De Toekomst van Toegang

Naar een fundamentele herschikking van beveiliging

TRAXION

Partners in Information Security

Uitgever: Traxion Consultancy BV
ISBN/EAN 978-90-820522-0-6

Deze uitgave wordt u aangeboden door Traxion, Partners in Information Security

www.traxion.com

Tijd voor een nieuwe wind

We leven in tijden van verandering. Mede als gevolg van digitalisering werkt de maatschappij al lang niet meer als twintig jaar geleden. Deze verandering lijkt in het dagelijks leven te zijn geslopen zonder dat mensen zich hier heel bewust van waren. Sommige staten en veel criminelen hebben dit al goed begrepen, maar overheid en bedrijfsleven lijken dit onvoldoende te beseffen.

Verouderde benaderingen van cybersecurity – mede ingegeven door wetgeving – hebben wel enig effect, maar blijken de problematiek toch niet zo te benaderen dat we de strijd goed voeren. Dat komt aan de oppervlakte als we hackers die aan de bel trekken als crimineel benaderen. Het vijandsbeeld lijkt compleet verkeerd te zijn ingeschoten. Of het blijkt als een probleem maar stil wordt gehouden zonder te beseffen dat andere organisaties met dezelfde software ook tegen exact dezelfde problemen aan lopen.

Maar een van de veranderingen is dat 'binnen' en 'buiten' nauwelijks bestaan en dat de echte waarde om te verdedigen in bits en bytes zijn vastgelegd. Peter Rietveld problematiseert dit terecht in zijn boek en weet dit goed te duiden. Waar anderen met het constateren zouden ophouden gaat Rietveld verder. Hij denkt na over oplossingen en doet nuttige handreikingen om de problemen aan te pakken.

Dit boek is de moeite waard om te lezen, erover te spreken en te zoeken naar het in stelling brengen van oplossingen. Niet alleen in de organisatie, maar juist met iedereen eromheen. Wees blij als je kritisch wordt benaderd, wees blij met de kans eindelijk na te denken over welke waarden er in het bedrijf zijn en hoe ze moeten worden beschermd en wees blij ICT over een andere boeg te gooien.

Rietveld reikt hier de hand om te beginnen met een verandering die ons uiteindelijk veilig de informatiemaatschappij in brengt. Wie die kans niet grijpt doet niet alleen zichzelf tekort, maar bewijst ook de maatschappij geen dienst. Dat kan ik niet alleen zeggen na het lezen van zijn boek, maar ook na het omgaan met letterlijk honderden datalekken.

Brenno de Winter
ICT-onderzoeksjournalist
Maart 2013

Voorwoord

De inspanning die organisaties leveren om informatie en informatievoorzieningen te beveiligen neemt ieder jaar toe. De kosten stijgen terwijl de boel minder veilig lijkt te worden. Dagelijks zijn er berichten in de pers over datalekken, cyberspionnen en cybercriminelen. Ook specialisten stellen openlijk dat de criminelen aan de winnende hand zijn. De trend heeft een omineuze richting. Is de groei van de bedreigingen zodanig dat er nog meer geïnvesteerd moet worden en houdt het ooit op? Of is al dat geld weggegooid omdat we het verkeerd aanpakken?

Het antwoord is, zoals te verwachten viel, genuanceerd. Per organisatie neemt het aantal bedreigingen daadwerkelijk toe. Door de snellere verbindingen en het gebruik van meer technologie door organisaties kunnen meer aanvallers op meer manieren aanvallen. Aanvallers kunnen dankzij de technologie meer doelen bereiken, zodat voorheen lokale criminelen wereldwijd kunnen opereren. Aanvallers kunnen door automatisering meerdere doelen tegelijk aanvallen en de aanvallen langdurig volhouden. De verdediging loopt stelselmatig achter de feiten aan, waarbij zeker een deel van de inspanningen niet rendeert en er met enige regelmaat een kostbare inhaalslag gemaakt moet worden. Er is dus ruimte voor verbetering en doelmatigheidswinst: de beveiligingsinspanning zal sneller moeten reageren op nieuwe situaties en daarbij minder lokaal georiënteerd, meer toekomstgericht en proactief moeten zijn.

Om deze noodzakelijke verbeteringen te kunnen realiseren is het essentieel de trends en de oorzaken te onderkennen. Een belangrijke oorzaak van het huidige falen van beveiliging is gelegen in uitbreiding van menselijke capaciteit in informatiebeveiliging. Deze is van zeer recente datum, met als gevolg dat het kennis- en ervaringsniveau lager ligt dan wenselijk is. Bedenk hierbij dat voor verdedigen veel meer kennis nodig is dan voor aanvallen. Een aanvaller hoeft maar één defect te vinden om succes te hebben, de verdediger moet alle gaten dichthouden die een aanvaller zou kunnen vinden om evenveel succes te hebben. Het ervaringsgebrek is gelukkig van voorbijgaande aard, maar de asymmetrie blijft.

Dit is niet de enige oorzaak. De aard van de werkzaamheden heeft namelijk ook een weerslag op de mensen die eropaf komen. De aanvaller heeft het voordeel van het initiatief, de verdediger moet gestructureerd werken en moet alle fronten afdekken. Terwijl de aanvaller creatief de gaten zoekt en vrijelijk innoveert, zijn beveiligers aan het conserveren. Beveiliging trekt dan ook eerder mensen met een conservatieve inslag en mensen die van structuur, orde en netheid houden. Met alle degelijkheid in de beveiligingsaanpak mist de verdediging flexibiliteit en snelheid. In een periode van snelle technologische verandering is een combinatie van pragmatisme en initiatief doorslaggevend.

Naast dit stijlverschil is er ook het besturingsvraagstuk. Aanvallers zijn autonoom en kunnen snel inspelen op nieuwe kansen. Dit geeft het voordeel van het initiatief. Beveiliging is echter reactief georganiseerd. De agenda van beveiliging wordt gedomineerd door beveiligingsincidenten in de eigen organisatie. Dit is goed verklaarbaar maar leidt tot een naar binnen gerichte houding. Incidenten bij andere organisaties worden zelden besproken. Als ze al besproken worden, worden ze niet geprojecteerd op de eigen omgeving. Hierdoor wapenen de meeste organisaties zich alleen tegen aanvallen die het proces doorlopen hebben waarmee ze in de Best Practices terecht komen. Afhankelijk van welke Best Practices gekozen worden als leidraad, leidt dit tot een achterstand van enkele maanden tot meerdere jaren. Door de huidige werkwijze beveiligen wij ons dus tegen aanvallen van vijf jaar geleden. Of langer. Het gevolg is: onvoorspelbare kosten en onbevredigende resultaten. Het enige dat zeker is, met de huidige aanpak, is dat de beveiliging achter de feiten zal blijven aanlopen. Dat is gewoon niet goed genoeg.

De leerboeken informatiebeveiliging versterken deze conservatieve cultuur. Tot niet zo lang geleden was beveiliging primair een zaak van het netwerk, omdat aanvallen conform het beveiligingsdenken daar tegengehouden moesten worden. Daardoor heeft een overheersend deel van de conceptuele kaders, de leerboeken én de ervaren krachten in informatiebeveiliging een achtergrond in netwerken. De aanvaller heeft zijn aandacht, mede door de maturiteit die beveiliging op de netwerklaag inmiddels heeft, verplaatst naar de applicatielaag. De verdediging is nog grotendeels verbonden aan de netwerklaag. Voor netwerkbeheer is beschikbaarheid het hoogste doel, wat leidt tot de keuze van degelijkheid boven features. Beveiliging heeft last van de culturele en doctrinaire erfenis hiervan. De gevolgen in de beveiligingswereld zijn voorspelbaar; “we gaan beveiligen, maar dan wel met bewezen technologie”. Met tal van nieuwe soorten bedreigingen waar de technologie nog geen tijd heeft gehad om bewezen te worden is dit een contraproductieve houding. Het gevolg

van deze culturele erfenis is dus dat als er geen bewezen oplossing voor een probleem bestaat, de keuze gaat tussen een onbewezen oplossing van een onbekende leverancier en géén oplossing. Maar al te vaak wordt het de laatste.

Omdat vrijwel alle grote organisaties kiezen voor een “Proven Technology”-benadering zijn ook al de nodige nieuwe oplossingen weer verdwenen, omdat aanbieders van producten ook met de economische realiteit te maken hebben. De vendor space in beveiligingssystemen is hierdoor weinig innovatief en wordt gedomineerd door een zeer beperkt aantal grote leveranciers. De grote leveranciers baseren hun productstrategie meer op wat de concurrentie doet dan op wat de aanvallers uitspoken.

Om het samen te vatten: aanvallers zijn multidisciplinair, de verdediging is verkokerd. Om dit te doorbreken, en naar een proactieve en innovatieve inzet te komen, moeten beveiligers de blik naar buiten, naar het heden en de toekomst richten. In dit document bekijken we het heden en verleden met een kritische blik en kijken naar de lopende ontwikkeling en trends, bij wijze van blik in de toekomst.

Hoe organisaties hun beveiliging uitvoeren en ingericht hebben zal de komende jaren ingrijpend veranderen. Dat moet over de gehele linie van beleid tot uitvoering en technologie. De logheid, de bestuurlijke insteek, de verkokering, het structurele MAG-NIET en de ‘Centre of the Universe’ benadering zijn niet langer vol te houden. Als beveiliging blijft grossieren in afwachten en problemen en niet komt met oplossingen en uitvoerende flexibiliteit, dan is het einde van het vakgebied nabij. De traditionele beveiliger, met een achtergrond in beheer, netwerken of service management, zal samen moeten werken met innovatieve ontwikkelaars en nog lang niet bewezen oplossingen. De werkelijkheid van informatiebeveiliging verandert te snel voor een verkokerde benadering: Security Management staat voor de zware opgave de balans te zoeken, creëren en onderhouden tussen de botsende krachten van behoud en innovatie. Want beide invalshoeken zijn onmisbaar.

Peter Rietveld
Waardenburg, 12 maart 2013

Dit document is tot stand gekomen met bijdragen van en onmisbare ondersteuning door Eric IJpelaar, Erica Rietveld, John van Westeneng, Michiel Stoop, Martijn Broos en Sylvia van Wel. De cartoon is gemaakt door mijn dochter, Louisa Rietveld.

Inleiding

Informatiebeveiliging is op dit moment bovenal een intern georiënteerde inspanning met de focus op compliance en doelmatigheid, waarbij problemen van de auditor en de helpdesk opgelost worden. De omloopsnelheid van dossiers is vrij laag en de cycli zijn lang. Het invoeren van een andere antivirus-oplossing kan maar zo een project van een jaar zijn. Achter de dikke firewall is de urgentie laag; we voelen ons veilig achter een hoge dijk.

Deze besloten werkelijkheid is aan het veranderen. Beveiliging van ICT blijkt randvoorwaardelijk in het ontsluiten van organisaties naar de buitenwereld, naar klanten, naar ketenpartners en naar externe leveranciers. Daarbij gaat het zowel om technische integraties als om operationele samenwerking. De Cloud en de mobiele dimensie zijn hiervoor de belangrijkste aanjagers. De Cloud toont het definitieve einde van de buitenmuur van het eigen rekencentrum als primaire beveiligingslaag. Met de doorbraak van tablets en smartphones wordt de klassieke ICT Enterprise Security benadering geconfronteerd met de werkelijkheid van de consumentenmarkt en het verdwijnend onderscheid tussen werk en privé, tussen werknemer en klant. Zelfs het eigen personeel blijkt te bestaan uit consumenten die eigen keuzes maken die in het bedrijfsbelang zijn, in plaats van het beleid na te leven en passief af te wachten tot Corporate ICT eens met een vernieuwing komt. Hierdoor verandert de rol van Security van een Cost Centre in een Profit Centre en verschuift de nadruk van preventie meer richting optreden, van opleggen naar begeleiden en van beleid naar uitvoering.

Tegelijkertijd veranderen de bedreigingen waar informatiebeveiliging zich op richt. Traditioneel gaat de meeste aandacht naar ongewenste handelingen door eigen medewerkers, nu betreden we een wereld van criminelen, spionage en zelfs cyberwar. Dat betekent dat de bedreigingen veel meer van buiten komen. Zij zijn professioneler, gerichter, grootschaliger en kundiger dan ooit. Dit punt is door de APT (Advanced Persistent Threat) hardhandig duidelijk gemaakt.

Met de verschuiving naar de buitenkant van de organisatie veranderen de traditionele zwaartepunten van informatiebeveiliging, te weten beleid en user awareness, ingrijpend. Het beleid zal inhoudelijk anders zijn en bovenal minder dwingend, want het gaat veel meer over de buitenwereld. Bij user awareness gaat het minder om de interne eindgebruiker die je een opdracht geeft, maar om de ICT-organisatie die verandert van een leveringsorganisatie in een inkooporganisatie enerzijds en de klanten, die je moet overtuigen en binden anderzijds. Hierdoor verandert de hele aanpak; medewerkers kun je wellicht iets opleggen en interne processen kun je dwingen, bij externe leveranciers is dat veel moeilijker en kost elke handeling geld. Klanten zullen helemaal op een hele andere manier benaderd moeten worden.

De grootste gemene deler in deze ontwikkelingen is dat er een grote innovatiedruk vanuit gaat en het de omloopsnelheid van technologie en werkwijze omhoog dwingt. Hiermee wankelen de fundamenten van de ivoren toren waar Enterprise Security zich in opgesloten heeft. Deze boodschap heeft nog lang niet alle bewoners van de toren bereikt.

Dit document schetst de kaders en de consequenties van deze ontwikkelingen om organisaties en individuen te helpen plaats, positie en koers te bepalen in deze ingrijpende verandering.

Doelgroep

Dit document is bedoeld voor een ieder die zich bezig houdt met de toekomst van informatiebeveiliging; zowel bestuurders, specialisten, leveranciers als (technologie) consumenten. Het document richt zich in het bijzonder op die personen die in organisaties onderdeel zijn van de strategie-, visie- en besluitvormingsprocessen op het gebied van informatie en ICT-beveiliging.

Waar we staan

Het is niet eenvoudig om een duidelijk beeld van de toekomst van beveiliging te schetsen, maar zeker niet onmogelijk. Beveiligingstechnologie ontstaat in reactie (en dus met enige vertraging) op bedreigingen die zich in de praktijk voordoen en ontwikkelingen aan de vraagkant in de markt. Voordat beveiligingstechnologie 'op de plank' ligt bij de grote leveranciers, is er een heel traject doorlopen. Dat traject begint bij de beveiligingsconcepten en de eerste technologische producten in de Open Source wereld. Na een fase bij kleinere en beginnende leveranciers komt uiteindelijk de maturiteit en de doorbraak naar de bovenwereld als ze door de trendwatchers (zoals Gartner) worden gesignaleerd. Uiteindelijk worden de kleinere leveranciers opgekocht door de grote marktpartijen dan wel de kleine leverancier wordt zelf een grote marktpartij. Vaak duurt het dan nog een paar jaar voordat de oplossingen op de agenda van de beveiligingsontwerpers staat. Een complete cyclus kan zo tien jaar in beslag nemen.

Als goed voorbeeld mag het SAML[1] protocol dienen. SAML is een lichtgewicht protocol waarmee versleutelde beveiligingstokens over verschillende (web) domeinen gedeeld kunnen worden. Dat is een erg handig middel binnen conglomeraten die technisch uit meerdere domeinen bestaan, of voor organisaties die samenwerken met andere organisaties en daarmee informatiesystemen delen. Een snelle invoering lag dan ook voor de hand. Maar zo werkt het niet.

Na een inceptiefase van een aantal jaren (1996-2002[2]) verscheen in 2004 de eerste door grote leveranciers beschreven documentatie en kwamen de eerste commerciële producten. De doorbraak van SAML naar de

[1] Security Assertion Markup Language, een protocol voor het delen cross-domain van authenticatie ten behoeve van beveiligde netwerksessies.
[2] In 2002 verscheen de eerste formele versie van de SAML standaard. Voorlopers en bijbehorende open source producten waren op dat moment al jaren in productie.

mainstream vond echter pas plaats in 2011-2012. De meeste organisaties hebben tot nu toe veel zwaardere, kostbaardere en complexere middelen ingezet om hetzelfde functionele doel te bereiken. Zij zijn nu pas bezig met de eerste implementaties van SAML en worstelen vandaag met concepten die vijftien jaar geleden uitgekristalliseerd zijn. Voor andere verbeteringen geldt een vergelijkbare gang van zaken en een vergelijkbaar tijdspad. Voor de tijdshorizon gekozen voor dit document gebruiken we bovenstaande ervaringen.

De cyclus van 'de tegenpartij' is minder lang, maar ook daar geldt dat er leiders en volgers zijn, en dat er kenbare ontwikkelingen zijn. Bedreigingen evolueren en er zijn trends. De trends zijn goed te volgen door het dagelijks spellen van het beveiligingsnieuws, iets wat met de opkomst van sociale netwerken een stuk beter te doen is dan voorheen. Deze studie heeft veel te danken aan een aantal discussiegroepen op LinkedIn, naast de traditionele bronnen als Securityfocus en Full Disclosure. Naast dit dagelijkse nieuws zijn er bij tijd en wijle belangrijke studies van meer theoretische aard die onderbouwde voorspellingen doen over zwaktes en aanvallen. De nieuwste trend waarbij PKI-certificaten ingezet worden voor aanvallen zijn al in 1994 door de Nieuw-Zeelandse professor Peter Gutman voorspeld, en de aanhoudende reeks zwaktes in de productenreeks van Microsoft Windows tot en met 2008 zijn in 1997 in een architectuuranalyse in Dr. Dobbs magazine al aangekondigd.

In dit document worden de belangrijkste trends aan de vraagkant als uitgangspunt genomen en doorgetrokken. De trends geven inzicht in het spanningsveld waar organisaties in meer of mindere mate nu al aangaande hun informatiebeveiliging aan onderhevig zijn. Met het doortrekken van trends komen de knooppunten van de komende jaren in beeld. Daarna worden de ontwikkelingen aan de aanbodkant erop geprojecteerd. Dit document gaat uit van vijf hoofdtrends, die gezamenlijk de richting bepalen:

1. Consumerisatie en Deperimeterisatie
2. De Just In Time economie
3. Nieuwe dreigingen op het digitale front
4. The Internet of Things
5. De regieorganisatie

Consumerisatie en deperimeterisatie

De perimeter is de buitenmuur van een organisatie, waar slechts enkele goed bewaakte toegangspoorten in aangelegd zijn. De perimeter is het belangrijkste onderdeel van de beveiliging; een systeem dat niet benaderd kan worden van buiten, kan ook niet aangevallen worden van buiten.

Door een aantal gelijktijdige technologische ontwikkelingen die wel worden gevat onder het begrip consumerisatie[3], zoals Outsourcing, Het Nieuwe Werken (HNW), Cloud Computing en As a Service, Social Media, Mobile devices, Bring Your Own Device (BYOD) en Big Data[4] is het aantal te bewaken 'poorten' in de buitenmuur om de bedrijfsinformatie enorm gegroeid. In principe is iedere smartphone die 'aan het netwerk hangt' een gat in de buitenmuur, omdat het een multihome device is. Onder de traditionele beveiligingskaders was dit absoluut taboe; een multihome systeem kan als brug tussen de verschillende netwerken fungeren en gebruikt worden om de firewall te omzeilen. Daarom gingen Best Practices in de jaren '90 zo diep in op pc's met modems. Als gevolg van outsourcing en de Cloud delen bedrijven nu infrastructuur met elkaar, zodat de kans dat een organisatie schade oploopt door een aanval op een ander, als collatoral damage, steeds groter wordt. Tevens is daarmee de hoeveelheid informatie van de Enterprise die niet binnen het eigen fysieke of zelfs maar ingehuurde domein woont, enorm gegroeid, zoals nu zichtbaar wordt in de Big Data discussies. We zijn voorbij het punt waarin de buitenmuur een bruikbaar begrip in informatiebeveiliging is. Dit wordt aangeduid met de term Deperimeterisatie, een beetje moeizaam woord dat in 2005 is uitgevonden door het Jericho Forum[5].

Door de consumerisatie is het aantal punten waarop een organisatie aangevallen kan worden en dat dus verdedigd zou moeten worden, sterk gegroeid. De financiële en operationele voordelen voor de business van

[3] http://cio.nl/opinie/50134/consumerization-is-veel-meer-dan-byod.html
[4] Big data is in strikte zin geen eigendom van het bedrijf. Gegeven de relevantie en het gebruik ervan is het echter wel noodzakelijke informatie en dus wel degelijk bedrijfsinformatie. Zeker waar het informatie over het bedrijf betreft.
[5] www.opengroup.org/jericho/vision_wp.pdf

consumerisatie zijn van die ordegrootte, dat beveiliging mee móet. Deze voordelen worden vanuit beveiliging vaak betwijfeld en zullen wellicht minder groot zijn dan sommige voorstanders beweren. Tegen zijn is echter geen reden deze zeer ingrijpende ontwikkeling te negeren.

De Just In Time economie

De concrete uitwerking van een geglobaliseerde economie leidt ertoe dat organisaties in nauwe samenwerking met ketenpartners optreden. Organisaties hebben massaal gekozen voor het model van kerntaken; de meanderende conglomeraten van het verleden zijn vrijwel uitgestorven en zelfs al grotendeels verdwenen uit het bewustzijn; welk bedrijf heeft nog een eigen technische dienst, eigen kantinepersoneel of bezit haar eigen vastgoed of voertuigen? In dit licht beschouwd is ook begonnen met het uitbesteden van complexere diensten als de ICT en de administratie, een ontwikkeling die minder succesvol is.

De opvolger van het conglomeraat is een keten van samenwerkende kleine en zeer specialistische bedrijven met 'korte voorraden'. Het huidige model schrijft voor dat organisaties met minimale reserves en minimale voorraden werken, zodat er zo min mogelijk kapitaal vast zit in de productieketen en de marges maximaal zijn. Vanuit logistiek is de naam hiervoor het 'Just In Time' model, zaken worden pas geproduceerd als er een kooporder is. De Just In Time economie is afhankelijk van goede en snelle communicatie in de productieketen en het logistieke apparaat. Dit is een belangrijke drijfveer voor integratie van ICT-systemen.

Dit model is ook buiten de traditionele industriële bedrijven ingevoerd. Voor innovatie wordt samengewerkt met gespecialiseerde onderaannemers, inclusief onderwijs- en researchinstellingen, met als hoofddoel de time-to-market van nieuwe producten na een innovatie zo kort mogelijk te houden. Personeel wordt zoveel mogelijk ondergebracht in een 'flexibele schil' van zzp'ers en andere flexkrachten. Vaste kostenposten als kantoorgebouwen en ICT-voorzieningen dienen als het enigszins mogelijk is vermeden te worden; het ideaal van de flexibele schil is dat zij zelf zorgt voor haar voorzieningen. Dat leidt ertoe dat een flexmedewerker zichzelf inroostert, zelf de vergaderplek boekt en werkt op de eigen laptop. In alle varianten van deze flexbenadering worden bedrijfsprocessen met ICT-middelen aan de buitenkant van de organisatie ontsloten. In alle scenario's spelen beveiligingsvraagstukken die niet passen binnen de traditionele denkkaders van informatiebeveiliging.

Nieuwe dreigingen op het digitale front

De meeste aandacht van beveiliging is in de regel gericht op de interne organisatie: beveiligingsbeleid, security awareness voor de medewerkers en fijnmazige autorisatiemodellen voor de interne infrastructuur. Security leerboeken stellen – nog steeds – dat 70 tot 80% van alle beveiligingsbedreigingen van binnenuit komt[6], en de meeste aandacht en budget van beveiligingsorganisaties is dan ook op deze dimensie gericht.

De laatste jaren is er een aantal bedreigingen bijgekomen, zodat we de aandacht meer naar buiten moeten richten. In dit document komen daarvan een aantal in meer detail terug, voor nu volstaat een lijstje met een paar bekende fenomenen:

- Cyberwar: het gebruik van de digitale dimensie in de internationale politiek, door overheden en krijgsmachten, zoals met Stuxnet en Flame.
- APT (Advanced Persistent Threat): geavanceerde, gerichte en georkestreerde langdurige aanvallen op organisaties[7].
- Cybercrime.

Het aantal en de kunde van de aanvallers waartegen een organisatie zich moet verdedigen, is hiermee sterk gegroeid.

The Internet of Things

Voor de meeste mensen is automatisering heel concreet en tastbaar: het zijn computers, laptops en servers. Allemaal dingen met een beeldscherm, een toetsenbord en een stekker. In organisaties vallen al deze zaken

[6] http://www.zdnet.com/insider-threats-evolving-still-main-risk-7000003491/
[7] http://en.wikipedia.org/wiki/Advanced_persistent_threat

dan ook in één bestuurlijk domein, dat van de ICT. Beveiliging van dat soort zaken is dan ook aan het ICT-domein gekoppeld. Dat is een hele heldere indeling. Helaas valt daardoor steeds meer overboord. Industriële automatisering is traditioneel al een ondergeschoven kindje in de beveiliging geweest, zoals de kwetsbaarheden van SCADA[8] de afgelopen jaren duidelijk aantoonden. Dergelijke systemen vallen in de regel niet onder ICT security. Maar industriële automatisering is niet het enige van dit soort dossiers; de witte automatisering (ziekenhuissystemen) kent ook al jaren een vergelijkbaar probleemgebied: zo hebben nu gangbare ziekenhuisscanners nog steeds embedded Windows NT als besturingssysteem. Dit knelpunt komt vrijwel alleen in de industrie en de zorg voor en is daardoor onder de radar van de meeste beveiligingsdenkers gebleven.

