te geven. Voor de opsporing kunnen de agenten hun privécomputer gebruiken, onder de populaire noemer Bring Your Own Device. Als ze dat dan ook nog thuis doen, is Het Nieuwe Werken ook gelijk ingevoerd.

Door de clash over BlackBerry zijn de Britse yobs in de buurt van Anonymous en halfdochters LulzSec en Antisec beland. Het lijkt erop dat deze elkaar rond de aanstaande verdere beperkingen van internetvrijheid al hebben gevonden. Er is meer dat ze bindt: afkeer van de politie en de gevestigde orde en een voorliefde voor technische hebbedingetjes. Bij elkaar een zeer explosieve cocktail. Zo komt het eindbeeld van de film V for Vendetta het door Anonymous gekozen stijlicoon, het opblazen van het Britse parlement, een forse stap dichterbij.

De onderste steen

Maandag 5 september 2011

Het is volop crisis in beveiligingsland. Vorige week bleek dat Diginotar een wildcard certificaat verstrekt heeft voor google.com. Hiermee begluurde de Iraanse overheid haar eigen burgers bij het gebruik van Gmail. Begluren klinkt schokkend en dat is het ook, maar zelfs in de virtuele wereld is Iran voor velen een ver-van-mijn-bedshow. De reacties waren sussend en er werd per ommegaande van staatswege verklaard dat de schade voor de Nederlandse overheid, als grootafnemer van Diginotar, nihil was. Raakt dit alles ook de Nederlandse burger? Jazeker, want "ook de veiligheid van DigiD was niet in gevaar geweest." Maar, zoals blijkbaar de standaardprocedure is bij crises, was hier sprake van wensdenken. De feiten over Diginotar lagen niet op tafel maar werden op voorhand ontkend. En dat terwijl het verband tussen eventuele feiten en kwetsbaarheid van bijvoorbeeld de Nederlandse overheid in de zogenaamd geruststellende verklaring voor iedereen impliciet was toegegeven. "Waar rook is, is vuur, maar er is geen rook, dus is er ook geen vuur." Van uur tot uur komen nog nieuwe feiten op tafel en zeker is, dat de schade voor de Nederlandse overheid en voor bedrijven aanzienlijk is. DigiD is op dit moment niet beschikbaar. Ook bij mijn werkgever moesten we snel een ander certificaat inzetten. Er is inmiddels een hele hoop rook.

Nu is het onderwerp certificaten voor de meeste mensen tamelijk schimmig. Ook onder beveiligingsmensen is PKI traditioneel een weinig bekende materie. Logisch ook, na een forse hype tussen 1997 en 2002 was er geen droog brood meer in te verdienen, dus de meeste beveiligingsspecialisten komen niet veel verder dan wat theorie uit de CISSP-boeken en soms wat ervaringen met certificate hell. Bovendien gaat de meeste literatuur in op de cryptografische

theorie, de asymmetrische cryptografie van PKI, en niet op de I, de infrastructuur. Hoe het echt werkt, weet dus bijna niemand.

Maar niet weten is niet meer acceptabel. Daarom hier een hele korte inleiding op de I van PKI. De infrastructuur is een hiërarchie, vergelijkbaar met een LDAP directory zoals AD. De top van de directory is de root, en de root is de basis van het vertrouwen van alles wat eronder zit. Netzomin als de hele wereld in één directory past, is er één PKI. Om te zorgen dat er tussen de verschillende hiërarchieën gecommuniceerd kan worden, zijn de PKI's onderling verweven, door zogeheten **cross-signing**. Samen vormen deze PKI's een wereldomspannend 'web of trust'.

Diginotar is een van de zogeheten RootCA's. De RootCA garandeert met haar digitale handtekening de echtheid van PKI-certificaten waarmee servers, applicaties en mensen hun echtheid in het digitale domein kunnen bewijzen. Om het leven voor de internettende mens overzichtelijk te maken, worden certificaten van de belangrijkste RootCA's op voorhand geïnstalleerd op de computer, via Windows of via een browser. Anders zouden we als gebruiker continu certificaten moeten beoordelen en zelf installeren. Het vertrouwen dat het web of trust biedt, is dus niet als tussen mensen een bewuste keuze, maar een van buiten opgelegd geheel. Het is verplicht vertrouwen, voor onze eigen bestwil. Wij zijn blijkbaar niet slim genoeg om zelf te bepalen wie we betrouwbaar vinden. En, laten we wel wezen, het doorgronden van de wereld van de PKI's zal inderdaad de meeste mensen echt boven de pet gaan.

De betrouwbaarheid van de RootCA wordt vooral bewaakt door strenge regels en scherpe auditoren. De RootCA staat immers aan de wortel van zo'n beetje iedere beveiliging op internet. Als je gaat telebankieren, dan wordt de echtheid van de server bevestigd door een servercertificaat, wiens betrouwbaarheid door een RootCA wordt gegarandeerd. Het gaat echter veel verder: het feit dat je op de juiste URL uitkomt is afhankelijk van DNS, het vertalen van de domeinnaam naar het echte IP adres van de server. Ook de betrouwbaarheid van DNS wordt op de schouders van PKI gebouwd, primair maar niet alleen via DNSSec. Oftewel, de veiligheid van DNS is rechtstreeks afhankelijk van PKI.

Als je updates of drivers installeert op je computer, zijn deze ook 'digitaal ondertekend'. De 'handtekening' waar je computer naar zoekt, is ook een PKI-certificaat. Als een nep-update voorzien is van de juiste digitale handtekening, dan zal je computer het gewoon installeren. Je telefoon ook. Het roemruchte Stuxnetvirus maakte hier gebruik van. Oftewel: de veiligheid van je computer is rechtstreeks afhankelijk van PKI. Zo zijn er nog meer. Met aanvallen op RootCA's – en Diginotar was niet de eerste – wordt de kern van alle beveiligde zaken op internet bedreigd.

Nu zou je zeggen dat dit alleen voer voor specialisten is. Helaas, dat is het niet meer. Omdat het door de staat en auditoren opgelegde vertrouwen niet werkt. De burger kan niet meer blind vertrouwen, en zal zelf de diepte van PKI en beveiligingstechnologie in moeten of de systemen als DigiD, telebankieren en wat dies meer zij niet meer gebruiken. En, helaas, dat punt ligt al enige jaren achter ons.

Hopelijk maakt bovenstaand een beetje duidelijk hoe belangrijk een goede afhandeling van deze affaire is en hoe ernstig het probleem is – voor iedereen, niet alleen de übergebruikers. De reacties in de sector zijn niet voor niets zo onverbiddelijk. Microsoft spreekt ronduit van een **frauduleus certificaat** en alle browserleveranciers nemen maatregelen tegen alle certificaten van Diginotar door het verwijderen van de RootCA uit de browser of het OS. Dit leidt tot waarschuwingen op het scherm aan iedere gebruiker; DigiD wordt voortaan als onbetrouwbaar aangemerkt en iedere gebruiker zal dat zien. Hier hielpen de vragen van Logius en **GovCert** niets aan.

Diginotar is begin dit jaar **overgenomen** door het Amerikaanse Vasco . Het staat centraal in veel beveiliging om ons heen, met name van rijkswege, in het toch al omstreden DigiD. We zijn met zijn allen dus een hele grote klant. Dat BiZa i**nitieel meldde** dat de beveiliging van DigiD en de PKI-overheidscertificaten door deze affaire niet geraakt is, zal in zekere zin nog steeds kloppen, zelfs na de bevindingen van de forensisch onderzoekers van Fox-IT, maar dat is op de hele affaire maar een detail. Laten we even verder uitzoomen, de dingen van iets meer afstand bekijken. En opnieuw wordt het kernprobleem alleen maar zichtbaarder. Vasco heeft niet alleen DigiNotar gekocht, maar ook **Alfa & Ariss**, de makers van de applicatie onder **DigiD**. Hiermee heeft het Amerikaanse bedrijf een zeer belangrijke positie in de digitale veiligheid in ons land verworven. Deze wordt verlengd door de vertraging in de oplevering van de opvolger van DigiD door een andere leverancier.

Diginotar zit ook als kennisleverancier in het voortraject van de Europese pendant van DigiD, **SSEDIC**. Dit geeft mij wel een heel ongemakkelijk gevoel. Minister Donner doet dan ook het enig juiste door Diginotar aan de dijk te zetten. Nu nog de **vertraging** met DigiD 4.0 oplossen, s'il vous plaît. Het uiteindelijke probleem is dat de overheid onvoldoende kennis en capaciteit heeft, zodanig dat zelfs het onderzoek naar Diginotar gedaan moet worden door een externe partij. Waar zijn de cybercops?

Nu er sprake blijkt van een hack moet de conclusie zijn dat er blijkbaar te veel vertrouwen is gesteld in de strenge procedures, het toeziend oog, en het eigen oplossend vermogen van de leverancier. Het lijkt mij zonneklaar dat er te weinig gedaan is aan beveiliging. Een webserver hacken is nog wel te doen, maar een goed beveiligd netwerk is hele andere koek. Zouden ze wel gekeken hebben in wat de SIEM **liet zien**? Dit is **overduidelijk** een organisatie die niet weet wat een heel goed beveiligd netwerk is. Dat is een kritieke fout.

Helaas is dit niet verbazend: in de hele PKI-wereld ligt de nadruk op de juiste procedure en de toetsing ervan. Dan gaat de aandacht vanzelf minder naar technische middelen die afwijkingen van de procedures uitsluiten dan wel signaleren. Ik ben dan ook heel benieuwd wat het rapport van Fox-IT zal melden.

Een RootCA staat onder een streng audit toezicht conform ETSI 101 456 en dat heeft blijkbaar gefaald. De betrouwbaarheid van de RootCA wordt primair gegarandeerd door de audit; in dit geval **PriceWaterhouseCoopers** en deze firma van faam heeft hier gefaald met haar **goedkeuring** tot 2013. Ik ben benieuwd wat de afdeling communicatie van PWC hierover te melden heeft, op dit moment hebben ze nog geen **bericht**. Dat is fout op fout.

Voor zover nu bekend heeft Vasco dus niet alleen de netwerkbeveiliging niet op orde, maar heeft het bedrijf ook de boel onder de pet willen houden. De eigen veiligheid ging blijkbaar voor op die van haar klanten, inclusief de Nederlandse overheid die pas op de 29e, toen het nieuws al zeker twee dagen **op straat lag**, op de hoogte **werd gesteld**. Diginotar dacht dat ze de problemen in de hand konden houden. Dat is drie keer fout.

Op 19 juli werd de hack ontdekt, die op dat moment zeker al een week aan de gang was. Diginotar veronderstelde zelf de schade te kunnen inschatten en bovendien in stilte te kunnen oplossen, iets wat overduidelijk mislukt is. De schade blijkt elke dag **nog groter** te zijn. We zouden er echter niets van gehoord hebben, als één van de certificaten niet zes weken later door een oplettende gebruiker in Iran **opgemerkt was**. Dit nieuws werd snel opgepikt door de Rijkshackers van Govcert, en pas toen werden de beveiligers van de bedreigde systemen op de hoogte gesteld. Diginotar dacht dat het allemaal wel meeviel. Vier keer fout.

In totaal zijn er enkele **honderden certificaten** door de hackers aangemaakt, naar verluidt. De meeste daarvan waren slechts enkele weken geldig en zouden dus inmiddels ongevaarlijk moeten zijn. Diginotar stelt dan ook dat het maar om enkele **tientallen certificaten** gaat. Die zouden via het **revocation mechanisme** inmiddels ingetrokken zijn. Maar het blijkt dat Diginotar ook een beveiligingsfunctie van PKI niet gebruikte, de zogeheten PathLenConstraint, zodat aanvallers ook nieuwe certificaten kunnen uitgeven **op naam van Diginotar**. Het aantal is dus niet 247, maar in theorie oneindig. Dat blijkt ook, nu er weer meer opduiken. En dat maakt vijf kritieke fouten.

De aanval kwam bovendien niet uit het niets. Sinds 2010 wordt de wereldwijde PKI onder vuur genomen, het meest door het **Zeus 2 botnet**. Collega RootCA Comodo werd bovendien eerder dit jaar slachtoffer van een **soortgelijke aanval**. En Comodo gaf het goede voorbeeld door onmiddellijk publiek te gaan en alle certificaten in te trekken. Diginotar was dus gewaarschuwd en had extra alert moeten zijn. Zes, dus. Het niet leren van het goede voorbeeld van Comodo maakt zeven. Zeven kritieke fouten.

Als klap op de vuurpijl biedt Vasco haar expertise als 'leading supplier' aan om samen met de Nederlandse overheid de problemen op te lossen. **Doorgaande arrogantie**. En dat maakt acht.

Acht dodelijke fouten. En er zullen er meer zijn. Er is meer dan rook: er is een uitslaande brand. En het is geen incidentele brand: de veiligheid van het hele PKI gebeuren is van meet af aan betwijfeld. In 2000 schreef Crypto-goeroe Bruce Schneier een **overzicht** dat nog staat als een huis. De enige reden dat we met z'n allen met PKI doorgingen was het gebrek aan een alternatief. Het is een veenbrand die nu uitslaat.

Inmiddels heeft dit onderwerp het achtuurjournaal gehaald. Ook hebben we voor het digitale domein ongebruikelijk goede **Kamervragen** gezien. Er wordt geroepen om een parlementaire enquête. En terecht. De onderste steen moet namelijk boven. Om veel meer redenen dan de veiligheid van je belastingaangifte en de websites van de Nederlandse overheid:

In het belang van de organisaties, zowel binnen als buiten de overheid die financiële schade hebben opgelopen en deze willen **verhalen**. Dit kan dus óók over gevolgschade gaan. De wetgeving is helaas **een beetje wazig**.

- In het belang van de naam van de IT-sector in het algemeen en IT Security in het bijzonder: we bouwen vrijwel geen enkel systeem zonder PKI. Ik denk dat genoeg beheerders zich niet realiseren dat proxies zelden de CRL's van certificaten uitlezen, en dat een boel organisaties nog een hele tijd kwetsbaar zullen zijn. We blijken als sector niet te kunnen doorgronden wat we inzetten in een kritieke rol. Dat blijkt wel uit de ridicule adviezen die we soms geven, zoals om de veiligheidswaarschuwingen van de browser maar te negeren of dat we bij Mozilla **klagen** over het intrekken van de RootCA.
- In het belang van PKI, het enige wereldomspannende beveiligingsmiddel. Als deze vertrouwenscrisis niet grondig bezworen wordt, herhaling niet wordt uitgesloten en het vertrouwen niet wordt hersteld, dan is de hele interneteconomie in levensgevaar. En we hebben al een economische crisis. Het ergste is dat er geen alternatief is.
- In het belang van de gevestigde naam in de audit: het falen van PWC raakt alle andere klanten van PWC die een PWC-kwaliteitsstempel voeren. En indirect het hele model van security by audit; PWC heeft conform de standaardnormen gewerkt van de NOREA en de **ETSI**.
- In het belang van de veiligheid van ons land en haar inwoners, omdat Vasco's beveiligingsproducten zo centraal staan in zo veel overheidssystemen en het bedrijf getoond heeft verkeerde prioriteiten te stellen.

- In het belang van de geloofwaardigheid van de overheid als kundige beschermer van de burger in het digitale domein. Niet voor wat de burger zelf kiest, maar voor wat de overheid creëert en verplicht stelt in een grootschalig programma. Dat programma heet '**Andere Overheid**' en na meer dan 8 jaar is dit het treurige resultaat.
- In het aanzien van Nederland in de internationale context, omdat het toch al fragiele weefsel van PKI dat wereldwijd dezelfde rol heeft een zware klap oploopt. Zo zijn dankzij het optreden van Diginotar niet alleen de Iraanse dissidenten, maar ook de CIA, MI6, de Mossad en het **Tor project** in gevaar gebracht. En als overtreffende trap, met het nepcertificaat voor Microsoft Update, is iedere Windowsgebruiker wereldwijd in gevaar.
- In het belang van de internationale veiligheid. Alle sporen wijzen naar Iran, dat de kritieke infrastructuur van Nederland heeft aangevallen, en al eerder andere NAVO-landen aanviel. De andere RootCA die is aangevallen, Comodo, is een Amerikaans bedrijf. De VS stelt dat een dergelijke cyberaanval op kritieke infrastructuur **een casus belli** is, oftewel een oorlogshandeling. Na Libië, Iran?

Voor als je het nog niet begrepen hebt wat de onderste steen is: dit is cyberwar.

De implosie van PKI

Dinsdag 13 september 2011

Dinsdag aanstaande zal patch Tuesday van Microsoft de laatste Diginotar-certificaten opruimen. De Nederlandse overheid is zeker dat haar systemen daar inmiddels klaar voor zijn en dat ze een meltdown afgewend hebben, na een hele drukke week voor de beheerders. We gaan het meemaken.

Het bericht maakt duidelijk dat de systeemcrisis van Diginotar vrijwel voorbij is. De vertrouwenscrisis echter, die woekert voort. En terecht, want er is veel meer aan de hand.

Voor de meeste mensen is de PKI-crisis net zoiets als wat ooit de Y2K-crisis was: iets ongrijpbaars met computers en het is allemaal heel gevaarlijk. Deze vertrouwenscrisis gaat heel diep. En niet zo verwonderlijk, gegeven de voorgeschiedenis; eerder zouden de OV-chipkaart en het EPD ook heel veilig zijn en bleken dat uiteindelijk toch niet. Veel mensen stellen de overheid per definitie gelijk aan mislukte ICT. Dat is dan wel weer heel kort door de bocht. We zien nu dat de overheid onderhand beter wordt in dit soort situaties; Donner heeft het keurig gedaan, toen de crisis eenmaal de aandacht van de top in Den Haag had.

Helemaal onder controle is het probleem met de 'comodohacker' voorlopig nog niet. Zaterdagochtend **meldde Globalsign** dat er daadwerkelijk één van haar systemen gekraakt is. Maar, luidt het persbericht, het gaat alleen om de webserver, de PKI-servers in het netwerk zouden niet getroffen zijn. Nu ja, we zullen zien. Hoewel de zaak onderzocht is door specialisten moeten we niet vergeten dat zelfs FOX-IT niet onfeilbaar is. Daarbij; met drie succesvolle hacks (Comodo, StartSSL en Diginotar) en mogelijk een vierde in vier maanden tijd, is het patroon gevestigd en de aanvaller niet gegrepen. Er komen er vast nog meer.

De huidige vertrouwenscrisis zal overigens nog veel dieper gaan. Niet omdat burgers nog niet gerustgesteld zijn, maar omdat de IT-sector zelf de schade begint te ontdekken. En dat sijpelt vanzelf door: met een paar honderdduizend IT-ers kent iedere burger er wel een paar. En de burgers zijn erg ontvankelijk voor horrorverhalen over onveilige technologie.

Hoe dat zo? Vanwege Diginotar en Globalsign zijn grote organisaties begonnen met het in kaart brengen van hun afhankelijkheden van certificaten. En wat blijkt: er zit nog veel meer poep op de ventilator. Het dossier PKI bevat nog een paar nare verrassingen. Ten eerste blijkt het zeer lastig om alle certificaten te vinden. Het is uitgesloten dat je de boel veilig kunt houden als je niet weet wat je gebruikt en waar het zit. Ten tweede is het vervangen heel veel werk waar je alleen in echte noodsituaties toestemming voor krijgt. Oftewel: de gewone IT-beheerder voelt wel aan dat wat we nu meemaken een eenmalige exercitie is, terwijl een structurele oplossing geboden is.

Maar de derde bevinding is de belangrijkste: veel beveiligingsfuncties van certificaten worden helemaal niet gebruikt. Wat zeg u? Ja, zij zijn niet in gebruik.

Ten koste van de beveiliging
In feite is een certificaat een digitale sleutel, die door een slot – een samenwerking tussen de server, de client en de PKI-infrastructuur – op echtheid gecontroleerd wordt. En waar lopen de controleurs nu tegenaan?

De controles die 'het slot' kan doen, staan vaak uit. Zo zie je dat sleutels die al lang verlopen zijn of ingetrokken zijn, nog steeds werken. De voorgespiegelde meltdown van overheidssystemen die

nu voorkomen zou zijn, lijkt met dit in gedachten dan ook wat overtrokken. De verklaring van waarom de controles uit staan is simpel, omdat het intrekmechanisme, CRL of OCSP, niet werkt of botweg uitgeschakeld is.

De verklaring voor het niet werken is eenvoudig: de machine moet zelf een verbinding met internet kunnen opbouwen. Bij webservers is dat vanzelf geregeld, maar bij Server Oriented Architectures (SOA's) en infrastructurele voorzieningen als proxies, federatieservers en loadbalancers wil je helemaal niet dat de machines naar 'buiten' kunnen. Het PKI-mechanisme voorziet hier niet in; het huidige PKI is voor dit soort systemen feitelijk ongeschikt. Toen PKI nieuw was, bestonden load balancers, proxies en SOA's nog niet, maar nu heeft iedere organisatie wel wat van die spullen in huis.

De verklaring voor het uitschakelen ligt in het verlengde van het voorgaande. Als een PKI-implementatie de controles van echtheid daadwerkelijk uitvoert, dan zal het systeem niet werken. Daarom worden de beveiligingsfuncties uitgeschakeld, anders werkt het systeem niet. Dat de beveiliging dan ook niet werkt, is veel mensen niet duidelijk of is onder tijdsdruk genegeerd. Het werkt, en daar gaat het om. Alleen, ten koste van de beveiliging.

Dat het PKI-echtheidsmechanisme niet bruikbaar is, wordt onderstreept door Google en Microsoft die eigen, hard-coded mechanismen gebruiken in plaats van het officiële om certificaten in te trekken. Dat maakt overigens de root-certificaten van Microsoft en Google de belangrijkste digitale bestanden ter wereld; als daar wat mee mis gaat is er geen herstel mogelijk. Zowaar geen fijn idee.

Er zijn nog meer toepassingen met PKI die op voorhand niet voorzien zijn, of niet voldoende doorzien. Daarbij gaat het vooral om ingebedde certificaten. Zo zijn er in smartcards en allerlei andere hardware devices certificaten en de bijbehorende algoritmes ingebouwd. Nu kunnen de certificaten in veel gevallen wel vervangen worden, met heel veel moeite, maar de toepassing eromheen (zoals in de chip van de smartcard) is vaak hardcoded. Dan zit er niets anders op dan alle kaarten te vervangen. Je begrijpt dat dat niet snel zal gebeuren – vergelijk maar met de gekraakte crypto in de OV-chipkaart. Hebben we al nieuwe? Nee, natuurlijk niet, dat is een hele grote operatie.

Als laatste lopen we nu aan tegen een massale inzet van self-signed certificaten. In een aantal gevallen is dat op zichzelf prima te rechtvaardigen – mits het beheer geregeld is, maar bij de meeste organisaties is dit een hele nare verrassing. Het beheer is namelijk niet geregeld en de chaos is compleet.

Zelfregulering
De wereld van PKI is opgebouwd uit enkele honderden organisaties die in meer of mindere mate onder toezichthouders vallen. In ons land valt het toezicht blijkbaar toe aan de OPTA, die dat weer gedelegeerd heeft aan de markt. Omdat het toezicht per land anders is en PKI internationaal, is het PKI-bouwwerk vooral afhankelijk van zelfregulering door de verschillende deelnemende commerciële ondernemingen. De gedachte onder deze zelfregulering is dat de RootCA's wel gek zouden zijn als ze hun zakies lieten versloffen, omdat ze anders hun klanten zouden verliezen. Dat dit geen werkende garantie is, is nu door Diginotar overduidelijk aangetoond; sommige RootCA's zijn gek. Het was ook een onjuiste aanname: een falende RootCA wordt niet gecorrigeerd door haar eigen klanten, want die zien het probleem in de praktijk niet. En de falende CA wordt niet gecorrigeerd door de concurrentie, want, eh, dat is de concurrentie. In het Diginotar-geval is de falende CA gecorrigeerd door de grote browserbouwers en die nemen nu het **voortouw**, maar de bron van het falen blijft.

Backwards compatibility
Cryptografie is per definitie (vanwege de wet van Moore) gevoelig voor veroudering. Bovendien bestaan er geen onfeilbare algoritmes. Bovenal omdat software niet werkt met theoretische algoritmes, maar met feitelijke implementaties. Daarom moeten sleutellengtes en gebruikte technieken met enige regelmaat, maar soms per direct aangepast worden. Dit is vanaf het allereerste begin van PKI een vereiste geweest en staat te lezen in alle leerboeken. Bij de huidige inspectie blijkt dat te kleine sleutels en sleutels die gebruik maken van technologie die al lang in de ban is gedaan, nog steeds in gebruik zijn. En de reden die vermeld wordt is backwards compatibility. Het systeem ondersteunt vanwege backwards compatability ook sleutels die niet meer zouden mogen werken. Oftewel: het werkt maar ten koste van de beveiliging.

Zo zouden CA's onderhand geen intermediate en end-entity certificaten met RSA key size kleiner dan 2048 bits moeten uitgeven. Bovendien zouden CA's met root certificates kleiner dan 2048 bits RSA key zelf moeten stoppen met het uitgeven van intermediate and end-entity certificates van deze roots. De meesten hebben dat wel meegekregen. Maar ernaar gehandeld hebben ze zeker niet allemaal. En wat gebeurt er dan? Inderdaad: helemaal niets.

Daar zijn nog ergere voorbeelden van: eind 2008 is een zeer gedetailleerde en zeer dodelijke aanval op PKI gepubliceerd, die gebruik maakte van collissions in MD5. Het blijkt nu dat er, ruim drie jaar later, nog steeds certificaten met MD5 in gebruik zijn. Als je kijkt welke certificaten op je machine staan, zul je meerdere root certificaten met MD5-RSA tegenkomen , zoals de "Thawte Premium Server CA" uit 1996: deze zouden geen probleem moeten zijn omdat ze uitgegeven zijn voordat MD5 gekraakt is. De gedachte is dat als deze gekraakt zouden zijn, dat dan wel bekend zou zijn geworden. Wellicht is dat zo.

Waar je voor moet oppassen zijn nieuwere certificaten met MD5. Niemand moet die accepteren, bij wijze van zelfreinigend vermogen. Maar dat vermogen ontbreekt ten ene male – want wie inspecteert nu ieder certificaat en weet wat al die waardes betekenen? Bovendien kun je dit als gebruiker helemaal niet: je browser of je besturingssysteem accepteert namens jou.

Ook hebben we een probleem gehad met debian OpenSSL: alle RSA & DSA keypairs die met OpenSSL op debian zijn gemaakt tussen de release van 17 september 2006 en de update van 13 mei 2008 zijn eenvoudig te raden. Zijn de certificaten met deze keypairs allemaal weggegooid? Waarom zouden ze? En voor de gebruiker: hoe kun je zien hoe waarmee en op welk platform een certificaat gemaakt is? Dat kun je niet.

Gelukkig is Mozilla **recent gestopt** met het accepteren van certificaten met MD5, maar andere browsers en zeker de oudere, accepteren ze nog gewoon. Als je vervolgens bedenkt dat de oudste browsers vooral bij de grootste organisaties voorkomen (Internet Explorer 5.5 en 6 komen nog steeds voor bij banken en de overheid) dan zou je je toch zorgen kunnen gaan maken.

