03/2013

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 3 - 2013

THEMA: CONSUMERISATION

DE EVOLUTIE VAN HET NIEUWE "MOBIELE" WERKEN

GEEN DIGITALISERING ZONDER DIGITALE VEILIGHEID

VEILIG INFORMATIEVERKEER IN EEN BYOD-WERELD

FILE-COLLABORATION OP DE ZAAK

VOORWOORD

Ik laat het nieuws van de wereld als een koude douche over me heen rollen. China hackt de westerse wereld, de westerse wereld hackt China. Georganiseerde misdaad is compleet ingestapt in de cyberwereld.
Perverse nerds jagen op de camera's in computers van dames om op afstand te gluren. Het dreigingsbeeld wat een security officer moet overzien, heeft in de afgelopen paar maanden een behoorlijke bijstelling gekregen.
Dit in een tijd waarin "consumerization" echt aan het doorbreken is. Als je nu nog denkt dat je het vanuit security kunt tegenhouden, dan sta je niet met beide benen op de grond - of je werkt voor die (naar mijn schatting) 2% van de security community waar de security afdeling het bedrijfsmatig voor het zeggen heeft. Die andere 98% mogen invullen hoe ze om willen gaan met de onbeheerde apparaten die je bedrijfsomgeving komen infiltreren.
Neem daarbij dat informatie, en dus ook nieuws en achtergronden, nog niet eerder zo toegankelijk en overvloedig was. De nieuwswereld zelf staat in een positie dat ze meer nieuwswaarde moeten leveren tegen minder kosten. De concurrentie is hoog en het jachtseizoen op scoops is dus geopend. Beveiligingsincidenten doen het hier goed bij. Als beveiliger moet je er dus rekening mee houden dat bij een incident er niet zorgvuldig omgegaan wordt met de berichtgeving.
De mogelijke impact op imagoschade is dus ook al toegenomen.
De risicoanalyse ziet er dus anders uit: Risico is kans maal impact. En kans is weer een functie van dreiging en kwetsbaarheid. Alle indicatoren bewegen in een richting die ons als beveiligers niet bepaald rustig in onze stoel doen terugzakken en achterover leunen. Nee, we moeten alert op het puntje van onze stoel zitten.

Het toverwoord: monitoring. Alles in de gaten gaan houden. De beveiliger transformeert van boekhouder van risico's en maatregelen naar oppasser. Als ik kijk welke producten nu in de markt gezet worden voor professionals in ons vakgebied dan gaat het om het in de gaten houden en kunnen rapporteren over het in de gaten houden. Op zich is dat geen slechte ontwikkeling. Meten is weten. Je moet meten om te kunnen regelen. Eigenlijk is het gek, als je terugkijkt, dat we met zo weinig informatie dachten goed te kunnen beveiligen.
Zoals bij alles zit ook hier weer een keerzijde aan. In feite dragen we met al dat monitoren weer bij aan alle veranderingen waar ik mee begon: meer functionaliteit in ICT om te monitoren leidt tot meer kwetsbaarheden, die allemaal misbruikt kunnen worden door de bedreigers. En we voeden de informatieproductie met alle monitoring.
Is dit een cyclus of is dit een spiraal die "out of control" is? Ik weet het gewoonweg niet. Het is net 1984. Maar dan 30 jaar later. Ik ga er maar vanuit dat die generatie van vertraging ook een generatie van wijsheid zal brengen. We hebben een nieuwe generatie van beveiligers nodig met nieuwe inzichten en een andere insteek.

Lex Borger, hoofdredacteur

INHOUDSOPGAVE

DE EVOLUTIE VAN HET NIEUWE "MOBIELE" WERKEN (HNMW)

Richard van Lent is Directeur Business Development bij mITE Systems. mITE is specialist op het gebied van enterprise mobility oplossingen voor bedrijven en biedt advies, consultancy, implementatie en operationeel management van smartphones, tablets, mobiele applicaties en "bring-your-own-device" (BYOD). Richard is bereikbaar via r.van.lent@mite.nl.

HNW anno 2013 gaat allang niet meer over arbeid loskoppelen van tijd en plaats. Werknemers kiezen steeds vaker voor het gebruik van eigen middelen, communiceren - naast e-mail - via verschillende media platformen en vertonen een intensief consumptiegedrag van informatie. Het is dit veranderproces in gedrag, waardoor steeds meer bedrijven de transformatie naar HNW serieus (moeten) nemen en waarbij werkgevers en werknemers leren hoe ze efficiënt en productief met elkaar om moeten gaan in deze nieuwe vorm van samenwerking.