De heldere kaders beginnen echter ook in andere sectoren te vervagen – steeds meer informatietechnologie wordt onderdeel van andere apparaten. Tablets, telefooncentrales en mobiele telefoons zijn al bestuurlijke probleemgebieden. Er wordt menig bestuurlijk loopgravengevecht om gevochten. En nu vraagt de leverancier van de koffiemachines ook al toegang tot netwerk.

Sinds een jaar of twee, drie zijn de mobiele telefoons aan de mailserver gekoppeld en het is een kwestie van tijd voordat de communicatiesystemen in de auto's van de medewerkers gekoppeld worden. De term The Internet of Things wordt gebruikt om deze ontwikkelingen te vangen; initieel (vanaf 1999) om de impact van RFID chips te vangen, inmiddels wordt het begrip steeds breder ingezet. Een goed voorbeeld is Vehicular Management: voor toekomstige personenauto's zijn al grote aantallen IPv6 adressen gereserveerd, zodat remote diagnostics en zelfs remote repair via het Internet mogelijk wordt[9]. Het is een logische ontwikkeling dat deze voorzieningen ook aan het bedrijfsnetwerk worden gekoppeld; een simpele koppeling tussen de agenda met afspraken en het navigatiesysteem in de auto zal menig beroepschauffeur veel tijd besparen. Omdat Vehicular Management veel informatie geeft over het rijgedrag zal dit ook de wagenparkbeheerder aanspreken, maar tevens de aandacht vragen van de Privacy Officer. Een dergelijke koppeling is vanuit beveiligingsperspectief een uitdaging, want de boordcomputer van het voertuig wordt onderdeel van het vertrouwde netwerk. Er zijn tal van vergelijkbare ontwikkelingen gaande, waarvan de impact nog verre van te overzien is. Bij de nieuwste verkeersvliegtuigen van Boeing is letterlijk ieder belangrijk component zelfstandig aan het Internet verbonden[10]. Het kan nog even duren voor het doordringt, maar het moment is in zicht dat de belangrijkste beveiliging van de burgerluchtvaart tegen terrorisme niet meer het douanepoortje is, maar ICT security. Door The Internet of Things groeit het aantal en de diversiteit van de systemen die verdedigd moeten worden, enorm.

De regieorganisatie

ICT-afdelingen veranderen steeds meer van interne leverancier tot integrator van wat externe leveranciers leveren. De ICT-afdeling ontwikkelde tot voor kort zelf spullen, huurde handjes in van ICT-bedrijven (het detacheringsmodel) en kocht van vendors halffabricaten en eindproducten. Ze verandert nu in de Broker organisatie, de makelaar die services inkoopt, combineert en wederverkoopt aan de eigen organisatie. Dit is een door technologie en de business gedreven ontwikkeling waar vrijwel geen enkele organisatie immuun voor is. Hiermee verandert de ICT-organisatie van een club van makers in een club van makelaars met een eigen aannemingsbedrijfje erbij. Dit model heeft daarmee een ingebakken conflict.

Het conflict zal blijven omdat lang niet alles 'buiten' te koop is en er dus maatwerk overblijft. ICT-organisaties zullen hybride organisaties zijn waarbij de interne leveranciers concurreren met de externe leveranciers. Organisaties zullen er evenmin toe overgaan om 'alles' bij één externe leverancier onder te brengen, al was het maar omdat geen enkele leverancier daadwerkelijk alles levert. Zo ontstaan bestuurlijke en uitvoerende lappendekens met veel kastjes en muren, waartussen lastige dossiers langdurig kunnen zweven. Onder het motto dat succes vele vaders kent en mislukking een weeskind is, is security bij uitstek een wees. Security is typisch een dossier waarin de schakels moeten samenwerken om succes te hebben.

[8] SCADA (Supervisory Control And Data Acquisition) is de besturing van grote industriële systemen. Het Stuxnet virus viel de SCADA voorziening van de Iraanse nucleaire installaties aan.
[9] http://www.autoweek.nl/nieuws/19613/porsche-stapt-toekomst-in-met-ipv6
[10] http://www.computerworlduk.com/news/infrastructure/3433595/boeing-787s-create-half-terabyte-of-data-per-flight-says-virgin-atlantic/

In de versnipperde omgeving waar de ICT naar evolueert, is het eigenaarschap van beveiliging ook verdeeld. Zonder heldere beleidskeuzes zal dit de doodsteek zijn voor iedere poging tot coherente informatiebeveiliging. Wat ook zeker niet helpt is een gebrek aan standaardisatie en samenwerking tussen ondersteunende faciliteiten – zoals EKMS, IAM, managementsoftware en de aansturing van beveiligingssystemen. Het gevolg is een verdediging bestaande uit een verzameling egelstellingen met daartussen grote stukken niemandsland. Dit gebrek aan samenhang en samenwerking leidt tot extra kwetsbaarheden en uiteindelijk tot te weinig vermogen om op te treden bij grote incidenten.

Het aansturen van meerdere interne en externe leveranciers vraagt een bestuurlijke behendigheid die veel verder gaat dan nu nodig is. De wederverkooporganisatie kan immers niet zonder enige reserve gebruikmaken van de vakkennis van de interne leveringsorganisatie, omdat deze het spreekwoordelijke kalkoen is bij de besprekingen over het kerstmenu. De regieorganisatie komt in de praktijk dan ook heel moeizaam van de grond, omdat het geen logische evolutie van het bestaande model is, maar een revolutionair andere aanpak. Juist nu de ICT-ontwikkelingen vragen om sterk leiderschap, is de besturing verlamd.

Deze verlamming wordt verstikkend vanwege een toenemend kennisdeficiet. Om de juiste aankopen te kunnen doen en de verschillende aanbieders te kunnen vergelijken, moet een wederverkoper juist meer weten dan een interne of een externe leverancier. Leveranciers hoeven maar één goede manier te weten en die dan te ‘productiseren’. De uitdaging van de Broker is daarbij niet de functiematrices en de SLA’s van die verschillende leveranciers te vergelijken, maar het veiligstellen van de functionele architectuur en de technische samenhang van wat ingekocht wordt. Alsof dat niet al moeilijk genoeg is, is er dan ook nog het veiligheidsvraagstuk.

De traditionele interne leverancier is een tactische organisatie die bij de dag leeft en een tijdshorizon heeft van een boekjaar. De regieorganisatie is een strategische operatie met een horizon van vele jaren. Zij moet immers zorgen dat de juiste functies er zijn, waarbij het de eindklant niets kan schelen of deze technisch gezien binnen dan wel buiten staat. Regieorganisaties zullen dan ook actief met potentiële leveranciers moeten spreken over toekomstige producten en kunnen niet zo onafhankelijk optreden als je op het eerste gezicht zou verwachten. Het is al gebeurd dat een leverancier in moeilijkheden opgekocht is door een klant omwille van de continuïteit van de functionaliteit, met als eindresultaat dat de klant nu leverancier van de concurrentie is. Het is helemaal niet ondenkbaar dat deze brokerfunctie zélf ingekocht gaat worden, omdat deze kennisintensiever en bestuurlijk complexer is dan het huidige model.

Hoe het ook zij, de uitdaging is de gewenste flexibiliteit én veiligheid over zoveel meer schakels dan voorheen te realiseren. Het aantal technische en organisatorische schakels in de verdedigende keten neemt toe. De Command & Control organisatie die de beveiliging moet coördineren heeft daarmee een zwaardere taak dan ooit tevoren.

Uitdagingen die we niet zien en waar we dus niets aan doen

Informatiebeveiliging is een overhaast dossier, gedreven door incidenten en hypes, waardoor grote deelgebieden en inzichten buiten het zicht blijven. Hieronder brengen we een paar ondergesneeuwde zaken onder de aandacht, zodat de inzichten die nodig zijn om daadwerkelijk vooruit te kunnen, weer helder op het netvlies komen.

Uitdaging 1: Beveiliging is logistiek

In de meeste beveiligingsdossiers is hand- en maatwerk de norm: iedere situatie wordt als losstaand incident behandeld zodra er een aanleiding voor is. Beveiliging is alleen zinvol als deze in stand gehouden kan worden: Sustainability van de inspanning is het hoogste doel. De uitdaging is alles te automatiseren dat zich daartoe leent, en dat zijn alle lineaire en repetitieve processen, zodat er aandacht en tijd is voor de uitzonderingen en complexe situaties. Want daar zullen er altijd genoeg van zijn.

Uitdaging 2: We beveiligen systemen, geen informatie

We noemen het werkveld informatiebeveiliging. Maar kunnen we dat zonder te weten wat en waar de informatie is? Daarom gaat beveiliging in de praktijk over systemen; we beveiligen waar we veronderstellen dat de informatie staat. Maar er is vrijwel geen relatie tot informatie en informatiemanagement.

Om informatie daadwerkelijk te beveiligen moeten regels afgedwongen worden op informatieniveau. Dat heeft bepaalde consequenties:

- Om informatie te beveiligen is het noodzakelijk te weten wat het is en waar het is. In de digitale context betekent dit dat de informatie correct gelabeld (geclassificeerd) is;
- Om informatie te beveiligen is het noodzakelijk dat het label onlosmakelijk verbonden is aan de informatie;
- Om informatie beveiligen is het label de identiteit van informatie.

De kern van toegangsbeveiliging wordt op dit moment gevormd door het DAC[11]-model: de gebruiker heeft de vrijheid informatie te plaatsen waar hij wil. Met die keuzevrijheid kan de gebruiker het feitelijke beveiligingsniveau kiezen; informatie in e-mail heeft in de praktijk een geheel ander veiligheidsniveau dan dezelfde informatie zou hebben in een document management systeem.

De definitieve keuze voor DAC is al heel vroeg gemaakt (rond 1980, omdat het alternatief, Mandatory Access Control, geen haalbare kaart bleek). DAC zit in alle haarvaten van ons denken en onze technologie, hoewel we dit vaak niet bewust zijn. Zo gaat RBAC[12] door de combinatie met DAC feitelijk over het uitgeven van autorisaties op plekken waar informatie zou moeten staan in plaats van het uitgeven van autorisaties op informatie.

De consequentie van het DAC-model is dat we de plek beveiligen waarvan we aannemen dat de informatie er staat. Dat leidt er op haar beurt toe dat we alle plekken waar informatie zou kunnen staan *moeten* beveiligen. De beperkte middelen moeten dus verspreid worden over alle voorzieningen, met als gevolg dat alle voorzieningen zwak beschermd zijn. De consequentie van de Deperimeterisatie in combinatie met DAC is dat we bovendien zo ongeveer het hele Internet moeten beveiligen als we onze bedrijfsinformatie willen beschermen.

Uitdaging 3: We beveiligen alleen tegen simpele aanvallers

De effectiviteit van beveiligingsmaatregelen is al heel moeilijk te meten, nog moeilijker is dat het rendement niet lineair groeit met de inspanning. Het is een asymmetrische werkelijkheid: beveiligen kost meer inspanning dan aanvallen en meer beveiliging dan een bepaald basisniveau vraagt een meer dan significante inspanning. Het tegenhouden van de gewone aanvallen slokt al alle aandacht op[13]. Daarom kiezen alle hedendaagse beveiligingsconcepten voor een beveiliging tegen drive by attacks en geven toe (als je doorvraagt) geen veiligheid te bieden tegen de huidige gerichte aanvallen[14].

---

[11] Discretionary Access Control; de discretionaire bevoegdheid het beveiligingsniveau te kiezen ligt bij de user.
[12] Role Based Access Control; het toewijzen van autorisaties op basis van een functie of rol binnen de organisatie.
[13] http://www.cnbc.com/id/100488076/The_Near_Impossible_Battle_Against_Hackers_Everywhere
[14] Zie o.a. http://tweakers.net/nieuws/87585/ict-beveiligers-lopen-achter-op-hackers.html en http://www.securityweek.com/securing-against-apt-%E2%80%93-integrating-security-more-effectively-enterprise

Drive by attacks zijn gelegenheidsaanvallen, zoals wereldwijde virussen laten zien – het systeem wordt aangevallen omdat het kán, niet om de informatie die erop staat. Dit is nog steeds het leidend paradigma, een visie die gegeven cybercrime, APT en Cyberwar niet meer voldoet. We hebben nog geen nieuwe visie ontwikkeld.

Uitdaging 4: Defense in Depth is een mythe

Gelaagde beveiliging (het layered security model ofwel Defense in Depth) is een militair concept[15] dat losjes is vertaald naar ICT-beveiliging. Dit model is feitelijk de opvolger van het 'chokepoint model' van de jaren '90. Bij Defense in Depth in de ICT-incarnatie wordt op componentniveau beveiliging aangebracht. Per component is er een beveiligingslaagje. Daaruit hebben 'we' de conclusie getrokken dat er sprake is van gelaagde beveiliging[16]. Die conclusie is voorbarig om verschillende redenen. De eerste is dat de technologie zelf gelaagd is. Ieder technologielaag heeft dan wel een eigen beveiligingslaag, maar per te verdedigen object is er maar één beveiligingslaagje. De tweede reden is dat de laagjes statisch zijn; als één laagje faalt, is er geen back-up voorziening (al zeker niet in real-time) en valt het geheel om. Een virusscanner kan nu eenmaal niet als IDS optreden. De derde reden is dat de lagen losse componenten zijn die niet samenwerken. Een falende firewall kan geen taken overdragen aan een systeem dat daar niet alvast voor opgesteld is. Een gelaagde beveiliging kan alleen als beveiligingsmiddelen permanent meervoudig uitgevoerd zijn. Dat zie je terug in de Best Practices voor de DMZ, die voorschrijven dat er twee verschillende firewalls opgesteld moeten worden. In de praktijk werd dit echter vrijwel nooit zo uitgevoerd. Wat je wel ziet is een border en een gateway firewall, maar dat zijn verschillende, complementaire maar niet 100% inwisselbare rollen.

Met de teloorgang van het chokepoint model hebben we meer dan één punt waar we meerdere lagen beveiligingsmiddelen zouden moeten opstellen, omdat we niet weten wat de kritieke punten zijn en we niet alle toegangsroutes naar de te beschermen informatie kunnen beheersen. De diepte in de defensie is dus een veronderstelde diepte. De bescherming die uit zou gaan van dit concept is dan ook een mythe.

Dat neemt niet weg dat Defense in Depth een uitstekend theoretisch concept is.

Uitdaging 5: We beveiligen het verleden, niet het heden

De huidige reeks van concepten, standaarden, audit kaders, inzichten en Best Practices die het denken over en handelen in informatiebeveiliging domineren komen voort uit het beveiligen van bedrijven tégen het internet, niet óp het Internet. Vanuit Enterprise-perspectief is het Internet immers de grootste bron van bedreiging. ICT security is bijgevolg niet toegesneden op de internetwerkelijkheid, terwijl de Enterprise nu onderdeel van het internet geworden is. Dit uit zich op tal van manieren en laat zich op meerdere manieren verwoorden:

- We beveiligen asynchroon in een synchrone wereld;
- We beveiligen met LAN concepten op het Internet;
- We 'gaan niet over' wat er buiten gebeurt terwijl binnen feitelijk niet meer bestaat;
- We beveiligen 'ons' tegen 'de rest', terwijl we niet weten wie wie is.

De impact hiervan wordt wellicht duidelijk met een paar voorbeelden:

- De besturing van de beveiligingsvoorzieningen is ad-hoc (na incidenten) en point (via projecten). Als de samenhang en samenwerking van de voorzieningen al bewaakt wordt, dan is dit bestuurlijk en asynchroon, via architectuurprocessen zoals die van TOGAF. Enterprise security leeft in het betrekkelijke comfort van achter de frontlinie, veilig achter de firewall en de provider. Enterprise security heeft geen haast. Beveiliging wordt niet als real-time vraagstuk ervaren en de meeste veranderingen zijn de uitkomst van een zeer goed doortimmerd maar ook uitermate traag proces. Het veranderingsproces in de Enterprise heeft als hoogste doel controleerbaarheid en voorspelbaarheid, ook waar dit ten koste van de doorlooptijd gaat. Een verandering van de beveiligingsopstelling is een kwestie van maanden of zelfs jaren. In de post-Jericho werkelijkheid leidt deze traagheid tot aanzienlijke vensters van kwetsbaarheid. Op het Internet is het hoogste doel immers snelheid; aanvallen via nieuwe kwetsbaarheden treden juist in de eerste dagen en weken op.

[15] http://nl.wikipedia.org/wiki/Diepteverdediging
[16] http://www.sans.org/reading_room/whitepapers/basics/defense-in-depth_525

- Een aanzienlijk deel van Enterprise security is opgebouwd rond de Best Practice benadering. Dit is een doelmatige benadering in een statische werkelijkheid, maar een onbruikbare in een snel veranderende werkelijkheid.

- We streven sinds 1994 naar Role Based Access Control, waarbij autorisatiebeslissingen genomen worden op basis van gebruikersattributen zoals deze in de bronsystemen staan en dan in het bijzonder de functie die iemand heeft. We nemen autorisatiebeslissingen dus op basis van statische rol-attributen van de gebruiker, waar andere factoren zeker zo belangrijk zijn; de machine waarmee de gebruiker toegang heeft en het netwerk waar hij gebruik van maakt zijn in een internetwerkelijkheid van even groot belang.

- Er bestaat op het Internet (inclusief de mobiele wereld) geen domein anders dan het web (DNS) domein, waar het LAN het 'Windows domein' heeft wat de kapstok van een groot deel van de beveiliging is. Binnen en buiten gebruiken dus een onvergelijkbaar model maar met dezelfde terminologie. Nu binnen en buiten door elkaar lopen, leidt dit tot structurele verwarring, die op haar beurt leidt tot ontwerpfouten.

- We staan gebruikers (soms) toe met mobiele devices gebruik te maken van informatievoorzieningen, maar alleen met door het bedrijf verstrekte. De beveiliging ziet dus geen verschil tussen een bedrijfsapparaat en een privé apparaat. Het onderscheid dat hedendaagse beveiliging kan maken is hetzij het MAC adres, hetzij een certificaat. Het eerste kan gespoofed worden, het tweede gekopieerd[17].

- We veronderstellen dat een beheerd device veiliger is dan een onbeheerd apparaat en dat ieder beheerd apparaat even veilig is, en ieder onbeheerd apparaat even onveilig. Netwerkhygiëne voorzieningen kunnen echter niet controleren of de door het bedrijf geselecteerde anti-malware oplossing daadwerkelijk alles gedaan heeft wat het geacht wordt te doen en kan niet vaststellen of de patchlevels die het systeem rapporteert, correct zijn. De inspectie is niet voor 100% betrouwbaar (ook niet voor 90%) gegeven de omvang van harddisks en de complexiteit van de devices. Sommige typen onbeheerde apparaten zijn categorisch beter beveiligd dan anderen – zo zijn apparaten op basis van het Trusted Device Model (voorlopig) veiliger dan traditionele apparaten. Het kan dus zo zijn dat een privé tablet technisch veiliger is dan een van bedrijfswege verstrekte laptop. Hierin zit de nodige dynamiek, die granulariteit en flexibiliteit van de beveiligingsoplossingen vraagt in plaats van de zwart/witbenadering die nu prevaleert.

Fouten in de toegangsbeveiliging op Internet worden snel en hard afgestraft, zoals vooral ISP's weten. Binnen een netwerk lijkt echter niets zo urgent, behalve wellicht op de firewall en de applicaties in de DMZ. Dat leidt tot een veel trager bestuurlijk proces en andere technologie in de Enterprise. Daar zijn meerdere voorbeelden van. Twee kenmerkende uit de wereld van autorisaties:

- LAN technologie gaat uit van impliciete beveiliging. Kortweg betekent dit dat veel toegang wordt toegekend door middel van de groep Everyone. Iedereen die bekend is (authenticated user) in een domein heeft op grond van het bekend zijn bepaalde rechten. Deze verwarrende situatie is vooral ontstaan omdat ingelogd zijn op de werkplek LAN-technisch hetzelfde betekent als ingelogd zijn op een applicatie. Op Internet is dat niet zo. Daar is autorisatie declaratief en applicatief - oftewel toegang moet expliciet toegekend worden en is per sessie. Het Internet is niet één domein waarbij alles centraal geregeld is, zoals het LAN dat is. De technologie rond autorisatie op het Internet is intrinsiek anders en bovendien veel arbeidsintensiever.

- Binnen een traditioneel LAN geldt dat de perimeter voor de belangrijkste beveiliging zorgt. Systemen die niet rechtstreeks verbonden zijn met de buitenwereld worden verondersteld alleen door interne bedreigingen geraakt te kunnen worden. Van interne bedreigingen wordt aangenomen dat deze

[17] Er zijn ook nog andere varianten, zoals de IMEI voor telefoons of het beschikken over de juiste client applicatie. De IMEI is echter de identificatie van de SIM-kaart, niet van het toestel. De juiste client applicatie kan iets bewijzen, maar doet dat in de regel niet. Client side security oplossingen zoals NAC/NAP worden in de praktijk al gespoofed.

technisch niet zo gevorderd zijn. Interne systemen worden dan ook niet 'gehardened'[18], zelfs niet als het beveiligingssystemen zijn. Met de zwakkere buitenmuren is dit niet meer vol te houden. Beveiligingstechnologie die niet kan werken in een dergelijke, gehardende werkelijkheid, zal het niet overleven. Veel hedendaagse beveiligingsproducten zakken voor deze test; dit geldt in het bijzonder de besturing van beveiliging en de logistieke systemen daarachter. Het favoriete doel van een aanvaller die zich op een grote organisatie richt is de werkplek van de beheerder. Met het vorderen van de techniek is de geautomatiseerde beheerder (zoals je bijvoorbeeld Identity Management systemen kunt beschouwen) een logisch doelwit.

We beveiligen dus het verleden. Best Practices zijn de geschiedenisboeken van ICT Security. En net als bij geschiedenis geldt dat het verleden niet de antwoorden voor de toekomst bevat, maar wel onmisbaar is bij het stellen van de juiste vragen.

Uitdaging 6: De ICT werkelijkheid is hybride

ICT beweegt in een slingerbeweging tussen centraal en decentraal. Het begon centraal, met mainframes en terminals. Toen kwamen de fat clients (de pc's) en peer-to-peer netwerken[19]. Nu zitten we in een golf naar tablets en de Cloud, wat weer een wending naar thin client en centrale applicaties en opslag is. Ook dit zal niet tot een definitief eindpunt leiden. Met de pc verdween het mainframe niet, en met de Cloud zal ook de pc niet verdwijnen. Er komen alleen maar steeds apparaten bij, want ook het huidige model kent tal van beperkingen. De Cloud is verre van af.

Omdat we altijd ergens in deze golfbeweging zitten, en beide uitersten niet ideaal zijn, zal de technische werkelijkheid altijd hybride zijn en beveiliging een balanceer-act en een stammenstrijd. Centraal en decentraal hebben elk hun eigen beveiligingsmiddelen en werkelijkheid, en organisaties kunnen niet autonoom het één of het ander kiezen. Bovendien is de voornaamste aanjager van de slingerbeweging de onoplosbaarheid van de klassieke paradox tussen de openheid en flexibiliteit die een deel van de business wil (mijn prospects moeten direct overal bij kunnen) en de veiligheid die een ander deel eist. "Alles gaat in de Cloud" zoals nu soms geroepen wordt, is gezien de historie extreem onwaarschijnlijk. Voor consumenten[20] wordt dat gesteld, maar je vakantiefoto's buiten de deur neerzetten is voor de meeste mensen toch iets heel anders dan je illegale MP3 collectie, je belastingaangifte of zaken gerelateerd aan de slaapkamer. Ook voor bedrijven[21] wordt het hosanna van de Cloud beleden. De Cloud is er en de Cloud blijft, zoveel is zeker. Maar de werkelijkheid is en blijft hybride – organisaties en consumenten zullen ook eigen spullen hebben. Zelfs als de Cloud op alle gebieden beter en goedkoper is, blijft dat zo. Al was het alleen maar voor het gevoel van autonomie. Zo gaan heel veel mensen met de auto naar hun werk, ook als het openbaar vervoer echt sneller en goedkoper is.

Maar bij een perfecte Cloud die alle wensen kan bedienen zijn we nog lang niet. En daar zullen we niet komen, want de Cloud zal niet agile en flexibel blijken te zijn, op termijn. Ze moet immers ook beveiligd worden. Dit laat zich het beste uitleggen met een parallel. De doorbraak van de pc in bedrijfsnetwerken was oorspronkelijk bedoeld om de gewenste flexibiliteit te brengen die de ivoren toren van de Mainframe ICT niet meer had, en als het goedkoper kon, dat dan ook, graag. De prijs van flexibiliteit is echter *per definitie* instabiliteit en onveiligheid. Nu de pc eindelijk een veilige en stabiele werkelijkheid begint te vormen, is ze te statisch. De prijs van veiligheid is per definitie minder flexibiliteit en hogere kosten. Nu jagen organisaties naar flexibiliteit in de Cloud. Naarmate we de Cloud beter beveiligen, wordt ze minder interessant, want minder flexibel. Op het moment dat de Cloud naar de wensen van beveiligers afdoende dichtgetimmerd is, wat gegeven dat de Cloud kwetsbaarder is (ze is immers opener) heel erg dichtgemetseld inhoudt, dan is de Cloud vrijwel al haar voordelen kwijt.