Al eerder is vastgesteld dat een ander essentieel mechanisme, de PathLenConstraint, door Diginotar niet gebruikt wordt. Nu we met z'n allen de boel eens goed bekijken, blijkt dat dit mechanisme hoogst zelden gebruikt wordt. Dit mechanisme zou ook de angel uit de MD5-aanval gehaald hebben, net als uit de Diginotar-hack. Maar gebruiken? In 2008 niet en in 2011 natuurlijk evenmin; want het beperkt de RootCA in de commerciële mogelijkheden. Als je de PathLenConstraint op 4 zet, wat een goede waarde zou zijn, kan niet iedere CA zomaar oneindig van alles uitgeven. Dan zouden de klanten duurder uit zijn en de winst van de CA's dus uiteindelijk dalen.

Gegeven het voorgaande is duidelijk dat de sector alleen tandeloos intern toezicht heeft en zelfreinigend vermogen ontbeert om het vertrouwen dat ze opeist, te verdienen.

Extern toezicht
Nu is er niet alleen intern toezicht, maar ook extern. Het toezicht door PWC in opdracht van de OPTA blijkt alleen het management van de organisatie te toetsen en niemand heeft zich daar druk over gemaakt. Een staaltje zinloze bureaucratie zonder weerga.

Nogmaals dan: computerbeveiliging gaat over het beveiligen van computers, dat gaat over techniek en alleen indirect over procedures, processen en protocollen. Mensen die geen kennis hebben van de techniek van beveiliging kunnen geen goede beslissingen nemen over de beveiliging als geheel.

Naast deze feiten is er een aantal hardnekkige geruchten die ook al niet helpen. Zo wordt er openlijk gesteld dat Diginotar gestraft is met de internetdoodstraf, omdat het maar een **kleine CA is**. Maar, zo gaat het verhaal verder, niemand zal het in z'n hoofd halen om één van de grote RootCA's aan te pakken. Simpelweg omdat de schade in dat geval te groot zal zijn. En inderdaad: de belangrijkste RootCA's, zoals Verisign, zijn daadwerkelijk too big to fail. Een scherpe en zeer geloofwaardige observatie. De droom van PKI is afhankelijk van een onbreekbare en onfeilbare top van de hiërarchie. En dat, weten we met de kennis van nu, is onmogelijk.

DigiD is lek sinds 2007

Maandag 26 september 2011

De laatste weken lijken de mensen die de overheid op ICT-gebied gelijkstellen aan een onvermijdelijk drama gelijk te krijgen. Zo zagen wij het drama DigiNotar, het lekken van de miljoenennota en aanhoudende berichten over fraude met DigiD, dit keer bij een paar straten in Rotterdam met aangiftes en andere belastingzaken. Het eind lijkt niet in zicht.

Ik ben eigenlijk een beetje verbaasd. Door de jaren heen heb ik voor verschillende grote overheidsclubs gewerkt, en ik zag daar best goede zaken op beveiligingsgebied. In een paar gevallen zelfs hele goede zaken. Maar het falen lijkt de laatste tijd structureel. Blijkbaar beschikt de overheid over onvoldoende kennis van computerbeveiliging om haar ambities als elektronische overheid waar te kunnen maken.

De overheid laat hierbij veel van haar ICT over aan de markt, en anders worden er vaak blikken externen opengetrokken. En niet alleen voor de technische uitvoering, maar ook voor de aansturing. Als er dus iets mis gaat met de ICT-kennis van de overheid, dan faalt de markt ook. De kennis is blijkbaar ook niet voor goed geld te koop.

Nu valt mij op dat diverse politici dit ICT-falen aangrijpen om de overheid als de categorische oorzaak van het probleem te kenmerken en om vervolgens te pleiten voor minder overheid en meer markt. Dat is het kapen van de discussie. Het leidt haar weg van waar het in de essentie over gaat. De essentie is dat een overheid niet dramatisch mag falen in wat ze doet, omdat de burger niet naar een concurrent kan gaan.

Overigens, als iemand serieus denkt dat de inning der rijksbelastingen geprivatiseerd moet worden, moet hij eens een geschiedenisboek over het **Ancien Regime** openslaan. Tot ver de 18e eeuw inde ‘de markt’ de belastingen, met massale ontduiking tot gevolg, op een schaal waar Griekenland niets bij is, en uiteindelijk **desastreuze** gevolgen voor de overheid.

Maar ik zou het over DigiD hebben. Deze rijksbrede voorziening toont het overheidsdrama met ICT in haar volle omvang. Laten we aan het begin beginnen. BZK is de formele eigenaar van DigiD. Het oorspronkelijke product is gebouwd door **BKWI** en uitgerold door de ICTU. ICTU stuurt het **tegenwoordig** aan. Logius beheert het. Andere organisaties koppelen hun applicaties aan de DigiD-voorzieningen.

DigiD beschermt de achterliggende systemen van heel veel verschillende eigenaren die op applicatieniveau netjes moeten integreren. Het is een omvangrijk schip met een heleboel kapiteins en de wendbaarheid van een mammoettanker. Of, in de terminologie van A-Select, de software onder DigiD, een federatie van beveiliging.

In een federatie is er een gedeeld beveiligingssysteem en zijn de aangesloten applicaties daarvan afhankelijk voor hun veiligheid, mits ze zelf goed koppelen. DigiD is dat gedeelde systeem. In de praktijk is er bij een federatie altijd sprake van leiders en volgers, maar dat is bestuurlijk niet mogelijk. Een op afstand geplaatst uitvoeringsorgaan van een kerndepartement kan immers geen opdrachten geven aan het kerndepartement van een ander ministerie, laat staan aan een gemeente of een verzelfstandigd bestuursorgaan. Dat is vragen om ongelukken.

DigiD is gebouwd op basis van een commercieel product, A-Select van **Alfa Ariss**, een dochter van Vasco. A-Select biedt een generieke aanlogservice voor applicaties die er ‘achter’ opgesteld

staan. De beschermde applicatie krijgt van DigiD door dat iemand correct is aangelogd én wie dat is, zodat de applicatie daar dan de juiste toegangsrechten aan kan koppelen.

Zoals je in NRC Handelsblad hebt kunnen lezen, kon de fraudeur aanloggen met het DigiD van iemand anders dan diegene van wie de gegevens aangepast werden. Dat betekent dat in de applicatie achter DigiD het tweede deel - de koppeling naar de user - ontbreekt. Je moet aanloggen, maar je kunt na het aanloggen naar de spullen van een andere gebruiker. Deze omissie maakt de fraude die het NRC in Rotterdam aantrof technisch mogelijk. Dat is heel ernstig, om het maar voorzichtig uit te drukken.

Gelukkig heeft de Belastingdienst deze mogelijkheid 'afgesloten'. Dossier gesloten?

Nee. Zo gemakkelijk gaat het niet.

Het echte probleem is dat dit misbruik jarenlang mogelijk is geweest. Weet je nog: de belastingdienst adviseerde in het voorjaar van 2007 om de DigiD van de buurman te **gebruiken** als je je eigen DigiD vergeten was en toch op tijd je aangifte de deur uit wilde hebben. Op technisch niveau betekent dit dat de koppeling tussen de user in DigiD en de user in de applicatie erachter op dat moment niet aanwezig was. Hetzelfde gat dus. Als er geen heel merkwaardig toeval in het spel is, bewijst dit dat DigiD in combinatie met de Belastingdienst zeker vier jaar heel erg lek is geweest. En waarschijnlijk al sinds de oplevering van de koppeling. Het advies uit 2007 bewijst tevens dat dit gat vierenhalf jaar geleden al bekend was – sterker nog, de burger werd aangemoedigd van dit beveiligingslek gebruik te maken. Feitelijk was het een oproep tot identiteitsfraude.

De enige conclusie die ik kan trekken is dat gedurende vier jaar het systeem van de Belastingdienst áchter DiGID bewust en categorisch onveilig is geweest. En pas dit jaar was er een handige buurman in **Rotterdam** die het geheel doorzag en omkeerde ten eigen bate, en tegoeden van z'n buren ging creëren en incasseren. De overheid wist niet beter dan de ten onrechte uitgekeerde bedragen op te eisen bij de bestolen Rotterdammers. Terwijl het gat al jaren bekend is, binnen de belastingdienst althans.

Zo'n gat vier jaar open laten. Onvoorstelbaar. Dat is niet een beetje dom. Dat is superdom. Van het verzwijgen van beveiligingsproblemen kun je failliet gaan, zoals DigiNotar nu uit eigen ervaring weet. De klanten lopen immers zo snel mogelijk weg en komen voor je het weet met schadeclaims.

Van de overheid weglopen is in de praktijk wat moeilijker en ertegen procederen bij voorbaat kansloos. En onbetaalbaar. Een overheid kan hooguit moreel failliet gaan.

Terug naar papier is ook uitgesloten. De problemen met DigiD moeten dus hoe dan ook opgelost worden. Er bestaan geen wondermiddeltjes, dus de oplossing moet passen binnen de bestaande mogelijkheden. Laten we eens zien welke dit zijn.

Een nieuw DigiD-systeem? DiGID 4.0 is nabij, en dat is een geheel ander systeem, van een andere leverancier. De belangrijkste vraag is of dit soort problemen dan nog kunnen voorkomen. DiGID 4.0 is weliswaar een moderner **WebSSO** (Web Single Sign On) systeem, maar ook daarbij geldt dat de koppeling met de achterliggende applicatie goed gelegd moet worden. Het antwoord is dus ja, in de nieuwe versie van DigiD kan hetzelfde mis gaan. Overigens is A-Select ook een prima product, maar in onbekwame handen is dat geen garantie. Beveiligingssoftware is nu eenmaal nooit hufterproof.

Strenger toezicht? Zoals het bij kritieke systemen van de overheid voorschrift is, worden ze met enige regelmaat door een auditor bekeken. De bevindingen zijn nooit zodanig geweest dat de systemen aangepast werden. De onderdelen zijn ieder op zich ongetwijfeld bekeken, maar wie heeft de keten bekeken? Is alleen het proces bekeken, zoals bij DigiNotar? Hoe het ook zij: er is niet goed gekeken.

Het idee uit de Tweede Kamer om voortaan ook hackers mee te laten kijken is zo slecht nog niet. Jammer genoeg is dat bij DiGID al lang **gebeurd** en toen was de boel blijkbaar in orde. De koppeling naar de belastingdienst is die keer hoogstwaarschijnlijk niet meegenomen, maar de belastingdienst laat zelf ook regelmatig dergelijke hackertests uitvoeren. Er wordt dus wél zorgvuldig gewerkt.

De waarde van testbevindingen door hackers - in jargon penetratietesters - is in praktijk knap lastig. Pentesten laten niet zien welke gaten er zijn, maar welke gaten de pentester op het moment van testen kon vinden. Iedere pentester zal dus weer andere dingen vinden. Bovendien mag een pentester alleen aangegeven doelen toetsen, en niet zelf op zoek gaan naar achterdeuren, want wie weet welke productiesystemen van andere partijen in de keten gestrekt gaan. De hacker met de witte hoed zal dus überbraaf bezig zijn en de bevindingen navenant. De opdrachtgever zit niet op dit soort verfijnde nuances te wachten, die wil gewoon een verklaring dat alles goed is. En de commerciële bureaus die pentesten uitvoeren, geven toch al zelden de beperkingen van de testbevindingen mee.

Daarom moeten we naar een samenhangend model van toezicht. Een breder model dat meer recht doet aan de technische vervlechting van de systemen in plaats van aan de bestuurlijke versnippering, zoals het huidige controlemodel waarin iedereen het eigen toezicht regelt ‘conform de richtlijnen’. Het geheel van een WebSSO-federatie is immers meer dan de som der delen. Toetsing moet daar rekening mee houden.

Wat écht ontbreekt in het toezicht is een klokkenluidersregeling voor de ICT-ers die met dit soort projecten te maken hebben, zoals ik begin 2009 al **bepleitte**. Dan kunnen de betrokken techneuten hun verhaal kwijt, wat in een normale projectcontext zelden mogelijk is. Deze regeling moet er bovenal voor zorgen dat repercussies uitblijven: boodschappers zijn immers onveranderd impopulair. Het heeft natuurlijk wel een stevig spamfilter nodig.

Een systeembrede aanpak van toezicht verschuift de discussies van het management naar de technische werkelijkheid. Dit maakt het geheel intern beduidend minder politiek gevoelig. Ik denk dat de securitytoppers die voor de overheid werken, al dan niet als inhuur, dan wel goed werk durven te leveren.

Een laatste punt. De minister heeft in dit dossier - wellicht onbewust en onbedoeld - de Kamer **misleid** in zijn poging tijd te rekken. Het gat was immers bekend, hoewel het bij de Belastingdienst zat en niet bij Donners eigen ministerie. Nu zal niemand dit Donner persoonlijk aanrekenen, gegeven zijn zorgvuldig gecultiveerde imago van fossiel op een opoefiets. Zo iemand snapt toch niets van computers? Toch? Je moet het Donner nageven, het is razend knap.

NRC Handelsblad had gezien het maatschappelijk belang van DigiD echter groot gelijk dat ze niet afwachtte en zelf op onderzoek uit ging. We hebben juist in het digitale overheidsdossier al een veel te lange traditie van ontkenning, woordenspelletjes, bagatelliseren en bestuurlijk traineren. Tegen dit gedrag is één **Brenno de Winter** veel te weinig, dus het is goed dat meer journalisten zich in dit dossier begeven. Ik hoop dat deze nieuwe lichting ook de benodigde scherpte heeft, want die is heel hard nodig om door alle leuterkakel heen te prikken.

Leuterkakel, zoals dat Donner na het vervangen van de DigiNotar-certificaten DigiD weer ‘veilig voor gebruik’ noemde. Dat is semantisch vast wel correct; en dat er maar een paar fraudegevallen met DigiD bekend zijn, ook. Er werd immers gefraudeerd ná de DigiD login, niet met DigiD zelf. Meer dan een woordenspelletje is dit echter niet. De systemen die met DigiD beveiligd zouden moeten zijn, zijn dat in minimaal één - zeer belangrijk - geval niet. En wie weet, zijn het er nog meer. Onkunde en onbekwaamheid zijn echter geen acceptabel excuus voor een minister, zoals het staatsrecht stipuleert.

En de burger? Die zit met de brokken, want de burger heeft ten opzichte van de overheid geen contractvrijheid en is veroordeeld tot het gebruik van systemen als DiGID. Ik raad iedere burger aan even na te kijken of de geldstromen van en naar de belastingdienst vanaf 2006 wel kloppen. Doe dan ook de stromen naar andere overheden, en dan niet alleen het geld. Wie weet kun je wel een bouwvergunning aanvragen voor het pand dat je over twee jaar wilt kopen, of wat dan ook dat er nog meer gekoppeld is. Gelukkig zijn dat er minder dan **bedoeld**. Er zouden immers nog meer handige buurmannen kunnen rondlopen, die nog niet betrapt zijn. Of die nu op het idee komen.

Maar wij zijn met z’n allen ook best wel dom: blijkbaar is bij niemand van alle kritische securitymensen in ons land een lichtje gaan branden in 2007 dat DigiD niet op de juiste manier gekoppeld was aan het achterliggende systeem van de belastingdienst. Het lijkt er veel op dat ook buiten de overheid niemand in dit land voldoende kennis van beveiliging heeft. Behalve dan die handige buurman in Rotterdam.

De Ontdekking van PKI

Donderdag 10 november 2011

Deze column is de uitgeschreven key-note speech op de infosecurity beurs 2011.

Ik neem aan dat u het goede nieuws al lang meegekregen heeft. Diginotar is gekraakt. Ja, dat nieuws was inderdaad moeilijk te missen. Hoezo goed nieuws? Nou, voor ons op een Security beurs waar we allemaal onze spullenboel willen verkopen, is dat goed nieuws. Meer aandacht voor beveiliging is meer geld voor ons. We hebben eerst rotzooi verkocht, een puinhoop aangericht en zijn daar goed voor betaald. Nu zullen we betaald worden om het beter te doen.

De vraag waar ik op in wil gaan bij Diginotar is de Waarom vraag. Die is in dit dossier nog niet gesteld. We zijn als echte IT-ers als wilden op het oplossen van het incident gesprongen, om zodra dat gelukt is, zo snel mogelijk weer over te gaan tot de orde van de dag. Niet goed. Laten we dan nu even stilstaan bij het waarom. Waarom is PKI het doel van deze aanval?

PKI is een wereldwijd beveiligingssysteem. Het is het enige wereldwijde beveiligingssysteem en de technologie zit in vrijwel ieder ander systeem ingebakken. Het is een onmisbare schakel in iedere beveiliging. Deze schakel is de afgelopen jaren slecht onderhouden. Zwaktes die aan het licht zijn gekomen, worden zelden gefixed. En er zijn nogal wat zwaktes bekend, sommige al sinds 1995. En sommige zijn erg goed gedocumenteerd.

Zijn er dan geen andere en betere doelen voor een aanvaller? Er zijn wel andere wereldwijde systemen, zoals BGP en DNS, maar die zijn al vaak aangevallen en inmiddels zijn ze heel robuust. Bovendien zitten die niet in allerlei andere systemen. Er is geen vergelijkbaar doelwit.

Om aan te tonen waarom PKI tegenwoordig zo zwak is kan ik natuurlijk alle gaten in PKI gaan uitleggen. Maar dan moet ik eerst uitleggen hoe PKI werkt, in alle varianten, om dan per variant de problemen te benoemen. Ik heb maar 45 minuten, dus dat gaat niet. Bovendien verzuip ik je dan in al de details en onthoud je waarschijnlijk helemaal niets. Daarom doe ik het als geschiedenisles - zodat hoofdlijnen hopelijk beter naar voren komen.

In den beginne, nou ja in 1978, waren er drie heren die met een oplossing kwamen voor het grootste probleem van cryptografie, te weten het op de juiste plek krijgen van de sleutels. Twee van hen - Diffie en Hellman - werden wereldberoemd in de cryptografie en gaven hun naam aan de eerste asymmetrische cryptografie.

We gaan nu niet in op het **klassieke verhaal** van Bob en Alice waarmee asymmetrische cryptografie normaal toegelicht wordt - daar gaat het helemaal niet om. We moeten alleen scherp hebben dat iedere gebruiker een private en een publieke sleutel krijgt. De private is jouw sleutel en de publieke is voor de rest van de wereld. En met deze combinatie kun je door middel van allerlei slimme trucjes veilig communiceren met andere mensen. Diffie, Hellman en Merckle konden het probleem net niet helemaal oplossen. Wat overbleef was de vraag hoe je publieke sleutel bij iemand die je niet kent te krijgen.

In 1988 kwam het antwoord, vanuit de leidende hype van dat moment. Stop de publieke sleutels in een hiërarchie, een directory. Dat zou dan het telefoonboek van het internet worden. Dat was nodig, want er zaten al een paar duizend mensen op en die kenden elkaar niet allemaal. Zo werd de "I" van PKI werkelijkheid en kreeg het de codenaam X509, omdat het onderdeel van X500, de wereldwijde directory werd. Hiermee kon iedere persoon zich identificeren op Internet. Identiteit

was nodig om vertrouwen mogelijk te maken; je moet immers weten wie je voor je hebt, nietwaar?

Bij PKI heb je het over 'trust', vertrouwen. Maar wel over verplicht vertrouwen. Die directory moet je vertrouwen. En die PKI sleutel, die je krijgt, die moet je met je leven bewaken. Anders ben jij de sigaar. Waarom moet dat? Omdat het anders niet werkt. En je hebt daar niets in te willen.

Met de directory kwam de exploitant van de directory prominent in beeld. Deze exploitant staat bovenaan de voedselketen en moet dus door iedereen geaccepteerd worden. Hiervoor kwam de naam Trusted Third Party in zwang. X500 ging uit van het AT&T van voor de splitsing in baby bells in 1984, een monolithisch staatsbedrijf dat gewend was dat alles en iedereen deed wat het bedrijf wilde. Omdat het een telefoonmaatschappij was, noemden ze het geheel een telefoongids. Vandaar de kreet directory.

De praktijk bleek echter weerbarstiger. AT&T werd vanwege onoorbare monopolistische handelingen opgesplitst en niemand anders kon de wereldwijde rol overnemen. Bovendien bleek de X500 directory een technisch gedrocht.

"The X.500 linkage [...] has led to more failed PKI deployments in my experience than any other. For PKI deployment to succeed you have to take X.500 and LDAP deployment out of the critical path".

- Phillip Hallam-Baker, Verisign principal scientist

X509 werd een oplossing voor een probleem zonder eigenaar. In 1993 werd de volgende poging gewaagd om tot één wereldwijde PKI structuur te komen, met PEM (Privacy Enhanced e-Mail). Ook hierbij kreeg ieder individu één PKI certificaat om met andere individuen te kunnen communiceren. PEM introduceerde een drielagenmodel met een strikte hiërarchie. Alleen: niemand durfde het aan om aan de top van de hiërarchie te staan: de top zou dan immers aansprakelijk zijn voor de schade. PEM verdween in een bureaulade, terwijl PKI X509 vanwege PEM inmiddels v2 was geworden.

Vlak daarna deed het World Wide Web zijn intrede. In plaats van enkele tienduizenden kwamen er miljoenen gebruikers. Dat bracht de nodige nieuwe problemen met zich mee, en PKI was als oplossing op zoek naar een probleem de aangewezen kandidaat om het grootste probleem van het opkomende web op te lossen.

Dat grote probleem was DNS - de identiteit van de server. Hoe weet een gebruiker dat ie op de juiste machine uitgekomen is? Van een client side oplossing voor identiteit werd PKI een middel om een server side DNS probleem op te lossen. PKI werd SSL. Zo werd X509v3 geboren. Volgens PKI-goeroe **Peter Gutmann** "an expensive way of doing authenticated DNS lookups with a TTL of one year". Sinds de opsplitsing van AT&T was er geen aangewezen Trusted Third Party meer, maar er waren wel een paar ondernemingen die dit durfden te worden. Maar wel met het expliciet uitsluiten van aansprakelijkheid.

Iedere TTP begon een eigen certificaathiërarchie, en deze werden hier en daar middels cross-signing aan elkaar geknoopt. Zo ontstond een jungle van meerdere directories waarin niemand de baas was en niemand aansprakelijk was. En omdat de ketens aan elkaar geknoopt werden, ontstond een langere keten met meerdere zwakke en deels onzichtbare schakels.

De oplossing van het DNS vraagstuk was verder echter een voltreffer. Om aan de vraag te kunnen voldoen werden TTP's uit de grond gestampt. In de internet bubble werd gesteld dat een goede

PKI randvoorwaardelijk was voor e-Commerce, zodat iedereen wel TTP wilde worden. Voor veel mensen wás beveiliging alleen maar PKI. Overheden investeerden miljarden en in ons land leidde dit tot een merkwaardig stukje wetgeving rond digitale handtekeningen die er ook nu nog niet zijn. Het grote belang dat aan PKI werd toegekend leidde tot veel aandacht: voor mooie auto's, luxe kantoren en interessante optieregelingen. Helaas ging dat wel ten koste van de aandacht voor PKI: het product was eigenlijk ergens anders voor bedoeld en nog niet af. De tekortkomingen werden niet opgelost bij gebrek aan aandacht. Nu ja, de showroom van een BMW-dealer is voor de meeste mensen nu eenmaal veel interessanter dan een stuk code.

Op 10 maart 2000 knapte de internet bubble en begon de lange val. PKI was niet doorgebroken en de internethype leidde tot een ongekende financiële crisis. En PKI viel nog harder dan de rest. De val van PKI eindigde met een harde klap toen in 2003 een topspeler in PKI-land, Baltimore, ooit 7 miljard dollar waard, verdween.

Na 2003 herstelde de ICT zich van de internetbubble. PKI herstelde zich echter niet: het was een besmette term vanwege tal van dramatisch mislukte projecten en iedereen hield zich daar dan ook zo ver mogelijk van. De tekortkomingen werden niet opgelost bij gebrek aan aandacht. We bleven bij X509 versie 3.

Nu werden er in die jaren wel verbeteringen bedacht, deels hele goede. Maar deze werden door vrijwel niemand doorgevoerd. PKI moest vooral goedkoop en dat leidde tot broodjeszaken zoals Diginotar, die nooit genoeg geld kregen om de beveiliging goed te doen of hun producten te voltooien. Hoeveel jaar heeft Diginotar ook al weer winst gemaakt? Precies: goedkoop is duurkoop en onze overheid liep hierbij voorop. Het is dan ook goedkoop om Diginotar alle schuld in de schoenen te schuiven.

In dezelfde periode groeide het gebruik van PKI door tot in de haarvaten van alle nieuwe technologie, omdat de behoefte aan sterke cryptografie nu eenmaal groot was. Smartphones, de Cloud, SOA, smartcards, tablets, iedere vernieuwing leunde op het fundament van PKI. Helaas is dit fundament nog steeds wankel.

Security is intussen een eerzaam beroep geworden, waarin tal van mensen een mooie carrière vonden. Kennis opdoen van hoe de "I" van PKI in feitelijk in elkaar zit, hoorde echter niet in het curriculum. Het bleef een besmet onderwerp. Het adagium is dat we certificaten gebruiken omdat het anders niet werkt. Maar voorbij dat punt komt vrijwel niemand. Zo besteedt het gemiddelde CISSP leerboek meer bladzijden aan exotische algoritmes als Twofish die niemand gebruikt dan aan PKI - en dat zit overal in. Dit gebrek aan aandacht en kennis is een recept voor rampen en de voornaamste reden van de wankele staat van PKI.

We kregen in 2010 een vooraankondiging van wat voor rampen kunnen gebeuren. Stuxnet, een virusaanval op het nucleaire programma van Iran, gebruikte gestolen Authenticode certificaten om een gemanipuleerde driver te installeren op de SCADA systemen. Certificaten die gestolen worden door Botnets zoals ZEUS. Dit had de beveiligingsindustrie wakker moeten schudden. Dat gebeurde niet. We hadden het te druk met de Cloud te beveiligen en andere frivoliteiten waar klanten wel voor wilden betalen.

Dit jaar begon het echt met de comodohacker. Bij een derde hackpoging trof deze naar verluidt Iraanse hacker de Nederlandse TTP Diginotar. Deze organisatie faalde in het crisismanagement en eindigde in een faillissement.

Probleem opgelost?

Verre van.

Het antwoord op de vraag waarom Iran inbrak bij Diginotar maakt duidelijk dat het geen geïsoleerd incident is. De Iraanse overheid brak in om de eigen burgers te kunnen begluren. Om dat te kunnen doen, was een aanval op PKI een logische keuze: de servers van Gmail en Facebook zijn zeker beter beveiligd dan die van de gemiddelde certificatenboer. En een inbraak daar zou zeker opvallen en snel gerepareerd worden.