Als we spreken over HNW dan is het fenomeen "Mobiel Werken" bijna onlosmakelijk met dit onderwerp verbonden. In de afgelopen decennia heeft er een ware revolutie en proliferatie van mobiele netwerken en mobiele toestellen plaatsgevonden, waardoor er een enorme groei en acceptatie/normalisatie is ontstaan in het dagelijkse gebruik van mobiele toestellen – zowel privé als zakelijk.

Deze groei van - en verscheidenheid aan - mobiele middelen creëert de nodige uitdagingen voor bedrijven en overheidsinstellingen - klein en groot. Deze uitdagingen hebben niet alleen betrekking op technische- maar vooral ook op organisatorische, sociale en operationele aspecten en maakt dat de relatie tussen werknemer en werkgever, en het gevoerde beleid, snel aan het veranderen is richting een relatie op basis van gelijkwaardigheid. Hierbij wordt de verantwoordelijkheid en aansprakelijkheid tussen werkgever en werknemer steeds vaker gedeeld en randvoorwaardelijk gemaakt.
Er is al veel geschreven en gesproken over de technische aspecten, zoals het inzetten van "Mobile Device Management" (MDM) oplossingen, om mobiele toestellen, binnen het bedrijfsdomein, veilig en gecontroleerd te ontsluiten.
Daarnaast woekeren de trendy modewoorden als BYOD en Choose Your Own Device (CYOD) zich ongehinderd voort met als resultaat dat een groot aantal bedrijven (voor alle bedrijfsonderdelen) aan het worstelen zijn over hoe zij met deze onderwerpen om moeten gaan en wat nu precies de consequenties (gaan) zijn.

> Goede verdeling van verantwoordelijkheden tussen werkgever en werknemer is randvoorwaardelijk voor veilig mobiel werken

Ook de keuze en hoeveelheid aan technische middelen, om mobiel werken in de dagelijkse operatie en bedrijfsvoering te vergemakkelijken, lijkt bijna een exponentiële kromme te doorlopen waarbij het voor bedrijven steeds lastiger wordt om te begrijpen welke middelen nu precies welke mobiliteitsvraagstukken oplossen. Het is juist daarom belangrijk om vooral de technische vraagstukken op en rond mobiliteit en mobiel werken op te delen in een gelaagde structuur. De belangrijkste lagen in deze structuur zijn als volgt benoemd:

- Netwerk laag (NAC – Network Access Control)
- Toestel en OS laag (MDM – Mobile Device Management)
- File collaboration/sharing (File/Document Management)
- Applicatie laag (MAM – Mobile Application Management)
- Data/Informatie laag (Data & Information Classificatie & Management)
- Identificatie laag (Authenticatie en Autorisatie)

Momenteel zijn veel bedrijven bezig om mobiele toestellen, door het inzetten van MDM, in eerste instantie veilig en gecontroleerd te ontsluiten naar de e-mail omgevingen, in combinatie met het vastleggen van het mobiele beleid tussen werkgever en werknemer. Ook wordt steeds vaker een separate zakelijke "container" op het mobiele toestel ingericht die centraal door de IT organisatie wordt beheerd. Deze container kan ervoor zorgen dat zakelijke informatie vanuit de beveiligde container niet op het privé-deel van het mobiele toestel terecht kan komen. Er zijn reeds een aantal bedrijven die de vervolgstap aan het maken zijn door het implementeren van enterprise-grade file-collaboration oplossingen die in combinatie met mobiele toestellen veilig,

> Beveiligingscontainer voorkomt vermenging zakelijke data en privé apps

gecontroleerd en beheerd gebruikt kunnen worden.
Daarnaast maken de meeste bedrijven reeds intensief gebruik van hun bestaande netwerkinfrastructuur (wel of niet in combinatie met NAC), authenticatie en autorisatiemiddelen om ook de mobiele gebruiker gecontroleerd toegang te geven tot de infrastructuur en toepassingen. Hierbij vindt er steeds vaker integratie plaats met de MDM spelers in de markt om vroegtijdig op netwerk niveau reeds toestellen te weren die buiten het ICT beleid vallen.