Hetzelfde speelt al met mobiele devices: functionaliteit, storage capaciteit en rekenkracht nemen snel toe, zodanig dat we de smartphone feitelijk als een fat client moeten zien en de bijbehorende maatregelen moeten treffen. Een smartphone kan heel veel dingen, maar is daarmee ook weer veel kwetsbaarder – niet voor niets wordt de beveiliging van Android al wel vergeleken met die van Windows 95. Functioneel heeft een gebruiker er sinds Windows 95 weinig bij gekregen, maar de huidige Windows-versie heeft een zeker tien keer zo grote

[18] Hardening is het zoveel mogelijk dichtzetten van een systeem, door alle niet noodzakelijke componenten te verwijderen en de instellingen zo strikt mogelijk te maken.
[19] Dit gaat niet over P2P protocollen op internet, maar over Windows For Workgroups.
[20] http://www.gartner.com/newsroom/id/1947315
[21] http://gigaom.com/2011/12/01/its-cloud-prediction-time-idc-gartner-and-i-weigh-in/

footprint op het systeem. De voornaamste reden is beveiliging. Een dergelijke groei zullen we op de mobiele platformen ook gaan zien.

Voor dit moment geldt: als een gebruiker met drie verschillende devices (laptop, tablet en smartphone) het netwerk op kan, wordt de beveiligingsinspanning verdrievoudigd. Als we in de Cloud én in ons eigen rekencentrum én bij een externe leverancier data onderbrengen, dan verdrievoudigt de beveiligingsinspanning. Ik moet concluderen dat de inspanning van de beveiliging met beide gelijktijdige ontwikkelingen niet zes keer maar negen keer zo groot wordt. En toch doen we dat, omdat we in onze jacht op kosteneffectiviteit en flexibiliteit de beste keuze van dat moment maken. Die keuze pakt nu eens linksom, dan weer rechtsom uit. En dat blijft zo.

Uitdaging 7: Toegangsbeveiliging tot applicaties is iets anders dan toegangsbeveiliging tot bestanden

Een gebruiker kan informatie in een bestand meenemen, in een applicatie niet. In toegangsbeheer wordt dit onderscheid hoogst zelden gemaakt. De realiteit is dat een fileshare als een applicatie gezien wordt en als zodanig beveiligd. Dit is een manier van beveiliging die geen enkel nut heeft als de organisatie enigszins open is.

Uitdagingen die we zien maar niet (kunnen) oplossen

Naast de ondergeschoven kindjes uit voorgaande opsomming, zijn er nog zaken die wel in beeld zijn, maar waar te weinig mee gedaan wordt:

Uitdaging 8: Beveiliging is een wapenwedloop

Als de gemiddelde verdediging beter wordt, dan wordt de aanvaller dat ook. Als het gemiddelde beveiligingsniveau geavanceerder wordt, zullen aanvallers geavanceerdere middelen inzetten. Natuurlijk is dit eindig, maar de aanvalsmiddelen die nu gangbaar zijn, zijn verre van het meest geavanceerd denkbare[22]. Het gevolg van de wereldwijde toename van beveiligingsinspanningen zal niet leiden tot een veiliger ICT werkelijkheid. Organisaties kunnen alleen hun relatieve positie verbeteren, in de hoop en verwachting dat een aanvaller de pijlen op een ander richt.

Uitdaging 9: De aanvaller is in het voordeel

Een hedendaagse aanvaller zal de meest simpele en meest effectieve methode gebruiken. De uitzondering is de klassieke hacker, die bij voorkeur de meest geavanceerde methode kiest zoals een bergbeklimmer een voorkeur heeft voor de hoogste berg. Aanvallers zijn niet gebonden aan de beheersilo's die bedrijven gebruiken, dus een grote inspanning op een deel van de beveiliging leidt alleen tot een verschuiving van wat onder vuur ligt. Dat zien we op dit moment gebeuren; nu de firewalls en de netwerklaag behoorlijk goed beveiligd zijn, heeft de aandacht zich naar de applicatielaag verplaatst en komen dankzij mobiele apparaten ook de bestanden in beeld, als een soort onbedoelde big data. De beveiligingsinspanning volgt schoorvoetend en met de nodige vertraging, vanwege de cultuur, de procesinrichting via achteraf-audits en Best Practices en niet te vergeten de traditionele beheersilo's.

Uitdaging 10: De Cloud is niet klaar

De huidige Cloud werkelijkheid volgt de traditionele client/server aanpak. Dit is een eerste fase van Cloud computing, maar gegeven de inherente beperkingen zal dit zeker niet de eindsituatie zijn.

Op dit moment zijn Cloud applicaties gesloten silo's en een afnemer die integratie van twee applicaties zoekt (zoals met een mail en een CRM systeem) kan dit alleen voor elkaar krijgen als beide applicatie van dezelfde leverancier zijn. Dit zal voor sommige bedrijven voldoende zijn, voor de meeste echter leidt deze nieuwe lock-in weg van de beoogde flexibiliteit.

Bij een client/server model in de Cloud gelden dezelfde nadelen als bij een client/server opzet in het eigen datacentre. Het grootste nadeel van client/server is dat gegevens die in meerdere applicaties nodig zijn, in al die applicaties afzonderlijk opgeslagen worden. Het gevolg daarvan is dat de gegevensverzameling op

[22] Zo is bij de veelbesproken hack van RSA in 2011 gebruik gemaakt van Poison Ivy, een Trojan die op dat moment al zeker 12 jaar oud was. De technische methode die de Trojan langs de antivirusvoorzieningen kreeg was nieuw, maar van een type dat in 2005 al in het wild gesignaleerd was.

verschillende plekken onderhouden moet worden, en dus: hogere kosten en meer fouten. De enige manier voor de Cloud om de beloofde flexibiliteit waar te maken is het te evolueren naar Multi-tier applicaties rond een Master Data model. Met een Multi-tier benadering bestaan applicaties uit los schakelbare blokken, wat hergebruik en herschikking van componenten mogelijk maakt. Dit verlaagt de kosten en vergroot de flexibiliteit. Het Master Data model betekent dat alle gegevens op één plek staan en dus ook maar op één plek onderhouden hoeven te worden, wat ook kostenverlagend werkt maar vooral kwaliteitsverhogend is. Deze aanpak is bekend geworden onder de naam SOA, Service Oriented Architecture. Dit model geldt als de opvolger van het client/server model en daarbij maakt het natuurlijk niet uit of de service componenten binnen dan wel buiten, in de Cloud, staan. Dan zullen organisaties de eigen Mash-Up (een user front-end met objecten uit verschillende applicaties van leveranciers, zoals een interne applicatie die gegevens projecteert in een landkaart van Google Maps) realiseren, zonder afhankelijk te zijn van één leverancier. Bovendien kunnen de organisaties dan delen verwisselen (of zelf invullen) als de behoefte zich voordoet.

Echter, door SOA te gaan gebruiken in de Cloud wordt de beveiliging beduidend complexer dan we nu gewend zijn. In de Cloud lopen de tiers over meerdere domeinen en dan praten Multi-tenant applicaties met Multi-tenant applicaties. Een Multi-tenant omgeving is een omgeving die meerdere klanten tegelijk bedient. Op dat moment wordt de identiteit van de applicatie en de identiteit van de transactie een heel dringend vraagstuk. Daarbij zullen bovendien de notoir lastige 'impersonatie' vraagstukken spelen: de vraag namens wie een applicatie de transactie uitvoert. Binnen het traditionele in-house SOA landschap worden applicatie naar applicatietransacties vrijwel zonder uitzondering als 'system' uitgevoerd, met alle voorspelbare gevolgen voor security en auditability. Voor beide vraagstukken is de technologie nog niet volledig uitgekristalliseerd, maar wel in ontwikkeling.

Als we de SOA in de Cloud hebben, komen de vervolgenvragen vanzelf in beeld. Als bedrijven een Mash-up/SOA doen met producten van verschillende leveranciers, hoe worden de leveranciers van achterliggende functies dan betaald? Een model met menselijke brokers zal ongetwijfeld een tijdje goed gaan, maar uiteindelijk niet schaalbaar en flexibel genoeg zijn. Daar zal dan vast een systeem voor Micro payments voor komen, met de nodige beveiligingsconsequenties die daar dan weer bij horen. Na het oplossen van deze puzzel zal er ongetwijfeld een volgende komen.

In de beslotenheid van het eigen rekencentrum is er vaak voor gekozen om de bijbehorende complexe beveiligingsvragen weg te managen door de beveiliging op de applicatielaag weg te laten. In de Cloud is dat geen optie. Organisaties moeten dus kiezen tussen niet-bewezen beveiligingstechnologie, geen beveiliging of geen Cloud.

Uitdaging 11: Cloud Security is niet afdoende gestandaardiseerd

Samenhangend met het voorgaande: ook rond Cloud/SaaS is een groot deel van de beveiliging nog niet klaar, terwijl de systemen in een hoog tempo in gebruik worden genomen. De enige enigszins gedragen standaard is SAML2, die oorspronkelijk ergens anders voor bedoeld is. Opvallend is dat de meeste Cloud aanbieders al moeite hebben deze standaard te ondersteunen. Feitelijk is de stand van zaken met SAML2 juist een uiting van de onvolwassenheid op beveiligingsgebied bij Cloud- en SaaS-aanbieders. SAML2 is als protocol bedoeld voor een flintertje van beveiliging en dan eigenlijk alleen nog maar het stukje waar eindgebruikers mee te maken hebben, namelijk het aanloggen. Met echte integratie van een Cloud in de beveiliging voorzieningen zullen aanbieders zich kunnen onderscheiden, maar dat is nog maar net een beetje in beeld.

Een paar voorbeelden:

- Hoe kan ik zien dat ik onder vuur lig? Is het mogelijk de IDS gegevens van de Cloud omgeving te koppelen aan de eigen interne IDS voor patroonanalyse? Hiervoor bestaan geen standaarden.

- Hoe organiseer ik de klassieke CIA voorzieningen (Confidentiality, Integrity & Availability). Availability is één van de kernwaarden bij SaaS, confidentiality en integrity zijn dat zeker niet. Confidentialiteit is gerelateerd aan autorisatie en integriteit aan cryptografie. Algemeen geaccepteerde standaarden en principes ontbreken hiervoor en elke applicatie gebruikt eigen inzichten. Dit leidt tot een grote diversiteit en dit maakt monitoring en management tot een kostbare zo niet onbetaalbare opgave.

- Hoe organiseer ik autorisatiebeheer over meerdere Cloud applicaties heen? SAML2 geeft de mogelijkheid een login van de klantorganisatie te gebruiken, maar om de gebruiker te synchroniseren met de Cloud applicaties worden de bestaande standaarden als SPML of de REST api's vrijwel niet ondersteund. XACML is een mooie belofte maar de acceptatie is – zoals zo vaak – zeer langzaam.

    - Wie heeft de cryptografische sleutels in handen die gebruikt worden bij de Cloud? Kun je als klant de leverancier opleggen welke sleutels waarvoor gebruikt worden en deze integreren in het eigen Enterprise Key Management Systeem? Hiervoor bestaan geen standaarden, alleen enkele technische producten.

De conclusie is dat de Cloud nog ingrijpend zal veranderen, en dat de beveiliging een inhaalslag zal moeten maken.

Uitdaging 12: Internet is internationaal, wetgeving nationaal

Het Internet is geëvolueerd als een open gebied waar techniek de toon aangeeft, niet de wet en de handhaver van de wet. Op Internet zijn technische standaarden de baas, niet een of enkele instanties. Je kunt van de standaarden afwijken op details en de enige sanctie op afwijking is dat het niet werkt. Overheden hebben er feitelijk niets te vertellen, zeker omdat landsgrenzen in de digitale ruimte niet aan te wijzen zijn.

De nationale staten zijn druk doende deze anarchie in te dammen zonder deze in alle gevallen even goed te begrijpen. Organisaties krijgen hierdoor te maken met een lappendeken van wetgeving, waarbij regelmatig elkaar uitsluitende voorschriften gelden. De rationale eronder verschilt van land tot land, maar feit is dat vrijwel ieder land voor één of meer dossiers morrelt aan het huidige model.

Zo heeft de Amerikaanse Patriot Act invloed op alle landen die zaken doen met bedrijven die iets in de VS doen. Dat geldt vrijwel alle grotere ICT-ondernemingen, zodat via het Internet iedere organisatie tegen de realiteit van de Amerikaanse wetgever aanloopt, zelfs als de organisatie alleen in eigen land opereert. Dit is het meest zichtbaar in de discussies rond de Cloud, waarbij de afnemer moet weten in welk land de data staat, vanwege lokale wetgeving in de VS. De Cloud aanbieders zullen deze risico's bagatelliseren, waar de concurrenten van de Cloud – zoals de interne ICT-aanbieders – de risico's benadrukken en er baat bij hebben deze te overdrijven. Andere landen volgen het Amerikaanse voorbeeld van lokale regulering op globale voorzieningen, maar dan met andere doelen. Het effect is hetzelfde, ze introduceren regulering en toezicht dat in de praktijk de landsgrenzen overschrijdt.

Een belangrijke nuance die nogal eens vergeten wordt is dat Cloud omgevingen vanwege de virtualisatie altijd op een of andere manier Multi-tenant zijn. Afnemers van de Cloud hebben niet alleen te maken met de regels waar de Cloud leverancier aan moet voldoen, maar in een stijgend aantal gevallen ook met de regels waar andere klanten van dezelfde leverancier aan moeten voldoen. Als de leverancier voldoende 'Chinese Muren' aanbrengt tussen de verschillende klantomgevingen zal dit niet meer spelen. De prijs van de Chinese Muren wordt natuurlijk wel doorberekend.

Een ander speciaal dossier is compliance: de regimes in verschillende landen en voor verschillende doelen zijn niet geharmoniseerd. Zo komen organisaties in aanraking met een diversiteit van voorschriften met eigen formats en toezichthouders, waardoor de totale regeldruk erg groot zal worden en zich situaties van elkaar uitsluitende voorschriften zullen voordoen. Het is evident dat de meerkosten hiervoor, immers behorende tot het domein van de Informatiebeveiliging, ten koste zullen gaan van de andere inspanningen.

De situatie wordt nog complexer als de EU de aangekondigde aanpassingen van de privacyregelgeving gaat doorvoeren. Het huidige en verouderde voorschrift EU 95/46 is al moeilijk na te leven, maar dat wordt niet heel strikt gehandhaafd omdat nieuwe regelgeving in de maak is. De slag om de privacy zal echter losbarsten als Privacy By Design[23] door de wetgever opgelegd en gehandhaafd wordt. Als de planningen waargemaakt worden, zal dat vanaf 2016 zijn.

[23] De eerste draft van de nieuwe regelgeving is te vinden op http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Traditioneel is privacy voor ICT geen groot onderwerp in beveiliging en toegang, omdat de gevoelige objecten toch vooral de eigen medewerkers zijn. Met Privacy By Design als opgelegde aanpak in combinatie met Consumerisatie staat informatiebeveiliging voor een zeer ingrijpende wijziging van haar takenpakket.

Uitdaging 13: Wij zijn niet het Centre of the Universe

In de beveiliging van de Enterprise is de Enterprise het middelpunt – hoe wij het doen, zo is het goed. Als wij het niet kunnen controleren, dan is het niet goed. In de hoogtijdagen van offshoring en outsourcing bleef dit geloof in stand, hoewel de externe leveranciers hun werk ook op hun eigen manier deden en niet op de manier van de opdrachtgever. Het geloof wankelt pas sinds de 'consumerisatie'. De eerste prominente uiting van consumerisatie was in 2009 met Identity 2.0. Dit stelt de gebruiker centraal, in plaats van de ICT-diensten aanbieder. Omdat het over klanten gaat en daarmee over inkomsten, is een aantal organisaties al van het Enterprise geloof gevallen. De volgende aanval op het ideologische bolwerk is BYOD, waarbij de gebruiker zélf bepaalt met welk device en applicaties gewerkt wordt. De mopperende opmerking vanuit de ICT-afdelingen dat dit wel heel moeilijk wordt qua support, schetst de kloof: de gebruiker wil helemaal geen support, de gebruiker wil dat de spullen gewoon werken en blijven werken. Als de tablet of de telefoon niet doet wat die moet doen, dan komt er gewoon een nieuwe. BYOD is door geen enkele organisatie te negeren. Consumerisatie onderstreept de noodzaak om beveiliging zowel op de applicatie- als op de informatielaag aan te brengen. Daarbij is de tweede de meest genegeerde; de vaak voorgestelde aanpak om een wipe te doen op het device is om overduidelijke redenen géén haalbare optie op een privé-apparaat.

Met deze ontwikkelingen komen alle organisaties in aanraking met het complexe beveiligingsconcept "Multi Level Security", dat vanuit de historie geldt als de heilige graal; hoe beveilig je informatie op een systeem waarop iemand anders – en jij niet – alle rechten heeft?

"The Orange Book defines "Multilevel Secure" as a class of systems containing information with different sensitivities that simultaneously permits access by users with different security without risk of compromise"[24]. Bij een Multi-domein werkelijkheid zoals de Cloud en in een federatie is dit per definitie het geval omdat de user uit een ander security domain komt waarbij het beveiligingsniveau vaak niet bekend is. Daarmee zijn we er echter niet: informatie beweegt over de grenzen van ons domein en verandert daarmee van security context. Multi Level Security is sterk gebonden aan een enkelvoudige security context, en dat bestaat niet meer. We zijn met BYOD in een werkelijkheid beland die nog complexer is dan waar Multi Level Security voor bedoeld is. En die geldt al als vrijwel niet haalbaar. Voor het veel complexere landschap waar we nu staan ontbreken de conceptuele kaders geheel.

Uitdaging 14: Beveiliging is een stuurloos schip

Op de keper beschouwd is de besturing van Security een raadselachtig fenomeen. De besturing loopt nu via architectuurprocessen in combinatie met een ad hoc, incident gedreven aansturing. De architectuurprocessen lopen via de Risk Based Approach en Best Practices; de mogelijke bedreigingen worden geclassificeerd naar impact en waarschijnlijkheid, uit de som van beide factoren volgt de prioriteit.

Tot zover de theorie.

De bedreigingen waar Risk Based Approach vanuit gaat, zijn niet eenvoudig te kennen. Weet het personeel wat een aanvaller zou kunnen doen? De meeste reguliere ICT-medewerkers hebben niet voldoende kennis (of fantasie) van wat een hacker zou kunnen doen, noch van potentiële vulnerabilities in de eigen systemen. De lijst bedreigingen kan dus beter uit een Best Practice gehaald worden. Maar Best Practices lopen achter de feiten aan. Welke organisatie heeft rond 2008, dus voor de activiteiten van Anonymous, de impact van hacktivisme tegen ketenpartners of zelfs tegen een willekeurige andere organisatie waar je klanten mee deelt, correct voorzien? Zelfs nu, geruime tijd na de babydump-affaire[25] met KPN is er nog geen weerslag in de handboeken.

Geen enkele organisatie heeft het vereiste complete overzicht van welke voorzieningen binnen de eigen bedrijfsmuren staan[26] en in welke relatie bepaalde middelen tot bepaalde bedrijfsprocessen staan. Om dit

[24] http://www.rand.org/pubs/reports/R609-1/index2.html, Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security - RAND Report R-609-1.
[25] http://webwereld.nl/nieuws/109493/-kpn-lek--blijkt-lektober-nasleep-van-baby-dump-nl.html
[26] http://www.informationweek.com/security/management/tenets-of-risk-based-security-management/229000951

inzichtelijk te hebben en te houden vraagt een aanzienlijke inspanning, zeker als bedrijfsprocessen en het systeemlandschap wel eens veranderen. Een inspanning die tijd kost.

Bovendien fluctueren bedreigingen per dag. De wegingsmethode voor risico's heeft daarom een eigen dynamiek; bij de Risk Based Approach beveilig je tegen theoretische risico's in een statische benadering. Voor de betrokkenen geldt dat bij ieder risico dat daadwerkelijk ooit kan voorkomen, de weging voor de zekerheid maar wat hoger uitpakt. Dit leidt bij de business wel eens tot het idee dat Security overdrijft.

De eerste besturingsmethode van beveiliging is dus te traag en heeft een hoge mate van onbetrouwbaarheid, de tweede is niet gebalanceerd ('achter de feiten aanlopen'). Een specifieke dimensie bij ad hoc is compliance: de grootste bedreiging is in feite 'niet door de audit komen'; bijgevolg loopt de besturing van Security via auditbevindingen. Dit zijn feitelijk ook incidenten; gegeven dat een auditor niet alles kan bekijken in de beperkte tijd van de audit, is het meer een loterij dan een gewogen en gebalanceerd verhaal. Bovendien is de auditor helderziend noch alwetend. En als laatste betreft het ongebalanceerde sturing; de keuze voor meer antivirus of meer Intrusion Detection kan en zal een auditor ook niet maken.

Het geheel van beveiligingsmaatregelen wordt als het goed is netjes geadministreerd in een ISMS (Information Security Management Systeem) conform ISO27001, zodat met één druk op de knop het rapport uitgedraaid kan worden dat vertelt hoe de beveiligingsmaatregelen ervoor staan. Dit type ISMS levert echter geen management van de Security op, maar is een administratief systeem van geïmplementeerde regels ten behoeve van de audit. Gegeven de frequentie van audits en het feit dat het achteraf controle betreft, moge duidelijk zijn dat er geen besturing zou moeten uitgaan van audits of ISO27001.

Nu is het idee dat auditkaders die gebaseerd op verzamelingen Best Practices zijn, een positief effect op de sturing en de balans van de getroffen maatregelen hebben. Er zijn audits waar een dergelijke goede sturing van uitgaat, maar dat is dan dankzij de kunde en ervaring van de auditor en niet dankzij de auditkaders. Dat zijn immers vinklijstjes zonder soortelijk gewicht. Dat kan ook niet, want auditkaders zijn generiek en soortelijk gewicht is organisatiespecifiek.

De laatste beperking van het auditmodel is de actualiteit ervan. Het is een op ervaring gebaseerd model en is daarom gericht op oplossingen voor problemen uit het verleden. Organisaties die middelen inzetten waarvoor geen uitgekristalliseerde beveiligingskaders bestaan (zoals Cloud en mobile) zien dit regie-deficit in de praktijk.

Uitdaging 15: Wij doen helemaal niets met Jericho

De logische conclusie van het einde van de perimeter zou zijn te stellen dat dit tevens het einde van de informatiebeveiliging is. Er zijn theoretici die dit stellen, vanuit de gedachte dat informatie te allen tijde en voor iedereen toegankelijk moet zijn. Dit moge op zichzelf een fascinerende gedachte zijn, maar lijkt toch vooral utopisch, omdat het pas werkt als iedereen meewerkt. We kunnen dus vaststellen dat informatie beveiligd zal moeten worden, ook in de toekomst.

De impact van Deperimeterisatie op het denken over beveiliging is echter nog lang niet verwerkt. In de folders van de allernieuwste beveiligingsproducten is dit duidelijk te zien: ook de nieuwste beveiliging van mobiele devices of de hipste Cloud maakt gebruik van slagboomconstructies. Net zomin is er een ingrijpende revisie van de Best Practices gevolgd sinds het Jericho Manifest. Vrijwel ieder beveiligingsmiddel, of het nu een organisatie of een technologie betreft, gaat uit van binnen versus buiten, van zonering. Het gebruik van zonering is een puur netwerkconcept, en hangt als zodanig samen met de netwerkvisie op beveiliging. Als we de conclusies van Jericho overnemen hadden zou zonering als beveiligingsconcept vervallen zijn. Gegeven dat de zonering nog steeds leidend is, moeten we vaststellen dat er helemaal niets mee gedaan is.

Uitdaging 16: De Business luistert wel

Klassiek onder beveiligers is de behoefte om op directieniveau gehoord te worden, en dat gebrek aan toehoorders op het hoogste niveau wordt aangevoerd als enige reden dat de doelen niet bereikt worden. De laatste jaren is dat luisterend oor, onder druk van de aanhoudende aandacht in de media voor beveiligingsincidenten, steeds vaker en in veel gevallen zelfs structureel aanwezig. Daar blijkt vervolgens dat het 'niet luisteren' niet de oorzaak van het falen is. Nu er welwillende aandacht is, zijn de resultaten niet beter. Opvallend aan het onderzoek "Security Organization 2.0: Building A Robust Security Organization" van

Forrester Research uit 2010[27] is de observatie dat Security organisaties die zich richten op het directieniveau de neiging hebben het operationele werk af te stoten of te negeren en zo het contact met de werkelijkheid verliezen. Forrester spreekt zelfs van het Ivoren Toren Syndroom. Dit zijn erg harde conclusies die op een solide basis van onderzoek staan.