De wens om de burgers te bespioneren is helemaal niet vreemd; dat willen alle overheden. Dat willen ze dan wel om verschillende redenen - en daar zitten best goede redenen bij. En nu we dankzij de social media zo veel meer kunnen op internet, zal daar ook meer gespioneerd moeten worden. De Nederlandse overheid wil dat om kinderporno te bestrijden, de Britse om relschoppers op te kunnen pakken, de Chinese om de Falun Gong te kunnen bestrijden, de Amerikaanse om filmpiraten te kunnen oppakken en de Iraanse om de oppositie te kunnen onderdrukken. Over de redenen kun je twisten, maar overheden moeten in bepaalde situaties kunnen inbreken op de beveiliging van de communicatie met computers.

Om dat te doen is het echter niet gelijk verdeeld op deze wereld. Als de Nederlandse overheid wil weten wat je op Gmail schrijft, kan zij dat via de samenwerking met de Amerikaanse overheid via de NSA achterhalen. Die optie hebben niet alle landen: een Amerikaanse inlichtingendienst zal een inzageverzoek vanuit Teheran vast niet honoreren. Sinds een jaar is ook de export van systemen om de eigen burgers te kunnen bespioneren aan banden gelegd: dictators kunnen niet meer terecht bij Siemen/Nokia of Bluecoat om commerciële apparatuur te kopen. Er blijven dus maar twee opties over voor de dictators van deze wereld: de oppositie laten winnen dan wel inbreken op de infrastructuur van westerse landen. Met een halve blik op de huidige positie van Moebarak moge duidelijk zijn wat de keuze is: ze zullen inbreken. En dat is dus cyberwar.

Immers: de aanval op Diginotar was het gebruik van geweld tegen de vitale infrastructuur van ons land. Als Diginotar in de VS had gestaan was het een formele casus belli geweest en waren wij via de NAVO meegesleurd in een oorlog. Nu ja, dat had kunnen gebeuren - het eerder gehackte Comodo is immers een Amerikaans bedrijf en een hele grote TTP. Dat de aanval een binnenlands doel diende is niet relevant - dat zie je ook bij andere oorlogen wel eens. Cyberwar blijkt dus in het echt heel anders te zijn dan voorspeld. Nu zijn oorlogen altijd anders dan de specialisten voorspellen, dus dat is niets bijzonders.

De schade die ons land opliep in de aanval op Diginotar was uiteindelijk 'collatoral damage' in een intern conflict van een verre dictatuur, dat zich niets aantrekt van hoe wij de landsgrenzen op internet voor ons zien. Een groot probleem van dit soort aanvallen is de knulligheid ervan en de daardoor grotere schade dan nodig is. Los van de abominabele beveiliging bij Diginotar was hetzelfde resultaat immers te bereiken geweest met één gekocht certificaat van een willekeurige TTP: er zijn er nog genoeg die certificaten uitgeven die misbruikt kunnen worden om zelf weer geldige certificaten te **creëren**. De schade had er niet hoeven zijn, en de kans op ontdekking zou ook kleiner zijn geweest.

Het probleem is dat overheden op het gebied van hacken beginners zijn. Een beetje googlen naar exploiteerbare gaten in SSL was blijkbaar te moeilijk. En dus richten ze schade aan waar die te vermijden is. Met bijna tweehonderd overheden waarvan bijna de helft dictatuur en in overgrote meerderheid Security prutsers, is herhaling van dit debacle dan ook gegarandeerd.

Hieronder zit een merkwaardige paradox. Overheden gaan moeite doen om technologie te breken die ze zelf gebruiken om zich te beveiligen. Hoe het ook zij, het is vast goed voor de Security Sector.

Dit jaar zijn we een nieuwe tijd binnengegaan in informatiebeveiliging. Eerst hadden we alleen de hackers om de eer. Het motto in beveiliging was dat die toch niet tegen te houden waren, en er waren er niet zo veel dus dat was niet zo erg. Beveiliging richtte zich op drive by attacks en technisch onbekwame interne bedreigingen. Meer kon immers niet. Sinds begin deze eeuw zijn daar de cybercriminelen bijgekomen - bij hun gaat het om geld. Maar cybercriminelen doen vooral aan oplichting via het web en richten zich bovenal op particulieren. Voor beveiliging van organisaties is er dus weinig veranderd en het paradigma bleef beveiligen tegen interne aanvallen en drive by: meer is immers niet mogelijk.

Sinds 2010 zijn echter de landen erbij gekomen en gaat het om de macht. Als meer dan beveiligen tegen drive-by en interne bedreigingen nog steeds niet mogelijk is, hebben we een groot probleem. Want terug naar papier en typemachine gaat niet meer. Macht raakt organisaties veel meer, zeker die internationaal opereren. En collatoral damage kan ons allen treffen, weten we sinds Diginotar.

In dit nieuwe paradigma van IT Security moeten we de grote problemen echt aanpakken en niet alleen de sexy stukjes doen; dus inclusief de dossiers waar we jarenlang verre van bleven omdat ze besmet waren - PKI voorop. We moeten beginnen met het achterstallig onderhoud weg te werken. Om dat te doen moeten we eerst de boeken induiken. En die blijken eerst herschreven te moeten worden: de meeste best practices schrijven doodleuk dat je certificaten bij een TTP moet kopen en dat je dan klaar bent. Dat is geen best practice, dat is marketing.

Om kennis op te doen moeten we eerst naar de basis - de waaromvragen. Dan ga ik even vloeken in de PKI kerk. Waarom zou ik communiceren met een bekende via een onbekende? Waarom moest ik als Nederlandse burger veilig communiceren met mijn overheid via wazige derde partijen zoals Diginotar of dan nu via de KPN? Waarom moet ik de KPN vertrouwen? Wil ik dat wel?

Uiteindelijk moet ik de KPN vertrouwen dat omdat anders de browser een foutmelding geeft als ik mijn belastingaangifte moet doen. En dat doet de browser omdat het zo in de boeken staat. PKI is de toevallig gekozen oplossing voor een ander probleem dat toevallig ook hiervoor wordt ingezet. De bouwers van de browsers weten dit het beste. Zo bleek bij de Diginotarcrisis dat Google en Microsoft niet geraakt konden worden door de namaakcertificaten van de comodo-hacker, omdat zij hun eigen certificaten ingebed hebben in hun software. Ze gebruiken de I van PKI niet. Ze weten blijkbaar al jaren dat PKI in de huidige vorm onbruikbaar is.

De essentie van veilige communicatie is vertrouwen. Iedere Nederlandse burger moet blijkbaar de KPN vertrouwen om de wet niet te overtreden. En dat is uiteindelijk geborgd in een verklaring van een accountant. Nou nou. Diginotar had ook een accountantsverklaring. Lehman Brothers, Icesave en Madoff ook.

Vertrouwen is niet iets wat je kunt opleggen of halen als een toelatingsexamen met een auditor als strenge meester. Je kunt het al helemaal niet doorverkopen als een broodje kroket. Daarom is de kerngedachte van de I van PKI intrinsiek verkeerd.

DNSSec met DANE dan - is dat een oplossing?

Niet echt. Immers, in plaats van de PKI TTP wordt dan de DNS leverancier de Trusted Third Party. Dat verschuift het probleem, maar lost het niet op. Zeker omdat we ze er niet voor gaan betalen - zodat ze alleen maar een extra aantrekkelijk aanvalsdoel worden. En bovendien - DNSSec met DANE kun je niet untrusten zoals het huidige PKI. DNSSec is een mooie oplossing van het DNS probleem, maar niet van het vertrouwens- en identiteitsprobleem op Internet.

Maar wat moeten we dan? Is er dan een opvolger in beeld? Nou, er zijn een paar leuke **studies** naar vervanging, maar die pakken maar een deel van het probleem aan. Het uiteindelijke probleem is niet de Trusted Third Party, maar het geheel van vertrouwen en identiteit op internet. Het huidige gedachtegoed in beveiliging geeft echter wel goede aangrijpingspunten voor hoe het dan wel kan. Hoe zou PKI 2.0 eruit zien als het nu nieuw bedacht werd? Laten we er met een Web 2.0 en Identity 2.0 blik naar kijken in plaats van met de ivoren toren Security denkwijze uit 1985. Simpele regels: de gebruiker kiest zelf en is zelf de baas over de eigen identiteit zoals geformuleerd door **Kim Cameron**.

Voor een oplossing tussen bedrijven wijst de Federatieve technologie (WS-FED en SAML) hiertoe de weg: bedrijven bouwen samen een vertrouwensweefsel op. Dat hoeft alleen met bedrijven waar ze zaken mee doen - met de rest van de wereld hebben ze eigenlijk niets te maken. Samen en bewust - en volledig declaratief: iets mag alleen als het expliciet toegestaan is.

Voor consumenten zou een crowd based oplossing voor de hand liggen. Want wie vertrouw je meer: tien bekenden of één onbekende accountant? Identiteiten in sociale media van mensen die je echt kent zijn immers veel betrouwbaarder - probeer maar eens die updates te spoofen. Een koppeling naar Facebook en dergelijke met een Like-mechanisme (maar dan met trust) zou ons een heel eind op weg helpen. Dan vertrouw je niet Facebook maar mensen die je zelf uitkiest die toevallig ook Facebook gebruiken. Je ziet, er zijn best interessante mogelijkheden, maar er zal niet binnen enkele maanden of zelfs jaren een product zijn.

Voorlopig zullen we het dus met het bestaande X509v3 PKI bouwwerk moeten doen. Dat betekent handen uit de mouwen en neuzen in de boeken om het nog een paar jaar zonder al te grote drama's te kunnen gebruiken. Want die cyberwar, die blijft.

Ik Zal *Niet* Handhaven

Vrijdag 25 november 2011

Na alle commotie over Diginotar en het aansluitende lektober is de macht van GovCert uitgebreid: het kan sancties opleggen aan andere instellingen. Daarnaast wordt het versnipperde ICT-landschap in een grootse beweging omgezet in één rijkswerkplek. De overheid herneemt de regie over het ICT-drama.

Hulde. Het zou tijd worden ook. Maar in mijn achterhoofd piept er een irritant stemmetje. Is het probleem dat de overheid elke keer faalt met grote ICT-dossiers zo eenvoudig oplosbaar?

Ik heb er een hard hoofd in. Omdat de gekozen koers ingaat tegen de hele structuur van de huidige overheid en de allesbepalende ideologie. Dat zal ik even toelichten.

Ten eerste: de heersende ideologie stelt dat de overheid kleiner moet en zich moet terugtrekken. De ontwikkelingen op het digitale domein staan hier haaks op. De schaalvergroting van de rijks-ICT is alleen in de verkoopfolder in lijn met een terugtrekkende overheid; grotere organisaties geven in de praktijk meer uit per gebruiker dan kleinere – of ze hebben minder functionaliteit. Wat er uiteindelijk gebeurt, is meer overheidstaken met minder geld. Dat geeft brokken en dus rommel.

Ten tweede: de structuur. De overheid is namelijk geen hiërarchie met de premier aan de top, en daaronder heldere lijnen naar helemaal beneden, de ambtenaar op straat of achter de balie. Het is meer een klassiek Hollands polderlandschap vol eigen miniakkertjes, struikgewas, molentjes en ontelbare sloten, paden en vooral hekken. En zoals het hoort, in een ijzige mist gehuld. Een organisatie die hier dwars doorheen banjert, zoals GovCert nu lijkt te mogen, wordt vermoedelijk door allen als een bedreiging ervaren en uiteindelijk gesaboteerd. Meer brokken, meer rommel.

Nu is de overheid niet altijd zo'n versnipperd geheel geweest. Maar in de jaren 80 is de overheid begonnen met het verpulveren van de hiërarchie en het afstoten van taken. De voornaamste reden was ideologisch: in een lokale variant van de Reaganeske visie dat de overheid het probleem was, moest alles op de schop. De overheid is in deze visie per definitie incompetent en moet zich daarom terugtrekken op de kerntaken. De markt is in deze visie per definitie beter, omdat daar concurrentie als zuiverend instrument optreedt.

De overheid taken laten afstoten omdat ze die niet zou kunnen uitvoeren, is op de keper beschouwd een hoogst merkwaardige gedachtekronkel. Het impliceert dat de overheid faalt omdat ze te veel taken heeft of omdat bepaalde taken niet bij haar passen.

De eerste mogelijke oorzaak - teveel taken - kan inderdaad een oorzaak zijn. Maar dat is eigenlijk geen oorzaak maar een gevolg, anders betekent het dat een organisatie boven een bepaalde

grootte onmogelijk is. Dat houdt in dat een Shell, een Philips of een Apple, allen groter dan de Nederlandse overheid, per definitie niet aan te sturen zouden zijn. Dat is aperte kolder.

De tweede genoemde oorzaak, dat taken die niet bij de overheid passen, vanzelf mislukken, veronderstelt een soort goddelijke voorzienigheid. Zo in de trant van: als een ambtenaar het vuilnis ophaalt of telefoons aansluit, dan mislukt het omdat het een ambtenaar is. Zou diezelfde persoon het na privatisering - of buiten werktijd – dan opeens wel kunnen? Wie dat serieus gelooft is volgens mij niet helemaal wijs. En áls er al taken zijn die mislukken omdat ze niet passen, dan zouden de taken die wel bij de overheid passen, dus wel moeten lukken? Haha. Daar hebben we ook voorbeelden van, allen in het dossier van de Nationale Veiligheid wat immers de bestaansgrond van de overheid is. Hadden we succes in Srebrenica, bij C2000, of in mei 1940? Nou dan.

Taken mislukken omdat je ze verkeerd uitvoert of omdat je ze niet aan kunt. En soms omdat ze onmogelijk zijn en dan had je er niet aan moeten beginnen.

De derde oorzaak is het doorslaan met het concept ‘de manager’. Begin twintigste eeuw bedachten Weber en Taylor de manager, een hoge functionaris met als enige opdracht de werkvloer efficiënter en effectiever te laten werken. De **cijfers** over de overheadlagen zijn veelzeggend: 14 procent in de industrie, 25 procent bij hogescholen en universiteiten, 45 procent bij ministeries. Deze rijksoverhead veeg je niet met een paar pennestreken weg – zelfs niet als je Donner heet en een goddelijke roeping hebt om het land te leiden. En zeker niet als je deze taak neerlegt bij de dames en heren rijksoverhead zelf.

Maar toch - hoe grootschalig en ingrijpend het bovenstaande moge zijn, het probleem kan dus uiteindelijk wel opgelost worden. En gezien de resultaten van de huidige inrichting, is dat hard nodig.

Om een probleem op te lossen moet je eerst de onderliggende oorzaak vinden. Als je een band plakt, moet je niet alleen het gat vinden maar ook de buitenband controleren op glassplinters. In dit geval moet je de film van dertig jaar overheidsbeleid terugdraaien en goed opletten. En patronen zoeken.

De oorzaak van het verval is niet de privatisering – de meeste taken zijn namelijk niet bij commerciële partijen beland. De oorzaak van de huidige chaos is daar echter wel aan gerelateerd. Bij wijze van compromis tussen marktgelovigen en traditionele overheidsdenkers werden taken weggeschoven van de overheid naar een nieuw gecreëerde tussenzone van ‘publiek-private’ instellingen. Vanuit de privatiseringsgedachte was deze verzelfstandiging een acceptabel tussenstation en voor traditionele overheidsdenkers was dit het maximaal acceptabele. Zo ontstond een nieuw middenveld. Dit bleek een zone waar overheids- noch marktprincipes grip op hebben; geen democratisch toezicht noch de beloofde zuiverende werking van markten.

In dit niemandsland heerst alleen de bureaucratie. En nu het daar iedere keer fout blijkt te gaan, krijgt noch politiek noch markt er grip op. Dit is de hoofdoorzaak: de scheiding tussen beleid en handhaving, waarbij handhaving belegd is bij voormalige overheidsorganen zonder tucht van de markt en zonder tucht door de politiek. Beleid is een Haags privilege, uitvoering is ‘op afstand geplaatst’. De overheid heeft haar vermogen tot handhaving uit handen gegeven aan een

niemandszone en kan alleen aansturen door beleid en wetgeving[60]. Allemaal papier. En zoals iedereen weet, is papier geduldig.

Let maar eens op – als de uitvoering van een wet faalt, komt Den Haag met een nieuwe wet. De falende uitvoerder blijft buiten schot. Falen zit per definitie in de handhaving, beleid als zodanig kan helemaal niet falen want het is gewoon een stapel papier en doet zelf niets. Zo hebben we een overheid die niet meer kan handhaven. Toch wrang gezien de Nederlandse wapenspreuk Je Maintiendrai, ik zal handhaven.

Het scheiden van beleid en uitvoeren is een bestuurlijke mode. De ontstane grijze zone wordt aangeduid als "quango", quasi onafhankelijke **overheidsorgaan**, ZBO (Zelfstandig Bestuursorgaan) of RWT (Rechtspersoon met een Wettelijke Taak).

Het scheiden van beleid en uitvoering is ingegeven door de verwachting dat dit leidt tot een efficiëntere, betere beleidsvoering. Politici zouden zich alleen maar met de hoofdlijnen van beleid hoeven bezig te houden en niet langer verzanden in allerlei vervelende uitvoeringsdetails á la Mauro. Uitvoerders zouden gevrijwaard worden van – het primaire proces belemmerende – overheidsbemoeienis. Bovendien zouden verzelfstandigde publieke eenheden een meer bedrijfsmatig beheersregime kunnen gebruiken; het baten-lasten stelsel. Dit geeft hun meer vrijheid om zelf beslissingen te nemen ten aanzien van de bedrijfsvoering, waarvan naar verwachting een stimulerende werking zou uitgaan om efficiënter te werken. En zelf wat geld opzij te zetten voor verstandige bedrijfsvoering. De praktijk is echter dat de veronderstelde impuls er niet is of niet tot de juiste reactie heeft geleid.

Als een streven naar een doelmatiger overheid de echte reden is… Waarom zouden we dan niet evalueren of het doel bereikt wordt? Dat mag wel na dertig jaar; vooralsnog lijkt de overheid er niet slagvaardiger op te zijn geworden.

Ons huidige kabinet pakt het handhavingsprobleem voortvarend aan: de politie wordt rechtstreeks onder de minister gehangen en ook het digitale domein krijgt directe bestuurlijke lijnen. De symptomen worden aangepakt en de rijksoverhead buitenspel gezet.

Dat zal echter niet helpen - want onder water speelt iets anders een forse rol, een probleem dat nog dieper zit en eerst opgelost moet worden. Er zit nog een stukje glas in de buitenband.

De splitsing tussen beleid en handhaving is niet alleen ingegeven door het streven naar efficiëntie, maar ook vanwege problemen rond de ministeriële aansprakelijkheid. Want hoe was het ook al weer? In de theorie en vaak ook in de praktijk werkt het als volgt: een foutje van een ambtenaar en de minister staat op straat. En de politiek moet met plakband en elastiekjes in de weer om een kabinet te redden.

Dat is het echte vuiltje, en dat moest onder de noemer van efficiëntie en kwaliteit weggewerkt worden. In het kort gezegd: de overheid wil wel de beslissingen nemen maar niet de gevolgen dragen. Wel de macht, maar niet de verantwoordelijkheid. Privatisering was het ene geloof, de scheiding tussen bestuur en uitvoering het andere geloof. En deze duivelse cocktail leidde tot een onstuitbare beweging richting de huidige overheid waarin niemand verantwoordelijk is en waar duizenden mensen dagelijks hun handen vol hebben om dat vorm te geven onder de noemer "Het was voor mijn tijd of na mijn tijd, maar zeker niet tijdens mijn tijd".

---

[60] http://www.novatv.nl/page/detail/uitzendingen/5132/Nederland+relatief+hoogste+aantal+beleidsambtenaren

De uitkomst van deze ontwikkelingen is dat de minister niet langer iets te zeggen heeft over die uitvoering, maar de pers die nuance niet wenst te zien en de burger deze niet accepteert. De minister is in de beleving immers nog steeds verantwoordelijk.

De buffer om de politiek te beschermen tegen falende uitvoering werkt niet en bereikt zelfs het tegenovergestelde, zoals te zien bij dossiers als de OV-Chipkaart, waar de politiek genegeerd wordt door de uitvoeringsorganen tot groot verdriet van volk en politiek. De politiek had afgesproken dat de strippenkaart alleen zou verdwijnen als 95% van de burgers vrijwillig overgestapt zou zijn. Maar dit soort beloftes worden door anonieme tussenlagen stilletjes weggemoffeld. Niemand krijgt er nog grip op, of het nu gaat om de uitgaven, zoals in de **zorg** of de bonussen en salarissen van de managers bij de politie, de COA's, onderwijsinstellingen of woningbouwverenigingen. Ondoorzichtig bestuur is het vaste kenmerk van uitvoeringsorganen[61] waar noch de staat noch de markt regeert, het bestuurlijke niemandsland. En de bestuurders van deze organen zijn zich hun macht bewust en negeren steeds vaker openlijk de politiek.

Maar hoe krijgt Den Haag deze geest weer terug in de fles? De realiteit van ongecontroleerde en autonome instellingen groeit immers autonoom door. Een omineus teken is te zien bij het EPD: de politiek stopt de ontwikkelingen en de uitvoeringsorganen gaan op eigen houtje door. Op weg naar het volgende debacle.

Het experiment met publiek-private instellingen heeft evident gefaald maar hebben we een alternatief? Het blijft kiezen tussen een onvolmaakte markt en een falende overheid. Met de huidige koers zal Opstelten verantwoordelijk zijn als een politieagent van de nationale politie in een schietincident een verkeerde afweging maakt en Donner via GovCERT voor een beveiligingsfout in de website van een gemeente. Dat is natuurlijk onzinnig.

Om de regering weer te laten regeren is veel meer nodig dan de wijziging van het beleid. Het gaat om een wijziging in de handhaving. Echter, iets dat over een periode van 30 jaar is ingevoerd is niet in een jaar ongedaan gemaakt. De beslissing om GovCERT over de beveiliging van de overheid in al haar geledingen macht te geven is onder de huidige omstandigheden gedoemd te mislukken.

In feite is de politiek het regeren verleerd. Het is net zo'n beleidsfabriek geworden als de kerndepartementen. Regeren is echter veel meer dan alleen beleid formuleren. Een goede eerste stap zou zijn om de ministeriële verantwoordelijkheid in haar huidige vorm af te schaffen. Het wordt toch vooral gebruikt voor politieke sluipmoorden, en het is een betekenisloos mantra omdat de toepassing ervan veel willekeur heeft. Toen Donner zelf formeel politiek verantwoordelijk was bij de illegale toegang tot de **GPD extranet** door zijn eigen voorlichters en hijzelf het illegaal verkregen materiaal onder ogen zag, heeft niemand hem daarbij op zijn ministeriële verantwoordelijk aangesproken. Onder de huidige regels een omissie van het parlement, maar ook een vingerwijzing dat niemand er veel behoefte aan heeft. En terecht: stel dat Donner gestruikeld was, dan zou de regering toch zijn blijven zitten en zou de coalitie met andere poppetjes hetzelfde beleid uitvoeren, na het verplichte houtje en het onmisbare touwtje. Het kabinet heeft immers een meerderheid.

Het opheffen van de status op afstand van de uitvoeringsorganen en toezichthouders is stap twee. Dit leidt overigens ook tot een zeer significante vermindering van de papieren werkelijkheid en de kosten van de overhead – prettig als je wilt bezuinigen. Dit is een levensgrote stap, zonder welke de positie van GovCERT een tandeloze tijger blijft en één rijks-ICT hooguit een nieuwe

[61] http://www.huubmous.nl/2006/11/09/quango/

akte in het bekende drama zal zijn. De essentie is het inzicht dat de huidige structuur geen oplossing is, maar juist een versterker van ieder probleem. En dat inzicht, dat is er nog even niet. Dus even geduld a.u.b.

De veiligheidsbureaucratie

Vrijdag 16 december 2011

2012 wordt een véél veiliger jaar dan 2011. Dan gaan namelijk het Nederlands Cyber Security Centrum NCSC, de Cyber Security Raad en de nationale cyber strategie van start. Onder het motto Slagkracht door Samenwerking zullen zij gezamenlijk onze digitale dijken bewaken. Vanaf 1 januari hebben wij een samenhangende aanpak van digitale beveiliging waarin alle relevante partijen meedoen. Het is op dit moment dus nog wat vroeg om iets over de resultaten van deze aanpak te zeggen. Toch ga ik dat doen.

Er komen geen resultaten.

Jeetje, Peter. Waarom nu meteen weer zo negatief?

Nou, het is namelijk een onmogelijke opgave. Ik zie vier levensgrote problemen.

Het eerste probleem is de algemene opzet. Het NCSC gaat coördineren tussen overheidsinstellingen en adviseren aan de rest. Dat houdt de digitale dijken niet dicht. Het is veel te vrijblijvend.

Bedrijven en burgers zullen er nog steeds alleen voorstaan. Coördineren en adviseren is niet genoeg. Daarmee krijg je nog geen samenhang tussen alle verdedigingen in ons land. De versnippering blijft. In cybercrime werken de bad guys steeds meer samen en onder steeds meer bitjes zit een Chinese hacker die onze bedrijfsgeheimen wil stelen om onze bedrijven weg te concurreren op de wereldmarkt. Bovendien leidt de sector onder een voortgaand gebrek aan onderlegd personeel. De noodzaak van verdere samenwerking is vrijwel iedereen duidelijk. Maar ja, hoe doe je zo iets?

Met coördineren en adviseren kom je er niet. Want ook probleem nummer 2 dient zich aan: cultuur. ICT Security kent van oudsher een sterke eilandencultuur. Iedere organisatie voor zich, en binnen iedere organisatie zit Security vaak ook op één of meer eilanden. Eilanden die elkaar het licht in de ogen niet gunnen. Er kan er immers maar één de beste zijn, en in Security geldt dat alleen het beste goed genoeg is. Het zien van de noodzaak tot samenwerken op rationeel niveau is niet hetzelfde als het ook emotioneel willen.

Samenwerken betekent autonomie inleveren. Dat willen we niet. Erger nog is dat samenwerken ook het inleveren van aanzien is. Binnen een organisatie de goeroe zijn, dat is nog wel te doen. Maar in een club van zeg honderd bedrijven kan er maar één de beste zijn, en dat is vast iemand anders. Zolang vrijwel iedere beveiliger vooral bezig is te bewijzen dat hij het beter weet dan een ander, zijn we nog helemaal niet toe aan een samenhangende aanpak.

Ten derde zie ik een vermelding dat het NCSC via de Cyber Security Raad werkt met deelname van alle relevante partijen. Wie zijn deze deelnemers[62] en waarom zijn nemen ze deel? En vooral, waarom een heleboel anderen niet?

[62] http://www.rijksoverheid.nl/documenten-en-publicaties/persberichten/2011/06/30/cyber-security-raad-geinstalleerd.html

Hoe het ook zij; de IT bedrijven die er via ICT~Office bij zitten zullen – zoals het een commerciële instelling betaamt - het verkopen van hun diensten laten prevaleren boven het oplossen van het cyber security probleem van Nederland. Natuurlijk zullen zij dit als hetzelfde zien, maar stel je voor dat IBM wél en bijvoorbeeld Microsoft niet in de club zou zitten – zou de overheid dan niet te veel van de één afnemen en te weinig van de ander? En natuurlijk gaan we ook nog kibbelen over Open Source, of het gebrek daaraan.