Uitdaging 17: Security gaat niet over verantwoordelijkheden

De leerboeken, Best Practices en standaarden voor informatiebeveiliging gaan diepgaand in op de verantwoordelijkheden binnen ICT Security. Kenmerkend is dat verantwoordelijkheden wel benoemd worden, veelal in een overzichtelijk organogram, maar dat er niet bij staat hoe dit geheel daadwerkelijk moet functioneren. Een aantal leerboeken gaat wat verder, door een aantal processen verder uit te werken, maar ook hier strandt het schip voordat de haven bereikt is. De realiteit is dat de aangewezen verantwoordelijke niet empowered wordt om de verantwoordelijkheid daadwerkelijk om te zetten in daden; verantwoordelijkheden zonder bevoegdheden dus. Dat is niet productief.

Een goede opsomming van de verschillende vormen die Security in organisaties aangenomen heeft, is te vinden in het hierboven al aangehaalde document van Forrester Research uit 2010. De (gedeelde of volledige) verantwoordelijkheden die security organisaties kunnen hebben, heeft Forrester als volgt opgesomd. Tussen haakjes staat het percentage security organisaties die voor dit onderwerp verantwoordelijk zijn.

- Threat en Vulnerability management (96%)
- Endpoint security en netwerk security (95%)
- Data security (97%)
- Identity en Access Management (95%)
- Application security (95%)
- Policy and risk management (95%)
- Privacy and regulations (92%)
- Third-party security (86%)
- Business continuity/disaster recovery (88%)
- Physical security (77%)
- Fraud management (78%)

Deze verantwoordelijkheidsgebieden schetsen op het eerste gezicht wat organisaties in Security zoal doen. Maar dat is alleen op het eerste gezicht. Een Security organisatie die zich inspant in Vulnerability Management zal aan ICT adviseren welke updates uitgevoerd moeten worden. Deze verantwoordelijkheid is een inspanningsverplichting, geen resultaatverplichting. Dit geldt evenzeer voor de andere gebieden: het gaat om een inspanningsverplichting. Alleen maar verantwoordelijk zijn *voor een inspanning* is wel erg vrijblijvend voor een taak die naar eigen zeggen zo belangrijk is. Dat helpt niet in de geloofwaardigheid. Security gaat uiteindelijk niet over verantwoordelijkheid, maar over daden.

[27] http://eval.symantec.com/mktginfo/enterprise/articles/b-article_security_organization_20_building_a_robust_security_organization.en-us.pdf

Bekende kwetsbaarheden, onbekende kwetsbaarheden

De kern van beveiliging is het treffen van maatregelen om misbruik te voorkomen dan wel de impact daarvan te verkleinen. Met de ontwikkeling van de technologie zijn er aanzienlijke veranderingen in waar we kwetsbaar zijn en dus welke fronten we moeten verdedigen. In essentie zijn we op steeds meer fronten kwetsbaar. Zoals een oud gezegde in de Security gaat zijn we het meest kwetsbaar op fronten die we niet zien, maar die wél bestaan.

Verleden en heden: local presence, local exposure

In de traditionele werkelijkheid is een organisatie geconcentreerd op één of enkele locaties en zijn de ICT-voorzieningen daar fysiek ondergebracht. Deze bakstenen vormen een essentiële laag in de beveiliging; de 'tegenstander' moet allereerst veel moeite doen om de ICT-systemen te bereiken alvorens iets te kunnen ondernemen. Het beheersen van de beperkte toegangsroutes is de kern van beveiliging: er zijn slechts enkele paden 'naar binnen' en die worden bewaakt. Het meest kansrijke pad naar binnen is op de fysieke locatie een machine 'inprikken' of een lokaal werkstation kapen en daarmee het netwerk op gaan. Een cruciale rol in ICT-beveiliging wordt dus ingenomen door de fysieke beveiliging: screening van personeel en bewaking aan de deur. Het ICT component van de fysieke beveiliging, Port Security, is kenmerkend genoeg zelden ingeregeld; de bewaking is de voordeur van het kantoor, niet die van het netwerk.

De kern van digitale beveiliging bestaat uit twee soorten 'muren'– buitenmuren op de netwerklaag, om de hackers buiten te houden, en binnenmuren op de applicatielaag, om het eigen personeel weg te houden bij de meest gevoelige informatie. De buitenmuren zijn technisch aanzienlijk sterker dan de binnenmuren. Dit staat ook wel bekend als het System High paradigma. De consequentie van System High is dat alle informatie in een netwerkzone beveiligd wordt als informatie van het hoogste niveau. Kostenbesparing is hiervoor uiteindelijk niet de belangrijkste reden: System High is de enig mogelijke aanpak als de benodigde dataclassificatie niet uitgevoerd is. Het gevolg hiervan is dat de belangrijkste beveiliging van de digitale dimensie nog steeds fysiek is: personeel wordt verzocht een Verklaring Omtrent Gedrag te overleggen en dat is de voornaamste hindernis voor aanvallen op de digitale dimensie.

Een andere uiting van dit klassieke denken is te zien in de uitvoering van de beveiligingstechnologie. Externe beveiligingssystemen moeten hackerproof zijn – wat te zien is aan de degelijkheid van firewalls en mail- en webservers. Interne beveiligingssystemen (local security) zijn in de regel veel zwakker. Local security is vanuit hackersperspectief een lachertje; de belangrijkste beveiligingssystemen in de interne zone zijn de beheerderswerkplekken en de Identity Management voorzieningen. Deze zijn nooit gehardened zoals machines in de DMZ, en krijgen slechts zelden aandacht in de Intrusion Detection voorzieningen. Sterker nog, Intrusion Detection is uiterst zeldzaam in interne netwerken. Dit zijn de evidente doelen voor een aanvaller.

Even kenmerkend voor het System High paradigma is de richting van de beveiligingsregels: de bewaking van het netwerkverkeer gaat van buiten naar binnen. Dit is de reden dat aanvallers bij voorkeur via de mail en de user aanvallen: verkeer dat door een gebruiker in het LAN geïnitieerd wordt door op een icoontje te klikken, geldt voor de beveiligingssystemen per definitie als veilig. Kijk het maar na: in de firewall regels staat 'Outbound Initiated' gelijk aan vertrouwd en dus aan goed.

De overgang: local presence, global exposure

Door de invoering van nieuwe businessmodellen vanaf eind jaren '90, ook wel aangeduid als de genetwerkte economie, zijn organisaties kwetsbaar geworden langs de randen van de eigen infrastructuur. Internetverbindingen zijn 'always on' en de variatie in wat er over de verbinding gaat neemt in hoog tempo toe. De tijd van alleen inbound e-mail en outbound webverkeer ligt ver achter ons. Tegelijkertijd wordt de klant gebruiker van de ICT-voorzieningen en heeft een steeds groter deel van de wereld breedbandverbinding. Dit is op veel manieren een bottleneck; bij traditioneel user management gaat het over medewerkers en daarmee bestaat een gezagsrelatie. Afgezien van gekibbel tussen HR en ICT over competenties is dat rechttoe, rechtaan. Nu klanten ook aanloggen kan ICT de users niet zomaar iets opleggen, en moeten voorzieningen werken met consumentenapparatuur.

Security verschuift van de netwerklaag naar de applicatielaag. Netwerkbeveiliging heeft een aanzienlijke mate van maturiteit bereikt; om succesvol te zijn op de netwerklaag moet een aanvaller van wel heel goede huize komen.
De grotere diversiteit op de applicatielaag maakt het aanvalsoppervlak kleiner waardoor grote, generieke aanvallen (zoals het ILOVEYOU-virus…) niet meer bestaan. Beveiligingsmiddelen zijn grotendeels gemaakt om dergelijke grote en generieke aanvallen te weerstaan, en zijn niet bestand tegen gerichte aanvallen. Dit verklaart ook het succes van APT; aanvallen moeten gericht zijn om te kunnen slagen. Beveiligingsmiddelen moeten hierin mee, en deze transitie is nog maar net op gang aan het komen.

Een goed voorbeeld hiervan is te zien in de wereld van de malware. Virussen worden als het goed is gevangen door antivirusproducten. Deze producten herkennen virussen op grond van signatures, strings die uniek zijn voor de infectie zelf. Nu maken AV-makers niet voor alle virussen signatures aan, omdat het om gigantische aantallen gaat. Kasperski becijferde in oktober 2012 dat er 70.000 nieuwe virussen per dag verschijnen. Overal een signature voor maken is een enorme operatie, die boven de macht van een individueel antivirusbedrijf gaat, mogelijk zelfs voor allemaal samen. Bovendien stijgt het aantal nieuwe virussen per dag. Al zou het lukken om overal signatures voor te maken, dan breekt het toch. Dan moet iedere user dagelijks een grote update van de AV-database binnenhalen alvorens aan het werk te kunnen, en moet iedere computer veel meer geheugen hebben om nog enige performance over te houden.

De keuze is dat signatures alleen ontwikkeld worden voor virussen die 'In The Wild'[28] voorkomen. De definitie van In The Wild is een bepaalde verspreiding; voor virussen die een sterke geografische beperking hebben, komen geen signatures en zijn organisaties feitelijk onbeschermd. Daarom heeft de AIVD besloten haar toch wel schaarse capaciteit op dit vraagstuk in te zetten[29].

Global exposure leidt voor organisaties tot zeer grote risico's en die vormen een onhoudbare situatie.

De toekomst: global presence, global exposure

"We're not winning. … I don't see how we ever come out of this without changes in technology or changes in behavior, because with the status quo, it's an unsustainable model. Unsustainable in that you never get ahead, never become secure, never have a reasonable expectation of privacy or security."
Shawn Henry, FBI, 2012

Het is bon ton onder security thought leaders om te stellen dat beveiliging de strijd aan het verliezen is[30]. Het aantal fronten is enorm toegenomen, met outsourcing, het Nieuwe Werken, mobile devices en de Cloud. Het aantal aanvallers is door de toename van breedband en de verdere verspreiding van internetgebruik, sterk gegroeid. De Security industrie verliest niet alleen de strijd tegen de malware, maar ook tegen nieuwe types aanvaller. We zijn op het punt gekomen dat overheden buitenlandse bedrijven[31] hacken in verband met binnenlandse aangelegenheden.

De belangrijkste verandering is dat organisaties gedeelde voorzieningen hebben in tal van landen, via leveranciers en ketenpartners. Iedere organisatie is een veel groter aanvalsdoel dan voorheen. Een aanval op een leverancier of een ketenpartner kan verregaande consequenties hebben, zoals de klanten van RSA en Diginotar aan den lijve hebben ondervonden. We zijn nog nooit zo bedreigd en zo kwetsbaar geweest.

Door de technologie zijn alle Enterprises grensoverschrijdend geworden, zelfs als de business zich alleen in één land afspeelt. Met de opkomst van Cyberwar gaan natiestaten zich bemoeien met de digitale dimensie op een tot nu toe ongekende manier. En daarom met moeilijk te voorspellen gevolgen. Zo heeft de Amerikaanse krijgsmacht zich ten doel gesteld de cyberdimensie te domineren[32], en daarvoor een zeer significant budget

[28] Voor meer informatie: http://www.wildlist.org/ en http://www.avien.net/
[29] https://www.security.nl/artikel/44940/1/AIVD_jaagt_op_onbekende_malware.html
[30] http://www.presstv.ir/usdetail/233604.html; http://news.techeye.net/security/apple-losing-battle-with-hacker; http://esj.com/blogs/enterprise-insights/2012/07/keeping-security-devices-safe.aspx;
[31] http://webwereld.nl/nieuws/113251/na-new-york-times-ook-wall-street-journal-gehackt.html. Eerder werd Google al gehackt in verband met de Dalai lama en de Falung Gong.
[32] http://www.ndu.edu/press/cyber-operations.html

vrijgemaakt. Het is evident dat landen als China[33] en Rusland dit niet zonder slag of stoot laten gebeuren. Dit kan zelfs zo ver doorwerken dat de werking van de kern van het Internet verandert; de regeringen van die landen (en ook andere landen) zullen de VS niet tot in de eigen achtertuin dergelijke dominantie gunnen. De digitale 'Chinese Muur' is een voorbode van wat komen gaat.

Soevereiniteit en de digitale wereld

De digitale dimensie was de ultieme uiting van de globalisering en is nu nog vrij van soevereiniteits-vraagstukken, maar dat is bijna voorbij. Als het technisch eenvoudig was geweest, zouden er al digitale grensposten met bijbehorende inspecties, kosten en vertraging zijn geweest.

Het aantal manieren waarop dit van invloed gaat zijn is groot. Een concreet en tastbaar voorbeeld van de opmars van soevereiniteitsvragen is gelegen in de regulering. We zien een opmars van compliance en privacy regulering in alle landen. Dit leidt ertoe dat de Enterprise verschillende beveiligingsregimes *tegelijkertijd* zal moeten ondersteunen. In de praktijk zal dit leiden tot nieuwe compartimenten binnen de bedrijfsinformatievoorzieningen die in ieder geval formeel afgebakend moeten worden, omdat ze onder andere auditregimes vallen. Dergelijke compartimentering is geboden, al was het alleen maar om te voorkomen dat een nationale opsporingsdienst onbedoeld buiten de jurisdictie treedt bij een lokaal onderzoek, met alle gevolgen van bestuurlijke drukte en uitloop van dien. Immers, als een onderzoek langer duurt, is de business langer verstoord. En als de overheid van een ander vestigingsland je organisatie verdenkt van onwenselijke samenwerking met andere overheden, zal dat omzet kosten. Deze afbakening zal tot nieuwe binnenmuren leiden, net als de traditionele "Chinese Walls[34]" zoals bekend van financiële instellingen, zullen ook andere sectoren hiermee te maken krijgen.

Deze vragen zijn al bekend bij organisaties die samenwerken met Chinese staatsbedrijven. Gegeven de regelgeving in China moet de verplichte partner toegang hebben tot de technologie die in de samenwerking gebruikt wordt. Hoe bescherm je het Intellectual Property dat geen deel uitmaakt van een dergelijke samenwerking? Juist, met het opstellen van binnenmuren in je omgeving.

Dit probleem doet zich in meer situaties voor. Stel je een organisatie voor die in een aantal landen in West- en Midden-Europa actief is, en in twee daarvan wordt uitgeroepen tot deel van 'Vitale Infrastructuur'. De NAVO en de EU zijn beide bezig met het optuigen van concurrerende entiteiten voor het digitale slagveld, en het ene land is meer op de NAVO koers, andere zien meer in de EU[35]. Voor je er erg in hebt leidt deze incongruentie tot twee bestuurlijke regimes en dubbele vergadercircuits. En voor je weet willen beide landen je dataverkeer monitoren en je opleggen dat zij voorgaan bij digitale calamiteiten. Het beeld van een digitaal Pearl Harbor is immers altijd vlakbij in de discussies rond cybersecurity, dus weigeren mee te werken zal niet eenvoudig zijn. Nog een reden voor compartimentering.

We zullen gedwongen zijn de binnenwereld te segmenteren terwijl we weten dat slagbomen en perimeters achterhaald zijn. Voor de Enterprise zal dit een deel van de synergievoordelen van de schaal weghalen: dit zijn kosten zonder baten.

Drie hiermee samenhangende ontwikkelingen zijn van groot belang:

- Cyberwar
- The war on IP
- Big Data

De impact van cyberwar

De wereld kent sinds enkele jaren zogeheten "State Sponsored Attacks", zoals Stuxnet en Flame. Dit soort aanvallen is na een aarzelend en soms ronduit knullig begin hard op weg om zeer geavanceerd te worden. Op termijn zullen zij kwalitatief veel gevaarlijker zijn dan aanvallen van individuen of kleine groepen cybercriminelen. We zien al dat de kennis van hoe aan te vallen via de publieke dissectie van aanvallen in allerlei online forums via een trickle down model leidt tot meer kennis bij traditionele aanvallers. Er wordt door

[33] http://www.wnd.com/2012/01/chinas-cyberarmy-could-number-half-billion/
[34] http://nl.wikipedia.org/wiki/Chinese_Muur
[35] De EU is in zekere zin ook een defensiesamenwerkingsverband. Tot voor kort was er de WEU, West Europese Unie. De WEU heeft nooit veel bereikt en werd vaak als 'Schone Slaapster' aangeduid. De WEU is als zelfstandige entiteit opgeheven in 2011, maar de taken en ambities zijn overgegaan naar de EU. De cyberdimensie is juist de plek waar de nieuwe entiteit ENCS zich doet gelden. Zie: http://www.cpni.nl/projecten/european-network-voor-cyber-security-encs

meer mensen nagedacht en meer gestructureerd nagedacht over hoe systemen aangevallen kunnen worden. De traditionele wereld van beveiligingsonderzoekers, de White Hats, bevat een paar honderd mensen, sinds enkele jaren zijn er duizenden mensen bijgekomen wiens werk het is gaten te ontdekken en exploiteerbaar te maken.

Het doorsijpelen van kennis is al goed te zien in de nasleep van de Flame en Stuxnet virussen. Beide gebruiken PKI certificaten als aanvalsvector. Dat er in deze hoek veel te halen is, is bij PKI specialisten al jaren bekend[36], maar het was onder hackers en cybercriminelen tot voor kort een onbekende en ongebruikte aanvalsvector. Maar nu gelden rogue certificaten[37] als een groeiend probleem. Door de opkomst van goedgeorganiseerde aanvallers in staatsverband wordt het technische niveau van aanvallen snel hoger, zonder een navenante kwaliteitsstijging bij de verdediging.

Een andere bijwerking van hackende natiestaten is dat aanvallen nog verder uit de hobbysfeer raakt van de jaren ´80 en ´90 en uit de louche oplichterssferen van de jaren ’00. Professionele beveiligers en commerciële bedrijven kunnen goed geld verdienen met het ontwikkelen van aanvalsmiddelen en deze verkopen op een snel groeiende internationale markt voor digitale wapens. Hierdoor wordt Vulnerability Management veel moeilijker dan het was. Tot enkele jaren geleden was Vulnerability Research een kleinschalig fenomeen van fijnproevers en liefhebbers dat zich redelijk aan de oppervlakte afspeelde, nu is ze uitgegroeid tot een onzichtbare en professionele industrie. Dat zou alleen maar goed zijn als de uitkomst minder gaten in systemen zou zijn, maar dat is niet wat er gebeurt. Nieuw ontdekte gaten (0Days in jargon) worden niet gemeld aan de makers van het betreffende product, maar verkocht via openlijke en onderhandse kanalen. Met de koopkracht van natiestaten is er een opwaartse prijsdruk ontstaan – een top Vulnerability is immers vele malen goedkoper dan een straaljager, terwijl door Cyberwar goeroes gesteld wordt dat ze even doelmatig kan zijn. De opkomst van cyberlegers heeft door de vraag naar cyberwapens de markt op zijn kop gezet. De kans op responsible Disclosure[38] is daarom veel kleiner – als ontdekker van een defect in een stuk software kan kiezen tussen het melden aan de maker (en daar misschien een nette behandeling en een klein geldbedrag voor krijgen), dan wel het gat verkopen in een grijs, crimineel of spionagecircuit tegen een veel interessanter bedrag, is de kans groot dat het laatste gebeurt. De kans dat het gat gedicht kan worden neemt daarmee snel af; het nieuwe type kopers heeft belang bij het veiligstellen van hun investering en zal het zeker niet melden aan de makers van de software. Als het gat gedicht wordt, is het cyberwapen immers niet meer effectief.

The War on IP

De rol van Intellectueel Eigendom en – in het verlengde daarvan – octrooien en patenten is met de globalisering enorm toegenomen; in een werkelijkheid waar de bedrijven zaken alleen bedenken en door onderaannemers in een lagelonenland laten produceren is dat een logische ontwikkeling. In een dergelijke constructie zijn bouwtekeningen, ontwerpen en studies van veel waarde en vragen veel van informatiebeveiliging, temeer waar de onderaannemers zelf ambities hebben of ook voor de concurrentie werken.

Voor informatiebeveiliging zijn de consequenties van deze veranderde productiewijze ingrijpend:

- Niet geheel betrouwbare partijen moeten bij gevoelige informatie kunnen.
    - Deze informatie moet ontvlochten worden uit de interne kennisprocessen. Waar informatiemanagement dit niet gestructureerd oppakt, betekent ontvlechting dat de informatie gemaild wordt. De business moet immers door. Beveiliging kan dan hooguit met een vermanend vingertje komen.
- Bedrijfsspionage is een traditionele tak van sport, maar in het digitale verbonden domein enorm veel eenvoudiger dan voorheen.
    - Vanuit beveiliging wordt vaak op grond van de IP-risico’s zaken als Het Nieuwe Werken en mobiele devices tegengehouden. Zo lang de ICT geen alternatieven biedt, is dat ook het enig mogelijke, waarbij bedacht moet worden dat de frictie met de business voortkomt uit de

[36] Er zijn defecten die al sinds midden jaren ’90 bekend zijn, maar nog niet opgelost. Een voorbeeld is de ambiguïteit in de specificatie van de Extensions van certificaten. De Nieuw-Zeelandse cryptograaf Peter Gutman voorspelde in 1994 dat de afwezigheid van beperkingen op inhoud en lengte van ‘Extensions’ in certificaten tot misbruik kon leiden. In januari 2013 zijn de eerste in-the-wild aanvallen bekend geworden op beveiligingsapparatuur van Fortinet.

[37] http://capec.mitre.org/data/definitions/459.html , http://arstechnica.com/security/2012/06/flame-malware-was-signed-by-rogue-microsoft-certificate/ en http://www.scmagazine.com/hackers-raid-adobe-compromise-certificate-to-sign-malware/article/261175/

[38] http://en.wikipedia.org/wiki/Responsible_disclosure

bedrijfsdoelstellingen – de medewerkers overtreden vaak regels omdat ze hun werk willen doen. De business moet immers door.

- De technologie is beschikbaar, maar is afhankelijk van informatie classificatie en digitale labeling van informatie. Het hiervoor passende Digital Rights Management dossier schrikt af; het is een complex vraagstuk met een onduidelijke probleemeigenaar. Dit antwoord is dus voorlopig niet daadwerkelijk op de vloer beschikbaar.

Big Data

Een laatste element van de toegenomen wereldwijde exposure is te vinden in wat aangeduid wordt als Big Data. Vanuit de resultaten van 'Open Source Intelligence' (OSINT) is overduidelijk geworden dat veel gevoelige informatie over overheden en organisaties te herleiden is met het doorploeteren van de enorme hoeveelheden informatie die organisaties onbedoeld rondstrooien. Dit wordt bevestigd door de inlichtingendiensten, die omschakelen van kostbare en riskante spionage operaties naar OSINT.

Sommige specialisten in de OSINT beweren dat hacken en spioneren niet meer nodig is, omdat alle informatie wel te vinden is in publieke bronnen. Dit moge overdreven zijn, feit is dat organisaties de enorme hoeveelheden informatie niet beheersen. Dus het is hoogst aannemelijk dat in iedere geval veel beveiligingsinspanningen zich richten op het beschermen van informatie die al lang op straat ligt. Big Data is in ieder geval een ondergewaardeerd deel in de taakstelling van een beveiligingsorganisatie – een aanvaller kan uit Big Data zonder veel moeite herleiden hoe de beveiliging van een organisatie eruit ziet. Een kwartiertje op LinkedIn kan al een verbijsterende schat aan informatie opleveren over beveiligingsmiddelen en kunde van een organisatie. Dan is een beveiligingsorganisatie met een taakstelling die beperkt is tot de eigen voorzieningen een verspilling van geld.

De geboorte van cybersecurity

Om te begrijpen wie wij zijn en waar we heen gaan, is het van belang om te weten waar we vandaan komen. Het vak informatiebeveiliging evolueert immers mee met de dreigingen waartegen beveiligd wordt.

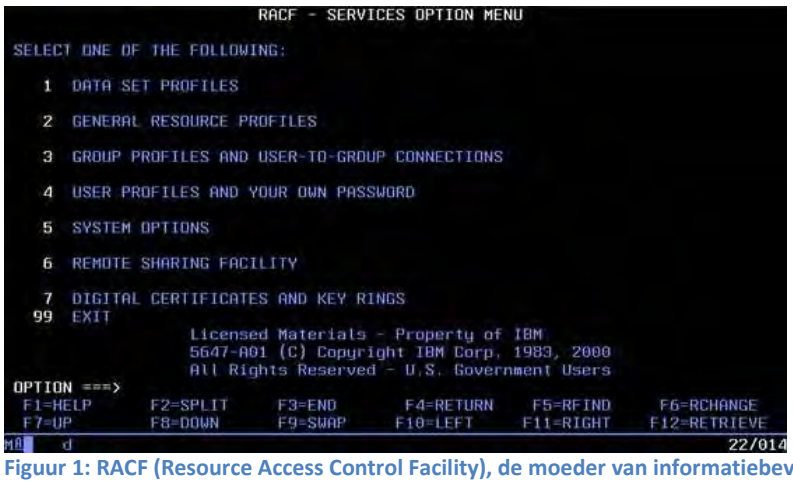
Traditioneel zijn er twee stromingen, Enterprise beveiliging en Internet beveiliging. Wat we op dit moment zien is dat deze twee hoofdstromingen convergeren tot een derde, geïntegreerde variant. Deze ontwikkeling loopt gelijk op met het in gebruik komen van de term Cyber Security en heeft daar ook duidelijke banden mee. Het is logisch om deze term te gebruiken voor de geïntegreerde omgang met informatiebeveiliging.

De convergentie is geen revolutie maar een evolutie. De oude vragen blijven immers bestaan, maar daar komen nieuwe bovenop. In de volgende paragrafen wordt deze geschiedenis in het kort beschreven, omdat dit ons denken en ons doen bepaalt.

Enterprise security: sinds 1968

Informatiebeveiliging is geen jong vakgebied. Waren de eerste computersystemen door hun complexiteit van zichzelf ontoegankelijk en single user, met de komst van de terminal en het netwerk ontstond de noodzaak van user accounts en al snel daarna van beveiliging. Gegeven de kosten van hardware en software was het computerbezit beperkt tot de hele grote organisaties en time sharing instellingen. In deze wereld van gedeelde mainframes die gebruikt werden voor meerdere multinationals ontstond de basis van het denken over informatiebeveiliging.

Enterprise Security gaat ervanuit dat informatiebeveiliging een probleem is van de infrastructuur en de gebruiker de grote bedreiging is. Een aantal jaren later kwam daar het inzicht bij dat de ICT-er met meer kennis en meer rechten in systemen, ook bewaakt dient te worden. In dit gedachtegoed hebben alle ICT-medewerkers beveiligingstaken, in een gestructureerd weefsel van preventie en mitigatie. En dus hebben ook alle ICT-medewerkers verstand van en taken in beveiliging, geheel in lijn met het denken in matrixorganisaties, zoals het uitgekristalliseerd is in ITIL® v2. De zwakte in dit matrixdenken is dat het securityprocessen wel benoemt en verdeelt, maar dat het de aanwezigheid van kennis, uitvoering en coördinatie van de inspanningen veronderstelt en niet verzekert. Dit wordt deels gecorrigeerd in ITIL® v3, dat in 2007 verschenen is, maar de samenhang en de uitvoering blijven een zwak punt.



Figuur 1: RACF (Resource Access Control Facility), de moeder van informatiebeveiliging

De grootste bedreiging voor informatie en informatiesystemen zijn in de gesloten wereld van toen de eigen medewerkers. In die tijd waren informatiesystemen alleen maar toegankelijk via eigen bedrijfsnetwerken en end-user devices die op kantoor stonden en daar ook bleven. De belangrijkste vraagstukken in die begintijd waren autorisaties en wachtwoorden die opgeschreven werden op het moment dat een medewerker veel verschillende soorten informatiesystemen moest gebruiken. Pas na de introductie van de pc in bedrijven[39] kwam daar het vraagstuk van virussen bij, enige jaren later versterkt door e-mail. Kenmerkend genoeg werden virussen in die periode (en soms nog steeds) meer als een ICT-vraagstuk gezien dan als beveiligingsvraag.

[39] Organisaties omarmden de pc veel later dan consumenten, tussen 1994 en 1997. E-mail en Internet op de werkplek zijn nog langer 'buiten' gehouden, met een beroep op security.

De buitenwereld is alleen bedreigend door hackers die inbreken. De inbrekers in deze periode van heel vroeg Internet breken in omdat ze het kunnen, als een bergbeklimmer die de Mont Blanc bedwingt. Dit type aanvallers richt zich op de ICT-voorzieningen, niet op de organisatie en de informatie zelf. De beveiliging is dan ook beperkt; de hacker is een technische goeroe die wil laten zien hoe goed hij is. Niet om schade aan te brengen, hoewel dat natuurlijk wel gebeurde, omdat sommige zelfbenoemde goeroes toch niet zo goed waren als ze zelf vonden.

Het ambitieniveau van Enterprise Security is laag: dit soort technisch geavanceerde hackers komt toch wel binnen, dus daar kun je uiteindelijk toch niets tegen doen. En daarbij stelden de meeste organisaties dat er toch niets te halen was, onder het motto dat onbekend ongehacked maakt. De aandacht gaat daarom veel meer uit naar de eigen medewerkers die technisch niet zo capabel zouden zijn, en naar preventie van incidenten. Dit gebeurt door middel van definitie van preventieve beveiligingsmaatregelen aan de beleidskant en het creëren van Security Awareness bij ICT-medewerkers en eindgebruikers. Technische maatregelen waren vooral duur en bordjes 'verboden toegang' een goedkoper en afdoend alternatief. De awareness aanpak gebeurde ook vanuit de positivistische aanname, dat als mensen weten dat iets niet goed is, dat ze het dan nooit meer doen. De resultaten vielen in de praktijk nogal tegen.

De grens met de buitenwereld is bekend en beperkt, hij bestaat uit een modempool of een huurlijn. Toen de bandbreedte toenam en Internet aan zijn opmars begon, werd de router uitgebreid met een ACL (Access Control List) en een zeer beperkt packet filter. In 1988 werd deze omgedoopt tot Firewall, de buitenmuur die de brand moet tegenhouden. De opkomst van de Firewall culmineerde begin jaren '90 in de Demilitarized Zone (DMZ), een "sort of crunchy shell (firewalls, mail relay servers en webservers) around a soft, chewy center[40]". Access bestaat in en bepaalt de buitengrenzen en toegangsbeveiliging is een taak van de netwerklaag. Tussen 1990 en 2000 was dit een bewuste keuze, die werd gemaakt uit kostenoverwegingen[41]. Het enige alternatief was immers ieder object afzonderlijk te beveiligen.

In de kern van dit kokosnoot-denken (harde buitenkant, zachte binnenkant) staat doelmatigheid: het is eenvoudiger de toegang tot informatie te beveiligen dan de informatie zélf, gegeven dat er veel minder toegangen zijn dan te beveiligen objecten. De informatie was bovendien de grote onbekende, een grote niet-geclassificeerde berg nullen en enen. De kern van dit denken is het zogenaamde 'chokepoint'; organisaties moeten het aantal toegangswegen minimaliseren en die dan goed beveiligen.

Sindsdien is de hoeveelheid informatie geëxplodeerd en het aantal toegangswegen daartoe evenzeer. Het chokepoint is nu het device[42], niet langer het netwerk. In de BYOD problematiek is de logische vraag dan ook hoe het device hetzelfde beveiligingsniveau te geven als devices die onderdeel uitmaken van het interne netwerk. Als je bedenkt dat fysieke toegangsbeperking de belangrijkste beveiliging van het interne netwerk is, is evident dat een mobiel device nooit dit niveau kan hebben. Daarom is de aanpak met chokepoints niet langer houdbaar. Indachtig het uitgangspunt dat lokale beveiliging uiteindelijk zwak is[43] en deze aan apparaten verbonden is, is het lang uitgestelde moment van beveiliging op objectniveau, aangebroken.

Internet security: sinds 1988

De opkomst van het Internet leidt tot nieuwe vraagstukken. Het Internet is op de keper beschouwd onbeveiligd. Er is één bedreiging waar het tegen bestand moet zijn, en dat is een kernoorlog. Voor andere bedreigingen, dus inclusief alle digitale vormen, heeft het Internet van zichzelf geen bescherming. Met IP v6 en DNSSec worden feitelijk voor het eerst serieuze stappen ondernomen om beveiligingsfuncties in de kern van Internet aan te brengen[44].

De afwezigheid van beveiliging wordt een probleem als de Morris Worm wordt losgelaten, op 2 november 1988. Morris legt binnen een dag een groot deel van het Internet lam. Dit moment is de geboorte van

[40] http://www.cheswick.com/ches/papers/gateway.pdf , 1990. In deze paper wordt de eerste firewall besproken.
[41] Onder meer in Firewall Systems, Norbert Pohlmann, 2001, p. 44 e.v.
[42] http://nakedsecurity.sophos.com/2012/07/13/perimeter-security-expansion-disintegration/
[43] Het is voor een aanvaller moeilijker toegang te krijgen tot een systeem waarop deze geen rechten heeft, dan om beperkte rechten uit te breiden. Dit heten 'elevation of priviliges attacks'; de gebruiker is de hoge buitenmuur gepasseerd en heeft in plaats van een zeer beperkte of zelfs geen interface een hele reeks van mogelijke aanvalsoppervlaktes.
[44] Strikt genomen ging de beveiliging van BGP hieraan vooraf. Dit Border Gateway Protocol is echter alleen iets voor de beheerders van het Internet zelf. Daarnaast was er nog RADIUS, waarop de gebruiker in de eerste jaren van Internet moest aanloggen (bij het inbellen). Deze login was omwille van de faktuur; het was niet bedoeld als beveiligingsfunctie.

beveiliging op Internet en heeft de denkwijze en de inrichting bepaald. De partijen die het Internet besturen, richten CERT-CC op, een samenwerkingsverband van CERTs (Computer Emergency Response Teams). Een CERT is de security-organisatie van universiteiten, vooral gericht op de buitenwereld waarmee informatie gedeeld wordt. In CERT-CC werken de CERTs samen, vooral bij incidenten.

De gedachte achter de CERTs is dat security een specialistisch werkveld is, waar niet alle ICT-ers zich mee bezig hoeven te houden. In een CERT zitten de slimste mensen bij elkaar. Zij houden zich vooral bezig met optreden bij incidenten. Security bestaat dus uit reactie. Preventie bestaat ook: het dichten van gaten in systemen en software voordat ze misbruikt worden. Maar dat is de taak van de makers in het softwareontwikkelproces, niet van de beheerders.

De BugTraq[45] revolutie

De CERTs boekten in de ogen van veel mensen onvoldoende resultaten, in het bijzonder op het gebied van het laten verhelpen van gaten. In de praktijk werden gaten zelden gedicht en als ze gedicht werden in een nieuwe versie, werd dat er niet bij verteld. Met de toename van het Internetgebruik vanaf 1993 kwamen er bovendien steeds meer organisaties zonder een eigen CERT, die dus niet op de hoogte waren van wat er in deze besloten gremia aan informatie gedeeld werd. De CERTs communiceerden alleen onderling en met de vendors, de informatie was niet publiek toegankelijk. Bovendien maakten vendors het moeilijk voor CERTs om informatie onderling uit te wisselen, met een beroep op het bedrijfsbelang en het risico dat andere gebruikers van de producten lopen als meer aanvallers van een gat weten.

In 1993 start de Amerikaan Scott Chasin daarom met BugTraq, een open platform waar beveiligings-verantwoordelijken over gaten in systemen konden lezen en ze konden publiceren, zodat bekend werd waar problemen zich konden voordoen. Bovendien konden vendors via publicatie van de gaten onder druk worden gezet om kwetsbaarheden op te lossen; als iedereen in een publieke bron kon lezen dat ergens een gat in zit, dan zou de fabrikant er werk van maken het op te lossen. Dit is het nog steeds niet opgeloste vraagstuk van Vulnerability Disclosure: met het posten van de kwetsbaarheid maak je ook aanvallers attent op de mogelijkheden, en kunnen meer doelen geraakt worden. De praktijk leert ook dat vendors alleen gaten dichten als er druk uit de markt op staat: het dichten van gaten kost immers serieus geld. Zeker tussen 1990 en 2005 was vrijwel geen enkele grote vendor in staat of bereid serieus aandacht te schenken aan de beveiliging van de producten. Ook nu nog zit er regelmatig twee jaar tussen het ontdekken van een gat door een security onderzoeker en het verschijnen van een fix door de leverancier. Er zijn grote leveranciers die geen standaardprocedure hebben voor het ontvangen en verwerken van Vulnerabilities. Na het uitbrengen van een fix kan het dan wel nog een jaar duren voordat de fix algemeen uitgerold is. Vóór BugTraq was de doorlooptijd echter nog vele malen langer. De situatie is dus verbeterd maar nog steeds niet goed. Individuele leveranciers hebben in een aantal gevallen heel veel verbetering gerealiseerd, er zijn echter geen ontwikkelingen gaande die een verbetering over de hele linie afdwingen.

Cybercrime en de enterprise

Met de opkomst van Internet ontstond een bijpassende vorm van criminaliteit; cybercrime. Op de werkelijkheid van beveiliging heeft dit echter weinig impact gehad; cybercriminelen richten zich in de praktijk vooral op consumenten en banken. De bedreigingen voor Intellectueel eigendom (‘IP’) die uitgaat van sommige cybercriminelen geldt slechts voor een klein deel van de organisaties (de meeste organisaties hebben immers geen trade secrets) en de meeste medewerkers bellen de systeembeheerder als er iets raars gebeurd op de pc. De werkelijkheid van cybercrime speelt zich primair af in het domein van Internet security en consumenten; voor de meeste organisaties is cybercrime dan ook alleen indirect een aandachtspunt bij het beschermen van de klanten.

[45] BugTraq is na een aantal overnames eigendom geworden van Symantec: http://www.securityfocus.com/.

Figuur 2: het Ukash virus - ransomware

Bij het beschermen van klanten is de rol van regulering groot: het gaat voor een groot deel over het beschermen van de privacy van de klanten. De druk die hierachter zit van overheidswege is beperkt en de sanctie laag. Vanuit die optiek is er nog wat tijd. Pas als de richtlijn van de EU over Privacy by Design[46] ingevoerd wordt, wordt het prominent. Gegeven de vereisten in het concept is er dan hoogstwaarschijnlijk te weinig tijd om alle veranderingen door te voeren.

Wat afgelopen jaren echter duidelijk is geworden, als bijwerking van het optreden van Anonymous, is dat de Enterprise niet immuun is voor cybercrime, omdat de klanten steeds meer ook users in de informatievoorziening zijn. Zo werd KPN onaangenaam verrast[47] met een lijst gebruikersnamen en wachtwoorden van klanten. Dit leidde tot een ongekende maar terechte ingreep; de voorzieningen van KPN werden afgesloten en de klanten gedwongen hun wachtwoorden te veranderen. Nu waren de wachtwoorden weliswaar niet via een hack op de voorzieningen van KPN verkregen, maar via een webwinkel van Babydump. KPN moest toch tot dit optreden overgaan om haar klanten te beschermen – de klanten gebruikten hun KPN mailadres om op andere sites aan te loggen en best vaak met hetzelfde wachtwoord. Dit toont aan hoezeer de wereld verbonden is en wat dat betekent voor beveiliging. Dat is natuurlijk niet nieuw, maar deze verandering is grotendeels genegeerd. Het duurt in de regel even voor het daadwerkelijk mis gaat, en als het dan mis gaat is er opeens paniek in de tent. De situatie illustreert bovenal dat Security heeft zitten slapen.

Conclusie
ICT security heeft een nieuwe taak: het beveiligen van de klant.

Cybersecurity: sinds 2010

Het Internet security denken is vooralsnog aan veel organisaties voorbijgegaan. Zij wanen zich nog veilig achter de firewall. Maar wat bij steeds meer organisaties is te zien is dat de twee hoofdstromen, Enterprise security en Internet security, bij elkaar komen. De aftrap van een integrale vorm van security is gegeven door het Stuxnet virus, een digitaal wapen gericht tegen de Iraanse atoomindustrie dat in 2010 bij het grote publiek bekend werd.

Bij Stuxnet vallen vier zaken op. Ten eerste het gebruik van vier zero days[48] tegelijk. Dit benadrukt het punt dat beveiliging meer aandacht moet besteden aan Vulnerability management. Ten tweede het aanvalsdoel. Dit doel is SCADA – Stuxnet richt zich op industriële automatisering en niet op de traditionele doelwitten als de werkplek of de mailserver. Hiermee treedt security buiten het pure ICT-kader van de kantoorautomatisering (KA). Ten derde de betrokkenheid van natiestaten – naar verluidt is de aanval uitgevoerd door Amerikaanse geheime diensten. Voor veel betrokkenen is Stuxnet het bewijs dat cyberwar een reëel gevaar is. Het vierde opvallende element is dat het gebruik maakt van gestolen PKI certificaten. Dit onderstreept een cruciale zwakte in het model van wereldwijd vertrouwen dat via de grote CA's en de preinstallatie van certificaten in besturingssystemen en applicaties ontstaan is.

[46] http://www.cbpweb.nl/Pages/med_20120307-herziening-privacywetgeving-eu.aspx
[47] http://webwereld.nl/nieuws/109493/-kpn-lek--blijkt-lektober-nasleep-van-baby-dump-nl.html
[48] Een zero day is een defect in de beveiliging van een systeem of een applicatie dat nog niet bekend is bij de makers ervan, en waarvoor dan ook nog geen verdediging (update, patch) beschikbaar is.

Stuxnet is instrumenteel geweest in de geboorte van de term Cybersecurity, een begrip dat de verschillende gelijktijdige ontwikkelingen in een enkel kader plaatst. Het kader van Cybersecurity is veel breder dan de traditionele kaders van Enterprise en Internet Security. Het ICT-kader van Security is de historisch bepaalde beperking van het mandaat van security tot waar ICT over gaat. Dit vormt een aanzienlijk risico, een risico dat de komende periode nog groter wordt.

Bij de meeste organisaties is de beveiligingskennis rond computers alleen aanwezig bij de organisatie die zich bezig houdt met kantoorautomatisering, terwijl een steeds groter deel van de business digitale middelen inzet zonder kennis van de bijbehorende beveiligingsvraagstukken. Discussies over mandaten en scope verlagen de weerbaarheid van organisaties op kritieke momenten in aanzienlijke mate, zeker als ze bewaard worden tot het uitbreken van de echte crisis.

Conclusie
De kennis van computerbeveiligingsvraagstukken is nu vrijwel het alleenrecht van de ICT afdelingen die zich richten op kantoorautomatisering; deze koppeling moet zo snel mogelijk doorbroken worden: hetzij door Security te ontkoppelen van KA, dan wel ICT breder in te zetten dan alleen voor KA. Gegeven de schaarste van kennis is de tweede oplossing voor de meeste organisaties de aangewezen weg.

Door het Internet of Things is het speelveld van Cybersecurity in omvang en complexiteit aan het exploderen. Sinds 2008 zijn er meer systemen verbonden aan het Internet dan er mensen op aarde zijn. In 2020 zullen dit er – volgens conservatieve schattingen[49] - tien keer zoveel zijn. Het kunnen er net zo goed duizend keer zoveel zijn. Daarbij hebben we het niet over iPads of andere spannende mobiele gadgets. Tegen die tijd zal iedere nieuwe auto enkele tientallen IP-adressen hebben en de luxere modellen enkele honderden. Een van die adressen zal willen verbinden met de bedrijfsmailserver om de agenda te tonen en de bijpassende route te plannen, terwijl een heleboel andere systemen de auto verbinden met de garage en de wagenparkbeheerder. Vanuit het traditionele perspectief bezien ligt de security perimeter van het bedrijf op dat moment ergens in het motormanagement systeem[50]. Zodra de autodieven digitaal gaan, zullen ze ook via het bedrijfsnetwerk aanvallen.

Een waargebeurd verhaal

Op 27 december 2005 werd bekend dat er een probleem was met WMF, het Windows Metafile Format. Dit is een basis-component van Windows, dat in alle versies van Windows en Office zit. Niet duidelijk werd, wat nu precies het probleem was. Wel was duidelijk dat het een zeer ernstig gat was, en dat er aanvallen mee uitgevoerd werden.

Bij vrijwel alle organisaties waren de bezettingen vanwege de kerstvakantie minimaal. De verdedigingslinies waren dus erg dun bezet. Er was een gat, en er was geen zicht op een fix.

De meeste organisaties hebben niets gedaan: als ze er al van op de hoogte waren, was het probleem dat er immers geen fix beschikbaar was. Microsoft kon in eerste instantie ook niet aangeven wanneer deze zou komen.

Een van de ministeries in Den Haag besloot als crisismaatregel alle externe toegang van Office-documenten te blokkeren, totdat de oplossing netwerkbreed was uitgerold. Hiervoor werden alle downloads en e-mailberichten gefilterd op attachments en berichten in de Outlook RTF-opmaak geblokkeerd. Dit was een ingrijpende aanpak, die de risico's tot op grote hoogte wegnam.

Uiteindelijk verscheen de Microsoft spoedfix op 5 januari. Dat was erg snel, maar door het testen en uitrollen van deze 'not fully regression tested' update zijn de meeste organisaties zeker een maand kwetsbaar geweest zonder enige mitigerende maatregelen. De meesten zonder het te weten; het was kerstreces.

De meeste organisaties hebben overigens ook niet de technische middelen voor dergelijke filtering in huis.

Een voorbeeld van de real-time werkelijkheid: Vulnerability Management

De nadruk op preventie en de traagheid van de beveiliging in de Enterprise was mogelijk zolang de eigen voorzieningen in hoge mate afgeschermd waren. Aan het vraagstuk van Disclosure wordt in de Enterprise dan ook relatief weinig aandacht besteed: de meeste systemen staan immers 'binnen'. Vulnerability Management wordt gedachteloos lineair vertaald naar Patch Management. Het niet beschikbaar zijn van een patch vereist – bij een kritieke applicatie – andere maatregelen maar dat kan heel ingrijpend zijn en wordt zelden gedaan, zoals in de kadertekst op deze pagina[51].

[49] http://www.frankwatching.com/archive/2011/09/23/the-internet-of-things-infographic/
[50] http://hackaday.com/2012/07/31/control-everything-in-your-car-with-the-car-kracker/
[51] Voor de details: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560

Het bekend zijn van een Zero Day in bijvoorbeeld een tekstverwerker zou moeten leiden tot ingrijpende maatregelen om dit gat zoveel mogelijk te sluiten tot er een update is, of het gewraakte product vervangen. Bijvoorbeeld het tegenhouden van alle attachments en downloads van bijbehorende bestanden – de organisatie is immers op één aanvalsvector onbeschermd.

Wat op het Internet een doodzonde is (wachten op een patch), is in de meeste enterprises echter nog heel normaal: een gat wordt in de regel pas bekend omdat er een update is. Toen de mode met virussen was via fileparsers[52] mailservers te hacken en een aantal leidende producten in AV-land soms maandenlang een groter risico voor de beveiliging vormden dan een hulp voor de beveiliging, is vrijwel niemand van product gewisseld. Met het verdwijnen van de buitenmuren is deze afwachtende houding niet vol te houden.

[52] Tussen 2004 en 2007 werden de parsers die gebruikt werden door antivirusproducten om gecomprimeerde bestanden te kunnen inspecteren met gemanipuleerde attachments rechtstreeks aangevallen.

Een nieuw beveiligingsparadigma

In het voorgaande is geïllustreerd dat het traditionele denkkader, de gevestigde werkwijzen en zelfs een aanzienlijk deel van de technologie van informatiebeveiliging niet meer past. In de volgende paragrafen worden de contouren geschetst van hoe het nieuwe beveiligingsparadigma er uit zou kunnen zien.

De reorganisatie van beveiliging

Om onze organisaties en de samenleving te beveiligen zal een aantal zaken op de schop moeten. Dit zijn in ieder geval:

- de cultuur van beveiliging
  - van reactief naar initiatief
- de besturing van beveiliging
  - Van een uitvoerende naar een lerende organisatie,
  - van een trage naar een real-time organisatie,
  - van verkokerde naar samenhangende processen en middelen,
  - van een verkokerde naar een samenwerkende organisatie[53].
- de technologie
  - van egelstellingen naar samenhangende beveiliging

Een cultuurverandering in beveiliging

Beveiliging is een reactieve, defensieve en intern gerichte exercitie. Het personele gebouw is niet in balans, er is teveel aandacht voor ICT-beheervraagstukken en te weinig voor innovatie van ICT-middelen en ontwikkelingen langs de buitenranden van de organisatie. Dit vraagt een cultuuromslag en zoiets kan niet per decreet gerealiseerd worden.

Een pragmatische aanpak die een cultuuromslag in gang kan zetten is het verbreden van de bezetting; beveiliging is nu sterk een monocultuur van liefhebbers. Het is de hoogste tijd voor professionalisering. Een goede weg is om voor een multidisciplinaire benadering te gaan: ontwikkelaars en communicatiemedewerkers zullen niet alleen hun expertise maar ook hun cultuur meenemen, wat tot een veel gebalanceerdere aanpak zal leiden. Ook het mede-opstellen van organisatiedeskundigen en business developers zal tot een betere culturele balans leiden.

De cultuur is ontstaan over een lange periode en wordt gedragen door individuen. De cultuur van informatiebeveiliging is reactief en veelal conservatief. De bijbehorende opvatting luidt dat alleen het allerbeste goed genoeg is. Het besef ontbreekt dat goed soms ook goed genoeg is.

De eerste stap is het doorbreken van de beleidskaders die een verbinding tussen informatiebeveiliging en LAN en/of netwerkbeveiliging leggen. Deze is niet in alle organisaties formeel – of zichtbaar – aanwezig, maar als deze er is, is het een grote barrière.

De tweede stap is het meer multidisciplinair maken van de beveiligingscultuur. Om een andere culturele mix te creëren is het toevoegen van mensen met een achtergrond als databasebeheer en software-development een pragmatische methode. Het toevoegen van andere disciplines, zoals communicatie en juridisch is op termijn ook een goed plan; deze invalshoeken zijn van groot belang en nu al vaak onderontwikkeld. Alles tegelijk kan wat veel van het goede zijn.