ICT~Office vertegenwoordigt 550 IT-, telecom-, internet- en officebedrijven[63] in Nederland, dat is maar een klein deel van al die bedrijven. De rest is dus volgens de overheid niet relevant. Nota bene cyberlieveling Fox-IT is geen lid. Dus hoe het NCSC dit ook doet, het is in alle gevallen verkeerd en schaadt het vertrouwen. Immers: als de overheid koopt van mijn concurrent, dan zal ik niet nalaten te benadrukken dat ze er nog steeds geen verstand van hebben. Bij ieder IT Security oplossinkje zal er wel een IT Security leverancier zijn die er zo over denkt en dat ventileert. Dat schaadt het aanzien van het NCSC, nog voordat ze het hebben kunnen opbouwen. Aanzien dat onmisbaar is voor een club die afhankelijk is van vrijwillige ondersteuning vanuit de markt.

Ten vierde en laatste is de rol van de overheid in het geheel nogal problematisch. De overheid voert de regie bij de 'samenhangende aanpak'. Bij bedrijven heerst een zekere minachting voor de overheid, wat in informatiebeveiliging nog versterkt wordt door het verleden. Dat je nu geadviseerd wordt door overheidsdiensten die nog niet al te lang geleden door pure onkunde de antivirus op je mail overbelastten, is niet geloofwaardig. Ook de statuur in de pers door recente zaken rond DigID, OV Chipkaart en andere toestanden helpt niet echt. We zijn dus al helemaal niet toe aan een samenhangende aanpak als dat moet onder de regie van de overheid.

Kortom, zolang de samenwerking vrijblijvend is, wordt het niets en als de overheid gaat dwingen wordt het nog minder.

Maar goed, het gaat toch door.

Oké dan. Bedrijf A gaat deelnemen aan een cybersecurity overleg van onze spiksplinternieuwe Slagkracht Door Samenwerking. Wie gaat ernaartoe? De opperspecialist? Die heeft het erg druk en hij kan bovendien 'niet zo goed communiceren'. En zijn haar is te lang. Ik vermoed dat de manager van de afdeling waar de opperspecialist werkt naar het overleg gaat. Of de manager boven de managers van alle afdelingen waar alle specialisten zitten. Het is natuurlijk een belangrijke samenwerking, met vertegenwoordiging van politie en inlichtingendiensten, dus de baas gaat het liefst zelf. En de baas, dat is vrijwel per definitie iemand die zich bezighoudt met hoofdlijnen en zeker niet met details. Laat Security nu toch eigenlijk gaan over details. En over details, en nog meer details, en nog eindeloos veel meer details. Daar zit de baas dus aan tafel, samen met alle andere bazen die zich bij voorkeur aan de oppervlakte bewegen. En daarna gaan deze bazen ons inhoudelijk advies geven.

Zo'n nieuwe bestuurlijke laag ontwikkelt haar eigen dynamiek. Die laag gaat groeien. Je kunt zeggen wat je wilt, maar je kunt met duizend man even goed adviseren en coördineren als met honderd man. Alleen: als je er duizend hebt, dan ben je belangrijker dan met honderd. Dat is marktwerking bij de overheid. Dus het worden tweeduizend man, minstens.

Tjeempie, Peter, dit is wel een heel zwartgallige visie. Kan het niet meevallen?

---

[63] http://www.ictoffice.nl/index.shtml?ch=ICT&id=9152

In sectoren waar er traditioneel een veiligheidscultuur bestaat, zal het inderdaad wel meevallen. Over de luchtvaart en de petrochemie maak ik me niet al te veel zorgen, omdat veiligheid daar in de genen zit, en alleen vertaald moet worden naar het digitale domein. Maar daarbuiten? Er zijn tal van sectoren die deel uitmaken van onze vitale infrastructuur die een dergelijke cultuur ontberen. Zeer verhelderend is dit al wat oudere stuk[64] over hoe extra bestuurlijke aandacht voor beveiliging uitwerkte in een elektriciteitsbedrijf. Hier heeft "de intensivering van het bureaucratische veiligheidsbeleid vooralsnog niet tot sterk verbeterde veiligheidsprestaties geleid", maar tot "acceptatie van de risico's vanuit het idee dat er 'toch niets aan te doen valt'"… Elektriciteitsbedrijven staan nota bene bovenaan de lijst van vitale infrastructuur.

Misschien is het voor de digitale dijkbewakers nog niet te laat om te leren van een vergelijkbaar dossier, de nieuwe bestuurlijke laag in rampenbestrijding genaamd veiligheidsregio's. De traditionele lokale brandweerkorpsen, grotendeels gedragen door vrijwilligers, werden van boven aangevuld met een bestuurlijke laag van veiligheidsregio's. Met als doel om taken bij de lokale overheden weg te halen, omdat gebleken is dat deze bij grote rampen onvoldoende bestuurlijke slagkracht hebben, zoals bij Enschede en Volendam. De veiligheidsregio's moeten voortaan deze slagkracht leveren. Het tweede doel is kwaliteitsverhoging, en het derde doel kostenbesparing.

Volgens de bestuurders van de veiligheidsregio's loopt de operatie over het algemeen naar wens. Politiek Den Haag geeft zichzelf dan ook uitgebreid schouderklopjes[65] en beschouwt de veiligheidsregio als bewezen oplossing, als Good Practice zo je wilt.

De uitvoerende mensen denken er echter faliekant anders over. Het recente rapport[66] over de veiligheidsregio Limburg-Noord[67] schetst een onthutsend beeld van een in zichzelf gekeerde bureaucratie die in alle bestuurlijke heisa van abstracties en strategieën geen millimeter extra slagkracht bij grote rampen op blijkt te leveren. En door de grotere afstand tot de lokale werkelijkheid, bij kleinere rampen juist minder slagkracht blijkt te leveren. De kamer heeft dit als een incident behandeld en minister Opstelten was daar dankbaar voor.

Maar is het wel een incident? Ook andere publicaties[68] over de veiligheidsregio's en de brandweer ondersteunen[69] het beeld van een autocratische, kissebissende[70] en falende bureaucratie, zoals recent rond de Moerdijkramp[71]. Intussen herkennen de brandweervrijwilligers[72] zich door de schaalvergroting[73] niet meer in hun organisatie en sluiten er steeds vaker kazernes[74] bij gebrek aan personeel. Want dat loopt weg.

---

[64] http://repub.eur.nl/res/pub/12749/MasciniRapport%20Veiligheidscultuur%20bij%20Eneco.pdf
[65] http://www.rijksoverheid.nl/documenten-en-publicaties/toespraken/2011/05/09/bestuurlijke-conferentie-veiligheidsberaad.html
[66] ttps://zoek.officielebekendmakingen.nl/ah-tk-20102011-2219.html
[67] http://www.ll.nl/mmbase/attachments/5034745/Definitieve_Rapportage_doorlichting_van_de_organisatie_Veiligheidsregio_Limburg_Noord.pdf
[68] http://www.haarlemmerliede.nl/fileadmin/HLSW/raad/2011/28_juni_2011/VRK2011.rv_1_.pdf
[69] http://www.brandweervrijwilligers.nl/user_files/file/landelijk/regionalisering/20110526_persbericht_schokkende_resultaten_spenquete.pdf
[70] http://www.binnenlandsbestuur.nl/openbare-orde-en-veiligheid/nieuws/nieuws/vernietigend-rapport-veiligheidsregio-limburg.735560.lynkx
[71] http://www.deltamagazine.nl/overheid-een-ramp-bij-moerdijk
[72] http://www.parlement.com/9353000/1/j4nvgs5kjg27kof_j9vvidrmzlxptz9/vircluc4wjzp/f=/blg124080.pdf
[73] http://www.berenschot.nl/publish/pages/1072/eindrapport_vrijwillig_dienen_en_verdienen.pdf
[74] http://www.alblasserdamsnieuws.nl/wordpress/2011/02/04/brandweerposten-nieuw-lekkerland-en-groot-ammers-verantwoordelijk-voor-streefkerk/

Andere kazernes sluiten vanwege geldgebrek. Er worden namelijk ook bezuinigingen opgelegd aan de blusbrigades. Officieel natuurlijk niet om de hogere kosten voor de overhead te dragen, maar dat is natuurlijk wel zo: het geld moet ergens vandaan komen en de operatie was bedoeld als bezuiniging. De kwaliteitsverhoging blijkt ook al niet te lukken: op steeds meer plaatsen worden de aanrijtijden[75] langer bij gebrek aan vrijwilligers[76]. De oplossing van onze veiligheidsbestuurders is briljant in zijn eenvoud: de burger moet zelf meer geld uitgeven aan preventieve middelen want de brandweer komt wat later! Als het meezit krijgen we een gratis rookmelder[77].

Dit is ernstig. Dit is extreem ernstig. Maar ook waardevol, vanwege de lessen die we hieruit kunnen leren. Worden die geleerd? Opstelten ja, die van die schouderklopjes aan zichzelf is als minister van Veiligheid tevens de dossierhouder van het NCSC. Hij ziet de veiligheidsregio en de regionalisering van de brandweer vast als een best practice voor het cyberdossier. Opstelten houdt wel van schaalvergroting, zoals ook de politie nu ondergaat.

Bedrijven die gaan bijdragen aan de nationale cyberbescherming zullen net als de brandweerlieden een soort vrijwilligers zijn. De nationale coördinatie ervan zal vooral een bestuurlijk karakter krijgen, met een grote kans op bodemloze bureaucratische putten, en bovenal op afhakende deelnemers: na een tijdje passen ze ervoor om nog langer de overheid te helpen met bestuurlijke luchtverplaatsing. Wat kost dat allemaal wel niet, en wat levert het op? Die Good Practices staan toch al lang gratis op internet. De enige die over zullen blijven in de samenwerking zijn bedrijven die de overheid iets willen verkopen.

Slagkracht Door Samenwerking? Het zou me niet verbazen als we in de praktijk minder veiligheid krijgen voor meer geld. Uit de Nationale Strategie[78]: “Alle gebruikers burgers, bedrijven, instellingen en overheden nemen passende maatregelen om hun eigen ICT-systemen en –netwerken te beveiligen en veiligheidsrisico’s voor anderen te voorkomen”. Juist. Uiteindelijk moet je toch alles zelf doen. Misschien blijft er ergens nog een klein gemeentelijk potje over om scharen uit te delen. Daar kunnen we dan onze internetverbinding mee doorknippen. Opdat het veilig worde.

---

[75] http://www.rtvutrecht.nl/nieuws/408253

[76] http://www.rtl.nl/actueel/rtlnieuws/binnenland/components/actueel/rtlnieuws/2007/03_maart/24/binnenland/0324_1830_brandweer_te_laat.xml

[77] http://www.schoonoordweb.nl/index.php?option=com_content&view=article&id=202:aanrijtijd-brandweer-langer-dan-15-minuten&catid=5:nieuws-berichten&Itemid=95

[78] ttp://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking.html

Klein Duimpje in Den Haag

Zondag 15 januari 2012

Kent u dat: heb je in september een reisje geboekt naar een zonovergoten Grieks vakantiehuisje, krijg je in januari nog steeds naast elk internetpagina een advertentie te zien van allerlei andere zonovergoten vakantiehuisjes. Dat mag straks niet meer. Of toch wel. Cookies worden in elk geval verboden, maar dit soort reclames, die zullen blijven.

Dat zit zo. Al bijna een jaar geleden vroeg SP-Kamerlid Sharon Gesthuizen staatssecretaris Fred Teeven van Veiligheid en Justitie of hij nadacht over een uitschrijfmogelijkheid voor gedragsprofilering op internet. De staatssecretaris antwoordde dat dit niet nodig was. Een uitschrijfoptie zou 'onwerkbaar' zijn, omdat gedragsprofilering 'alle landsgrenzen overschrijdt'. Internet is immers niet gebonden aan landsgrenzen, nietwaar. Bovendien is er op dit moment genoeg wettelijke bescherming tegen gedragsprofilering, aldus Teeven.

Gedragsprofilering is populair bij advertentiebedrijven, omdat ze je daarmee advertenties kunnen tonen die toegespitst zijn op je interesses. Traditioneel gebeurt dat met persistent cookies, kleine tekstbestandjes die op je computer geplaatst worden en als een spoor van broodkruimeltjes laten zien wat je zoal bekeken hebt op het web. De nieuwste methode van gedragsprofilering is 'device fingerprinting[79]'. Hierbij krijgen apparaten op basis van specifieke eigenschappen en instellingen, zoals de versie-strings, ingestelde tijdzone, lettertypes en plugins, een unieke id toegewezen. Zo word je geïdentificeerd en kan je interesseprofiel bijgehouden worden. Volgens onderzoek[80] is op deze manier 94,2 procent van alle apparaten uniek te identificeren. De gebruiker is kansloos: er is geen manier bekend om device fingerprinting te omzeilen. Teeven vindt deze techniek echter 'niet onwenselijk', zo lang bedrijven zich aan de wet houden. Gevolgen voor de veiligheid van gebruikers zijn er niet, schrijft hij.

Volgens Gesthuizen is Teeven 'niet helemaal juist geïnformeerd'. "Het ging niet om een uitschrijfmogelijkheid zoals bij het bel-me-nietregister", zegt ze tegen Tweakers[81]. Hoe een opt-out voor device fingerprinting eruit moet zien, weet Gesthuizen echter ook niet. Goed punt.

Maar ze had haar vraag wel nauwkeuriger moeten stellen. Het gaat over device fingerprinting via de browser. Natuurlijk kan een webserver ook een IP stack fingerprint[82] van iedere bezoekende machine maken, door een NMap scan of iets dergelijks. Hiervoor zijn, zoals Teeven stelt, inderdaad stevige regels beschikbaar. Dat is namelijk hacken en dat mag niet.

Nog nauwkeuriger: het gaat over passieve fingerprinting via de browser. Er is ook actieve fingerprinting, daarbij gebruikt het bedrijf een stukje software op de client die de benodigde informatie vergaart. Dit duiden we normaliter aan met Spyware en hoewel de grenzen op detailniveau wazig zijn, is ook dit verboden. Passieve fingerprinting is echter iets anders. Het is het loggen van informatie die de client computer onbedoeld aanbiedt en vervolgens die logs correleren om gedrag te analyseren. En dat is heel veel informatie, zoals je hier[83] kunt zien, en hier[84] uitgelegd krijgt. Er is geen interactie met de gebruiker; een opt-out is dus onmogelijk. Het

---

[79] http://en.wikipedia.org/wiki/Device_fingerprint
[80] https://panopticlick.eff.org/browser-uniqueness.pdf
[81] http://tweakers.net/nieuws/72474/regering-ziet-niets-in-opt-out-optie-voor-gedragsprofilering.html
[82] http://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting
[83] http://browserspy.dk/
[84] http://www.techrepublic.com/blog/security/browserspydk-reveals-more-than-enough-information/3118

enige wat er mogelijk tegen te doen is, is een verbod van de overheid. Maar juist deze manier van fingerprinting is niet verboden.

Op het eerste gezicht heeft Teeven wel ongeveer gelijk. Voor veel scenario's zijn er regels. Maar voor dit scenario niet. De intentie van de vraagsteller, of de regering iets gaat doen aan passieve browser fingerprinting, is daarmee beantwoord. De regering gaat niets doen. Met dit ongeïnformeerde en ongeïnteresseerde antwoord van Teeven eindigde de discussie in de Kamer.

Maar dan, vier maanden later: het cookieverbod[85]. De aanleiding was dat cookies een grote bedreiging van de privacy zouden zijn. Ze werden misbruikt om gebruikers te profileren en gerichte advertenties mee te presenteren. En daar moet de burger tegen beschermd worden, stelde de PVV. En dat leidde uiteindelijk tot een strikte wetgeving: cookies mogen alleen als de gebruiker expliciet toestemming geeft. Dat wordt dus lekker veel klikken op Ja.

Het lullige is dat cookies een minder grote bedreiging voor de privacy vormen dan browser fingerprinting. Cookies staan op je eigen computer, je kan ze zelf verwijderen. Je kan ook zien welke sites er veel gebruik van maken, en besluiten deze te boycotten. Er zijn ook hele handige plugins en ook browsers helpen inmiddels behoorlijk mee. Tegen passieve fingerprinting staat zelfs de meest slimme gebruiker met lege handen.

Het had helemaal niet zo ingewikkeld hoeven zijn. In principe is het enige dat nodig is, een eenduidige uitspraak van het College Bescherming Persoonsgegevens CBP dat browser fingerprints persoonsgegevens zijn, net zoals bijvoorbeeld IP-adressen. Gesthuizen had haar vraag kunnen stellen op de website van het CBP[86], waar hij thuishoort. Dankzij dit parlementair gestuntel ligt er een uitspraak van de verantwoordelijke bewindsman dat bedrijven deze technologie mogen gebruiken, een gegeven dat de rechter niet zomaar kan negeren.

De bedoeling van het cookieverbod was gerichte reclames en verminderen van privacy tegen te gaan. Nu is de meest gangbare techniek daarvoor verboden, maar een andere, veel ingrijpender techniek juist toegestaan. Goed gedaan, Fred.

Zo leidt de onkunde van regering en parlement tot een verbod op de mindere van twee kwaden, de cookies. En wat gebeurt er dan: juist, bedrijven nemen hun toevlucht tot passieve fingerprinting, zodat ze toch gepersonaliseerde advertenties kunnen plaatsen. Mijn browser krijgt geen cookies meer maar de advertenties voor zonovergoten vakantiehuisjes op mijn webpagina's blijven. Maar dan op een manier dat ik er niets aan kan doen. Behalve misschien mijn computer vervangen of opnieuw inrichten. Want passieve fingerprinting is nu, dankzij het gerommel in Den Haag, expliciet toegestaan. Het zou komisch zijn als het niet zo triest was.

[85] http://webwereld.nl/nieuws/107052/cookieverbod-aangenomen--verwarring-blijft.html
[86] http://www.cbpweb.nl/Pages/med_20110701_vraag+privacy+cbp.aspx

De kleine oorlog op het web

Donderdag 2 februari 2012

Anonymous is 2012 begonnen met een grote reeks aanvallen op de gevestigde macht. Dat is zeker geen toeval. 2011 was het jaar waarin de gevestigde macht de aanval doorzette op de vrijplaats die internet tot nu toe is. Feitelijk is Anonymous in de tegenaanval gegaan, de laatste weken gesterkt door de aandacht voor en de voorlopige zege op SOPA. Maar intussen gaat ACTA door en is op 26 januari officieel door de ministers van Landbouw en Visserij van de EU ondertekend. Omdat een ratificatie van het verdrag door de EU dit voorjaar gepland staat, zullen we tot die tijd in Europa het nodige aan acties gaan zien.

Anonymous is een ongrijpbare beweging, met een even ongrijpbare ideologie: als je de lijst met aangevallen doelen[87] bekijkt, is er weliswaar een zeker patroon te zien, maar wat vooral opvalt, is de diversiteit van de doelen. Wellicht worden er aanvallen geclaimd door mensen die helemaal niet bij Anonymus horen. Er verschijnen dan ook al waarschuwende vingers: Anonymous loopt het risico dat de goede naam besmeurd wordt omdat iedereen zich met de naam kan tooien. Dat zou niet mogelijk zijn geweest als Anonymous zich meer naar het normale gebruik zou schikken, met een bestuur, een zegsman of -vrouw en een organisatie die netjes de verantwoordelijkheid opeist, met liefst een helder programma waar je over kunt praten.

Dat is zeker een punt. Het nadeel van zo'n 'gewone' koers zou echter zijn dat de beweging binnen enkele maanden van de aardbodem weggevaagd zou zijn. Zoals WikiLeaks en Assange. Met legale en pseudo-legale middelen is WikiLeaks immers monddood gemaakt en Assange in een verguld kooitje opgesloten, voor onbepaalde tijd in het juridisch vagevuur. Het risico van misbruik van een goede naam acht Anonymous blijkbaar kleiner dan het risico van een keiharde vervolging met alle macht die een staat maar kan opbrengen. En als die machtsmiddelen niet legaal zijn, dan is een gelegenheidswetje zo ingevoerd en dan mag het toch ineens wel. Tja, daar heeft Anonymous ook wel weer een punt.

Het patroon van de aanvallen maakt één ding wél duidelijk: Anonymous richt zich tegen de gevestigde orde. De héle gevestigde orde, van casinokapitalisten, bonusbankiers en overheden tot en met de veiligheidssector, de huidige variant op het militair-industrieel complex. Dat is nogal een ambitieus doel, en een heel machtige tegenstander. Overeenkomsten met de Occupy-beweging zijn zeker geen toeval en de samenwerking is in een aantal gevallen openlijk. De twee organisaties hebben dezelfde tegenstander en dezelfde ongrijpbare aard. Om dezelfde redenen. Hun tegenstander gaat als het moet over lijken. Ook letterlijk.

De onderdrukking van WikiLeaks – waarbij misdragingen van overheden aan het licht kwamen – heeft Anonymous momentum en ongrijpbare vorm gegeven. Waarom is Anonymous ongrijpbaar? Omdat de tegenstander, het establishment, zo veelomvattend en sterk is. Waarom zoveel verzet? Niet noodzakelijk omdat het establishment altijd verkeerde zaken nastreeft, zie de strijd tegen kinderporno of steun voor democratische bewegingen in Syrië bijvoorbeeld. Maar omdat de oude gevestigde orde onder de noemer van law and order de burgers iets af dreigt te nemen dat als volkomen normaal wordt beschouwd, en waar velen hun identiteit aan ontlenen: een vrij en ongecontroleerd Internet. Anonymous is in die zin misschien wel de bevrijdingsbeweging van Internet.

[87] https://paulsparrows.wordpress.com/2011-cyber-attacks-timeline-master-index/

De aanval op de Internetvrijheid speelt zich af over meerdere aanvalsassen. SOPA geeft bepaalde bedrijven ongekende macht over de vrijheid van anderen op Internet. Als dit doorgaat – en de kans is uiteindelijk heel groot – dan hebben we een heel ernstig precedent. En er zijn geen aanwijzingen dat het na ACTA en SOPA ophoudt. Er zijn wel aanwijzingen dat het daarna nog **veel erger** wordt. Lees daarvoor de analyse van Don Eijndhoven over hoe de nieuwe **Cybermonroe doctrine** het Internet reduceert tot de achtertuin van de VS, zoals de originele Monroe doctrine Zuid- en Midden-Amerika tot verboden terrein verklaarde voor alle andere grote mogendheden. Onder deze doctrine geldt dat een ieder die zich daartegen verzet, mag rekenen op inzet van militaire middelen. Het is maar dat je het weet. Of lees wat wannabe presidentskandidaat Newt Gingrich in **petto** heeft. Het is zeker dat het Internet in de toekomst niet meer van de burger en de techneuten is. De vraag is of het van mediabedrijven of van de militairen wordt.

Even voor de volledigheid: onder de **Monroe doctrine**, geformuleerd in 1823, heeft de VS traditionele én vuile oorlogen **ontketend**, samengewerkt met voormalige Nazi's en de terroristen van **Gladio**, dictators in het **zadel geholpen** en democratieën aan **flarden geschoten**. Het is de ultieme illustratie van 'het doel heiligt de middelen'. Daar komt dus nu een cybervariant van. Een ieder zij gewaarschuwd.

Ook even voor de volledigheid: op dit moment overtreedt Anonymous de wet. Dat mag niet. Foei!

Soms wordt iemand van Anonymous opgepakt. Wordt de beweging daardoor zwakker? Integendeel. Wat we zien volgt het traditionele pad van de Guerrilla 'kleine oorlog'. De acties van Anonymous leiden tot repressie. Anonymous heeft al de sympathie van veel burgers, omdat zij het als underdog opneemt tegen de gevestigde orde, een sympathie die verder toeneemt als de repressie door de gevestigde orde de gewone mensen raakt. Dit zal de beweging nieuwe aanhang bezorgen en politieke legitimiteit verlenen. Zo wordt zij sterker, wat vervolgens weer tot een nieuwe botsing en daarmee tot verdere escalatie leidt. Deze spiraal zie je op dit moment rond het optreden tegen Megaupload en The Pirate Bay[88]: dit raakt zoveel gewone burgers dat het zelfs de law-and-orderpartij bij uitstek, de PVV[89], te gortig wordt. Dit conflict escaleert.

De vraag is of je die escalatie moet willen. De uitkomst is immers niet te voorspellen, de weg erheen wel. Een spiraal van onderdrukking en toenemend geweld.

De geschiedenis van de Guerrilla en Counter Insurgency **leert** dat snelle de-escalatie de enige uitweg is: meer repressie leidt immers tot verheviging en verlenging van het conflict. Dit helpt juist de Guerrilla omdat de repressie onschuldigen treft, en die onschuldigen de guerrillero's passief en op termijn zelfs actief zullen gaan ondersteunen.

Guerrilla gedijt het beste in onoverzichtelijk terrein, zoals jungle of berggebieden. Het internet is extreem onoverzichtelijk terrein, en voor de overheid bovendien vrijwel terra incognita. Op Internet weet je niet wie je tegenover je hebt en wat die ander kan en heeft. Een overheid is in deze een gewone internetgebruiker, zij kan aan het feit dat zij een overheid is geen bijzondere positie ontlenen. Maar dat besef heeft ze overduidelijk niet. Dergelijke zelfoverschatting is een dodelijk nadeel.

---

[88] http://www.bbc.co.uk/news/technology-16642369
[89] http://www.nu.nl/internet/2715087/pvv-wil-maatregelen-blokkade-the-pirate-bay.html

Ontbladering was in de grootste van alle guerrillaoorlogen, die in Vietnam, de aangewezen oplossing. Dan kan de tegenstander zich niet meer verstoppen en kan deze met chirurgische precisie opgeruimd worden. Tenminste, zo is de idee. Ontbladering van het internet lijkt dan ook de logische volgende stap. Vertaald naar internettechnologie is dat opheffen van de anonimiteit van de gebruiker en het ontnemen van de zeggenschap over de eigen computer. Beide is al aan de gang.

Voor de anonimiteit op Internet: zoek naar voorstanders van het internetrijbewijs[90] en op de bestrijders van de verhuftering. Van wat je vindt, word je niet vrolijk. Je mag in de toekomst niet anoniem op Internet omdat sommige mensen op Facebook of Twitter net zo openlijk en direct spreken als in de buurtkroeg of in de eigen woonkamer. En soms is dat beledigend en soms is dat bedreigend.

Gaat het daar om? Nee. Bedenk eens hoe moeilijk het is om advertenties te richten op onbekenden. Google, Apple, Facebook en alle andere bedrijven met een vergelijkbaar verdienmodel zijn de grootste bedreiging voor het anonieme Internet zoals we dat hebben leren kennen. Bedenk vervolgens hoeveel gemakkelijker het is om burgers te vervolgen voor digitaal gedrag als je weet wie het zijn? Ja, dat willen 'ze' graag weten, van BREIN tot de digitale politie van Ahmajinedad. De vraag is hoe het internet eruit zal zien na deze digitale dosis Agent Orange[91]. Ik denk een stuk minder interessant dan nu. Overigens heeft de ontbladering in Vietnam niet geholpen, de guerrilla won.