[53] Samenwerken met entiteiten buiten de eigen organisatie, zoals leveranciers, klanten en ketenpartners. Dit zal zich ook gaan uitstrekken tot ad hoc samenwerkingen met overheden, bij cybercrime of cyberwar incidenten.

Kennis en metakennis

Voor de organisatie geldt dat op een breed terrein hoogwaardige kennis nodig is. De logische vraag is dan ook welke kennis rendabel in-house is, welke kennis in-house moet zijn, en wat er van derde partijen afgenomen kan worden.

Informatiebeveiliging is historisch gebonden aan de interne ICT-afdeling en zal geraakt worden door de veranderingen die de regieorganisatie met zich mee brengt. Hoe het ook precies uitpakt, zeker is dat beveiliging op meer afstand van de leveringsorganisatie zal komen te staan. Dat legt de bijl aan de kennisstroom; op dit moment wordt de technische kenniscomponent van informatiebeveiliging onderhouden door te doen. Dat zal verdwijnen of veel minder worden. De onderwijsmarkt zoals deze nu bestaat kan dit gat niet opvullen, of het nu regulier dan wel commercieel onderwijs is, zij is bovenal productgeoriënteerd en gericht op de onderste regionen van het kennisgebouw. Er zijn geen aanwijzingen dat dit snel zal veranderen, en mocht dit gebeuren dan is enige terughoudendheid op zijn plaats. Een opleiding voor gevorderden in informatiebeveiliging zal immers voor recruiters een populair jachtterrein zijn. Zo lang er kennisschaarste is in informatiebeveiliging – en die zou maar zo heel lang kunnen aanhouden.

Zaak is dus de directe voeding met de praktijk in stand te houden, omwille van de kennisstroom. Het onderhouden van de benodigde kennis is verre van eenvoudig, maar een pragmatische insteek zou tot resultaten kunnen leiden. Zo zou een organisatie afspraken kunnen maken met externe leveranciers of andere organisaties voor kennisstages, waarbij de eigen medewerkers in projecten van de leverancier of bij een ander bedrijf meewerken. Dit past absoluut niet in het traditionele leverancier-klant model, maar dat model staat met de regieorganisatie toch al op zijn kop. Een bewezen aanpak is het proces van Vulnerability management; door het bestuderen van nieuwe bedreigingen als ze binnenkomen is het een uitermate goede leerschool. Een andere aanpak is het gestructureerd doornemen van post-mortems van beveiligingsincidenten en het uitvoeren of bestuderen van de resultaten van penetratietests. Een laatste aanpak voor een gestructureerde methode is het zelf onderhouden van de gedetailleerde normenkaders voor beveiliging.

De marktvraag van organisaties zal meer expliciet uiteenvallen in een diensten- en een kennisvraag. Voor alle specialistische maar slechts incidenteel noodzakelijk kennis geldt immers dat het onderhoud ervan de mogelijke baten zal overstijgen. Dit zal het onderscheid tussen onafhankelijke consultants, Value Added Resellers en implementatiepartijen helderder zal maken en de consultants dwingen zich onafhankelijker van de vendors op te stellen. Daar hangt uiteindelijk wel een prijskaartje aan, en zoals dat gaat, wordt dit doorbelast.

Toezicht versus levering

Bij een toenemend aantal bedrijven komt informatiebeveiliging in een operationele spagaat terecht: Security gaat over beleid en toezicht maar levert ook beveiligingsdiensten, al dan niet extern ingekocht. In dat geval heeft Security te veel petten op. Als toezichthouder kan ze andere ICT-leveranciers (zowel intern als extern) op de vingers tikken en in de leveranciersrol beconcurreren. Dit is een onverkwikkelijke combinatie, zeker in een hybride organisatie met interne en externe leveranciers. In de praktijk leidt dit nog eens af van een andere en vaak vergeten Security taak, te weten het bedienen van de beveiligingsmiddelen. Het beheer van de beveiligingsmiddelen mag geen taak zijn van Security. Diensten en producten leveren en beheren is een taak van ICT, zowel bij Security als bij andere diensten.

Security is een feitelijk onderdeel van de business, en dient zich als zodanig op te stellen. Te vaak is de historische context met de ICT-afdeling hiervoor een hindernis. Zaak is de scheiding van verantwoordelijkheden goed door te voeren, zodra de schaalgrootte dit toelaat. Dat is in de Enterprise eigenlijk altijd het geval.

Zo ontstaat er een Security beleidsorganisatie, een Security architectuurorganisatie en een Security toezichtorganisatie naast een operationele organisatie die de operationele beveiligingsdiensten uitvoert. Daarnaast zal er een interne leverancier van Security diensten bestaan die organiek onder ICT valt. Hoe beleid, architectuur, toezicht en operatie optimaal in te passen in de organisatie is afhankelijk van de organisatie. Indien informatiemanagement vanuit de business ingericht is, is dat de aangewezen plaats voor beleid en architectuur. Toezicht valt logischerwijs toe aan de andere interne toezichtorganisatie, zoals een Interne Audit organisatie. Het uitvoeringsorgaan voor Security zal een losse entiteit zijn.

De besturing van beveiliging

In de voorgaande analyse is vastgesteld dat de activiteitenbeveiliging nu bestuurd wordt vanuit drie bronnen

- als verlengstuk van ICT;
- in reactie op incidenten in de eigen organisatie en in de media;
- in de uitvoering van standaarden, versterkt door compliance en audit.

Uit de regieorganisatie komt een heel andere ICT-organisatie voort dan de ICT-organisatie zoals we die vandaag kennen. Hoewel sommige organisaties hier al geruime tijd en vol optimisme over de lonkende vergezichten[54] naartoe werken, blijkt dit een zeer moeilijke transitie. Grotendeels kan dit toegerekend worden naar een aantal onjuiste aannames[55], bovenal de aanname dat een regieorganisatie alles in de markt kan vinden en dat alles goed samenwerkt als de magische invloed van open standaarden haar werk doet en het geheel geïntegreerd zal samenwerken.

Voor de Security geldt dat zij bij de transitie naar de regie-organisatie een onnodige en extra complicerende factor is en in sommige situaties zelfs een struikelblok. Zeker gegeven de verleiding vanuit ICT om Security argumenten te gebruiken tegen allerlei nieuwe ontwikkelingen. Deze zijn overigens niet per definitie als obstructie bedoeld, maar komen ook vaak vanuit valide zorgen en betrokkenheid voort. Dit is echter een contraproductieve vermenging van rollen. Daarom is het noodzakelijk om toezichthoudend Security af te scheiden van ICT, alvorens de transitie naar een regieorganisatie in te zetten.

Security als verlengstuk van ICT is dus een onwenselijke en niet houdbare situatie; deze verbintenis moet verbroken worden. De andere twee bronnen verdienen juist meer nauwgezette aandacht:

- Incidentafhandeling zal gestructureerd moeten worden; een formeel post-mortem proces[56] helpt met het leren van de lessen en vermindert de neiging om klaarliggende oplossingen opportunistisch te koppelen aan toevallige incidenten.
- Het blind volgen van Best Practices als checklists is bestuurlijk gezien begrijpelijk, maar stelt slagen voor het examen boven het beheersen van de stof. Organisaties zullen hun eigen actuele normenkader moeten onderhouden, en kunnen hiervoor gebruik maken van de verzamelingen Best Practices. Met het onderhouden van de eigen normenkaders zal de actualiteit en bruikbaarheid toenemen, daarnaast zal het de kennisstroom op een positieve manier beïnvloeden. Dit verandert het audit-proces, maar de auditoren kunnen en zullen hier positief aan bijdragen.

Dit geheel zal aangevuld moeten worden met informatie uit andere bronnen:

- Analyse van incidenten bij andere organisaties, bij voorkeur op basis van post-mortems (zie boven).
- Resultaten van oefeningen, wederom op basis van incidenten elders of van theoretische incidenten.
- Volgen van ontwikkelingen en plannen in de organisatie, niet om er goed- of afkeuring op te geven, maar om erop te anticiperen.
- Volgen van ontwikkelingen en plannen in de markt om erop te anticiperen.

Immers, nog belangrijker dan het organiseren van de bronnen van handelen is het organiseren van de kennis. Het is natuurlijk vermakelijk als je hoort dat de competitie ook gehacked is, maar het wordt pas zinvol als de organisatie wat leert van fouten die anderen maken.

De organisatie van Security vraagt naast kennismanagement nog meer. Notoir lastig is het invullen van een organisatie met veel en diverse verantwoordelijkheden. Is ieder vakje in het organogram één functionaris, of tien? Welke functies kunnen gecombineerd worden? Zo kent het Forrester-model 26 blokken[57], en menig Security organisatie zal niet precies dat aantal medewerkers hebben. En indien het er toevallig wel 26 zijn, hoe passen de individuen die er zitten precies in de hokjes? Hetzelfde geldt voor andere modellen[58].

---

[54] http://www.twynstragudde.nl/pdf/publicaties/Deregieorganisatiealskansvooractievefacilitairesturing.pdf
[55] http://dspace.ou.nl/bitstream/1820/2994/1/BPM%26ITAdeSwart090310.pdf. In het overzicht op p.6 is goed de veronderstelde compleetheid van het marktaanbod te zien.
[56] Denk hierbij aan onderzoeken na ongelukken in de luchtvaart. ICT organisaties in organisaties in de luchtvaart zijn niet toevallig op dit punt goed ingericht.
[57] http://eval.symantec.com/mktginfo/enterprise/articles/b-article_security_organization_20_building_a_robust_security_organization.en-us.pdf
[58] http://www.ossie-group.org/media/PROF-001-Wheeler.pdf

Volgens het Forrester model zou een organisatie van per 500 ICT users één FTE security hebben. Voor de meeste organisaties is het organogram dan ook zinloos: met 4 medewerkers 26 hokjes vullen is een onmogelijke opgave. De verschillen tussen organisaties zijn bovendien te groot om een dergelijke vuistregel met enige nauwkeurigheid te kunnen opstellen. Factoren als complexiteit van de ICT, de fluctuaties in de organisatie, de mate waarin in ketens gewerkt wordt, de formele kant van de werkelijkheid zoals de mate van privacygevoelige data of een wettelijke opdracht als het VIR-BI, maar ook de grote verschillen tussen individuen maken het uitermate moeilijk om hier een kant-en-klaar model van te maken. De leerboeken en de methodes zouden hiervoor handvatten moeten aanreiken, maar die zijn uitermate schaars.

Uitgaan van de verantwoordelijkheden is daarom niet de aangewezen werkwijze. Zoals iedere manager weet is de aansturing van een omvangrijk apparaat bestaande uit eigenwijze vakspecialisten geen sinecure. Voor ideeën hoe hiermee om te gaan, is een klein uitstapje naar organisatietheorie op zijn plaats. Van grote hulp kan het inzicht van de 'span of control' zijn. Een span of control is het aantal mensen dat een persoon kan aansturen[59]. Dat aantal is afhankelijk van een aantal factoren[60], zoals de hoeveelheid interacties en de hoeveelheid veranderingen. In de oudste gestructureerde organisatie, de krijgsmacht, geldt als uitgangspunt dat het optimale getal 4 is. Een leidinggevende in de krijgsmacht stuurt 4 mensen aan en verzorgt de liaison met de bovenliggende en onderliggende laag. In deze opzet is de leidinggevende per definitie een meewerkend voorman, en alleen in de top van de organisatie is er ruimte voor fulltime bestuurders. In bedrijven is dit model in meer of mindere mate verlaten sinds de jaren '80, in een zoektocht om de overhead te verminderen. Het gevolg is dat in de bestuurlijk 'platte organisatie' een span of control voor de vrijgestelde manager[61] van 20 tot 75 medewerkers bedraagt[62].

De consequentie van dit type management op afstand is dat:

- het management met de voeten ver van 'de klei' staat;
- abstractie en procesfocus overheersen, herkenbaar aan formele rapportages, procedures en checklists;
- een tweede, vaak informele hiërarchie van mee (of tegen-)werkende voormannen rond de inhoud ontstaat.

Op zichzelf is management door processen en op afstand niet per definitie een probleem, maar dit vraagt een hoge mate van autonomie (in taakopvatting en taakuitvoering) van de medewerker op de vloer en aandacht voor alignment tussen de formele en de informele hiërarchie. Een hoge mate van autonomie van de medewerker zal wel een probleem vormen als de besturing een verandering van de werkwijze wil bewerkstelligen, want verandering gaat over de inhoud.

Voor de benodigde verandering van beveiliging is een nauwe samenwerking van de proceshiërarchie en de inhoudhiërarchie een vereiste. Het loslaten van het besturing-op-afstandsmodel is voor de transitiefase noodzakelijk, anders is het best haalbare beleidscosmetica.

[59] http://www.mkbservicedesk.nl/315/wat-span-control.htm
[60] http://www.kluwermanagement.nl/files/downloads/Watiseenoptimalespanofcontrol.ME2012-04-03[1].pdf
[61] Vrijgesteld van uitvoerende werkzaamheden
[62] Vuistregel voor aantal managers, Mark Hijben en Arno Geurtsen, Holand/Belgium Management Review, Berenschot 2008

Naar een samenhangende beveiligingstechnologie

Aan de slag met Jericho en Defense in Depth

De zoektocht is hoe beveiliging in te richten zonder de bakstenen en gecontroleerde slagbomen van weleer. Jericho stelde dat de grens tussen binnen en buiten niet meer helder te trekken is en dus als leidend concept voor beveiliging onbruikbaar. Met Jericho is het verhaal niet afgelopen – daar begint het eigenlijk pas. Jericho heeft geconcludeerd dat het oude concept niet meer werkt, zonder een concept neer te zetten dat alom overgenomen is. Het aloude beveiligingsmodel van System High is niet opgewassen tegen de bedreigingen en andere veiligheidsvraagstukken van dit moment. Dit denken is na 2004[63] feitelijk vervangen door het concept van de gelaagde beveiliging. Deze meerlaagse beveiligingsstrategie[64] staat ook wel bekend als Defense in Depth[65], het is een militair concept dat losjes is vertaald naar ICT beveiliging. De idee van Defense in Depth is dat als één beveiligingslaag wordt geslecht, de beveiliging als geheel nog steeds weerstand kan bieden. Het liefst maken deze verschillende barrières gebruik van verschillende technologieën, zodat het voor inbrekers lastiger is om meerdere lagen te doorbreken; daarvoor is veel en veelsoortige technische kennis nodig en iedere laag leidt tot een hogere pakkans. Als laatste doel moeten de meerdere lagen voor onzekerheid zorgen: hoeveel lagen moeten er nog worden doorbroken en hoe lang gaat dit nog duren? Hoeveel geduld heeft de aanvaller?

Defense in Depth is een aansprekend idee en heeft een brede aanhang verworven, maar is zoals vastgesteld in de praktijk niet gerealiseerd. Vanuit de beveiligingsarchitectuur komen er toch wel wat nare vragen naar boven. Want wat zijn dan de lagen en hoe kunnen ze elkaar versterken? Moeten *alle* lagen beveiligd worden voordat we kunnen spreken van een goede beveiliging in de diepte? En moet elk laagje door twee verschillende middelen beveiligd worden? Zijn applicaties lagen? En is één product meerdere laagjes als het meerdere protocollen snapt? Zijn protocollen dan lagen? Of zijn de beveiligingsproducten dat?

Nu kennen we natuurlijk 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; een spamfilter kan geen een DNS amplifier attack tegenhouden. Alleen de netwerkkant bestaat theoretisch al uit – minimaal – vier lagen, of zeven als je het OSI-model[66] aanhangt. Iedere applicatie die gebruikt maakt van het netwerk, werkt met een deel van de lagen en heeft eigen functies en componenten die beveiligd kunnen worden. Zo zijn er onnoemelijk veel virtuele lagen naast de traditionele fysieke lagen: het beveiligen van mail is iets heel anders dan het beveiligen van een VPN[67] over SSL, hoewel beide op de applicatielaag wonen[68].

Dit wordt uiteindelijk een vooral theoretische exercitie; er zijn veel meer technische lagen te onderscheiden dan er beveiligingsmiddelen zijn. Van belang is dat beveiligingsmiddelen gelaagd opgesteld worden, dat wil zeggen dat ze elkaar kunnen ondersteunen en eventueel (tijdelijk) vervangen. Beveiligingsproducten zijn meestal een soort Zwitsers zakmes; een verzameling middelen tegen een verzameling aanvallen. Iedere producent heeft weer een andere verzameling opties gekozen en producten zijn hierdoor nooit volledig inwisselbaar. Een breuk van een beveiligingslaag breekt niet alleen de laag, maar ook het beveiligingsproduct dat op die laag werkt. In bepaalde gevallen is het beveiligingsproduct zelf gecompromitteerd, wat betekent dat veel meer veiligheidsvoorzieningen uitvallen of niet meer vertrouwd mogen worden. De belangrijkste vraag is dus uiteindelijk hoe de lagen interacteren om bij breuk van de ene laag versterkend op te treden. Voor een echte defensie in de diepte moeten de lagen samenwerken. En dat moet in real-time, het heeft geen zin meer als de Change op de infrastructuur pas drie maanden later uitgevoerd wordt.

Wat Defense in Depth mogelijk moet maken laat zich het beste aantal beschrijven in een aantal scenario's; daaruit volgt hoe de techniek 'georkestreerd' moet kunnen worden. In alle scenario's is enige spoed geboden,

63 http://www.computerworld.com/s/article/89861/Using_a_layered_security_approach_to_achieve_network_integrity?taxonomyId=017

64 http://content.dell.com/us/en/business/smb-by-technology-security.aspx

65 http://nl.wikipedia.org/wiki/Defense_in_depth

66 ISO Reference Model for Open Systems Interconnection, een gestandaardiseerd model om te beschrijven hoe data wordt verstuurd over een netwerk.

67 Virtual private Network, een virtueel netwerk via een ander, meestal publiek, fysiek netwerk.

68 Het verschil is beperkt tot het gebruik van andere poorten. Poorten zijn echter alleen een abstractie omwille van de adressering op de netwerklaag.

bij de virus/worm gerelateerde voorbeelden is zelfs het een kwestie van minuten. Hieronder een aantal concrete voorbeelden van scenario's:

1. De organisatie besluit op grond van een algemene waarschuwing van de NCTV[69] een verhoogde staat van paraatheid in te voeren. Alle loglevels worden centraal van de defaultwaarde naar de maximale waarde gebracht en om ruimte te maken worden alle normale logs weggeschreven, en alle geprivilegieerde gebruikers kunnen alleen aanloggen binnen een beveiligde locatie.
2. De organisatie besluit op grond van een gerichte waarschuwing voor een mailworm een deel van de systemen scherper te laten controleren: de antivirusvoorziening voor de binnenkomende e-mail wordt langs een externe service voor antivirus in de Cloud omgeleid, alle attachments worden extra geïnspecteerd en ontdaan van externe links, tevens worden de toleranties (AV filter regels) op alle desktops anders ingeregeld, zodat alle bestanden gescand worden in plaats van alleen de meest gevoelige.
3. Een SIEM[70] systeem signaleert een zich ontwikkelende aanval op de organisatie. De logging instellingen worden automatisch bijgesteld, zodat al het dataverkeer gerelateerd aan de aanval gelogd en digitaal ondertekend wordt. Omdat de hoeveelheid data hierdoor veel groter is dan normaal, wordt alle verkeer omgeleid naar een Cloud Bursting[71] scenario. Tevens worden de logs van de Cloud leveranciers op een hoger niveau ingesteld en die data naar de tijdelijke omgeving weggeschreven.
4. De organisatie besluit bij een grootschalige aanval op de kritieke infrastructuur in één van de vestigingslanden de beveiligingsmiddellen te koppelen aan de voorzieningen van de nationale overheid in dat land, voor de duur van de aanval, zodat de bevoegde instanties real-time kunnen zien wat er gebeurt en indien noodzakelijk en mogelijk in kunnen grijpen.

Dit zijn het type scenario's waar een gelaagde beveiliging in de diepte op ingericht zal moeten worden. Zo verandert informatiebeveiliging van een formele en grotendeel papieren exercitie in een systeem dat veel weg heeft van een Goalkeeper[72].

De samenwerking van de beveiligingsmiddelen is dus afhankelijk van geautomatiseerde interactie tussen de lagen. Als één laag knel komt te zitten of niet werkt, dan springt een ander bij. Een desktopfirewall zou haar werking dus moeten afstemmen met de Enterprise firewall, maar ook met applicatiebeveiligingsmiddelen zoals Claims Based Security mechanismen. Dit laat zich best aanduiden als de orkestratievraag. Deze orkestratie is een voortbouwen op de werkelijkheid van het Intrusion Prevention Systeem, waarin Artificial Intelligence op basis van voorgeprogrammeerde regels automatisch reageert op realtime bedreigingen.

De essentie van Security Orkestratie is de bestuurbare beveiligingscomponenten ook bestuurbaar in te richten. Beveiligingsmiddelen zoals Antivirus en Intrusion Detection Systemen hebben parameteriseerbare instellingen, zoals toleranties voor false positives/negatives, of loglevels in beveiligingssystemen: op het moment dat er patronen zijn die lijken op een aanval, dat dan automatische bepaalde beveiligingscomponenten meer loggegevens gaan vastleggen of dat Intrusion Prevention[73] Systemen sneller ingrijpen, applicaties sterkere authenticatie vragen etc. Nu kun je veronderstellen dat alle beveiliging altijd in de zwaarste stand moet staan, in veel gevallen zijn er echter zeer goede redenen (zoals Perfomance en user experience) om dat niet te doen. Bedenk dat als een laptop pas verbinding krijgt met het bedrijfsnetwerk als een volledige antivirus-scan afgerond is, de wachttijd snel kan oplopen tot een paar uur.

[69] Nationaal Coordinator Terrorismebestrijding en Veiligheid (http://www.nctv.nl/)
[70] Security Incident en Event Management. Een systeem dat loggegevens van aangesloten applicaties en systemen correleert en daar patronen in herkent.
[71] Cloud Bursting is een model waarbij private applicaties 'on demand' tijdelijk (opslag- en/of reken-) capaciteit van een cloud leverancier afnemen.
[72] Een Goalkeeper is een geautomatiseerd anti-raketsysteem in gebruik bij de Nederlandse marine.
[73] Een IDS (Intrusion Detection Systeem) is een passief en voor een aanvaller onzichtbaar bewakingssysteem. Een IPS (Intrusion Prevention Systeem) is een actief verdedigingssysteem, dat op grond van instelbare regels netwerkverkeer kan blokkeren als daar aanleiding toe is. Een IPS is slimmer dan een IDS maar kan ook misleid worden en zelfs als aanvalsversterker misbruikt worden. Daarom bestaan beide producten naast elkaar.

	**Conclusie** Defense in Depth is alleen mogelijk met een universele besturingslaag voor parameteriseerbare beveiligingsmiddelen.

Defense in Depth is mogelijk en zinvol. Het zal echter nog een tijd duren voor het zo ver is: er is geen vraag uit de markt, omdat het inzicht dat beveiliging samenhangend en schakelbaar moet zijn nog niet wijdverbreid is. Deze vraag zal in de komende periode ontstaan, in reactie op het aanhoudend falen van de huidige standalone beveiligingssystemen. Pas als de markt erop aandringt, zullen de leveranciers in beweging komen: uit zichzelf zullen ze dit niet doen. Dat zie je in de praktijk al zoals bij antivirus waar producenten alles doen om het product van de concurrent van de pc af te houden, tot en met het corrumperen van het klantsysteem aan toe. En dat terwijl een goede antivirusaanpak per definitie meerdere scanners van meerdere leveranciers heeft.

De meeste beveiligingsmiddelen zijn puntoplossingen en niet gebouwd om in samenhang te opereren. Alleen de toegangsbeveiliging is in een aantal gevallen via een centrale backend gekoppeld, via een IDM provisioning systeem. De ontwikkeling rond Claim Based Security verandert IAM van een asynchroon tot een realtime beveiligingslogistiek en maakt het mogelijk en waarschijnlijk dat IAM zal uitgroeien tot het centrale punt van een steeds groter deel van de beveiliging. Het is wellicht niet de best denkbare koers, maar omdat IDM het enige condensatiepunt is, is dit het paard om op te wedden.

	**Conclusie** Defense in Depth is een overtuigend concept maar voorlopig nog zeer beperkt. In de toekomst zullen beveiligingsmiddelen integreren tot een real-time defense in depth. Dit vereist een centrale orkestratie met real-time provisioning. IDM biedt hier het enig beschikbare startpunt aan.

Van blacklisting naar whitelisting naar greylisting

De essentie van beveiliging is toegang: wat mag en wat niet mag. Daarvoor bestaan normaliter twee manieren: alles tegenhouden wat niet mag (Blacklisting), dan wel alleen toestaan wat wel mag (Whitelisting). De eerste manier is eenvoudiger en goedkoper, de tweede effectiever.

Bij toegang gaat het om *logistiek van de identiteiten*; in de praktijk komt dit neer op procesautomatisering van beveiliging, met als doel de gewenste beveiligingsniveaus te leveren én in stand te houden. Bij Blacklisting zijn dit identiteiten van alles wat je niet toelaat, bij Whitelisting de identiteiten van wat je wél toestaat.

Informatiebeveiliging is in theorie altijd uitgegaan van Whitelisting: *welke persoon* iets mag of niet mag. Bij computerbeveiliging zie je juist meestal Blacklisting: in de wereld van malware (antivirus) en netwerk security geldt als je iets verdachts ziet, dat je het tegenhoudt. Daar zie je ook goed de beperking van Blacklisting: een niet-identificeerbaar stukje code of instructie mag actief worden. Malware gaat uiteindelijk over identiteit, maar dan die van een applicatie - mag deze draaien of niet? De AV-middelen proberen vast te stellen op grond van een signature of een applicatie kwaadaardig is of niet en de signature wordt bewaakt door het AV-product. De signature database van de AV is een blacklist, en alles wat niet verboden is, is toegestaan. Iets vergelijkbaars speelt met de firewall; deze moest slimmer worden dan de klassieke statefull firewall[74] op de netwerklaag en groeide uit tot een Intrusion Prevention Systeem dat ook op de applicatielaag optreedt. Een IPS is net als een AV signature based en daarmee een Blacklisting benadering. Ook hier geldt dat alleen bekende aanvallen tegengehouden worden, en ook hier geldt dat dit model houdbaar is zolang vrijwel alle aanvallen bekend zijn en er tijdig signatures beschikbaar zijn. Het Blacklisting model is minder complex en beheersgevoelig dan een Whitelisting model, maar uiteindelijk ook zwakker.

[74] Een stateful firewall houdt informatie bij van connecties die over de firewall lopen. Zo kan onderscheid gemaakt worden tussen sessies en onderscheid afgedwongen, ook op protocollen die zelf geen state bijhouden. Door sessie state bij te houden kan de firewall netwerkconservaties tussen computersystemen op protocolnveau volgen.

Met de komst van de APT (Advanced Persistent Threat) blijkt het zwakke punt van het Blacklisting model zonneklaar. Bij antivirusproducten is de blacklist gebaseerd op de wildlist[75], een lijst van virussen die in het wild voorkomen en waar antivirusproducten detectie voor inbouwen door middel van een signature. Virussen die het niet halen tot deze lijst, de long-tail, worden niet gevangen. Malware komt niet de op deze lijst indien de verspreidingsgraad te beperkt is; malware die maar één keer gezien wordt in het wild, wordt niet bestreden door generieke AV-middelen. Met de enorme schaalvergroting van het Internet in de laatste tien jaar, is dit model steeds minder toereikend - steeds meer malware is statistisch niet significant en wordt dus niet 'gevangen' door traditionele AV. APT is dus niet een reeks zeer geavanceerde aanvallen zoals soms gesteld wordt, maar aanvallen die niet onderschept kunnen worden *omdat ze gericht zijn*. Het Internet zal blijven groeien (consumerisatie is de volgende ronde) en het Blacklisting model zal nog verder uit haar voegen barsten. Blacklisting is als benadering voor het antivirus gekozen om acceptabele resultaten tegen zo laag mogelijke kosten te krijgen. Een goede en verantwoorde keuze in 1989, maar geen keuze voor de eeuwigheid; Blacklisting schaalt niet voldoende.

De opkomst van op anomaliedetectie gebaseerde beveiliging

In de meeste gevallen wordt beveiliging ingericht vanuit het perspectief van het tegenhouden van onwenselijke acties. Een wachtwoord geeft geen toegang tot een systeem, maar sluit personen zonder wachtwoord uit. Een virusscanner herkent gevaarlijke instructies of een signature in de code, herleidt deze naar het virus, en verwijdert het bestand in kwestie. Een Intrusion Prevention Systeem analyseert verkeersstromen en zoekt naar bekende patronen van bekende aanvallen, en sluit de connectie van de verdachte machine. Al deze benaderingen zoeken de afwijking, de anomalie. We kunnen dus spreken van een Anomaly Based Security Architectuur.

Met een Anomaly Based benadering valt of staat de veiligheid met detectie. Een applicatie die onder de radar weet te blijven, kan vrijwel ongelimiteerd zijn gang gaan. Via webmail en downloadservices worden volledige databases weggesluisd. En als je er dan achter komt dat er iets mis is gegaan? Van een ongewenste financiële transactie kan alleen vastgesteld worden wie er op dat moment aangelogd had, maar zelden aangetoond worden wie de actie uitgevoerd heeft.

Een meer sluitende benadering kennen we van firewalls, waarin alle handelingen die niet expliciet toegestaan zijn, niet uitgevoerd worden, maar wel geregistreerd. Aan de buitenkant van onze netwerken doen we ‘toegang mits’, maar voor de meeste omgevingen binnen geldt ‘toegang tenzij je aantoonbaar fout bent’. Dit is ook een uiting van het kokosnootmodel. Dit model blijkt in de praktijk zelden houdbaar. Mobiele systemen als een iPhone maken de netwerkperimeter nog minder herkenbaar. Mobiele gebruikers werken met interne gegevens op thuissystemen of worden tijdelijk gedetacheerd bij een andere organisatie en hebben toegang nodig tot de 'eigen' systemen. De laptopgebruikers zijn bovendien vrijwel altijd de baas op dat systeem, omdat ze 'anders niet kunnen werken'. Hiermee is het kokosnootmodel voor vrijwel alle organisaties achterhaald en wordt het tijd voor een nieuw model.

Per beveiligingsdossier geldt deze als regel: zo lang Blacklisting voldoet, verdient dit de voorkeur. Waar het niet (meer) werkt, moeten we richting Whitelisting. Randvoorwaardelijk voor Whitelisting is identificatie; als je iets expliciet wilt toelaten moet het geïdentificeerd kunnen worden. Voor applicaties en besturingssystemen is de richting van een Whitelisting model bijeengekomen in het Trusted Platform model (ook bekend als Trusted Computing, zie http://en.wikipedia.org/wiki/Trusted_Computing). In het Trusted Computing model mogen alleen vertrouwde (en dus bekend en identificeerbare) applicaties transacties uitvoeren.

Whitelisting als beveiligingsmethode is in de Internetcontext ook nog eens veel moeilijker dan in de beslotenheid van een eigen netwerk. Binnen de eigen omgeving zou je alle objecten kunnen kennen (met heel veel inspanning), op het Internet is dat uitgesloten; enerzijds puur door de omvang van het Internet, anderzijds door de technologie – het Internet is in essentie anoniem. Zonder een volledige herbouw van het Internet zoals bepleit wordt vanuit de Cybersecurity hoek, is de toepasbaarheid van Whitelisting aan de Internetkant – en door Deperimeterisatie dus überhaupt – zeer gelimiteerd.

Identity Management is al vanaf het begin een Whitelisting benadering; gebruikers mogen iets nadat zeker is gesteld met een authenticatiemethode wie ze zijn. De beheersing van een Whitelisting benadering is zeer

[75] http://www.wildlist.org/

arbeidsintensief, en automatisering noodzakelijk; dit is de complexe en kostbare werkelijkheid van Identity Management. Identity Management was het allereerste dossier in ICT-beveiliging en vanaf het begin ingericht conform Whitelisting.

De wereld van Identity Management schudt echter ook op haar grondvesten, door de Cloud en de mobiele dimensie; hiermee treedt een schaalvergroting op waardoor het ideaal van Whitelisting verder weg komt te liggen. In de kern van Identity Management staat namelijk de Identity provider; de autoriteit voor het gehele domein die betrouwbare identificatiemiddelen verstrekt. Binnen een LAN is dat te overzien; op het wereldwijde Internet bestaat geen centrale identiteit.

Blacklisting en Whitelisting delen een specifieke beperking: beide zijn statische verdedigingsmodellen, die geen voorwaardelijke beslissingen in real-time kunnen nemen. De omslag naar Whitelisting is niet absoluut en niet voor alle technologie in één keer. Tussen Blacklisting en Whitelisting is een tussengebied, Greylisting. Greylisting is op dit moment al een van de krachtiger middelen in SPAM-bestrijding[76], waarbij op grond van een enkel opvallend gedragskenmerk van spamverzenders gefilterd wordt.

Ook in andere beveiligingsmiddelen is een verschuiving gaande van signature based approach naar gedragsanalyse. Dat is in de praktijk soms verre van eenvoudig, zoals te zien bij de moeizame strijd van de AV-makers met heuristische engines, waar sinds eind jaren ’80 al veel geïnvesteerd wordt maar de resultaten niet doorslaggevend zijn. Gegeven de kosten en beperkingen van een pure Whitelisting aanpak zijn alle serieuze alternatieven het onderzoeken waard.

In de kern zijn Whitelisting en Blacklisting statische beveiligingsmiddelen, waar gedragsgerelateerde beveiligingsmiddelen in de kern dynamisch zijn. Een gedragskenmerk is een real-time factor in een security decision; zo kan een toegangssysteem bijvoorbeeld toegang weigeren als dezelfde user vanaf twee geografisch uiteenliggende locaties probeert aan te loggen. Dit zien we al in de bestrijding van skimming. Dit type ‘grijze’ of fuzzy logica heeft de toekomst, nu Whitelisting en Blacklisting beide niet geschikt zijn gebleken in een grootschalige en open omgeving.

Conclusie
Blacklisting oplossingen zullen in afnemende mate afdoende zijn. Whitelisting lijkt in een aantal dossiers de oplossing te bieden, maar deelt een aantal van de tekortkomingen. Gegeven de Deperimeterisatie is de toekomst dan ook aan Greylisting concepten: systemen zullen beveiligingsbeslissingen nemen op basis van gedragsgerelateerde kenmerken.

Naar een virtuele perimeter

De grootste uitdaging is om beveiliging vorm te geven zonder de bakstenen barrière van weleer. Om tot een antwoord te komen moeten we teruggaan naar de centrale beveiligingsvraag Wie Mag Wat. Zonder de bakstenen kunnen we de identiteit van geen enkel object voetstoots aannemen: ieder object heeft een identiteit nodig. De uitdaging is om middelen te maken die Wie kunnen onderscheiden en ook Wat,om op grond daarvan beslissingen te kunnen nemen.

Het centrum van een identiteitsverstrekker is de autoriteit (de Identity Provider). In een LAN is de meest onzekere factor de gebruiker[77], en de aandacht gaat dus uit naar de correcte identificatie van de gebruiker. Daarmee is de directory de kern van de beveiliging, de autoriteit. Binnen een virtuele perimeter is de identificatie van de gebruiker net zo belangrijk als in het LAN, maar wordt deze aangevuld met de noodzaak tot betrouwbare device-identificatie, informatie-identificatie en applicatie-identificatie. Op dit moment is er maar één middel, PKI.

[76] http://en.wikipedia.org/wiki/Greylisting
[77] Zoals al aangegeven is de beveiliging van de rest impliciet, aangenomen: alle machines die je kunt zien zijn onderdeel van het netwerk en dus vertrouwd, en alle applicaties die er op staan dus ook.

Conclusie
De virtuele perimeter is de logische opvolger van de fysieke perimeter. Deze vervangt de baksteen door cryptografie. PKI is hiervoor de basis.

Als alle applicaties en informatie een identiteit krijgen is het huidige PKI aan een forse herwaardering en technische verbouwing toe; PKI is weliswaar het enige middel dat de digitale wereld kent voor identificatie van digitale entiteiten, maar het is in de huidige vorm niet erg geschikt. De opzet van de hedendaagse publieke TTP's was het verstrekken van gekwalificeerde certificaten aan personen; digitale handtekeningen met rechtskracht. Die markt kwam er niet en de markt die er wel kwam, de webserver certificaten-markt, wordt bediend zonder dat de techniek daarvoor aangepast is. Dit leidt tot een boel overhead, kosten en beveiligingsvraagstukken. De prijs per certificaat weerspiegelt dit: certificaten met enige mate van betrouwbaarheid (zogenaamde Extended Validation[78]) van een serieuze leverancier kosten enkele honderden euro's per jaar. Dit is bij een enkele webserver geen echt probleem, maar als alle devices, applicaties en bestanden een certificaat nodig hebben, is dit nogal een ander verhaal.

PKI is op dit moment bovendien vooral SSL: een systeem dat de identiteit van servers in de publieke (Internet) namespace bewijst. Veel noodzakelijke voorzieningen (zoals die voor het intrekken van certificaten) zijn daarom alleen in SSL scenario's beschikbaar. De meeste andere toepassingen van PKI zijn onderdeel van gesloten systemen (zoals code signing) en in de huidige vorm niet beschikbaar voor andere toepassingen. Bedenk eens hoe handig het zou zijn als het mogelijk was via een interface te kunnen vaststellen dat een client die verbinding maakt met je applicatieserver daadwerkelijk de juiste client software gebruikt, als in een NAC[79] scenario. Dat is echter niet mogelijk, zelfs bij Trusted Platforms die alleen gesigneerde code toestaan is het niet mogelijk op afstand te zien welke applicatie er daadwerkelijk gebruikt wordt door de gebruiker.

Als PKI gebruikt wordt om applicaties, informatie en transacties te identificeren moeten deze stevig gebonden zijn aan wat ze beveiligen. Bij een user is dat redelijk eenvoudig op te lossen (met een pincode), het vraagstuk is voor alle andere identificatievormen niet opgelost: wanneer certificaten gebruikt worden om de identiteit van een apparaat aan te tonen, is de identificatie weinig betrouwbaar als dit alleen betekent dat het certificaat op het apparaat staat. Een certificaat is immers niet meer dan verzameling bytes, en kan eindeloos gekopieerd worden. Dit is een traditioneel[80] aandachtspunt: de veiligheid van de sleutels. Een certificaat dat op een computersysteem staat, kan uitgelezen worden door het computersysteem; dus ook door software op dat systeem. Dat betekent dat virussen certificaten kunnen vinden en kopiëren. Er zijn veel vendors van software smartcards en dergelijke die beweren dit vraagstuk softwarematig opgelost te hebben – zoals met soft tokens, toch is het hoogst twijfelachtig omdat de sleutel op enig moment in memory zal zijn en vandaar uitgelezen kan worden[81].

PKI is het samenstel van asymmetrische cryptografische middelen (de P en de K, zeg maar de feitelijke sleutels) en de infrastructuur (de I) die beheersing mogelijk maakt. Het Internet is één 'I', één cryptografische trustzone die opgehangen is aan de Internet namespace. Organisaties kunnen ervoor kiezen om de beveiliging van de informatie daar aan op te hangen. Feitelijk is dit waar een ieder nu heen koerst: we gebruiken in steeds grotere mate publieke identificatiemiddelen voor de beveiliging in het private domein. De certificaten voor onze webservers, de Cloud omgevingen en de certificaten van onze devices worden verstrekt door partijen buiten ons directe bereik. Voor zolang dit ten behoeve van de encryptie van netwerksessies is, is dit geen groot beveiligingsvraagstuk, afgezien van de risico's die kleven aan de Trusted Third Party zélf. Dit hebben we recent kunnen zien met Diginotar: hoewel de klanten van die organisatie niet gehackt zijn, moesten ze met grote spoed aanpassingen doen toen Diginotar uit het wereldwijde web van Trust werd verstoten.

[78] In principe zijn er twee smaken certificaten: Domain Validation en Extended Validation (bekend van de groene balk in de browser). Bij het eerste kan iedereen met een mailadres in dat domein een certificaat kopen bij een specifieke leverancier. Bij EV kan de organisatie opgeven wie gerechtigd zijn certificaten te bestellen en wordt er daadwerkelijk door mensen contact gelegd bij een bestelling. De enige zwakte is dat een kwaadwillende bij een andere TTP toch nog EV-certificaten zou kunnen kopen.
[79] Network Access Control is een middel dat de identiteit en status van een client systeem toetst als dat verbinding wil leggen. NAC inspecteert patchlevels, de aanwezigheid en het actief zijn van AV en eventueel enkele andere parameters.
[80] http://www.schneier.com/paper-pki-ft.txt
[81] Cryptografische sleutels zijn relatief eenvoudig te herkennen omdat ze volledig random zijn. Utimaco toonde in 2000 aan dat een key op disk binnen enkele minuten gevonden kan worden. Uit computergeheugen (immers kleiner) kunnen ze nog sneller gevonden worden. Meer beperkingen van soft tokens op: http://securology.blogspot.nl/2007/11/soft-tokens-arent-tokens-at-all.html

Het is evident dat voor de andere taken van certificaten, te weten identificatie (van devices, gebruikers en applicaties) en blijvende encryptie bovenstaande veel ernstiger is dan voor SSL. In deze scenario's vormt PKI de blijvende sleutels tot de gegevens; organisaties zullen deze zelf willen bewaren. Om een virtuele perimeter vorm te geven zullen organisaties dus hun eigen sleutelketens (in cryptografie een Circle of Trust) moeten beheersen.

De labels zoals noodzakelijk zijn voor de virtuele perimeter zullen dus gebaseerd zijn op de concepten van PKI. Cryptografie en identiteit vormen de kern van deze virtuele perimeter, en *het beheer en de logistiek* van de sleutels daarin – meer nog dan de productie ervan – wordt dus de ruggengraat van de beveiliging. Deze provisioning van PKI sleutels raakt aan een concept dat de laatste paar jaar in beeld is gekomen: het Enterprise Key Management systeem (EMKS). Het grootste probleem met PKI is in de praktijk van alledag niet het maken van de juiste sleutels, maar de juiste sleutels op de juiste plek te krijgen. PKI heeft een levensgroot provisioning vraagstuk dat pas sinds kort enige aandacht krijgt in de vorm van het Enterprise Key Management Systeem. EKMS is na Identity Management het tweede dossier dat beveiligingsprocessen automatiseert en dezelfde weg wijst.

	**Conclusie** Met het verdwijnen van de fysieke perimeter zullen organisaties overgaan tot het instellen van een virtuele perimeter. Deze wordt gedefinieerd door private cryptografische Circles of Trust die de identiteit verstrekken aan de eigen objecten. De organisatie zal de eigen Circle of Trust beheren met een EKMS.

Naar een declaratieve beveiligingslogica

De vraag van toegang is in normale taal de **Wie Mag Wat** vraag, met de impliciete vraag **Waarom** en de sinds BYOD, HNW en mobiel werken bijkomende vraag, **Waarmee**. Van deze vier W's worden in de eigen infrastructuur sommige als vertrouwd aangenomen – in Enterprise Security worden alleen de Wie en in mindere mate de Waarom vraag met veel aandacht omringd om de 'mogen' vraag te beantwoorden. De identiteit van de applicatie of de server is in een LAN geen serieuze vraag; op het Internet is het juist één van de hoofdvragen, zoals de geschiedenis van SSL aantoont (in het kort: SSL is geëvolueerd tot een methode om de identiteit van de server te garanderen *omdat DNS dat niet doet.*[82]) Binnen het LAN is ook veel beveiliging impliciet georganiseerd: de gebruiker mag iets omdat hij aangelogd heeft; de belangrijkste rol in de gemiddelde directory is de Authenticated User. Deze beveiliging moet over naar een expliciet model.

Op het Internet kan de identiteit van een server of applicatie nooit als veilig verondersteld worden: als informatiebeveiliging op grond van de vier W's ingericht wordt, zal ze declaratief zijn: de gebruiker mag iets op grond van expliciete regels en op grond van vastgestelde kenmerken. Dit type logica is goed zichtbaar in 'Claims Based' security, waar IF THEN ELSE statements op basis van attributen uit meerdere systemen in de keten de real-time autorisatielogica bepalen.

- **Wie** is de actor, in de wereld van het LAN is dat de persoon, en de Internetwereld is dat ook de transactie, de applicatie en de host.
- **Mogen** is de beveiligingsregel, ingevuld vanuit de waarom regel.
- **Wat** is het te beveiligen object.
- **Waarmee** is het device, en het daarbij passend beveiligingsniveau (denk aan hygiëne en NAC).

Een kanttekening is op zijn plaats. Als dit type logica strikt geïmplementeerd wordt, dan zal er vooral weinig voorspelbaars zijn aan de toegangsbeveiliging. De transitie zal zeker niet pijnloos zijn: statische matrices lenen zich stukken beter voor audits dan dynamische logica. Ook voor de helpdesk wordt trouble-shooting een stuk lastiger.

Vertaald naar technologie kunnen we grofweg spreken van:

[82] Met de komst van DNSSec vervalt dit vraagstuk.

- **Identificatiemiddelen**: middelen om het object te herkennen (Wie, Wat en Waarmee). Dit is hoofdzakelijk een zaak van cryptografie.
- **Beslissingslogica**: een idealiter generieke taal om de logica te bouwen en af te dwingen, die over alle lagen (dus ook in n-Tier omgevingen) inzetbaar is. In de praktijk van vandaag spreken van WS-FED/SAML in zowel active als passive mode, maar op enige termijn zullen we er OpenID-Connect[83] voor gaan gebruiken, omdat WS-FED/SAML hiervoor te beperkt is.

Ondersteunend voor deze technologie zal nodig zijn:

- Classificatie van alle objecten: informatie, applicaties, devices, transacties, geolocaties en netwerksessies
- Security regels op basis van veiligheidseisen en bedrijfsprocessen
- Provisioningsystemen voor identiteiten (dus niet alleen van gebruikers) en beslissingslogica

Van SSO naar USO

SSO is voor veel organisaties een ultiem streven: een enkelvoudige login tot applicaties maakt toegang voor gebruikers simpeler, vermindert het aantal wachtwoorden en maakt het mogelijk sterkere wachtwoord policies in te voeren. De boel wordt ook veiliger omdat gebruikers één wachtwoord gemakkelijker kunnen onthouden dan 25, en het dus niet meer op een Post It op hun beeldscherm plakken. Het klinkt ideaal maar is een gepasseerd station; SSO past bij een gesloten omgeving, wachtwoordgebaseerde toegang en het System High denken waarbij alle informatie en informatiesystemen dezelfde gevoeligheid hebben.

Er zijn veel minder aanvallers die fysiek toegang hebben tot iemands werkplek om de Post It op het beeldscherm te kunnen lezen, dan er mogelijke aanvallers via Internet zijn. 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 hiervoor niet werkt. Op Internet hebben miljarden mensen toegang tot het loginscherm, en is het hoogst ongebruikelijk een Lock Out policy te gebruiken dat een account afsluit na drie keer een verkeerd wachtwoord te hebben ontvangen. Dat is op Internet immers een instant Denial of Service aanval. Facebook, LinkedIn en Salesforce hebben daarom ook geen lock-out policy.

Dat SSO bij wachtwoordauthenticatie hoort, is geen algemeen gedeeld inzicht. Een organisatie zou er immers voor kunnen kiezen iedere gebruiker een hard token te geven. Dat is inderdaad mogelijk, maar in een tijd waarin niet alleen medewerkers maar ook klanten toegang hebben, wordt het opeens een heel ander verhaal; dat wordt veel te kostbaar.

Dat SSO niet het gedroomde ideaal is, wordt nog duidelijker als we het PAM (Privileged Account Management) dossier erbij betrekken: vanuit beveiliging is het eigenlijk wenselijk dat toegang tot accounts die zo ongeveer alles mogen op een systeem extra beveiligd wordt: PAM staat haaks op het System High gedachtegoed. Als we de toegang voor beheerders extra beschermen is de Sign On niet meer Single.

Een ander bewijs is de werkelijkheid van Strong Authentication: binnen de SSO-logica houdt dat in dat alle toegang tot informatie en informatiesystemen met dezelfde sterke authenticatie beveiligd moet zijn. In een gesloten en weinig complexe technische wereld is dit soms te doen; in een Enterprise is dit een niet-realistische droom gebleken, met alle meervoudige interne domeinen en technologieën. Na Jericho is het al helemaal niet realistisch. 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 Cloud applicatie die de gekozen technologie niet ondersteunt.

Als laatste gedachte rond het eind van het traditionele SSO-model kunnen externe validaties gelden: voor steeds meer toepassingen moeten authenticatiemiddelen van andere partijen ingezet worden, zoals DiGID, eID of de UZI pas. Organisaties die de toegang willen beheersen, zullen hiervoor dus een andere manier moeten bedenken.

[83] http://nat.sakimura.org/2012/01/20/openid-connect-nutshell/

De geünificeerde centrale login (feitelijk Unified Sign One) wordt in de praktijk vormgegeven met SAML en WS-FED standaarden, met uitlopers naar specifieke technologieën met andere protocollen. De organisatie biedt een login aan op basis van webtechnologie, die aan de achterkant tegen de user store of stores authenticeren. Dit werkt zowel binnen een LAN als daarbuiten.

Federatieve producten worden intussen meer en meer uitgebreid met ondersteuning voor sterke authenticatie, zodat deze centrale login voorzien kan worden met deze vorm van extra beveiliging. Als deze centrale login alleen voor medewerkers is, dan is het mogelijk hiervoor te kiezen en iedere medewerker een hard token te geven; het wordt echter opeens veel lastiger als er klanten en medewerkers van zakenpartners toegang moet worden gegeven. Nu is het mogelijk een tweede centrale login op te stellen die een zwakkere login toestaat, maar dat is hoogst onlogisch; waarom moeten vertrouwde medewerkers meer moeite doen om ergens bij te komen? Bovendien is een centrale login niet meer centraal als er twee zijn.