Trusted Computing ontneemt vervolgens de gebruiker de mogelijkheid dingen te doen met de computer die de belangen van anderen zouden kunnen schaden; het einde van MP3 en DivX is in zicht, maar ook van Open Source[92]. Als het aan de gevestigde orde ligt bevat je thin client computer straks alleen een browser en huur je verder alles wat je ermee doet. Een eigen harde schijf wordt op enig moment een verzetsdaad tegen deze gelijkschakeling van de digitale dimensie. Dit alles gebeurt onder de nobele noemer van het uitsluiten van virussen en de strijd tegen cybercriminaliteit. Yeah, right. Microsoft heeft dit Trusted Computing[93] gebeuren een aantal jaren opzettelijk getraineerd om het fat client model veilig te stellen, vast niet voor hogere doelen maar Microsoft wordt allengs minder machtig. Van Apple hoef je dit soort gedrag niet verwachten. De virussen van de toekomst komen uit de appstore. En vast niet gratis.

We zullen nog terugverlangen naar Tim Kuik en zijn schimmig clubje BREIN, de poedel van de entertainmentbazen die als handpop wordt ingezet tegen de bestaande vrijheid op internet, in al hun vertederend amateurisme en bescheiden doelen. Het wordt namelijk nog veel erger.

De vraag is of deze ontkiemende burgeroorlog op het web tijdig gede-escaleerd zal worden. Wie kan dit conflict de-escaleren? Is willen dan ook kunnen? En zal kunnen dan ook doen betekenen?

Anonymous zal het niet willen, dat zou het opgeven van haar streven betekenen. Ze voert juist de **campagne** verder op met nieuwe aanvallen en methodes. Daarbij zal Anonymous zich zeker realiseren dat de tijd in het voordeel van de guerrillastrijder werkt.

Het establishment is zeker geen eenheid met een samenhangende agenda, zoals samenzweringsliefhebbers betogen. Ze kan dus niet snel en beslissend optreden en alle tegenstanders verpletteren. Dus de-escalatie moet een andere vorm vinden en van een deel van

---

[90] http://www.security.nl/article/17386/1/Eugene_Kaspersky_wil_internetrijbewijs_verplichten.html
[91] http://nl.wikipedia.org/wiki/Agent_Orange
[92] http://www.schneier.com/crypto-gram-0208.html#1
[93] http://en.wikipedia.org/wiki/Trusted_Computing

het establishment komen. De politiek? Logische keuze, maar zij heeft de wijsheid niet. Zelfs als ze die wel zou hebben, heeft ze noch de daadkracht noch de prioriteit. Internet blijft groter dan natiestaten en landen werken nooit echt samen. Kijk maar naar de kredietcrisis.

De mediabedrijven hebben de wijsheid om het initiatief tot de-escalatie te nemen zeer zeker niet: ze willen nog steeds de Pianola en de VHS-band verbieden en je auteursrechten laten betalen aan Disney als je Happy Birthday zingt op de verjaardag van je dochter. De militairen hebben een nieuw dingetje in een tijd van bezuinigingen en de digitale dimensie van oorlog is nog zo ongrijpbaar dat ze er erg onrustig van worden. Ook al geen goede mix voor wijsheid. Reken ook niet op de grote IT-bedrijven: die verdedigen hun verdienmodel en hun overleven, niet de vrijheid op het internet. Google verdedigt de advertentieopbrengsten van al die downloadsites.

De veiligheidssector heeft de wijsheid ook zeer zeker niet. Zij is in toenemende mate een doelwit van hacktivisme, zoals Symantec en MacAfee al ondervonden, en heeft juist direct belang bij escalatie van de kleine oorlog op het web. Security marketeers verkleed[94] als specialisten gooien juist met veel goesting olie op het vuur, met onnavolgbare claims gevangen in prachtige hyperbolen, bij voorkeur gelardeerd met Chinese spionnen en de Russische maffia. Angst verkoopt, nietwaar?

Niets tegen te doen, zo te zien. Laten we er dan tenminste maar van meeprofiteren. Werk genoeg in de Security de komende jaren.

[94] http://www.boozallen.com/consulting/transform-technology/cyber-technologies

Tunnelvisie

Maandag 5 maart 2012

Als consumenten zich houden aan de adviezen van banken en hun computer goed beveiligen, kan er namelijk nog steeds van alles gebeuren.

Ik denk wel eens dat we alle belangrijke zaken onderhand wel beveiligd hebben. Dat we alleen nog de nieuwste ontwikkelingen hoeven te volgen. Maar nee. Dat is niet zo. Regelmatig duikt er weer een blinde vlek op in zaken die al jaren meegaan. En dat zijn geen bugs in software, welnee, we missen complete dossiers en cruciale inzichten. Dit gaat samen met een heel verontrustende trend: de tijd tussen het aanbrengen van een substantiële verbetering en het moment van invoering ervan in de praktijk wordt steeds langer. Veel nieuwe dingen worden zelfs pas ingevoerd als ze al achterhaald zijn. Het lijkt erop dat we als beroepsgroep aan een collectief oogkleppensyndroom lijden en de prioriteiten structureel verkeerd leggen.

Wat we zijn geworden is een ultiem conservatieve beroepsgroep die de stroop die de ICT-bureaucratie van nature al is, nog wat dikker maakt. Dat is acceptabel als de resultaten goed zijn. Maar de resultaten zijn niet goed: met grote regelmaat komen ICT Security drama's naar voren. Die stroom neemt niet af maar toe. Er blijken nog tal van lijken in de kast te liggen, ondanks tien jaar van commerciële voorspoed in de beveiliging, dertig jaar **best practices**, over elkaar buitelende structurele aanpakken en methodieken en veertig jaar wetenschappelijk **onderzoek**.

Denk ook niet dat er geen Security mensen bij die drama's betrokken zijn: bij het EPD, de OV-chip, Diginotar, de KPN hack – daar zitten echte professionals, geen amateurs. En toch gaat het Niet Goed. Met Hoofdletters.

Want we zien tal van zaken over het hoofd. Met ons allen. Structureel. En dat beangstigt mij.

Dat had ik laatst heel sterk toen een oud-collega, die nu bij een software vendor werkt, mij attent maakte op het verschijnsel 'Privileged Account Management' PAM. PAM is het beheer van toegang door beheerders, in het bijzonder voor de techneuten van externe leveranciers. Het product van die oud-collega legt alle toetsaanslagen vast van de gevoelige accounts. Mja, dan heb je tenminste iets.

Toch knaagt het gevoel dat er nog meer bij komt kijken, want met het vastleggen van de toetsaanslagen weet je weliswaar wat er allemaal gedaan is, maar nog niet door wie. Bovendien kijk je pas als je weet dat er iets aan de hand is en heel vaak weet je dat niet. Daarbij heb je de hele tijd een root account dat actief is en gebruikt kan worden, ook als er niets aan de hand is. Dat moet je niet willen.

Dus ik ging eens zoeken wat de literatuur te melden heeft op dit punt en of de andere aanbieders in deze niche misschien een beter verhaal hebben. Dat blijkt wel beter maar niet goed te zijn – blijkbaar hebben nog maar weinig mensen aan het PAM-dossier gesnuffeld. Terwijl het toch echt een relevant onderwerp lijkt, zeker nu er massaal geout-, off- en near- shored en –tasked wordt. Blijkbaar hebben de Security-mensen andere prioriteiten: PAM verkoopt dan ook voor geen meter.

Ik kreeg hetzelfde angstige gevoel bij de DNSSec training van de **NGN** door Olaf Kolkman die je **hier** kunt zien. Dat is nogal een andere wereld dan de alledaagse Security-wereld. Twee dagen

over Security waarbij het woord borging is niet gevallen en een proces iets is in een computer … Wat een verademing.

Eindelijk een oplossing voor een levensgroot probleem in de veiligheid van het Internet - het is nu immers nog de vraag of je wel op het adres uitkomt wat je ingetypt hebt. Weet je wel zeker dat je op security.nl zit, en niet op een onbetrouwbare server in Griekenland die je pc volstopt met virussen en je netwerk toevoegt aan een megabotnet? Je weet het niet, en je kunt het nu niet weten. DNSSec lost dat op. Eindelijk. Gaan we DNSSec dus zo snel mogelijk uitrollen met z'n allen? Nee, integendeel. We hebben het immers al zo druk…. Gebruikers vragen niet om DNSSec – **meldt SiDN** - alleen de bewakers van Internet werken er aan. Dus met al die Security mensen die ons land rijk is, is de uitrol van deze cruciale verbetering van het internet en alles wat aan die namespace hangt aanbodgedreven. Geen klant die erom vraagt, terwijl het problemen van de grootste orde oplost. Maar wie weet welk levensgroot probleem DNSSec oplost? Nu nog niet, ja nee, wellicht, waarschijnlijk, want, maar….

Als we het wel weten komt het ultieme argument: anderen doen het ook nog niet en we gaan geen unproven dingen doen. Een nieuwe oplossing zal nooit proven genoeg worden als niemand het gebruikt. Bovendien zijn de problemen zélf absoluut proven technology en erg goed gedocumenteerd. De anonieme jongelui met **witte maskers** hebben ze gelukkig nog niet ontdekt, maar er komt een moment dat zij er massaal gebruik van zullen maken in het hippe hacktivisme. En dan zijn we te laat.

Internet domeinnamen zullen de komende jaren dus nog **gespoofed** kunnen worden, vooral bij **grotere instellingen** die hun eigen zones beheren. Vervelend genoeg als het de website van je bank betreft, maar er zijn doelen met nog veel meer impact. Nu ja, we gaan het meemaken.

Het is niet beperkt tot bovengenoemde dossiers. Het is een terugkerend patroon. Er zijn goede oplossingen en die gebruiken we niet. Zo zijn man-in-the-middle aanvallen op https mogelijk en **gedocumenteerd** door de sessie te onderscheppen vóórdat die overschakelt naar https. Dit breekt het meest toegepaste beveiligingsmiddel volledig. Gelukkig is daar een oplossing voor: **HSTS** – weet iemand wat het is? Veel belangrijker nog – wie gebruikt het? De grote massa niet – hoezo dan, nog even niet, ja nee, want, maar. Toch?

HSTS vraagt natuurlijk wel om browserondersteuning, en niet iedereen heeft dat al, dus dan hoeft het blijkbaar niet uitgerold worden. Zo roept de consumentenbond dat de **banken veilig zijn**, terwijl dit op dit punt Strict Transport Security aantoonbaar **niet het geval** is. HSTS is overigens niet het **enige puntje** van aandacht voor de bankiers, zo worden ook zwakkere cryptografische cijfers als RC4 en MD5 ondersteund dan noodzakelijk. Want dat vraagt ook weer browserondersteuning.

Ik kan dus niet optimaal veilig internetbankieren omdat sommige andere klanten een oudere browser draaien en mijn bank dit blijkbaar geen doorslaggevende zaak vindt. En bij andere banken is het niet beter. Dat de Nederlandse Vereniging van Banken NVB stelt dat er geen reden voor de consument is om zich zorgen te **maken** is een prachtig bewijs voor de semantische strijd die computerbeveiliging in de praktijk is. De uitspraak van Tutert van de NVB dat "internetbankieren [] absoluut veilig"is, klopt alleen in die zin dat banken de schade vergoeden – niet omdat de veiligheid technisch gegarandeerd is. Als hij al weet hoe het precies zit kan hij moeilijk zeggen hoe het precies zit, want dan breekt geheid een mediarel uit. De consumentenbond heeft vast wel goede bedoelingen maar zeker niet de goede kennis. Als consumenten zich houden aan de adviezen van banken en de consumentenbond, en hun computer goed beveiligen, kan er namelijk nog steeds van alles gebeuren. En ondanks gigantische inspanningen van tal van competente computerbeveiligers en bijpassende kosten blijft het

gatenkaas. Kosten die gewoon doorberekend worden, want de financiële positie van de banken, nou dat weten we onderhand wel. Ik moet dus extra betalen voor brakke beveiliging omdat de beveiligers van banken conservatief zijn. En jij betaalt ook.

Ook klagen we massaal over de problemen met PKI. Ik ook. Het punt is echter niet dat de PKI niet klopt, maar dat de kwesties die opgelost zijn en die in updates van de standaarden benoemd zijn, door niemand doorgevoerd worden. Er wordt dus ook nergens met of zelfs maar naar RFC3280 toe gewerkt. Maar we klagen wel over de onveiligheid van PKI. Certificaten kunnen dus de komende jaren nog gewoon **gespoofed** worden. Slotje in de groene balk, verklaringen, adviezen – puur theater.

In 2005 beargumenteerde het Jericho gebeuren overtuigend dat het kokosnootmodel voor IT-beveiliging niet houdbaar meer is. Voor diegenen die dit niet kennen: het kokosnootmodel stelt dat het eigen netwerk hard van buiten is de buitengrenzen zijn sterk beveiligd en binnenin niet zoveel behoefte aan echte beveiliging heeft en dus zwakke of afwezige binnengrenzen heeft. Iedereen beschouwt de kokosnoot als iets uit het verleden. Ja, vroeger, toen waren we naïef.

Nou, dat zijn we nog steeds.

Met Anonymous blijkt dat we nog steeds mentaal in de Kokosnoot zitten. Waarom denken vrijwel alle Security mensen dat Anonymous bedrijven niet raakt, behalve dan wellicht de webservers? Waarschijnlijk omdat Anonymous alleen op internet actief is. Maar, wat is de grens dan - die firewall toch? Ga je schamen en lees voor straf het **Jericho manifest** drie keer.

Uiteindelijk doen we niets aan oncontroleerbare root accounts in ons netwerk, de spoofbaarheid van onze certificaten en de zwaktes van het huidige DNS, want we zitten knus achter onze beschermende firewall. Tuurlijk joh. Bovendien zijn we te druk met processen en beleid, of als we technisch bezig zijn, met GRC in a Box of Security as a Service in elkaar te klikken. De managers vertellen hoe erg het is, is blijkbaar harder nodig dan het minder erg maken. En al die nieuwerwetse dingen staan toch nergens in ons jaarplan en we krijgen er toch geen budget voor.

Denk eens na.

Waarom komen bepaalde dossiers onder de aandacht maar de meesten niet? Zelfs de herrie van grote, sexy hacks dringt uiteindelijk niet door. Weet je een jaar na Comodo en Diginotar wat je organisatie moet doen als je Internet Trust Anchor wegvalt? Heb je ook al getest of dat kan?

Nou dan.

Heb je er een maand na het bekend worden van de VeriSign hack al over **nagedacht**? Dit keer vast wel, maar wie verder?

Wat gaan we doen met dit inzicht? Volgend jaar blijkt ongetwijfeld dat we niets gedaan hebben, omdat andere zaken een hogere prioriteit hadden. Alles moet toch wijken om de iPads van de directie toegang te geven tot het netwerk, nietwaar?

In de praktijk blijkt alleen de herrie van mensen die je met plezier en vakkundig uitleggen welke problemen jij hebt, door te dringen tot de planning. Professionele sales dus. Zo bepaalt Gartner de beveiligingsagenda. En dat klopt niet. Gartner is een trendwatcher die de aanbodzijde van oplossingen uit de commerciële hoek toont, en die volgen we dan op geruime afstand. Die commerciële hoek loopt een paar jaar achter op de Open Source producten, die een paar maanden achterlopen op de aanvallers. De vraagzijde – wij dus – is intussen oorverdovend stil.

Wij wachten af tot er iets nieuws komt en zeggen dan dat het te nieuw is. Conservatief is dus een te vriendelijke beschrijving: inert is beter. En het resultaat is navenant. Geen enkel.

Klagen is natuurlijk gemakkelijker dan fixen. Wij doen hier ook aan branchevervaging – ik ook, ik weet het. In de Security worden alleen auditoren betaald om te klagen en de rest is er om problemen op te lossen en te voorkomen.

Wat kun je hieraan doen? Bovengenoemde dossiers op de lijst van je organisatie zetten? Ja, dat kan, maar dat is niet het belangrijkste. Vraag je af waarom je ze nog niet had. En waarom de dingen die je zelf wel hebt gezien niet op de to-do-lijst van je eigen organisatie staan en die verhalen van dat stomme Gartner wél.

En als je bovenstaande onderwerpen allemaal wel had, verwacht je nu zeker hulde. Nou, die krijg je niet. Mijn lijstje is namelijk ook maar toevallig tot stand gekomen... Ik zit in die innovatiehoek en daarom zie ik bepaalde dossiers, mijn dashboard is zeg maar wat beter verlicht. Er zijn echter ongetwijfeld bendes dringende onderwerpen die ik totaal niet ken. We zitten echt met zijn allen in deze tunnel. Er is weliswaar licht aan het eind ervan, maar ik denk dat dat een tegenligger is.

Eigen internet eerst

Maandag 2 april 2012

Het is best een mooi initiatief, het nationaal privacydebat, dat 11 juni gaat plaatsvinden. Maar het is natuurlijk wel weer gewoon praten. Met gelijkgestemden. En dat doen we altijd al. Praten praten.

Dit debat is nationaal. Kennelijk is privacy een Nederlands vraagstuk. En **kennelijk** heeft de overheid een belangrijke taak op dit gebied. Is dat zo? Wat heeft Den Haag te vertellen over de digitale wereld? Of Brussel? Wat zouden ze kunnen doen – en willen ze dat ook? Den Haag wil volgens mij **helemaal niets**. Kijk naar het EPD: dat is nu op instigatie van minister Schippers een private onderneming geworden, nadat het verworpen is in de Eerste Kamer, omdat de privacy niet gewaarborgd kon worden. Alsof het EPD bij de verzekeraars in betere handen is. Je weet wel, die van die woekerpolissen.

Mijn voorstel: we gaan eens ophouden met praten over privacy. Laten we – voor de verandering – eens iets doen. Problemen los je op door de oorzaak weg te nemen. Als je de spijker niet uit de buitenband haalt, kun je plakken wat je wilt maar voor het je weet rammel je weer op de velg. Het EPD is een gat in de binnenband, maar als we iets willen bereiken moeten we de spijker vinden.

De spijker is in deze een overheid die niet optreedt. Dat moet anders. De overheid moet aan de bak. Spijkers met koppen slaan. Daadkracht, doorpakken. En zo.

Hoe? Ik heb wel een idee. Waarom zou de overheid wel de media-industrie beschermen tegen het downloadgedrag van burgers, maar niet de burger beschermen tegen de grijpgrage vingers van Google en consorten? Oh, u zegt censuur. Ach, censuur, censuur. Voor een virusmaker is een antivirusproduct ook een vorm van censuur. De vrijheid van de een is nu eenmaal de onvrijheid van de ander. Ja, de overheid moet vormen van censuur invoeren in het digitale domein. Dat is heel erg 2012. Zie ACTA, SOPA, PIPA enzovoorts. De tijd van het Internet als geglobaliseerde vrijplaats ligt ruimschoots achter ons. Laten we niet treuren om wat is geweest.

Van doorpakken is op dit moment geen sprake voor de Nederlandse overheid. Zij is immers geen eigenaar is van de digitale dimensie. Nou, dat gaan we dus veranderen. De overheid moet eigenaar worden van de Nederlandse digitale dimensie. Afbakenen welk stuk van ons is. Nationalisatie. Heus, het kan niet anders. De andere mogelijkheden zijn namelijk zo langzamerhand wel uitgeput. Boetes zoals Microsoft die ooit opliep hebben hun doel niet bereikt, dus het is tijd voor zwaardere middelen. Als je de Pirate Bay legaal kunt blokkeren, waarom dan niet Google? Je kunt toch niet serieus beweren dat de veiligheid van de Nederlandse burger minder waard is dan de commerciële belangen van een paar buitenlandse multinationals zoals bij de Pirate Bay?

Digitale grensbewaking, dat is het idee. Zo ontstaat dan eindelijk de mogelijkheid de Nederlandse burgers te beschermen tegen de tsunami van buitenlandse privacyschenders en andere internetcriminelen. Hiertoe moet het .nl-domein exclusief Nederlands worden, en binnen onze landsgrenzen gehost worden. Daarmee is het jurisdictieprobleem, dat ons veroordeelt tot nietsdoen, eindelijk opgelost. Nu mag een organisatie natuurlijk een ander top level domein kiezen, zoals .com of .xxx, maar dan kies je voor de status en behandeling van buiten de Nederlandse landsgrenzen. En stel je je gebruikers bloot aan alle gevaren van dien.

Het nationaliseren van ons deel van het internet is onvermijdelijk. De VS beschouwen .com als hun rechtsgebied, zoals we laatst zagen met het uit de lucht halen van Canadese .com domeinen. De Britten stellen dat google.com **voortaan** zoekresultaten moet filteren. Google.com moet blijkbaar voldoen aan Amerikaans én aan Brits recht. Als dat zo is, zal google.com eveneens moeten voldoen aan Nederlands recht, en Amerikaanse neonazistische websites moeten blokkeren. En het moet voldoen aan Chinees recht: alle verwijzingen naar de Dalai Lama tegenhouden, en onder Egyptisch recht: alle verwijzingen naar pornografisch materiaal blokkeren.

Google strijdt een verloren strijd. Google kan uiteindelijk niet op tegen autonome landen. De aftocht uit China was slechts een voorbode. En hier kan Nederland al helemaal niets aan doen, op het grote internet. Nederlandse internetbedrijven zijn dan nog veel kwetsbaarder dan Google en andere Amerikaanse bedrijven, omdat die nog gesteund worden door de grootste krijgsmacht ter wereld en de machtigste inlichtingendiensten. De VS behoudt zich namelijk het recht voor iemand plat te bombarderen als die een kritiek stuk internet raakt. Dat zou dus ook voor Google kunnen gelden. Dat kunnen wij Wehkamp niet beloven.

Dus: nationaliseren. Door .nl expliciet onder Nederlands recht te plaatsen en de rest expliciet daarbuiten, kan deze juridische willekeur beëindigd worden. Iedereen die rechtszekerheid wil - van de Nederlandse rechtsorde weliswaar - kan dan kiezen voor een .nl domein. Daarbinnen worden Nederlandse wetten afgedwongen, en kunnen onze burgers en ondernemingen daadwerkelijk beschermd worden. En wie de digitale grens overgaat, draagt zelf de risico's.

De staat der Nederlanden dient dan wel deze grenzen in de internationale politiek af te dwingen en kenbaar te maken deze effectief en desnoods gewapenderhand te verdedigen. Als duidelijk is wat 'ons internet' is, in plaats van een wazig en arbitrair begrip als 'vitale infrastructuur' wat we dan nu zeggen met de macht der wapenen eventueel misschien te verdedigen, dan betekent cyber defence ook daadwerkelijk iets. Nu betekent het helemaal niets. Behalve eindeloze gespreksstof voor de volgende impotente bestuurlijke lappendeken.

Is vitale infrastructuur wazig? Ja, langs de randen zeker - dat de stroomvoorziening daaronder valt is evident, maar er is een heel groot grijs gebied. Valt internetbankieren van de SNS er onder? Nee, die is te klein.... Het SWIFT netwerk? Ja. Waarschijnlijk. Maar waar zit de grens - als twee grote banken twee weken offline zijn is de economische schade toch heus wel immens.

Onze nieuwe cybersoldaten, waar Hillen zo trots op is, hebben na de nationalisatie eindelijk een duidelijk te verdedigen front. Nu mogen ze alleen defensie zelf verdedigen, en zelfs daarvan is nog steeds onduidelijk waar de **grens** ligt. Missie en mandaat, nu onherkenbaar en onwerkbaar, zijn dan opeens helder. Binnen de grenzen beveiligt onze politie de burgers en bedrijven, defensie en de douane doen de grenzen zelf. Als andere landen hier problemen mee hebben, moeten zij hun stuk internet ook maar nationaliseren en de grenzen militariseren.

Betekent dit balkanisering van het internet? Wellicht. Maar het open wereldwijde internet heeft zichzelf overleefd: de 21e eeuw is er één van nationalisme. Het globalisme van het net, ontstaan vlak ná de val van de Muur, is net zo passé als neoliberalisme en Paars. Preventieve nationalisatie van ons deel van het Internet is de aangewezen stap voor dit moment.

Daarnaast komt er natuurlijk ook nog een Europese digitale douane, die de Europese Schengen grenzen afdwingt. Met de snelheid van Brussel kan dat echter wel een jaartje of tien, twintig duren, daar kunnen wij niet op wachten. Maar dan kan de opvolger van mevrouw Reding eindelijk optreden tegen de **Android spyware**. Hoe ze dat netwerktechnisch gaan doen moeten ze in Brussel maar uitzoeken.

Mochten bedrijven als Google, Apple, LinkedIn en Facebook zich terugtrekken uit ons land omdat ze weigeren zich aan onze wetten te houden, dan biedt dat ook weer interessante kansen voor onze nationale industrie. Vooral als de EU dan ook zo ver is, omdat de Europese interne markt dan wel een heel interessante zone wordt, zonder de Amerikaanse competitie.

Naast alle veiligheidsvoordelen biedt nationalisatie ook nog interessante mogelijkheden om de benodigde bezuinigingen te halen. Met een digitale douane kunnen we gelijk btw, kansspelbelasting en invoerrechten heffen. Het is toch van de zotte dat digitale transacties belastingvrij zijn. De wet stelt immers dat over iedere transactie btw afgedragen moet worden. Bij gebrek aan middelen langs het digitale front gedoogt de Nederlandse staat echter allerlei vormen van belastingontduiking. Zo betalen de internationale gokboeren geen **belastingen**, tot groot verdriet van onze staatsboekhouders, onze begroting en bijgevolg ieders portemonnee. Een andere notoir gedoogdossier is de handel in financiële producten als aandelen, derivaten en wat ze nog meer uitgevonden hebben. Dat is grensoverschrijdend verkeer bij uitstek. Daar is belastinginning inderdaad in de huidige situatie heel moeilijk. Voor die vrijstelling is naar verluidt nóg een goede reden, de financiële sector wil het namelijk niet **betalen**. Tja, dat vind ik zelf eigenlijk niet zo'n sterk argument.

Het recept is dus duidelijk: mijnheer Opstelten, excellentie, dit is uw kans om de veiligheid van de Nederlandse burgers in het digitale domein ingrijpend en blijvend verbeteren, met als prettige bonus een significante bijdrage richting de 3% norm in 2013.

De Security Bubble

Vrijdag 18 mei 2012

Credit rating agencies zijn net mensen. Ze produceren ratings zoals de bakker brood, dag in dag uit volgens vaste patronen en inzichten. Ook negeren ze, net als gewone mensen, risico's. Totdat het echt niet meer kan. Zo hebben de agencies jaren lang diverse landen bestraft met lagere ratings en dus hogere rentes omdat ze de banken niet vrij genoeg lieten om aan iedereen geld uit te lenen.