De oplossing is differentiatie: verschillende gebruikersgroepen via dezelfde login *andere authenticatiemethodes* te 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 inlogt met een zwakker authenticatiemiddel hoeven aan te loggen dan dezelfde medewerker vanaf een eigen tablet thuis. Bovendien biedt dit mogelijkheden om binnen een applicatie (mits deze dit toestaat) te differentiëren. Zo zal deze medewerker aanvullend moeten authenticeren alvorens een gevoelige transactie uit te kunnen voeren. De eerste applicatieservers die een dergelijke differentiatie ondersteunen zijn al verkrijgbaar, en Microsoft ondersteunt dit sinds .Net 4.5.

Conclusie
Toegangsbeveiliging in de gedeperimeteriseerde werkelijkheid is step-up authenticatie en -autorisatie: een authenticatiemethode die gelijke tred houdt met de gevoeligheid van de gevraagde toegang.

Classificatie van informatie en systemen

In alle leerboeken rond informatiebeveiliging staat prominent vermeld dat informatie geclassificeerd moet worden om het te kunnen beveiligen. Dit is in de praktijk heel lastig gebleken; vrijwel geen enkele organisatie ter wereld heeft dit daadwerkelijk doorgevoerd. Daarom hebben we feitelijk gekozen voor de impliciete beveiligingsaanpak van System High; alle informatiesystemen van de organisatie hebben hetzelfde feitelijke beveiligingsniveau en daarmee dezelfde classificatie (al dan niet expliciet). Binnen de eigen omgeving worden zwakkere binnenmuren ingezet, die deels alleen een proces zijn, deels uit relatief zwakkere technologie bestaan. Omdat we de interne bedreigingen als technisch minder competent beschouwen, wordt op de binnenkant zelden actieve bewaking ingezet. Intrusion Detection en SIEM zijn vrij gangbaar voor het bewaken van het binnenkomende verkeer, zij bewaken soms ook het uitgaande verkeer maar worden zelden of nooit ingezet voor de binnenmuren.

ICT security is in de regel niet in staat de waarde van informatie te meten of vast te stellen wat juiste en wat onjuiste informatie is. Het achterwege blijven van de labels is daarom een uiting van een levensgroot Governance-vraagstuk in beveiligingsland. Voor Informatiebeveiliging is het labellen van informatie en hulpmiddelen als applicaties en systemen echter een conditio sine qua non; zonder labelling kunnen we *niet meer doen* dan de systemen beveiligen. Labellen van informatie is een onderdeel van informatiemanagement en behoort tot het business domein.

Om zonder bakstenen informatie te kunnen beveiligen, moet nog een aantal andere zaken eveneens geregeld zijn. De uitdaging is de handhaving van het beleid. Organisaties stellen heel vaak dat medewerkers thuis mogen werken, maar dan alleen met door het werk verstrekte apparatuur. De beveiliging die dit moet afdwingen is al een stuk minder stevig; de meeste identificatiemiddelen die ingezet worden voor netwerktoegang identificeren de gebruiker, niet het systeem. En als ze het systeem identificeren, is die identificatie verre van tamperproof. Bij bijvoorbeeld de inzet van een client X509 certificaat wordt alleen aangetoond dat het certificaat op de

machine staat. Uiteindelijk is een certificaat een reeks bytes die gekopieerd kan worden, dus het certificaat kan ook op tien machines staan[84]. De gebruiker een PIN code laten invoeren bij het certificaat identificeert de gebruiker, niet de machine. Nu zullen goedwillende en technisch incompetente gebruikers dit niet voor elkaar krijgen, zeker[85]. Maar alleen beveiligen tegen goedwillende en technisch incompetente aanvallers is wel een heel laag ambitieniveau. Dit geldt ook andere objecten in de technische keten – een door de zaak verstrekte pc is op een vijandig netwerk toch beduidend minder betrouwbaar dan op een wat beter netwerk. Voor een goede beveiligingslogica moeten de gevolgde paden ook geclassificeerd worden en technisch geïdentificeerd. Als informatiebeveiliging het handhaven van het beleid als doel heeft, dan moeten alle objecten die in beleidsbepalingen meewegen, ook technisch herkenbaar zijn. Anders kun je er geen policy aan hangen en meenemen in security decisions.

Voor toekomstige Informatiebeveiliging geldt daarom het labellen van informatie én middelen als netwerksessies, transacties, applicaties en systemen, als randvoorwaarde. Als het beleid geografisch gebonden voorschriften heeft, dan moet er ook een geolocatiedienst gekoppeld worden, anders is het een dode letter. Dit betekent dat objecten voorzien worden van een uniek en niet of uiterst moeizaam falsificeerbaar kenmerk, een identiteit. In de regel bestaat deze identiteit alleen in de beleidsstukken, omdat bitjes, bestanden en computers geen label kunnen krijgen. Met de ontwikkelingen in de beveiligingstechnologie is het op veel punten mogelijk digitale 'assets' te voorzien van een label. Voor bestanden hebben we DRM, voor systemen kunnen we een klein deel van de puzzel maken van beveiliging op de informatielaag.

Dit betekent dat objecten voorzien moeten worden van een uniek kenmerk, een identiteit. Met het plaatsen van digitale en niet (of heel moeilijk) manipuleerbare labels is het mogelijk om declaratieve beveiliging te bouwen. Als sturingslogica in een dergelijke declaratieve beveiliging is ook een herziening van het in theorie leidend autorisatiemodel zoals we dat nu kennen, RBAC, aan de orde[86]. De bestaande matrices van rollen zijn in de praktijk nog maar half ingevuld, en moeten nog verder uitgebreid worden.

Rolmanagement en informatieclassificatie eisen een gestructureerde aanpak om toegang tot informatie en systemen te ordenen en te beheren. Met de mislukkingen van RBAC en het achterwege blijven van classificatie in gedachten, is het noodzakelijk om lering te trekken uit wat daar mis ging.

Bestanden versus applicaties

Beveiliging van Toegang kent eigenlijk twee afzonderlijke vraagstukken: toegang tot informatie gebonden aan een systeem (lees: in een applicatie) en toegang tot informatie die onafhankelijk is van het systeem (lees: bestand). Dit onderscheid wordt zelden gemaakt maar het is wel noodzakelijk. De vraagstukken vergen een afzonderlijke aanpak en afzonderlijke technologie. Het overgrote deel van de toegangsbeveiligingsmiddelen gaan – gezien de historie – dan ook over applicatietoegang en beschouwen een fileshare ook als een applicatie. Gegeven dat een Word-bestand na het mailen op iedere andere willekeurige machine geopend kan worden is dat een hoogst kenmerkende denkfout.

Beveiligingsoplossingen moeten dit onderscheid maken en vragen afzonderlijke voorzieningen. De hierboven benoemde beveiligingslogica is voor applicatietoegang, voor bestandsbeveiliging is een DRM-achtige oplossing absoluut noodzakelijk; er is geen andere manier om informatie buiten de context te beveiligen. Er zijn natuurlijk wel verschillende producten. DRM-technologie is al tien jaar beschikbaar, de toepassing in de praktijk is echter zeer beperkt. Dat maakt duidelijk dat er redenen zijn om de technologie niet toe te passen, die weggenomen moeten worden.

De meest prominente reden is de associatie van de technologie met de kopieerbeveiliging van muziekbestanden. Deze associatie heeft de DRM-technologie in een kwade reuk geplaatst. Vooral omdat de implementaties van DRM de goedwillende klant benadeelde en de kwaadwillenden niet significant hinderden,

[84] De bescherming van het lokale certificaat is een functie van het lokale systeem. Sinds 1998 is de zwakte van deze benadering gedocumenteerd onder de naam 'lunchtime attack', verwijzend naar de benodigde hoeveelheid tijd. Dit type aanvallen is sinds een aantal jaren – in ieder geval vanaf 2007 – in het wild te zien. Zie http://www.cs.jhu.edu/~astubble/600.412/s-c-papers/keys2.pdf.
[85] De simpelste truc is een image trekken van de harddisk en deze 'mounten' als virtuele disk op een andere machine. Dit is een handeling die binnen het bereik van vrijwel iedere computerhobbyist valt.
[86] RBAC geldt als de gewenste eindsituatie in autorisatiebeheer. In de praktijk is het een doel waar naartoe gewerkt wordt, maar dat iedere keer een bocht verder ligt dan gehoopt.

of in iedere geval niet in die mate dat de betalende klanten er enig voordeel van hadden, zoals een prijsdaling. De technologie bleek ook niet bestand tegen de gecoördineerde aanvallen vanuit de Internet community. Beveiligingsspecialisten wereldwijd is dit niet ontgaan. Uiteindelijk is DRM-technologie in dit dossier doodgebloed[87].

Naast deze externe oorzaak zijn er nog andere redenen die de invoering van DRM in organisaties hinderden. De belangrijkste is dat DRM raakt aan het probleemgebied van informatieclassificatie en informatiemanagement. Hierdoor is de implementatie afhankelijk van medewerking buiten de ICT-organisatie.

Als laatste geldt dat DRM een cryptografische oplossing is. ICT en ICT-beveiliging hebben in de regel weinig tot geen kennis van deze materie, een gebrek dat ook zaken als harddisk en mailencryptie tegenhoudt.

Alleen de tweede van de genoemde redenen, de bewezen zwakte van de implementatie, is een echt probleem; de associatie met media DRM is al in de vergetelheid aan het raken, en ICT is vanuit allerhande andere beveiligingsdossiers meer en meer vertrouwd aan het raken met cryptografie.

DRM geldt dus als gekraakt. Het kraken was en is mogelijk omdat media DRM geen gebruik kan maken van beslissingslogica van een achterliggende beveiligingsvoorziening als een certificateninfrastructuur, user authenticatie en een directory. De ervaring is dus niet te projecteren op Enterprise DRM omdat de media DRM technologie wereldwijd is, en dus door de hele wereld aangevallen werd, en Enterprise DRM een veel kleiner en een beweeglijk doelwit vormt.

De identiteit van informatie: Enterprise DRM en DLP

Wat overblijft bij Enterprise DRM is het probleem van de Governance van Informatiebeveiliging; ICT en ICT security hebben de taak op zich genomen informatie te beveiligen zonder actieve deelname van de eigenaar van de informatie. Dezelfde problematiek zien we rond RBAC en Mandatory Access Control, wat ooit leidde tot het kokosnoot-model.

Een belangrijke oorzaak van invoeringsproblemen bij DRM, RBAC en informatie classificatie trajecten is een te hoog ambitieniveau in relatie tot de gevoelde noodzaak. Er komen naar de zin van de informatie-eigenaren te veel rollen en te veel classificaties. Bovendien is een dergelijk systeem zelden bestand tegen reorganisaties. De zoektocht naar de juiste granulariteit is nog altijd gaande.

Er is lering te trekken uit de praktijkervaringen met het VIR-BI, het Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie. Het VIR-BI kent vijf beveiligingsniveaus (Publiek, Departementaal Vertrouwelijk, STG Confi, STG Geheim en STG Zeer Geheim). Men gebruikt daar in de praktijk slechts twee van – STG Zeer Geheim wordt alleen bij hele hoge uitzondering gebruikt en de grens tussen STG Confi en STG Geheim is ‘fluïde’ en weinig concreet, zoals de toezichthouder in 2012 vaststelde. Dat hoeft helemaal geen probleem te zijn; er gebeuren weinig ongelukken. Blijkbaar is drie niveaus gewoon genoeg, want het onderste (default) niveau zegt dat iedereen erbij mag. Dat drie afdoende is zal voor de meeste organisaties ook gelden.

Nu is het VIR-BI formeel helemaal niet zo plat; naast de classificaties in de vijf niveaus kent het ook het ‘Need To Know’ voorschrift. Dat is een zeer fijnmazige eis, die stelt dat er een operationele noodzaak moet zijn om toegang tot bepaalde informatie te hebben. De les van het VIR-BI is dat een dergelijke eis niet werkt; in de praktijk wordt dit principe alleen op het hoogste niveau STG Geheim met handmatige registratie bijgehouden. De prijs is echter hoog: vanwege het gedoe met handmatige registers en verzegelde enveloppes wordt zeer gevoelige informatie stelselmatig ondergerubriceerd en de compartimentisering in het geheel niet afgedwongen. Stel je de situatie voor dat een ambtenaar over informatie beschikt van een niveau dat nergens in de eigen organisatie verwerkt kan worden. De logische keuze is om dan het hoogst beschikbare bruikbare niveau te kiezen. Dit is de consequentie van de combinatie met Discretionary Access Control; voor de zekerheid wordt een hoog maar werkbaar niveau gekozen.

Het tegenovergestelde treedt ook op; onder het VIR-BI zijn de complete netwerken van een aantal ministeries geclassificeerd, in de regel op DepV. Individuele documenten worden alleen expliciet gerubriceerd als ze

[87] http://opensource.com/life/11/11/drm-graveyard-brief-history-digital-rights-management-music

gedeeld moeten worden buiten het eigen domein[88]. Deze praktijk schetst de realiteit van alle organisaties, niet alleen de Rijksoverheid[89]. Het grootste resterende probleem met VIR-BI is op dit moment dat de classificatie in het document staat en alleen door mensen gelezen kan worden. Een hoog gerubriceerd document wordt door de mailserver van een supergeheim overheidsdeel gewoon doorgelaten. De oplossing is een digitaal leesbare markering. Dan kan er op gefilterd worden en de beveiliging is op de informatie zelf gebonden. Dit is de basisgedachte onder de samenwerking van Enterprise DRM met DLP (Data Leakage Prevention).

Deze combinatie van DRM en DLP vormt een onmisbare bouwsteen in iedere toekomstige informatiebeveiliging. Bij DRM-oplossingen zijn documenten versleuteld en is de beveiliging onderdeel van het bestand. Met een gecentraliseerd policy management dat een catch all policy afdwingt kunnen organisaties betrekkelijk eenvoudig de beveiliging van bestanden op een hoger niveau tillen: stel dat de instelling wordt gekozen dat alle bestanden alleen geopend mogen worden door users die ingelogd zijn en dat niemand de beveiliging van de bestanden kan veranderen. Op die manier kan DRM een grote factor in de Virtuele Perimeter vervullen. DLP kan het afdwingen van dit type beperkingen versterken, door de DRM-bepalingen als <Niet Verspreiden> af te dwingen.

In bepaalde Enterprise DRM implementaties is het al mogelijk over bedrijfsketens te gaan door de identiteiten te federeren. Dit zal in een aantal scenario's een doorslaggevend voordeel zijn.

Om valkuilen te vermijden is het van belang te bedenken dat DLP en DRM strijdige beveiligingsstrategieën vertegenwoordigen – DLP bewaakt de buiten- en binnenmuren, waar DRM op informatieniveau acteert en agnostisch is voor systemen, zones en netwerken. DLP-oplossingen worstelen ook zichtbaar met het classificatievraagstuk. Zo hebben sommige DLP-oplossingen een Discovery functie, waarmee het systeem automatisch informatie classificeert. Dat is zinvol als informatie heel herkenbaar is, bijvoorbeeld bij creditcardnummers, waar deze aanpak voor bedacht is[90]. Maar als classificatie zo simpel was voor de rest van de wereld, dan zou informatiebeveiliging een veel eenvoudiger beroep zijn.

Conclusie
In de toekomst wordt de beveiliging op de informatie zelf aangebracht in plaats van op de toegang ernaartoe. DRM zal een plaats vinden in iedere organisatie.

Next Generation 'dynamische autorisaties'

De nieuwe uitdaging met rollen zal zijn de basis te vormen voor de dynamische autorisaties zoals hiervoor beschreven voor toegang tot applicaties (On en off premise) 'Any Time', 'Any Place' en 'With Any Device'. Organisaties moeten matrices opstellen die bepalen hoe het in detail gaat werken. Bijvoorbeeld: een gebruiker van de zakelijke laptop op het eigen kantoor heeft andere autorisaties dan dezelfde gebruiker op zijn smartphone in de trein. Dit betekent dat rolmanagement uitgebreid moet worden om ook een rol te spelen in de bepaling van autorisaties in dynamische context. Ook kan een dergelijke matrix enige ruimte voor onzekerheid laten: voor niet alle applicaties zullen alle variabelen bekend hoeven te zijn.

Bij traditioneel rolmanagement à la RBAC wordt meestal uitgegaan van HR als bronsysteem. Bij dynamische autorisaties wordt niet alleen uitgegaan van HR maar ook van andere attributen zoals locatie, verbinding en device. De gebruiker krijgt vanuit traditioneel rolmanagement met behulp van HR nog steeds autorisaties toegewezen. Alleen worden de autorisaties beperkt door middel van de context zoals locatie en device.

De enige manier om dat te doen is gebruik maken van Attribute (ABAC) of Claim Based Access Control (CBAC). Bij ABAC worden attributen, zoals IP-adres, locatie en overige identiteitsgegevens verzameld en doorgestuurd. Op basis van deze verzamelde attributen worden de autorisaties van de gebruiker bepaald. Bij CBAC wordt op

[88] http://www.securitymanagement.nl/files/downloads/IB%20Rubriceren%2011-10.pdf
[89] Een duidelijke schets is te lezen op www.ctivd.nl/?download=CTIVD%20rapport%2033.pdf, het TOEZICHTSRAPPORT inzake DE RUBRICERING VAN STAATSGEHEIMEN DOOR DE AIVD uit 2012.
[90] De basis van DLP ligt in PCI-DSS compliance; geldige creditcard nummers kunnen met een simpel algoritme gevonden worden. In ons land zouden we deze functie kunnen gebruiken voor Burger Service Nummers.

een gecontroleerde manier informatie gedeeld met behulp van claims. Indien een gebruiker claimt autorisaties nodig te hebben tot een bepaald object, dan wordt op basis van attributen bepaald of de gebruiker toegang heeft. Door gebruik te maken van ABAC en CBAC in samenwerking met rolmanagement kan dynamische de autorisaties voor applicaties bepaald worden Any Time, Any Place en with Any Device.

	**Conclusie** De toekomst is Claim Based.

Conclusie

De fusie van Enterprise Security en Internet Security gaat maar moeizaam. Zij komen vooral bij elkaar door de APT (Advanced Persistent Threat), Cloud en BYOD, dus in praktische gevallen en gedreven door incidenten. De veranderingen zijn niet of nauwelijks vertaald naar het conceptuele of het bestuurlijke niveau. Hoe het resultaat eruit zal zien, is daarom nog lang niet uitgekristalliseerd. Daar zit bovendien de tijdsdruk van The Internet of Things op; er is geen ruimte of tijd voor rustig delibereren; de vijand staat voor de poort. Dit tijdsgebrek is opgedrongen door de veelheid en de diversiteit van omstandigheden; zaak is desondanks de blik vooruit te richten, innovatief te denken en voorbij onze bestuurlijke kaders te denken.

De werkelijkheden van Enterprise security en Internet security raken elkaar, maar in de beleving van veel mensen is dit maar heel beperkt. Voor een enkele organisatie is dit daadwerkelijk zo, voor het overgrote deel van de organisaties en dus de beveiligers is het beeld dat het zo snel niet loopt struisvogelpolitiek.

Om in de toekomst de aanvaller met meer kans op succes tegemoet te kunnen treden moeten we veranderen hoe we informatie beveiligen. Veranderen begint met inzicht. Deze studie heeft als primair doel dit inzicht te geven. Maar dat inzicht is natuurlijk beperkt tot het niveau van het individu.

Via het individu kunnen en zullen organisaties veranderen. De transitie moet worden gedreven door minimaal onderstaande inzichten:

1. Beveiliging is logistiek.
2. Beveiliging is real-time. Een aanval kan in enkele minuten de wereld rond. De verdediging moet even snel kunnen optreden.
3. Binnen bestaat niet meer. We moeten ons beveiligingsdenken aanpassen aan de gedeperimetiseerde wereld
    - Impliciete beveiliging moet vervangen worden door expliciete beveiliging
    - Expliciete beveiliging is declaratief
4. We moeten weten wat we beveiligen. Zonder classificatie van informatie en systemen is beveiliging kansloos.
5. We moeten ons beveiligen tegen geavanceerde aanvallers.
6. Defense in Depth is vereist. We moeten zorgen dat onze beveiligingssystemen samenwerken zodat ze een beveiliging in de diepte vormen.
7. We moeten informatie beveiligen los van de systemen: applicatietoegang en bestandstoegang zijn twee afzonderlijke dossiers.
8. Het Internet zal opgedeeld worden in nationale stukjes.
9. Cyberwar is de nieuwe realiteit.

De logische vraag die alles in dit document opwerpt is niet waar de ontwikkelingen ons heenvoeren, maar hoe wij daar tijdig aankomen? Zullen wij dezelfde achterstand als vandaag op de aanvallers hebben, of zullen we nog verder afgezakt zijn? Of zullen we er beter voorstaan, door tijdig te veranderen?

Slotwoord

Informatiebeveiliging als vakgebied is begonnen aan een lange reis. In deze wereld waar het streven naar zekerheid het doel is, zijn de zekerheden verdwenen. We staan aan de vooravond van de invoering van een grote hoeveelheid nieuwe technologie in een volledig nieuw besturingsmodel. Dit is een vooruitzicht dat beangstigend kan zijn, maar ook een mooie toekomst kan bieden. Hoe het ook zij, er gaat een heleboel gebeuren en we zullen in interessante tijden leven.

Begrippenlijst

Term	Omschrijving
APT	Advanced Persistent Threat; geavanceerde, gerichte en georkestreerde langdurige aanvallen op organisaties.
DAC	Discretionary Access Control: een model dat de gebruikers als eigenaar van informatie de feitelijke mogelijkheid geeft zelf het beveiligingsniveau te bepalen.
Deperimeterisatie	Een generieke term om de door de business en technologie gedreven erosie van de netwerkperimeter (de buitengrens) aan te duiden.
EKMS	Enterprise Key Management Systeem: een computersysteem dat beheer en logistiek van certificaten van verschillende aard en herkomst centraal regelt.
IAM	Identity en Access Management: het geheel van processen en systemen dat de toegang van identiteiten tot systemen beheert.
Jericho	Het Jericho Forum is in 2004 opgericht. Toen kwam een aantal corporate CISO's (Chief Information Security Officers) bij elkaar om informeel van gedachten te wisselen over de aanpak van Deperimeterisatie, ofwel de erosie van de netwerkperimeter. Het Jericho Forum richt zich tegenwoordig op de Cloud.
MAC	Mandatory Access Control (Bell-LaPadula e.d.), een model dat beveiligingsniveaus oplegt aan gebruikers en afdwingt; tegenhanger van Discretionary Access Control.
Mash-Up	Het bijeenbrengen van verschillende webdiensten van verschillende leveranciers in één front-end.
Master Data model	Mastergegevens - zoals klant, leverancier, partner, product, materialen en werknemers - worden verspreid over het hele bedrijf bijgehouden, in heterogene, verkokerde applicaties. Een master data management systeem legt op gestructureerde wijze metadata vast. Idealiter worden deze gegevensverzamelingen ontdubbeld. Hiërarchische relaties tussen gegevens worden door het MDM bepaald en afgedwongen. Dit vereenvoudigt het gegevensbeheer; het effect is wel een hogere mate van systeemintegratie.
Multi Level Security	Het gebruik van één computersysteem om gegevens te verwerken of bevatten met verschillende formele sensitiviteiten (met verschillende security classificatie), ten behoeve van gebruikers met verschillende security screening levels en needs-to-know, waarbij het systeem voorkomt dat gebruikers bij informatie kunnen komen waarvoor zij niet geautoriseerd zijn.
Multi-tenant	Een computersysteem dat ten behoeve van meerdere organisaties ingezet wordt.
Multi-tier	Een applicatie die afzonderlijke lagen heeft voor verschillende functies. In de praktijk is dit vaak een portal met een losse transactielaag en weer een ander systeem voor de gegevensopslag.
Patriot Act	Amerikaanse wet die in 2003 is aangenomen met het doel terrorisme te bestrijden. Het geeft meer mogelijkheden aan de Amerikaanse overheid om informatie te vergaren over en op te treden in geval van de verdenking van terrorisme. De wet geeft ten aanzien van 'het buitenland' zeer verregaande bevoegdheden. De oorspronkelijke wet had een looptijd van twee jaar, en is in 2005, 2010 en 2011 in iedere keer beperkter vorm verlengd.
Peer-2-Peer	Een communicatiemodel tussen computers waarbij alle computers een gelijke rol hebben; er is geen hiërarchie, iedere machine is client én server.
PKI	Een public key infrastructure (PKI) is een geheel van systemen waarmee de uitgifte en het gebruik van digitale certificaten wordt gerealiseerd.
SAML	Security Assertion Markup Language is een protocol voor het cross-domain delen van beveiligde netwerksessies.
SCADA	Supervisory Control And Data Acquisition, is het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in grote industriële systemen
Spoofing	Het vervalsen van een netwerkafzender adres, IP dan wel DNS.

Over de auteur

Peter Rietveld (1964) is in 1989 afgestudeerd in de Krijgsgeschiedenis en het Internationaal recht. Hij is sinds 1996 werkzaam in de informatiebeveiliging en sinds 1999 is hij de huiscolumnist van Security.nl.
Hij werkt sinds 2006 voor Traxion als Solution Architect en heeft opdrachten uitgevoerd voor onder meer het Ministerie van Defensie, het Ministerie van Buitenlandse Zaken, de Hogeschool Utrecht, DSM en ECT.

TRAXION
Partners in Information Security