Banken moesten marktaandeel kopen, zakenbank worden en ook nog dingen doen als verzekeraar – wat beloond werd met hoge ratings en dus goedkoop geld en hogere winsten. Dat leidde tot een samenklontering in de bankenwereld tot de onoverzichtelijke en onbestuurbare lappendekens die in 2009 omvielen. Ook werden overheden lager gewaardeerd omdat ze geld leenden buiten de internationale kapitaalmarkten om, bijvoorbeeld van de eigen pensioenfondsen, zoals in ons land ooit de gewoonte was. Bedrijven die onvoldoende schulden maakten en dus teveel eigen vermogen bezaten, werden negatief beoordeeld omdat dat een uiting zou zijn van onvoldoende ondernemend vermogen en omdat ze een aantrekkelijk doel werden voor de Leveraged Buy Out, de non plus ultra methode van de hedgefunds.

En dan vallen de schellen van de ogen en moet alles helemaal anders. De credit rating agencies maken een draai van 180 graden. Bedrijven moeten plotseling juist eigen kapitaal aanhouden en banken moeten vereenvoudigen. En iedereen moet deze nieuwe inzichten per direct volgen via de machtsregels van de financiële markten, ongeacht de krakende portemonnees van burgers, gevestigde rechtsbeginselen of lopende contracten.

Na de erkenning van een ontwikkeling en de draai rechtsomkeert schieten de agencies eerst een tijdje door, totdat het oordeel uiteindelijk tot normale proporties wordt teruggebracht.

De toekomst voorspellen kunnen de economen van deze agencies dus niet. Maar ze doen het wel, met als gevolg dat hun voorspellingen rond de eurocrisis net zo sterk uiteen lopen als de horoscopen van de Flair, de Telegraaf en Girls Magazine. De invloed van de rating agencies is echter wel iets groter dan 'pas overmorgen op voor lange donkere vrouw'. Die invloed is zelfs bijzonder groot en wordt ook telkens maar groter, want de kant en klare binaire voorspellingen zijn de grondstof voor de computer trading systemen, en die zijn weer allesbepalend in de huidige economie. De agencies zijn bovendien feitelijk bij **wet** bóven onze regeringen gesteld, zodat de credit rating van een land inmiddels belangrijker is dan de stembusuitslag.

Er is geen weg terug. Maar er is wel een weg vooruit. De credit rating agencies gebruiken steeds geavanceerdere modellen met steeds meer factoren om nauwkeuriger uitkomsten te hebben. En wie weet; de overgang naar fuzzy logic en de doorgaande groei van het rekenvermogen maken ongekende zaken mogelijk. Maar makkelijk is het niet. **Vertaalcomputers** moeten een veel eenvoudiger taak uitvoeren – het omzetten van één taal in een andere is vele malen simpeler dan het voorspellen van de wereldeconomie. Na meer dan veertig jaar van grote inspanning begint de vertaalmaterie eindelijk enigszins duidelijk te worden. Het verbeteren van de voorspellingslogica van de rating algoritmes is dan ook een hele lange weg met ongetwijfeld hard vallen en moeizaam weer opstaan. Heel veel vallen. Maar het is de enige weg.

Mocht je nog denken dat we na de huidige crisis een tijdje rust krijgen om bij te komen, dan moet ik je teleurstellen: ons economisch model is manisch depressief met trekken van borderline. Paniek zit ingebakken in dit systeem, omdat het gebaseerd is op een maakbaarheidsgeloof van de economie waar de Sovjets liberaal bij afsteken. En dat allemaal door een onwrikbaar geloof in wat computers vermogen: de wereld wordt bestuurd door rekenmodellen.

In de Cyber Warfare scenario's wordt daarom voorzichtig onderzocht hoe digitale oorlog ooit de computerbesturing van onze wereld kan raken, via de systemen van de credit rating agencies. Voorwaar een beangstigende gedachte.

We maken op dit moment een omslag door van ICT security naar Cyber security: de digitale weerbaarheid van landen en organisaties staat inmiddels ruimschoots in de schijnwerpers, getuige de dagelijkse nieuwsitems. En, dat moet gezegd, daar is ook wel aanleiding toe – voor een deel van de criminaliteit is of wordt 'cyber' de belangrijkste dimensie. De buit van cybercrime lijkt nog nergens naar – de totale wereldwijde opbrengst van digitale bankenfraude komt overeen met ongeveer twee geldwagenovervallen. Niet te vergelijken dus met de kosten van simpele interne besturingsfouten als de London Whale van JP Morgan, Nick Leeson van Barings Bank of Jerome Kerviel van de Société Générale. Maar, het is een feit, de opgaande trend is onmiskenbaar.

Het is een kwestie van tijd voordat de gevoeligheid van een land of een bedrijf voor cyber incidenten mee gaat tellen in de credit rating. En zo dus een daadwerkelijke factor wordt in de bedrijfsvoering of de regering. Deze relatie wordt overigens al jaren geclaimd door de adepten van ISO-normering. Maar een tegeltje in de receptie van een hoofdkantoor en een logo op de website is nog iets anders dan een positieve waardering van Moody's. Toch hebben de tegeltjes wel gelijk, de relatie is terecht. Als cyber security zo belangrijk is, dan geldt dat ook de financiële kant van de zaak. Rating Agencies rekenen in risico's, dus de link is er gewoon ook echt.

Deze ontwikkeling is uitermate interessant voor ons vakgebied. Ongetwijfeld zal het soortelijk gewicht van Cyber security in eerste instantie doorschieten, net als rond 2000 de verwachtingen van wat internet vermocht de boel nogal uit balans trokken. Ik geef het alvast maar een naam: de Security Bubble. Gouden tijden voor alle security toko's, en dan in eerste instantie voor de stropdassenvariant die zich bezighoudt met compliance. Dat gaat een tijdje goed, tot de rating agencies er na een paar grote incidenten – en dus met een beetje geluk pas na een jaar of tien - achter komen dat je met papieren exercities en colonnes managers geen gaten kunt dichten in de beveiliging van computers. Dit inzicht is het afgelopen jaar al doorgedrongen tot de cyber warfare wereld, waar de cyber warrior tot het hoogste goed is uitgeroepen. Cyber warriors: pure techneuten. Hun marktwaarde is het afgelopen jaar in de Verenigde Staten dan ook al scherp gestegen. Er komt al wat lucht in de ballon.

Iedere IT-er die iets met Security doet of wil doen kan hiermee zijn voordeel doen als hij in staat wil blijven de rekeningen te betalen – ga iets doen met security management, zoals grossieren in dashboards, matrices, best practices en allerhande hoge abstracties rond het woord cyber. Als deze benadering dan uiteindelijk bij de toekomstvoorspellers van de rating agencies door de mand is gevallen volgt de eerste Security Bust. Dan moet je je in de technologie verdiepen en je stropdas in de prullenbak gooien. Er komt immers nog die tweede cyclus met een tweede Security Bubble en ook daar kun je bij zijn.

Als ik een beleggingsadvies zou mogen geven, bijvoorbeeld om je verdampte pensioen te compenseren: koop eerst aandelen in security stropdassen. Laat je niet beïnvloeden door je eigen vakkennis die zegt dat het double-zero's, n00bs en prutsers zijn. Deze gebakken-lucht-profeten gaan een goudgerande tijd tegemoet. Niet over zeuren: profiteer ervan. Maar blijf bij de les, want

zodra ze door de mand vallen – en dat gebeurt vanzelf – moet je je aandelen kwijt zijn. Ruil ze op tijd in voor security slobbertruien.

Te Wapen!

Dinsdag 5 juni 2012

“Dat meen je toch niet serieus hè, van die security slobbertruien?” vroeg mijn salescollega bezorgd toen hij mijn vorige column uit had. “Nee”, zei ik. “Nou, een beetje. Natuurlijk ligt het genuanceerder. Maar de security sector is een leger waarin iedereen generaal wil zijn. Daar winnen we de oorlog niet mee. Om de schaarse fronttroepen in het zonnetje te zetten heb ik hun belang een beetje overdreven.”

“Fronttroepen? Kunnen we nog wel geld verdienen met beleid en architectuur?”

“Jawel hoor. De komende jaren is er wel overcapaciteit in die markt, dus ik zou er niet al te veel van verwachten. Maar als je goed bent is er vast wel werk.”

De collega aarzelde. “Maar wat zou jij dan doen?” vroeg hij.

Ik kon het niet laten om weer half serieus te antwoorden en zei: “Ik dacht aan een digitale wapenfabriek. Cyberwar, daar zit toekomst in.”

Of ik nou echt een digitale wapenfabriek wil beginnen, mwoah. Maar ik zie wel serieus een gat in de markt. De NAVO heeft de oorlog verloren in Afghanistan en zoekt haar bestaansreden op het nieuwe strijdtoneel van de digitale dimensie. In Nederland is Cyber het enige krijgsmachtdeel waarop niet bezuinigd wordt, waar zelfs geld bij mag. Zo gaat het overal ter wereld. Dit levert een regelrechte revolutie in ICT security op. Maar dan wel eentje die de meeste mensen nu nog niet in het vizier hebben.

Defensie is er namelijk erg snel achter gekomen dat wij ICT security mensen alleen maar goed zijn in statische egelstellingen: stilzitten en wachten tot de aanvaller komt. Zo win je de oorlog ook niet, natuurlijk. Ze weten bij defensie wel niets van digitaal maar meer dan genoeg van oorlogvoeren. Zitten wachten in een schuttersputje staat gelijk aan zelfmoord. Deze klant wil ook kunnen aanvallen. Deze klant wil cyberwapens. Middelen om macht te projecteren in het domein van de tegenstander. Een digitale bom sturen naar een enge dictator is immers verre te prefereren boven het sturen van een collega van vlees in bloed in een vrijwel afgeschreven straaljager. En deze klant heeft haast, zodanig dat er zelfs een pot subsidie via het Topsectorenbeleid klaar ligt.

Er wordt al volop gedelibereerd over de impact van cyber warfare op oorlogsvoering als zodanig. En over **regulering** ervan. Toch hebben de meeste mensen geen idee wat wel en wat niet kan. En het ingezette tuig maakt echt wel uit voor het gebruik. Hoewel de principes van oorlog (mits voldoende abstract) gelijk zijn, is een oorlog met vliegdekschepen heel iets anders dan eentje met roeiboten.

Die wapens, die moeten we dus maken. En als de hut goed loopt, verkopen we de boel aan de traditionele wapenindustrie en gaan met een stampvolle portemonnee een sabbatical doen.

De meeste discussies over cyberwapens gaan over het gebruik ervan en welke systemen je zou willen **aanvallen**. Alsof iedereen weet wat een cyberwapen is.

Sinds Stuxnet is het algemene beeld dat een cyberwapen een virus is **of iets dergelijks**. Dat klopt maar gedeeltelijk: een hond is inderdaad een zoogdier maar niet ieder zoogdier is een hond. En

deze specifieke hond is niet zo'n gezeglijk en betrouwbaar huisdier. De huiver voor cyberwapens is een soort angst voor de golem, die een eigen wil dreigde te krijgen en zich uiteindelijk tegen zijn maker Rabbi Löw keerde.

Virussen worden namelijk geplaagd door het probleem van het mikken – net als gifgas kan de schade aan **eigen troepen** of aan de bondgenoten knap rottig uitpakken. Een virus is ook niet geschikt voor het concept 'tegenaanval' in dezelfde dimensie. Dat zie je goed aan wat Japan nu doet. Zij laat door **Fujitsu** een **tegenaanvalsvirus** bouwen. Het volgt de aanvalsketen omgekeerd en schakelt de aanval uit door alle zombies in de keten op te schonen. Dat klinkt wel mooi, maar is niet veel meer dan het aloude concept van een goedaardig virus – dat uiteindelijk de aanvaller alleen stopt maar niet uitschakelt. De waarde is dan ook zeer beperkt. Bovendien, als bekend wordt dat je virussen inzet, beschadig je je imago als morele kruisridder in de digitale dimensie[95].

Er is een veel breder scala aan cyberwapens nodig en vrijwel niemand heeft echt een helder beeld. De Verenigde Staten nodigen daarom partijen uit via DARPA[96] om met goede ideeën te komen. Er is ruimte voor creativiteit. Veel ruimte.

Er zijn wapens en wapens. Tanks en geweren natuurlijk, maar er is ook zoiets als economische oorlogsvoering. Het bekendste voorbeeld is de Koude Oorlog, die vrijwel zonder wapens werd uitgevochten. Een wapen is dus een rekbaar begrip - iets wordt een wapen door het gebruik. Het gebruik is het dwingen van een andere partij tot iets wat deze niet wil. Zo kan in voorkomende gevallen een kruissleutel een prima wapen zijn, en toch valt het niet onder de wapenwet.

Om de digitale wapenmarkt te bepalen en daar geld mee te verdienen, moet je zo helder mogelijk zijn over wat je levert. Cyberwapens zijn wapens die uniek en onderscheidend moeten zijn van ander wapentuig. Wapens zijn alleen cyber door hun toepassing in elektronische netwerken of die alleen toepasbaar zijn via die dimensie. De essentie is het netwerk - elektronisch dus, en niet per definitie digitaal.

Het blijft wazig, ik zie het aan je blik. Ik zal het toelichten met wat voorbeelden.

Via de radio propaganda verzenden, hoort natuurlijk niet bij cyberwarfare. Via de radio executable code verzenden en activeren wel – hoewel het transport elektronisch is en niet digitaal. Het inbreken op de OTA beheerinterface van de iPhone is tenslotte overduidelijk een cyberwapen.

Via Internet propaganda bedrijven is geen cyberwar – het gebruikt alleen een meer hedendaags medium dan een krant of een strooibiljet. Via Internet inbreken om desinformatie in door de tegenstander betrouwbaar geachte kanalen te injecteren? Dat is dus wel weer cyber warfare. Een nepsite die er levensecht uitziet en met een adres dat ook echt had kunnen zijn, zoals whitehouse.com? Nee, dat is een **False Flag** operatie zoals de boekaniers in de 17 eeuw. Verkeer middels een spoof naar die nepsite brengen, zodat de bezoeker daadwerkelijk whitehouse.org in de adresbalk ziet? Dat is dan weer wel cyber warfare. Dat iets op Internet gebeurt of ergens door een computer gaat maakt nog het lang het niet cyber. Maar zodra je de cyberruimte een beetje buigt - dán wordt het cyber.

---

[95] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[96] http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html

De definities zijn nooit 100% helder, maar dit lijken mij hanteerbare kaders om het bereik van een digitale wapenfabriek te bepalen.

De cyberruimte bijbuigen, dat gaat de meeste Security mensen een stap te ver – aanvallen doe je niet. Je bent juist getraind om de digitale dimensie goed en netjes te laten werken, niet om hem te buigen. De Security bestaat voor het merendeel uit volgzaamheid aan wijze lessen (best practices) en nog verder strekkend moralisme; de strijd tegen afwijkend gedrag en pornokijkend personeel op de werkvloer is immers altijd belangrijker geweest dan de strijd tegen echte aanvallen. Niet voor niets stelt ICT Security het beleid centraal, en niet het optreden. Een beveiligingsincident is het overtreden van een regel, wat vrijwel altijd toch iets heel anders is dan de boel daadwerkelijk in gevaar brengen. Het overgrote deel van de Security mensen is dominee, geen zondaar; ze hebben nooit een zwarte hoed gedragen en geen idee hoe je een systeem moet breken, of wat ermee te doen nadat ze binnen zijn. Dus er zullen weinig aanbieders zijn van digitale wapens. Zoals ik al zei, een gat in de markt.

In het begin zul je in deze nieuwe markt nog een heel eind komen met opgeleukte oude exploits. Immers, als het Flame virus - wat niet meer is dan een opgeleukte Back Orifice - al serieus als state-of-the-art cyberwapen wordt gezien, kun je de eerste jaren nog een aardige boterham verdienen met troep. In deze parade der zotheid loopt de huidige Security industrie met Kaspersky[97] voorop. Kaspersky stelt dat er drie soorten bronnen van aanvallen bestaan: staten, hacktivisten en criminelen. En omdat het Flame-virus niet simpel is, is het geen hacktivisme – want hacktivisten doen alleen maar simpele aanvallen. Omdat Flame geen geld steelt, is het ook geen cybercrime. En dus is Flame door een staat gebouwd en DUS is het een cyberwapen. Nog steeds aldus Kaspersky die blijkbaar nog nooit van hackers gehoord heeft. Nu zal deze clown er nog even mee wegkomen: een klantenkring met weinig kennis en veel geld is een open uitnodiging voor dit soort cowboys.

Maar ik denk dat de wildwestfase toch niet zo lang zal duren. De militairen hebben al door het statisch defensiebeeld heen geprikt die onze sector predikt en al dertig jaar beoefent. Dat deden ze verbijsterend snel. Daar houden ze hoogstwaarschijnlijk niet mee op. Die wapenfabriek moet dus wel goed zijn en over een jaar of twee operationeel. Tijd om door te pakken dus.

Om cyberwapens te ontwikkelen moet je je eerst verdiepen in de anatomie van een aanval.

Een aanval bestaat uit propagatie (er komen) en payload (iets doen), of het nu een hack of een virus betreft. Propagatie is de eerste uitdaging.

Klassiek is het gebruik van kwetsbaarheden. 0-Days geven een aanvaller een tijdelijke kans om door een beschermingslaag te dringen, totdat de patch uitgerold is. Er zit nog een korte kans voor extra slagkracht, tussen het beschikbaar komen van de patch en de daadwerkelijke installatie ervan. Je kunt immers door een patch te reverse engineeren het gat exact vinden. En je weet, het kan even duren voor een patch daadwerkelijk gedraaid is.

Er is nog een andere leuke invalshoek. Waar in een applicatie heb je de grootste kans om een gat te vinden? Als je ooit geprogrammeerd hebt, dan weet je dat: in de backwards compatability. De proggers vinden het oude slecht – vooral als het van een ander is, en besteden er dus minder aandacht aan. De opdrachtgever is er ook niet in geïnteresseerd om het oude te blijven ondersteunen, dus het is nogal een ondergeschoven kindje. Vaak bevat de oude versie überhaupt

97 http://www.infosecisland.com/blogview/21464-Kasperskys-Problematic-Flame-Analysis.html

al minder Security mogelijkheden, dus is het een ingecalculeerd gat. Maar dan een waarvan de koper niets weet.

De cyberwapenmarkt op basis van kwetsbaarheden zal echter dringen zijn, en de houdbaarheid van dergelijke wapens is zeer beperkt. Het zijn enkelschots wapens: als je het één keer serieus gebruikt hebt, zal je tegenstander het gebruikte gat dichten. Het lijkt mij een hele stressvolle toekomst die ook bedrijfsmatig erg onzeker is. Moeten we niet willen, dus.

Gelukkig is dat niet alles. Er is nog een hele wereld te winnen met het uitbuiten van voorspelbare configuratiefouten. Een lek in een stack is minder dodelijk dan een vinkje vergeten, en wordt ook niet gefixed met een patch. Toch focust de Security industrie zich op het lek in de stack – want dat is overal hetzelfde. Een foute config in een router blijft keurig staan, zodat er ook na de patch nog vrolijk gebridged wordt. Dit soort gebruiksfouten zijn standaard en voorspelbaar. Dit is een subsport van social engineering die niet in de boeken staat en die een heel interessant spectrum voor wapensystemen opent.

Bij sommige systemen zitten gebruikersfouten in de GUI ingebakken, bij anderen in de handleiding. En – in de vertaling van de handleiding. Een Rus die een Engelse handleiding leest, zal bepaalde zaken anders interpreteren dan een native speaker. Welke dat zijn, kun je voorspellen, als je een paar vergelijkende taalwetenschappers weet te vinden. En daar maak je dan je wapen van.

Payload is het volgende probleem – en uiteindelijk het grootste. Stel nu dat je door die buitenmuur heen bent gebroken en je hebt een Shell op een SSO-server. Je kunt overal bij. Wat dan? Stel je wilt informatie, hoe ga je die vinden? De meeste medewerkers kunnen al de juiste versie van de juiste documentatie nooit vinden, dus wat kun je dan als hacker? Noem dat maar een uitdaging.

Of stel, je wilt een SCADA-systeem manipuleren – hoe kom je daar en wat tref je aan? Voor payload is informatie verzamelen essentieel. Dus tussen propagatie en payload zit een essentiële schakel: doelinformatie. Denk aan een tank: het heeft geen zin met je antitank kanon (propagatie) een 'high explosive' granaat op de tank af te schieten – je moet Armor Piercing gebruiken (payload). Als je met hetzelfde kanon een huis wil kapot schieten, moet je juist high explosive gebruiken, want die AP zou er dwars doorheen gaan. Om dus een effectief cyberwapen te maken, heb je drie delen nodig: propagatie, doelinformatie en payload.

De uiteindelijke kernvaardigheid is doelinformatie verzamelen. Het aan elkaar plakken van onvolledige informatie tot een plaatje dat bruikbaar is. Daarbij komt zeker evenveel toegepaste psychologie kijken als ICT-kennis. Een cyberwapenfabriek wordt een multidisciplinair intellectueel hoogstandje. Dat zal inderdaad wat gaan kosten, dus het is maar goed dat de klanten van wapentuig gewend zijn aan grote bedragen. Maar leuk wordt het zeker met wetenschappers en programmeurs in één hok. In slobbertruien.

Het EPD en de marktillusie

Maandag 25 juni 2012

In een poging het gezonken EPD weer in de vaart te brengen nadat het getorpedeerd was door de Eerste Kamer, heeft minister Schippers het 'overgedragen aan de markt'. De markt is immers, zo leert het VVD-programma, kundiger dan de rijksoverhead. Zoals ieder kind al weet wordt de markt gedreven door doelmatigheid en kostenefficiëntie, en dit gaat zorgen voor een veilig, privacyvriendelijk en betaalbaar landelijk EPD. Een combinatie van zorgaanbieders zal op verzoek van de minister de klus gaan klaren waar een andere combinatie van dezelfde zorgaanbieders onder regie van de overheid faalde.

Zou het werkelijk?

Marktwerking is gebaseerd op vraag en aanbod. In vrijwel iedere markt zit er tussen producent en afnemer een marktkoopman, bijvoorbeeld een supermarkt. In de zorg is de marktkoopman de verzekeraar. Hij wil dus het aanbod zo goedkoop mogelijk inkopen en zo duur mogelijk verkopen.

Zo simpel is het, in theorie. In de praktijk niet, maar minister Schippers **denkt van wel**. De verzekeraar is de supermarkt die volgens haar "zijn best [doet] om voor de verzekerde goede zorg in te kopen tegen een scherpe prijs". De idee hieronder is dat de klant de leverancier kan sturen door bij gebrekkige kwaliteit over te stappen naar een andere verzekeraar, net zo makkelijk als dat je naar een andere supermarkt fietst. De verzekeraars zijn dus de Albert Heijn, en de ziekenhuizen de pindakaasfabrikanten. Supermarkten leveren goedkoop prima producten en daarom zal dat in de zorg ook zo werken. Verwacht de politiek.

Het zal anders gaan. Er zit een nijdig addertje onder het gras, dat bestaat uit de regels van de markt zelf.

Het landelijke EPD is ooit bedacht om de kwaliteit van de zorg te verbeteren. Het kan alleen indirect wat bijdragen aan de kostenefficiëntie omdat minder fouten maken leidt tot minder behandelingen en omdat betere doorstroming leidt tot minder ligdagen van patiënten. De informatie die je daarvoor nodig hebt, de inhoud van het EPD, is voorbehouden aan de zorginstellingen. Het gaat immers om patiëntgegevens en dan hebben we het over privacy.

De markt heeft van minister Schippers dus de opdracht gekregen een systeem te bouwen waar ze zelf niets aan heeft, want ze heeft geen toegang tot de inhoud van dat systeem. Deze opdracht getuigt van een maakbaarheidsgeloof waar Den Haag, ongeacht politieke kleur, blijkbaar patent op heeft.

Dit EPD is namelijk niet het gedroomde informatiesysteem van een door de markt gedreven sector. Het nieuwe EPD is een informatiesysteem waarmee de zorgverleners samen deze markt zouden kunnen besturen. Maar waarom zouden ze samenwerken? In een markt werk je niet samen, in een markt beconcurreer je elkaar. Ook in de zorg is samenwerking absoluut **geen praktijk**. Bedenk ook dat in geen enkele andere markt is een dergelijk marktbreed producentensysteem voorhanden is. Logisch, want een dergelijk systeem bevat namelijk de bedrijfsgeheimen van de concurrentie. Een zorgverlener kan met creatieve queries via het EPD achterhalen hoe de directe concurrent het er vanaf brengt.

Een markt vraagt om eigen, gesloten informatiesystemen. En vooral om onbelemmerde toegang tot relevante informatie daarin. Om te concurreren moet je betere informatie hebben dan de competitie. Zorgverleners die moeten concurreren, gunnen elkaar daarom geen inzage in elkaars gegevens. De discussie over het eigenaarschap van patiëntgegevens spreekt hierover boekdelen. Voor de buitenstaanders: de gegevens over de patiënt zijn niet van de patiënt zoals je zou verwachten, maar van de zorginstelling die ze ooit vastgelegd heeft. Die gegevens deel je niet. De verzekeraars, die de markt moeten tuchtigen, mogen die inzage dus al helemaal niet hebben. Heus niet omwille van de privacy, maar gewoon omdat de zorgfabrikanten in dat geval helemaal overgeleverd zijn aan de verzekeraars en hun marktpositie en marges bedreigd zien. Zij hebben de marktwerking veel beter begrepen dan de minister. Een volgend debacle van 300 miljoen euro tekent zich dan ook al af.

Een markt heeft een eigen dynamiek en eigen doelen, die niet per definitie de doelen zijn die passen bij de droomkoker van politici. Het zou een goed idee zijn als de mensen die de zorgmarkt willen invoeren eens een tijdje in een daadwerkelijke markt zouden werken. Een supermarkt is een uitstekende plaats om veel te leren. Ik denk dat Albert Heijn of C1000 wel een plekje wil vrijmaken voor een praktijkstage voor politici. Daar zouden ze de volgende inzichten kunnen opdoen.

Een supermarkt leeft van massa.

Op producten die iedereen toch koopt, worden relatief hoge marges gemaakt. Op ondersteunende producten zitten lagere marges, want anders worden ze niet gekocht. Ondersteunende producten zijn er om klanten te lokken, en kunnen zelfs bewust met verlies aangeboden worden. De mate waarin kosten doorberekend worden is dus niet lineair, maar afhankelijk van de plaats in het assortiment. Echter: als een product te weinig oplevert, dan verdwijnt het uit de schappen. De ‘uit het assortiment’ bak ligt elke dag vol. Zo zullen eenvoudige bevallingen goedkoper worden – want die kunnen ook thuis – maar ingewikkelde operaties duurder. De klanten kunnen gemakkelijker naar een ander ziekenhuis dan naar een andere verzekeraar. Zeker tijdens een behandeling. Producten die zelden voorkomen moeten verdwijnen uit het assortiment. Aldus de markt. Mensen die die schaarse spullen toch willen moeten maar naar de speciaalzaak. En als die er niet is, doen die mensen maar zonder. Dus, lezer, de volgende keer dat je naar India op vakantie gaat moet je maar geen parasiet oplopen, want in een marktgedreven zorg zal je naar de speciaalzaak moeten die iedere prijs kan en zal vragen voor de verlossing van het ongedierte.

Een supermarkt leeft van trouwe klanten.

Door te registreren wie wat koopt, weet de kruidenier in welke vestiging linzen in het schap moeten staan, en in welke niet. Albert Heijn heeft daarom samen met Shell en V&D in 1994 Air Miles opgericht. Het doel van dit systeem is het verzamelen van sturingsinformatie om klanten te kunnen belonen voor trouw aan de leverancier. De klanten krijgen korting als ze vaker kopen en de supermarkt krijgt informatie. Weten wat de klant wil kopen en hoeveel hij daarvoor bereid is te betalen is essentieel voor een markt. De klant levert wat privacy in, dat is waar, maar deelname aan Air Miles is niet verplicht. Er doen blijkbaar genoeg mensen vrijwillig mee want het systeem wordt 18 jaar nog steeds gebruikt. Op die vrijwillige deelname kun je natuurlijk wel iets afdingen. Twee tientjes in de maand is voor een Security consultant misschien niet belangrijk, maar voor genoeg burgers aan de steeds bredere onderrand van de samenleving een wezenlijk bedrag. Als een patiënt toestemming geeft gegevens te laten delen ‘voor betere en goedkopere zorg’ is dat evenmin helemaal vrijwillig. Partijen in een markt zijn nu eenmaal niet allemaal even machtig en vrij.

Een supermarkt leeft van goedkope leveranciers.

Een supermarkt is een inkoopcombinatie die de fabrikanten afknijpt en daarom hogere marges heeft bij lagere prijzen dan wat een kleine winkel voor elkaar krijgt. Hoe groter de inkoopcombinatie, hoe groter de winstmarge. Daarom zijn alle lokale supermarkten verdwenen en blijven er uiteindelijk **drie giganten** over: er is een oligopolie ontstaan. Als de spelers in een oligopolie weten wat de marges van de concurrentie zijn en deze respecteren, ontstaat er een marktmonopolie. Dan kunnen de marges omhoog en stijgen de prijzen. Grote spelers hebben er dus alle belang bij de om de drempel voor toetreding tot de markt zo hoog mogelijk te maken. Het monopolie is de natuurlijke eindsituatie in alle markten waarin het toetreden voor nieuwe spelers een **hoge drempel** heeft. De markt heft uiteindelijk de marktwerking op. De fabrikanten verdienen zo min mogelijk en de klant betaalt zoveel mogelijk.

Een supermarkt domineert de leveranciers en de leveranciers willen niet gedomineerd worden. Zo zullen de fabrikanten er uit lijfsbehoud alles aan doen om de informatiestroom naar de inkoopcombinatie zo klein mogelijk te houden. Een goede manier is het geheimhouden en manipuleren van gegevens. Zo zijn ook de zorginstellingen niet gebaat bij een volledig kloppende en open informatiestroom naar de zorgverzekeraars en naar elkaar, zeker niet waar het de kosten aangaat. De sturingsinformatie waar de politiek op rekent om de kosten in de zorg te beheersen zal uit welbegrepen eigenbelang vervalst worden. Dit is de normale manier in de markt om de dominantie van inkooporganisaties verzekeraars te beperken. De kwaliteit van de gegevens in een landelijk EPD zal door deze marktregel laag zijn. Wel jammer voor de patiënt, natuurlijk. Want oja, die was er ook nog.

Uiteindelijk leeft een supermarkt van informatie – over de besteedbare budgetten van de klanten, de marges van de fabrikanten en de proposities van de competitie. Niets vreemds aan: iedere markt leeft van informatie, zoals het grootste bedrijf ter wereld, Google, dagelijks bewijst. Privacy en markt gaan in geen enkele sector samen. Bij informatie geldt: hoe meer, hoe beter.

Gebrekkige informatie is het kenmerk van imperfecte markten. Een imperfecte markt leidt tot **een lage uitnutting** van de middelen, hogere kosten en hogere prijzen. Hoe imperfecter een markt, hoe erger dit wordt.

In de door de minister gewenste constellatie in de zorg zit al deze marktinformatie in het EPD – maar de verzekeraar mag daar van de wetgever niet bij kunnen, terwijl andere zorgaanbieders juist overal bij moeten kunnen. Dan werkt de markt dus niet. De wetgever lijkt te geloven in het fenomeen marktwerking zonder te beseffen dat besturing van informatie de kern van iedere markt is.

De opdracht van de minister aan de markt kan maar op twee manieren uitpakken. De ene optie is dat de verzekeraars zich via een achterdeur toch toegang verschaffen tot het EPD. Bijvoorbeeld door de boel te hacken mag niet of door een zorgpartij te kopen mag ook niet, of door de informatie bijeen te sprokkelen en op te slaan in een al dan niet gekoppeld schaduw-EPD. Dat laatste is in principe grotendeels **verboden**, maar de grenzen van wat mag en wat niet mag in een dergelijk klantinformatiesysteem zijn wazig. Bovendien is de pakkans nihil. Dit zullen de verzekeraars dan ook doen, scherp laverend langs de randen van wat toegestaan is, en de kosten van dit schaduw-EPD zullen doorbelast worden. Daarbij zal de kwaliteit van de informatie in dit schaduw-EPD nog lager zijn dan in het gewone EPD, want bovenop de gewone fouten komt de opzettelijke desinformatie van de zorginstellingen. Bovendien kunnen we met meer systemen rekenen op meer datalekken en hacks. Ongelukken zullen er dus zeker van komen. De extra beveiligingskosten worden gewoon doorbelast en tegen de mensen wier privacy op straat ligt wordt hooguit sorry **gezegd**. Als het lek aan het licht komt, wat natuurlijk meestal niet gebeurt.

Den Haag doet wel mee **zodra** het op TV is geweest. Dan komen er Kamervragen en nieuwe richtlijnen voor de verzekeraars en uiteindelijk schadevergoedingen voor gedupeerden. Ook dat kost wel een paar stuivers. Met als gevolg lage uitnutting, hoge kosten en hoge prijzen.

De andere optie is dat de verzekeraars zich geen toegang verschaffen tot het EPD. Ze houden zich aan de letter en de geest van de wet. Ze opereren op een markt maar ze hebben geen marktinformatie. Zonder informatie kan de zorg helemaal geen markt worden. De beloofde voordelen van de markt komen er niet en de nadelen van een hoogst imperfecte markt komen er wel. Lage uitnutting, hoge kosten en hoge prijzen.

Dit zal niet goed uitpakken.

Bring Your Own Ding

zaterdag 21 juli 2012

De Security hit van het moment is BYOD. Voor die twee security.nl lezers die er nog niet over lastiggevallen zijn, het staat voor Bring Your Own Device. Door IT-ers en beveiligingsmensen al lollig verbasterd tot Bring Your own Disaster. Want weet je wel hoeveel virussen je op die manier binnenkrijgt? Mobile devices doen vanzelfsprekend aan wisselende contacten, en dat doen ze zonder de digitale condomerie van antivirusproducten die de organisatie gekozen heeft. Wil je een security officer een slapeloze nacht bezorgen, dan moet je dus melden dat BYOD 'ingevoerd' gaat worden.

Ik zou eerlijk gezegd rustig verder slapen. Veel 'Own Devices' zijn feitelijk veiliger dan de gemiddelde zakelijke XP-laptop met IE6 voor compatiblity en met een zelf in elkaar gekleuterde web app. Sommige privéspullen zijn Trusted Platforms zoals de Blackberry en de iPhone met alle beveiligingsvoordelen van dien. Ja, ook daar zijn virussen voor, maar de 'viruscount' lig heel veel lager dan voor een pc-platform dat we allemaal kennen.

BYOD als Security probleem heeft onderhand mythische proporties. Terwijl het eigenlijk oude wijn in nieuwe zakken is. Het gaat namelijk over Port Security en dat probleem bestaat al jaren. Het is alleen zelden echt opgelost. Voor draadloze netwerken zie je nog wel af en toe een redelijke oplossing, maar prik je netwerktouwtje maar in een willekeurige ethernetpoort in een willekeurig kantoorpand en je snapt wat ik bedoel. Met de komst van computer accounts in de directory is er weliswaar een logon, maar dat is geen aanloggen op 'het netwerk', dat is aanloggen op het Windows-deel daarvan. Al sinds de opkomst van de pc en het netwerk geldt dat het aansluiten op het netwerk van eigen apparatuur gewoon lukt. Het probleem was vroeger wel minder dringend dan nu natuurlijk. Er liepen gewoon veel minder mensen rond met een portable 'sjouwable[98]' pc dan nu met een mobiele telefoon.

Waar het om gaat is toegang tot je informatie. Mobile Device Management MDM is niet toereikend. Informatiebeveiliging in een mobiele omgeving vraagt beveiliging op informatieniveau, niet op device niveau.

Als je de oplossingen uit de markt bekijkt zie je dat BYOD als een discussie over de netwerk perimeter gebracht wordt. Ze doen een VPN naar een digitale slagboom en ze doen een emulatie van het netwerk met een portal of een terminal server. Daar gaat het dus juist niet om. We weten sinds **Jericho** dat de netwerkperimeter meer fictie dan feit is.

Maar goed, de vraag op de perimeter is hoe een eigen device te onderscheiden van een door de baas verstrekt apparaat. De meeste MDM-oplossingen negeren deze kernvraag, en focussen zich op policy enforcement. De onderliggende aanname is dat een device 'goed is' als de policies afgedwongen zijn. Dat is een interessante gedachte: een apparaat mag op het netwerk als er een wachtwoord op de screensaver zit en het device gewiped wordt na drie mislukte Pincodes. Kan goed zijn, daar niet van, maar het heeft er veel van dat de policies die toevallig in het apparaat zitten hier maatgevend zijn. Want welke organisatie heeft nu een wipe policy op de laptops staan? Of op de thuis-pc van de medewerker die aan het Nieuwe Werken doet? Wiens Dropbox wordt automatisch gewiped? Want het is uiteindelijk geen device vraag, het gaat om de inzet van eigen middelen ten bate van de baas. Niet alleen je eigen Device, maar ook je eigen data in een cloud

[98] http://www.grotescheur.nl/wp6/2011/02/vooruitgang-wet-van-moore/

applicatie zoals LinkedIn of je thuis wifi netwerk met je zakelijke telefoon. Zeg maar Bring your own Ding.

Wat er nu geroepen wordt rond dit onderwerp klinkt allemaal erg onvolwassen. Het komt niet verder dan puntoplossingen die bepaald worden wat bepaalde techniek toevallig in huis heeft. Weinig doordacht, inderdaad. Organisaties zullen vanzelf ontdekken dan een reeks puntoplossingen naast elkaar vooral hoge kosten maar weinig veiligheid brengt. Het is al snel goedkoper om iedereen een iPad van de zaak te geven.

Voor we volwassen kunnen omgaan met niet-bedrijfseigen apparatuur en informatievoorzieningen, al dan niet in de cloud, hebben we als beveiligers nog veel meer vraagstukken op te lossen.

Stel nu dat iemand met een eigen device voor je werkt via het bedrijfsnetwerk en dat er vanaf dat device aanvallen op het serverpark van de CIA plaatsvinden? Dan krijg je heus wel gedonder. Wat als de thuis-pc van de Nieuwe Werker de C&C van een groot botnet blijkt dat het toevallig op je concurrent voorzien heeft? En als een medewerker de mp3s op de iPad deelt met de hele wereld, thuis en op de zaak, krijgt je bedrijf dan **Tim Kuik** van de Stichting Brein op bezoek?

Als eerste zal de beleidsfabriek op dit onderwerp springen: Er Moet Nieuw Beleid Komen. Beleid als universeel wonderdrankje.

Nou, nee. Als beleid gerelateerd is aan het device dan is het wel erg tijdelijk beleid. Je wilt ook geen ander beleid per type device - hoeveel beleidsdocumenten wil je er op na houden? Er hoeft al helemaal geen aanvullend beleid te komen over ongewenste content en aanpalende handelingen, zoals mp3s delen. Het gaat in dit voorbeeld immers om evident illegaal gedrag, ongeacht het apparaat.

Het vervelende van beleid is dat je het moet handhaven. En dat is bij BYOD nog veel moeilijker dan in een traditionele omgeving. De huidige houding van corporate beveiliging zal gebruikers er vooral weerhouden om te werken op hun eigen ding. Heb ik zelf ook. Ik mag van mijn baas mijn zakelijke e-mail op mijn eigen telefoon lezen, mits ik een screensaver password, een Phone Home appje zodat we een verloren toestel kunnen terugvinden en een wipe functie heb. Dat wil ik helemaal niet. Het is mijn privémachine en de baas mag mijn privédata helemaal niet wissen. En die pincode iedere keer intikken.... kansloos. Dan maar geen zakelijke e-mail op mijn telefoon, dus de klant of prospect moet maar wachten tot ik achter mijn laptop zit.

Als je de lijn doortrekt naar thuiswerken wordt al snel helemaal te zot. Dan ben ik als beheerder van mijn eigen thuisnetwerk zeker verantwoordelijk en aansprakelijk wat er daarvandaan allemaal gebeurt? Voor wat mijn huisgenoten op het internet uitspoken bijvoorbeeld. En dan krijg ik ook de schuld als de buren mijn WiFi printer van HP gehackt hebben en zo meeliften op mijn verbinding. Straks komt Corporate Security nog met Deep Packet Inspection kijken of het allemaal wel door de beugel kan wat hier thuis gebeurt. Nee dank u.

Wat wij beveiligers over het hoofd zien is dat BYOD en Het Nieuwe Werken grote voordelen voor bedrijven hebben. Mensen zetten eigen middelen in, zodat de organisatie die niet hoeft te kopen of te beheren. Medewerkers doen, zo blijkt, werkdingen in hun eigen tijd. Ze beantwoorden bijvoorbeeld een vraag van een klant op zondagmiddag op een terrasje met een latte macchiato. Zonder dat ze de uren schrijven. Dat is goed. Dat is goedkoper. Daar moet je blij mee zijn. Bedenk ook dat mensen over het algemeen beter zorgen voor hun eigen spullen dan voor die van de baas: je eigen iPad raak je minder snel kwijt dan de duurdere Dell van de zaak. BYOD en HNW zijn goede ontwikkelingen en daarom niet tegen te houden.

Het huidige treiterbeleid van Security is dus niet de weg om te gaan. BYOD categorisch tegenhouden omdat het onveilig is, is een bestuurlijk zwaktebod en zonder stevige beveiliging helemaal niet af te dwingen. De vraag is wat er eigenlijk beveiligd wordt: de baas of de baan? Als eigen devices op het netwerk mogen, waarom zou een bedrijf nog computers beschikbaar stellen? Dat kost allemaal geld, en er zijn een boel mensen nodig om dat allemaal maar uit te rollen. Als mensen eigen clouddiensten meenemen, waarom zou ik daar als bedrijf dan nog allemaal dure voorzieningen neer zetten?

Het is logisch dat IT-ers benadrukken hoe gevaarlijk BYOD is. En dat het uiteindelijk heel **duur** is en het reputatierisico gigantisch. Natuurlijk. Maar wat we nu zien is misbruik van Security argumenten - BYOD is vooral een gevaarlijke concurrent van de traditionele IT afdeling. De Security vraagstukken zijn verre van nieuw, bestaan ook zonder BYOD en hadden al lang opgelost moeten zijn. En kunnen zijn.

Flexicurity

maandag 24 september 2012

Je kent ze wel, de IT-cowboys. Ook in de Security zijn zij geen onbekend fenomeen, sinds er geld te verdienen is. Victor is er zo eentje. Ik ken hem nog uit de internetbubbeltijd en vorige week sprak ik hem op de rokersplek bij een securitycongres. Hij had een ideetje.

“Luister Peet, haal je hoofd eens uit de bits en bytes en denk eens met me mee. Ik heb namelijk een dingetje en daar wil ik snel mee van de wal, want mijn geldorgaan ruikt geld. Veel geld.

Het toverwoord is Flexicurity. Weet je wat dat is, Flexicurity[99]? Nou, daar zul je achter komen – jij loopt immers ook al tegen de vijftig toch? Flexicurity is de uitkomst van de arbeidsmarkthervorming die er aankomt om de eurocrisis te verhelpen. De arbeidsmarkt moet soepeler om ons uit de crisis te concurreren. Met Flexicurity is het eenvoudiger om dure oude bokken zoals jij en ik eruit te kieperen. In plaats van een gouden handdruk krijg je een opleiding. Die helpt je dan weer aan een volgende baan. De maakbare arbeidsmarkt. Leuk hè?”

Ja, ik wist van flexicurity was en nee, dat vond ik niet zo heel erg leuk. “Het lijkt me een typisch voorbeeld van een oplossing dat het eigenlijke probleem helemaal niet verhelpt”, zei ik. “Die ontslagen oude bokken blijven te duur, dus die komen toch in de bijstand. En bovendien, waarom zou je de arbeidsmarkt willen aanpassen terwijl de eurocrisis is veroorzaakt door de geldmarkt en de vastgoedmarkt? If it ain’t broken, don’t fix it. Gips om je been helpt niet tegen een hersentumor. En kijk eens naar Duitsland, een sterke economie met hartstikke veel ontslagbescherming.”

“Nou”, hernam Victor. “Het kan in elk geval mijn eigen crisis oplossen. Het toverwoord, jongen, is concurrentie. We moeten concurreren. Want de Chinezen komen! Weet je wel hoeveel ingenieurs daar per jaar afstuderen? En die komen allemaal onze bedrijven wegconcurreren. Daar moeten we iets aan doen, nietwaar? Nou, dat tel je dan op bij dat andere toverwoord, kenniseconomie. Hoe kom je aan kennis? Leren! Waar leer je? Op school! Ook daar is niets tegen in te brengen, toch?”

Daar had hij een punt. Deze toverwoorden hebben zelfs de gestaalde kaders van GroenLinks omgekregen[100], dus het nieuwe kabinet zal dit heus wel overnemen. Nu kwam Victor met het toverwoord voor zijn persoonlijke crisis: omscholingsbudgetten. “Denk aan de omscholingsbudgetten die vrij gaan komen als het ontslagrecht wordt aangepast. Stel dat er per jaar 100.000 mensen een jaarsalaris aan omscholingsbudget meekrijgen. Ontslagen ouderen krijgen het meest, namelijk 75.000 euri per persoon. Honderdduizend keer vijfenzeventigduizend harde pegels per jaar – Peet, dat is een markt van zeven en een half miljard, give or take.”

Ik zag waar hij heen wilde. Zijn volgende toverwoord was waarschijnlijk security en daarom was hij bij mij terechtgekomen. Bijna goed. Victor: “Security Management! Dat is het toverwoord! Dáár ga ik die mensen dan voor opleiden. Laten we wel wezen, wie wil dat nu niet worden. Ben je 56, eruit geknikkerd bij een bank, kun je Security Manager worden. Dat is *leuk*!”

---

[99] http://www.managementenliteratuur.nl/1265/flexicurity
[100] http://www.ontslagdossier.nl/index.php/nieuws-over-ontslagrecht/111-nieuws/213-lenteakkoord-hervorming-ww-en-ontslagstelsel

“Security Management?” zei ik. “Maar dat is eigenlijk geen vak. Dat is het aansturen van de beveiligingsmensen, maar niet van de beveiligingsinspanning. Want de beveiliging zelf wordt bestuurd door noodsprongen bij crises, toevallige bevindingen van audits en verder door checklistjes en architectuurprocessen. Structuur ho maar. Dus voor Security Management heb je geen bijzondere opleiding nodig.”

“Ho ho Peet, denk nou eens commerciéél. Wat bóeit het nou helemaal dat het geen vak is. On-der-ne-mer-schap, daar draait het om. En dat ben ik. Ondernemer in hart en nieren. En jij gaat meedoen. Samen stampen we zo een Security Management opleiding uit de grond. Een vrindje van mij heeft nog het perfecte stulpje aan de Vecht waar we de boel kunnen vestigen, leuk lapje grond erbij, en voor een vriendenprijsje maakt hij er aanbouwtje aan met een klaslokaal. Flatscreentje erin en je kunt aan de slag. Kun jij dan wat tekstjes voor de website en de subsidieaanvraag in elkaar knutselen?”

“Ja maar Victor”, probeerde ik nog. “Er is wel een levensgroot probleem om op te lossen. Security heeft de flexibiliteit van een granieten aanrecht, terwijl de aanvaller elke dag verandert. Over flexicurity gesproken. Niet de arbeidsmarkt, maar de Security kan wel wat flexibiliteit gebruiken. Bedrijven hebben een **goalkeeper** nodig die binnen enkele seconden optreedt, maar wat ze krijgen is een bureaucratisch proces dat na een paar jaar een mogelijke oplossing oplevert voor een probleem dat ooit acuut was maar tegen die tijd allang weer voorbij. Niemand weet wat Security Management eigenlijk is anno 2012. Dus die Security Managers van jou gaan zich rechtstreeks naar een burnout werken. Bij gebrek aan flexicurity, zeg maar. ”

“Jongen, Peet, doe je dat nou nog steeds, echte problemen oplossen? Dat is toch niet spannend. We hebben het hier wél over zeven en een half miljard per jaar. Daar pis je toch niet op? Enne, Security Management bestaat wel hoor. In mijn onderzoekje vond ik **CISM** opleidingen, gecertificeerd Information Security Management. Dit staat erbij: “highest paying and sought after IT certifications”. Leuk toch? Die banen zijn er **echt** dus je hoeft je calvinistische moraal om kwaliteit te willen leveren niet eens echt overboord te gooien. En als je wilt, betaal ik je weinig, oké?”

Nu werd ik Victor wel een beetje zat. “Luister Victor, CISM zegt op te leiden om alle beveiligingstechnologie en -maatregelen inhoudelijk samenhangend en werkend te ontwerpen. Dat is geen management, dat is supertechneutenwerk en dat leer je niet in een paar maanden. Wat je eigenlijk leert bij CISM is hoe je securitybudget binnen kan **halen** en dat is ook hartstikke fijn, maar voor het management van de maatregelen geeft CISM je niet meer dan een beetje blokjes-en-pijltjeskennis. Wat die blokjes en pijltjes betekenen gaat CISM je niet leren. Dat kan namelijk niet in dertig **dagen** en met **één boek**. Eigenlijk zijn ze gewoon een stelletje oplichters.”

“Jongen, Peter, kom eens van je hoge paard. Er is geld te verdienen. Serieus geld. Denk er nog eens goed over na.”

En weg was hij. Dit idiote gesprek zette me aan het denken. Niet over die flexicurity op de arbeidsmarkt, dat gaat gewoon gebeuren. Maar wel over Security Management. Want het is echt een probleem: hoe bestuur je al die beveiligingslagen die we sinds de invoering van ‘layered security’ hebben? Langzaam, als het al lukt. Flexibiliteit, of agility zoals IT-ers het tegenwoordig graag noemen eigenlijk: behendigheid, buiten onze wereld vooral bekend als paarden- en hondentraining is **ver te zoeken**. Wij security mensen zijn specialisten in betonnen zwembroeken.

Beveiliging is vooral een reactieve tak van sport; we lezen of merken dat er ergens iets heel erg mis gaat en plakken daar een noodverbandje op. De samenhang en effectiviteit van wat we doen

wordt feitelijk niet bestuurd. Als we het al proberen te besturen hebben we middelen als het ISMS van ISO27002 en architectuurprocessen à la TOGAF. Het eerste is een exercitie in best practices met geautomatiseerde rapportages. Best practices zijn als het goed is bewezen oplossingen voor problemen die iemand ooit heeft gehad. Reken maar dat je daar niet vreselijk agile van wordt. Je voorstel moet immers eerst ergens anders bewezen effectief zijn geweest en in een boek beland zijn. Pas dan mag je die maatregel invoeren. Dat duurt wel een paar jaar. Het tweede, de architectuurbenadering, is een zeer grondige maar daardoor ook eindeloze en trage oefening in functionele behoeftes, waarin als het goed is ook plek is voor beveiliging. Schiet dus ook niet op. Nee, Security wordt niet flexibel op deze manier.

Beveiliging in laagjes

donderdag 18 oktober 2012

Vroeger was IT-beveiliging de ‘slagboom aan de poort’ of, andere metafoor, de ‘schil van de kokosnoot’. Dat werkt niet meer en daarom denken we niet meer in kokosnoten maar in laagjes. Gelaagde beveiliging is een militair concept, losjes vertaald naar IT-beveiliging: op componentniveau is beveiliging aangebracht, dat is per laagje, dus er is gelaagde beveiliging. Deze meerlaagse beveiligingsstrategie staat ook wel bekend als Defense in Depth.

Een rondgang langs wat de specialisten[101] te melden hebben, leidt tot een duidelijk verhaal over het waarom van deze strategie. "Als één beveiligingslaag wordt geslecht, dan is de beveiliging [] nog steeds intact. Het liefst maken deze verschillende barrières gebruik van verschillende technologieën, zodat het voor inbrekers lastiger is om meerdere lagen te doorbreken (veel technische kennis nodig). Elke laag kan voorzien worden van een IDS (Intrusion Detection System) of andere maatregelen om inbraken op te merken (pakkans verhogen). Bovendien zorgen de meerdere lagen voor onzekerheid: hoeveel lagen moeten er nog worden doorbroken en hoe lang gaat dit nog duren? (demotivatie)”.

Een geïntegreerd en samenhangend stelsel van beveiliging dus. Helder en overtuigend. Waar kan ik tekenen?

Zo reageerden we allemaal en zo werd Defensie in de Diepte het leidende model voor ICT-beveiliging. Maar bij nadere beschouwing is gelaagde beveiliging in de diepte eigenlijk helemaal niet zo helder. Wat betekent het in het echt? MT magazine[102]: “Gasten mogen alleen het internet op, veilige apparaten kunnen gewoon bij de bedrijfstoepassingen en gegevens, en eigen apparaten kunnen bijvoorbeeld alleen gebruikt worden om mail, agenda en documenten te bereiken”. Aha, apparaten zijn lagen. Of toch niet? Bij Trend Micro[103] zijn de lagen “applicaties die meervoudig beveiligd worden”. Zijn applicaties dan lagen? En is één product dan meervoudig omdat het meerdere protocollen snapt? Dus zijn protocollen dan lagen?

Tja. Wat is een laag? Hoeveel lagen moet ik beveiligen? Allemaal misschien? Zoals ik al zei, toch niet zo helder allemaal.

Sommige lagen zijn duidelijk. We hebben de netwerklaag, de applicatielaag en de informatielaag. Deze lagen liggen niet op elkaar, maar bestaan ook náást elkaar; ze zijn afzonderlijk te adresseren. Dus is er op iedere laag beveiliging nodig. Logisch ook, want de lagen kunnen fors verschillen en de beveiligingsmiddelen dus evenzeer; ik heb nog nooit een spamfilter een DNS amplifier attack zien tegenhouden. Daarbij bestaat iedere laag ook weer uit lagen. Alleen de netwerkkant bestaat theoretisch al uit – minimaal – vier (of zeven) lagen waarvan er geen enkele per design beveiliging heeft, en iedere applicatie die op de netwerklaag staat is op zichzelf aangewezen.

Zo zijn er onnoemelijk veel virtuele lagen naast de traditionele drie: het beveiligen van mail is iets heel anders dan het beveiligen van een VPN over SSL, hoewel beide op de applicatielaag wonen en alleen virtueel (op portniveau, wat overigens ook alleen maar een abstractie omwille van de adressering op de netwerklaag is) anders zijn. Alle computertechnologie is namelijk gelaagd.

---

[101] http://www.sjaaklaan.nl/pivot/entry.php?id=55
[102] http://www.mt.nl/95/63652/ict/ict-security-blijft-zorgen-baren.html
[103] http://www.trendmicro.nl/producten/enterprise-security-for-endpoints-and-mail-servers/index.html

Echte gelaagde beveiliging zou zijn: op iedere laag en iedere mogelijke aanvalsvector meer dan één beveiligingsmiddel. Dan zou iedere desktop (minimaal) twee antivirusproducten hebben, twee lokale firewalls en twee mechanismes om file access te beperken. En eigenlijk zouden er twee AV-producten op de mailverbinding moeten acteren, twee op de web access, twee op IM en twee op fileniveau. Minimaal. Maar de meeste antivirusproducenten doen er alles aan om de concurrent bij je pc vandaan te houden. En dit is maar één voorbeeld.

Kijk ook naar de beveiliging op bestandsniveau – daar heb je één middel voor, in de regel NTFS. Nu kun je beargumenteren dat één AV op de desktop voldoende is, omdat er op de gateways zoals de mailserver en de http-proxy ook antivirus draait, maar dan doe je de portable waarheid behoorlijk wat geweld aan, want een mailserver of een webproxy zijn afzonderlijke componenten die weliswaar voor een deel overlappen met wat een lokale AV vermag, maar niet helemaal. Zeker niet als de pc een laptop is die best wel eens in een ander netwerk hangt.

Als je zegt dat je gelaagde beveiliging hebt, dan heeft ieder van de honderden technologielagen een eigen beveiligingslaag van ongelijke technologieën, die ook nog goed met elkaar samenwerken. Dat heb je niet. Dat heeft niemand.

En dan nog dat diepteverhaal. Iedere aanvalsvector zou door meerdere beveiligingslagen moeten; dat is in een aantal gevallen ook zo, maar even vaak is die diepte niet meer dan een veronderstelde diepte, omdat lang niet alle aanvalsvectoren bekend zijn. De tegenstander heeft er immers baat bij om ongebruikelijke vectoren te kiezen waar de beveiliging niet op rekent. Zo houdt een statefull firewall aanvallen op de netwerklaag op een laptop in het LAN tegen, maar niet als er data op de laptop kan komen via een andere route. Of als de laptop niet altijd in het LAN hangt. Hier sluiten de lagen soms wel en soms niet aan.

De integratie van de beveiliging zou moeten bestaan uit slimme en geautomatiseerde interactie tussen de lagen; als eentje knel komt te zitten of niet werkt, springt een ander bij. Gegeven dat de lagen geen interactie hebben met elkaar (een lokale firewall die de rules afstemt met de enterprise firewall ben ik nog niet tegengekomen, laat staan één die interacteert met een applicatiebeveiligingsding zoals een Claims Based Security decision) bestaat er helemaal geen integratie in de diepte van de beveiliging. Een gezamenlijke interface[104] om allerlei losse functies in te stellen is geen integratie; die zit op z'n best in de persoon die één en ander bedient.

In de praktijk is de beveiliging op de laagjes statisch en enkelvoudig; als één laagje faalt, is er geen back-up (al zeker niet in realtime) en valt het geheel om. Computerbeveiliging bestaat niet uit soldaten die de ene keer als infanterist en de volgende keer als luchtdoelgeschutsbemanning kunnen werken. In plaats van een gelaagde beveiliging in de diepte hebben we een lappendeken van niet samenwerkende technologieën, met de nodige gaten tussen de lapjes en geen enkele diepte. Defense in depth via gelaagde beveiliging is dus een hele stompzinnige illusie.

Geen wonder dat de bad guys aan het winnen zijn.

[104] http://www.techrepublic.com/blog/security/understanding-layered-security-and-defense-in-depth/703

Het einde van Single Sign On

Donderdag 10 januari 2013

Single Sign On ofwel SSO: het ultieme streven in beveiligingsland. Een enkelvoudige login maakt toegang simpeler, vermindert het aantal wachtwoorden en maakt het mogelijk om sterkere wachtwoord policies in te voeren. Met een enkelvoudig account zijn audits bovendien eenvoudiger uit te voeren en is provisioning en deprovisioning van autorisaties beter te regelen.

De boel wordt veiliger omdat je één wachtwoord gemakkelijker kunt onthouden dan 25. Hierdoor kun je ook sterkere wachtwoorden invoeren. Immers, 25 moeilijke wachtwoorden onthouden, die je eigenlijk ook nog elke maand moet veranderen, dat gaat gewoon niet. Eentje lukt nog wel. Heb je niet eens een Post It op je beeldscherm voor nodig.

Ideaal dus, dat SSO. Maar het is een gepasseerd station. Om verschillende redenen, waarvan de bekendste is: als een user account wordt gekaapt, en dat account geeft toegang tot een stuk of vijftien systemen, dan zijn ze alle vijftien gecompromitteerd. De oplossing die daarvoor aangereikt wordt is sterke authenticatie. Dat heeft slechts een heel enkele organisatie daadwerkelijk ingevoerd, dus met SSO is de veiligheid verminderd.

Maar goed, dit is nog te overzien. Een wezenlijker zwakte ligt besloten in het verschijnsel toegangsbeheer in het algemeen. Toegangsbeveiliging bestaat uit twee afzonderlijke vraagstukken. De eerste is toegang tot informatie gebonden aan een systeem, applicatietoegang dus. De tweede is toegang tot informatie die onafhankelijk is van het systeem: in een bestand, zoals een Excelsheet. Deze twee manieren van toegang vragen ieder een eigen aanpak en een eigen beveiligingstechnologie. Het overgrote deel van de toegangsbeveiligingsmiddelen gaat over applicatietoegang en beschouwt een fileshare ook als een applicatie.

Gegeven dat een Excelsheet op iedere andere willekeurige machine geopend kan worden, is dat een zeer merkwaardige denkfout. En daarmee ook een probleem. Dat al behoorlijk dringend werd met de opkomst van de laptop, maar dat nu, sinds de smartphone, de tablet en de cloud een levensgroot probleem is.

Nu kun je een dergelijke fout pas oplossen als je de oorzaak onderkent – er is geen simpele oplossing want dan zouden we het probleem helemaal niet hebben.

SSO komt voort uit het traditionele gesloten netwerk, waarbij de bakstenen de belangrijkste laag vormen in de informatiebeveiliging. Toegang is in die werkelijkheid een probleem van het netwerk en van de firewall. In dit Old School denken is de eigen omgeving een gesloten geheel, met een harde buitenkant. De beveiliging is dan ook geconcentreerd op die buitenkant. Toegangsbeveiliging is de beveiliging van de poort. De beveiliging van de binnenkant is in deze opzet veel minder belangrijk, want daar kunnen alleen medewerkers bij en die zijn technisch niet zo slim als de hackers buiten. Dit gedachtegoed wordt wel het kokosnootmodel genoemd (hard van buiten, zacht van binnen), of, meer theoretisch, System High Mode[105]

Nu het gesloten netwerk iets van het verleden is, is het kokosnootmodel dat ook. Met het verdwijnen van de buitenmuren is toegangsbeveiliging niet zo simpel meer. De impact van

[105] http://en.wikipedia.org/wiki/System_high_mode

Jericho[106] is echter bij de meeste mensen nog steeds niet doorgedrongen. Zij zien het grootste gevaar nog altijd in de Post It met het wachtwoord op het beeldscherm. Dat is achterhaald: er zijn veel minder aanvallers die fysiek toegang hebben tot je werkplek om de Post It op het beeldscherm te kunnen lezen, dan er mogelijke aanvallers via het internet zijn.

Dus: liever een heel sterk wachtwoord op een papiertje dan een wat zwakker wachtwoord dat gebruteforced kan worden. Wat de meeste mensen zich niet realiseren is dat het Brute Forcen van een wachtwoord op internet veel beter uitvoerbaar is dan op een LAN en de oplossing van het LAN op het internet niet werkt. Op het internet hebben miljarden mensen toegang tot het loginscherm, en is het hoogst ongebruikelijk een lock-out policy te hebben dat een account afsluit na drie verkeerde wachtwoorden achter elkaar. Dat is immers een instant Denial of Service aanval. Facebook, LinkedIn en Salesforce hebben daarom ook geen lock-out policy. Dus als een organisatie Single Sign On 'doet' met een cloudapplicatie, betekent dit effectief het einde van de lock-out policy, ook voor het interne netwerk.

Natuurlijk zouden we helemaal zonder wachtwoorden moeten werken. Want ook na twintig jaar gebruikersopvoeding staan 123456 en password nog bovenaan de keuzelijst [107].

Strikt genomen hoort SSO niet onlosmakelijk bij wachtwoordauthenticatie. Maar in de praktijk werkt het wel zo. Een organisatie zou er immers voor kunnen kiezen iedere gebruiker een hardware token te geven. Dat kan, maar als behalve medewerkers ook klanten toegang hebben, wordt het opeens een heel ander verhaal; een kostbaar verhaal vooral. En, nog veel belangrijker: hoe koppel je Dropbox of LinkedIn aan die corporate strong authentication? Bovendien moet dat dan met een technologie die het doet op een iPhone of op die kekke Android tablet. Dream on.

Dat SSO over wachtwoorden gaat en niet voor andere authenticatietypes werkt wordt nog duidelijker als we het PAM (privileged account management) dossier erbij betrekken: vanuit beveiligingsoptiek is het eigenlijk wenselijk dat toegang tot beheerdersaccounts (die zo ongeveer alles mogen) extra beveiligd wordt – dus zeker met sterke authenticatie. We willen ook dat beheerders aparte accounts hebben, omdat ze anders de hele tijd alle rechten hebben en dat vergroot de risico's.

Wat we zien is iets heel anders: in plaats van een smartcard voor de beheerder hebben we een procedure met een envelop.Want die beheerders moeten op al die dozen aanloggen met lokale accounts. Als we de toegang voor beheerders erbij betrekken dan is de Sign On nooit Single geweest.

In de post-jericho-tijd is dit de realiteit: als organisatie kun je niet de enkelvoudige sterke authenticatie afdwingen op de eigen tablet waarmee de klant toegang zoekt, de medewerker thuiswerkt of op de cloudapplicatie die de gekozen technologie niet ondersteunt. Wil je de toegang gecentraliseerd beheersen (en beheren), zullen hiervoor een andere manier moeten bedenken. En dat kan. Sommige organisaties zijn hier al mee bezig. Hoe ziet zoiets er dan uit?

Je moet het kind natuurlijk niet met het badwater weggooien. Je wilt wel dat gebruikersaccounts zo gecentraliseerd mogelijk zijn, voor auditing en provisioning. Het wordt dus wel een geünificeerde login. Laten we het de Unified Sign On noemen, de USO. Zo'n omgeving zal gebruik maken van directories (je zult de users toch ergens moeten opslaan) en het daarbij

[106] http://www.opengroup.org/jericho/vision_wp.pdf
[107] http://nakedsecurity.sophos.com/2012/07/13/yahoo-voices-poor-passwords/

gebruikelijke LDAP. Omdat niet alleen medewerkers toegang moeten hebben, maar ook mensen van buiten, zul je verschillende directories inzetten.

De interne directory geeft ook LAN toegang, alle andere gebruikers doe je op een extern gerichte directory die geen Kerberos doet. Beide logins koppel je aan een federatieve login, waarbij je met een trucje die Where Are You From[108] wegmoffelt. Klein beetje extra werk, een stuk minder sores.

Op de netwerk-laag zal de USO een Multi-protocol voorziening zijn. Dat Multi-protocol komt zo: het klassieke SSO project bevatte onlosmakelijk de term kerberisatie: de aanpak om alle logins koppelen aan de login van AD. Dat is een prima aanpak: Kerberos is een mooi protocol en cryptografisch sterk. Maar het heeft een vervelende beperking; het werkt niet op het internet. Op internet gebruiken we SSL of niets. Nu kunnen we in het netwerk wel SSL gebruiken, maar SSL is zwakker dan Kerberos, met name vanwege de offline rootCA en omdat we het altijd single side gebruiken. Voor dual side moet je continu die certificaten verversen op al die PC's en zeg nou zelf, daar hebben we toch geen tijd voor?

Internet SSL is bovendien gebonden aan de Internet namespace (de common name in het certificaat bevat de hostname) en dat werkt weer niet binnen een afgesloten namespace. Dus een Unified Sign On die systemen binnen en buiten bestrijkt zal geen technische eenheid zijn; het zal een samengesteld systeem worden dat op de grens tussen binnen en buiten Kerberos tickets omzet in SSL tokens en vice versa.

Bovenstaande Unified Sign On wordt in de praktijk vormgegeven met SAML en WS-FED standaarden, met uitlopers naar specifieke technologieën met andere protocollen. Daar horen producten bij als OpenAM en ADFS. Dergelijke Federatieve producten worden intussen meer en meer uitgebreid met ondersteuning voor sterke authenticatie, zodat de centrale login voorzien kan worden van extra beveiliging. Als deze centrale login alleen voor medewerkers is, dan is het mogelijk hiervoor te kiezen en iedere medewerker een hardware token te geven.

Het is echter opeens veel lastiger als klanten en medewerkers van zakenpartners ook toegang moeten krijgen, of van die lastige mensen met die eigen apparaten. Nu is het mogelijk een tweede centrale login op te stellen die een zwakkere login toestaat, maar dat is dan weer hoogst onlogisch; waarom moeten vertrouwde medewerkers méér moeite doen om ergens bij te komen? Bovendien is een centrale login niet meer centraal als er twee zijn. Waarschijnlijk zal de integratie met wat erachter zit ook losser worden, wat het geheel onveiliger maakt.

De oplossing is differentiatie: verschillende gebruikersgroepen via dezelfde login /andere authenticatiemethodes/ bieden. De logische volgende stap is deze differentiatie ook te gebruiken voor de verschillende device typen. Dit mondt dan uit in een step up systeem waarbij de gekozen applicatie een vereist authenticatiemiddel krijgt, en dat op basis van een aantal variabelen. Zo zal een eigen medewerker die met een beheerd werkstation vanuit het eigen LAN aanlogt met een zwakker authenticatiemiddel toe kunnen dan dezelfde medewerker vanaf een privé tablet thuis. Hiermee komt de identiteit en de locatie van de device in de beveiligingsafweging bovendrijven, als extra variabelen in een Risk Based Access control.

Het plaatje wordt echt mooi als ook binnen een applicatie gedifferentieerd kan worden. Zo zal deze medewerker aanvullend moeten authenticeren als hij een gevoelige transactie wil uitvoeren: als je honderdduizend euro wilt overmaken vanaf je thuis PC, moet je het One Time Password

[108] http://saml.xml.org/blog/saml-20-usability

invullen dat op je hardware token verschijnt. Heb je dat al gedaan in een sessie, dan hoeft dat niet nog een keer.

De eerste applicatieservers die dergelijke differentiatie ondersteunen zijn inmiddels beschikbaar, en step up is de ontbrekende schakel in toekomstige toegangsoplossingen. Het wordt dus tijd om de traditionele RBAC matrices uit te breiden met devices en locaties, want de rol van een persoon is al lang niet meer het enig relevante gebruikersattribuut in een toegangssysteem.

Een dashboard zonder stuur

Vrijdag 25 januari 2013

De dag begint goed hier in het Security Operations Centre. Er ligt een bericht van de NCTV dat niet nader benoemde randfiguren het voorzien hebben op kwetsbare systemen van organisaties, mogelijk zelfs in ons land. Nadere details ontbreken, maar de coördinator nationale veiligheid zal ons aanstonds op de hoogte brengen zodra dit spannende verhaal nieuwe ontwikkelingen vertoont.

Ik zit op het puntje van mijn stoel.

Uit de Deepsight[109] dienst blijkt dat er een aantal kwetsbaarheden is ontdekt in een PHP script en een aanzienlijk aantal defecten in Microsoft software, waar vooralsnog geen patches voor zijn. Naar verluidt wordt één van de defecten in het wild gebruikt voor aanvallen. Voor de andere is geen informatie over daadwerkelijke aanvallen bekend. De defecten zitten in ieder geval in een aantal nieuwere versies van gangbare producten, zowel in Windows 2008 in alle versies behalve één, en in een aantal niet nader aangeduide Office 2010 producten. Over de mogelijke impact op oudere software in de extended support wordt niet gerept. De verwachting is dat de volgende patch Tuesday een ingrijpende wordt, maar het is niet zeker dat alle defecten gefixed worden.

Afwachten dus.

Deepsight meldt verder dat er erg veel gescand wordt op TCP 3389, die gebruikt wordt door Microsoft Remote desktop. De PKI groep op LinkedIn meldt dat er een ontwerpfout zit in het SCEP protocol, en dat deze in veel implementaties voorkomt. Het Internet Storm Centre[110] zegt dat 2,9% van alle poortscans op poort 3389 gericht is. Het ISC ziet echter wel een spike in TCP 23682 verkeer. Mja. Bittorrent.

Dat is heel bedreigend. Jaja.

Maar goed, volgens Deepsight is de wereldwijde status groen. Volgens ISC ook. Volgens de Nederlandse overheid **ook**. Hoewel de laatste update[111] al weer van een week geleden is.

Dus het is niet bedreigend. Ook goed.

Op Full Disclosure is een heftig debat van onduidelijke kwaliteit gaande tussen de vaste gasten over een denial of service die eventueel zou kunnen leiden tot een stack overflow in een browser die op veel mobiele devices geïnstalleerd is.

Zucht.

In de firewall logs zie ik dat een Belgische host continu een half open connect doet naar een bridgehead mailserver in de DMZ, en de IDS laat zien dat er vanuit een aantal Chinese netwerken connects worden opgezet met een aantal developersystemen in het netwerk van een dochterbedrijf. Maar ja, dat zit ook in een joint venture met een Chinese toko, dus of dat wat betekent?

---

[109] https://tms.symantec.com/
[110] https://isc.sans.edu/
[111] http://www.waarschuwingsdienst.nl/

Informatie, informatie. Héél véél informatie. En dat moet allemaal geclassificeerd worden. Saai werk, maar de schoorsteen moet roken.

Het NCTV bericht vind ik niet specifiek genoeg; ik zie geen reden dat het ónze organisatie zou kunnen raken en daarom zet ik hem op 'laag, laag'. Dat staat voor: waarschijnlijkheid laag, impact laag. Dat PHP script dat ken ik niet en ik weet niet of we dat ergens gebruiken. 'Laag, laag' dan ook maar. Gaten in Microsoft: of dat speelt in de versies met de patchlevels die we hier hebben, kan ik niet bepalen. Ik gooi hem op 'laag, midden'. Want ja, we hebben vast wel iets van die spullen. SCEP? Nooit van gehoord. Laag, laag. Wat zal ik eens met die Chinezen doen?

De vraag hier luidt: wat is het nut van classificeren van bedreigingen? De theorie ken ik, het gekozen Security Framework schrijft dit voor, opdat we de actuele bedreigingsniveaus kunnen bewaken. Deze worden getoond op het 100 inch scherm op 'de brug', ons management dashboard waarop iedereen in één oogopslag kan zien hoe veilig het is. Groen betekent veilig, oranje staat voor bedreigingen die niet acuut zijn. En rood… nou ja, je begrijpt me wel.

Dat scherm hangt er nu ongeveer een jaar en vormt inmiddels een vast punt bij iedere rondleiding. Er verschijnen vaak hele delegaties mannen in pak op de tribune achter de brug, soms zelfs mannen in uniform. Security is nu eenmaal een hot topic en het management dashboard is een goede methode om 'het' zichtbaar te maken. Het is wellicht zelfs de enige methode, want hoe laat je een mogelijke aanval op een niet nader bekende host zien?

Sommige cynici in ons team noemen het dashboard managementporno. Dat kan ook, maar wat ik zelf zo merkwaardig vindt is dat dit dashboard alleen maar verklikkerlichtjes heeft, en geen stuur. Als ik een paar bedreigingen op 'hoog, hoog' zet, of zelfs maar op 'midden, hoog', wat dóen de bestuurders 'op de brug' van dit beveiligingsapparaat dan?

Een tijdje terug kreeg ik het antwoord op de vraag. Mijn collega Threat Analysts en ik hadden een paar zaken tegelijk op 'midden, hoog' en 'midden, midden' gezet en jawel, direct lichtte het grote scherm omineus oranjerood op. Een enorme heisa barstte los, de brug liep vol zorgelijke stropdassen en volgens mij zag ik zelfs een minister met haar neus tegen de ruit gedrukt staan dus dan is er echt iets aan de hand. Dat was tot daar aan toe, maar iedereen moest vervolgens in de buurt blijven; Alle Hens Aan Dek en Alle Verloven Ingetrokken. Een typerende uiting van bestuurlijke daadkracht. Alsof de IPS-en beter werken als wij maar goed naar de web interface blijven kijken. Ik bedoel maar, we kunnen niets aan de verdediging veranderen zonder een change proces van een paar weken te doorlopen, dus meer dan naar het scherm turen zat er niet in.

Ik zet dus nooit meer iets op midden en al helemaal niet op hoog. Sommige collega's doen dat wel, maar dat is dan omdat ze een bepaald project willen of omdat ze van hun account manager een paar collega's binnen moeten hengelen. So much voor classificatie.

Dus, volgende vraag: wat betekent besturen van beveiliging, eigenlijk? Hoe sturen de bestuurders de veiligheid? Ze hebben niet eens een stuur. In de praktijk hebben ze alleen een gaspedaal en een rem meer of minder mensen inzetten en een dodemansknop alle verbindingen dichtzetten waar een heel groot bord bij hangt dat misbruik gestraft wordt.

Wat doet zo'n bestuurder dan zoal, de hele dag? Zit dat daar maar een beetje verantwoordelijk te zijn en een naventante schaal op te strijken? Ron, de nachtchef hier op de brug, geeft dat gewoon toe, als er niemand bij is tenminste, dat security management eigenlijk een heel nikserig beroep is. Paniekvoetbal of rust maar niets daartussen, zoals hij het zegt.

Dit fenomeen speelt overal volgens mij. Zo las ik dat security held Ronald Prins van Fox IT ziet[112] dat de digitale veiligheid ook van rijkswege niet gestuurd wordt. Ja, logisch toch? Besturen bij de overheid is ook alleen een kwestie van een gaspedaal en een rem? Ik bedoel maar zo: gaat er iets mis, dan gaat er meer geld heen en gaat het niet meer echt fout, dan halen ze dat geld weer terug. Gas en rem. Maar ze noemen het sturen. De enige bestuurder die zo kan rijden is een treinbestuurder en zijn spoor ligt van tevoren vast. Dat kun je van IT security niet zeggen. Wij hebben geen rails liggen. Nee, ook al die hoogdravende claims van de systeemdenkers met de imposante slidedecks van methode XYZ of ABC vormen geen rails.

De governance crisis waar Ronald het over heeft speelt wereldwijd, niet alleen bij de Nederlandse overheid. Daarom verliezen[113] we de strijd tegen de 'bad guys'. De IT security verkeert in een existentiële crisis; we krijgen meer geld en daardoor steeds meer specialisten die kunnen adviseren hoe een ander het moet doen, maar tot meer dan een kakofonie van adviezen leidt dat niet. En de bestuurders, die geven nog maar eens wat gas of die remmen maar weer eens wat bij.

Je lost het niet op door te doen wat de specialisten zeggen, want zij zeggen allemaal wat anders. Het lijkt er toch op dat bestuurder bij gebrek aan beter maar luistert naar de persoon die het verhaal het best kan inpakken in een elevator pitch of het verhaal dat het beste past bij de overtuigingen die de bestuurder toch al heeft. Net als bij de economische crisis dus, want ook economen zeggen weer allemaal wat anders en zo zijn we hard op weg naar de triple dip. Meer geld naar die en minder geld naar die – pappen en nathouden is het, meer besturing is er niet.

Met bestuurders die niet weten waar je heen moet, kom je nergens. Besturen is blijkbaar de kunst van het laveren tussen wat de goeroes te vertellen hebben. Voorwaar geen geringe opgave; daar zouden ze eens een procedure voor moeten schrijven. Wat mij het meest beangstigt, is dat het de meeste bestuurders niet eens is opgevallen dat ze geen stuur in handen hebben.

[112] http://www.thehollandbureau.com/2013/01/15/the-governance-gap-an-interview-with-fox-its-ronald-prins-pt-i/?goback=%2Egde_4101749_member_205665295%20
[113] http://www.presstv.ir/usdetail/233604.html

Nawoord

Ik wil voor de columns de mensen bedanken die bij de originele plaatsing nooit bedankt zijn maar zonder wiens hulp, ideeën en bereidheid om als klankbord op te treden, deze columns nooit tot stand waren gekomen.

Bovenal wil ik mijn echtgenote, Anneke Paul bedanken voor het jarenlang redigeren van al mijn kromme zinnen en taalkundige nukken en het toevoegen van de nodige droogkomedie en het helpen ontdekken van mijn toonsoort. Dank ook voor de redactie van security.nl voor het bieden van een plekje op hun mooie platform. Dit is ook de plek om mijn vaste meelezers/meedenkers te bedanken, Suzanne Visschedijk en Tiel Notenboom. Ook wil ik al mijn collega's en ex-collega's bij Traxion bedanken die tijd, ruimte en inspiratie gaven, in het bijzonder John van Westeneng, Evert van den Branden, Gijs van der Laken, Daniëlle Kaland, Frank Peeters, Dennis Lauw, Philip van Gendt, Amar Ramdaras, Bram van Pelt en Eric Ernst.

Veel ideeën en inspiratie heb ik ook uit mijn bredere netwerk gekregen. Ik kan hier uit die groep niet iedereen benoemen, maar ik wel de steunen en toeverlaten van de Dutch Cyberwarfare Community, Ad Koolen en Don Eijndhoven expliciet bedanken. Tenslotte wil ik Cees Paul en Erica Rietveld bedanken voor de onmisbare achtergrond en inzichten rond de respectievelijk financiële wereld en leiderschap en organisatiekunde.

“De IT security verkeert in een existentiële crisis; we krijgen meer geld en daardoor steeds meer specialisten die kunnen adviseren hoe een ander het moet doen, maar tot meer dan een kakofonie van adviezen leidt dat niet”.

“Het lijkt er toch op dat de bestuurder bij gebrek aan beter maar luistert naar de persoon die het verhaal het best kan inpakken in een elevator pitch of het verhaal dat het beste past bij de overtuigingen die de bestuurder toch al heeft”.

“Besturen is blijkbaar de kunst van het laveren tussen wat de goeroes te vertellen hebben. Wat mij het meest beangstigt, is dat het de meeste bestuurders niet eens is opgevallen dat ze geen stuur in handen hebben”.

Peter Rietveld beschrijft in een reeks eerder online verschenen columns hoe cyber security, zoals het tegenwoordig heet, ervoor staat. Stuurloos en kansloos.