Bedrijfsinformatie zichtbaar maken op een mobiel toestel kan op een aantal manieren. De meest voorkomende zijn:

- Via een dataverbinding en een "viewer". Op deze manier zal er geen informatie te vinden zijn op het mobiele toestel ingeval van verlies of diefstal en kan de dataclassificatie, die reeds is ingericht voor de desktops, doorgevoerd worden voor deze remote sessies. In veel situaties is dit echter geen werkbare situatie vanwege de kwaliteit van de mobiele verbindingen of een slechte gebruikerservaring in verband met de vormfactor van het mobiele toestel.
- Bedrijfsinformatie zichtbaar maken in speciaal hiervoor gebouwde applicaties, welke reeds encrypted zijn en waarbij eerst ingelogd dient te worden alvorens de applicatie gebruikt kan worden. De informatie kan hierbij lokaal of remote ontsloten worden. Als extra laag van beveiliging kan deze verbinding worden opgebouwd via een VPN-tunnel en/of Applicatie-tunnel (via een MAM "Mobile Application Management" oplossing).
- Bedrijfsinformatie zichtbaar maken via een beveiligde browser - al dan niet via een beveiligde SSL-tunnel naar het bedrijfsnetwerk (VPN-tunneling/ Applicatie-tunneling via MAM).

Samenwerking tussen technologiespelers zorgt voor interessante oplossingen

Eén van de belangrijkste trends die momenteel in de mobiele industrie waarneembaar is, is dat de Best-of-Breed leveranciers voor oplossingen in de hierboven beschreven technologielagen elkaar steeds beter weten te vinden. Daarbij tonen zij een grote bereidheid om samen te werken en ook een bepaalde mate van integratie tussen de verschillende mobiliteitsoplossingen mogelijk te maken. Het doel hierbij is om bedrijven en dus de IT organisatie beter, sneller en transparanter te kunnen bedienen met oplossingen die goed op elkaar aansluiten.
Juist in deze mobiliteitsmarkt, die volop in ontwikkeling en in beweging is en waar voorlopig geen enkele speler op de verschillende technologielagen dominantie kan claimen, is deze ontwikkeling van samenwerking en het creëren van een ecosysteem veelbelovend.

Technologiespelers die in de mobiliteitsmarkt een "One-size fits-All" benadering hanteren, zullen er verstandig aan doen om deze tactiek te herzien! Bovenstaand figuur geeft een indruk van de positionering van de verschillende oplossingen en samenwerking tussen deze leveranciers.

Er is tevens langzaam maar zeker een trend zichtbaar, waarbij bedrijven steeds vaker genegen zijn om, met de groei van haar mobiele applicaties, een applicatiebeheeroplossing te implementeren in combinatie met applicatie-tunneling en applicatie-wrapping technologieën.

Applicatiewrapping plaatst bedrijfsapplicaties in beveiligde container

Dit is een logische vervolgstap om mobiel werken en de mobiele werkers nog beter en veiliger te kunnen ondersteunen in de dagelijkse werkzaamheden en de continuïteit van de bedrijfsvoering te borgen, omdat die steeds afhankelijker wordt van het fenomeen mobiel werken.
Veel MAM en MDM oplossingen bieden

tegenwoordig de mogelijkheid om zakelijke applicaties te "wrappen", waardoor deze applicaties in een beveiligde container op het mobiele apparaat geplaatst worden. Ook bieden deze oplossingen API integraties, waarmee een aanvullende laag van beveiliging aangebracht kan worden in geval van verlies of diefstal. Ook kan er met deze API's configuratie-informatie naar deze applicaties worden gestuurd. Er zijn momenteel echter weinig mobiele applicaties die rekening houden met de classificatie van bedrijfsdata. Dit zou in combinatie met een NAC oplossing als eerste laag opgepakt kunnen worden.

Vanwege het feit dat een hoge beveiliging van een mobiel toestel ten koste gaat van het gebruikersgemak, kiezen veel bedrijven voor een hybride oplossing, welke voor alle wensen beveiliging kan bieden. Voor gebruikers met een hoog beveiligingsniveau kan er, door het implementeren van een beveiligde container gekozen worden voor een volledig afgescheiden zakelijke omgeving. Een container kan, afhankelijk van de leverancier, zijn ingericht op basis van een tweede virtuele machine, of een afgeschermde file/folder structuur (software gedreven) of twee toestellen (op één fysiek toestel) die van hetzelfde OS gebruik maken (op toestel niveau gecodeerd). Voor de medewerkers met een wat lager beveiligingsniveau, kan een combinatie gebruikt worden van "native" applicaties op een mobiel toestel, in combinatie met een beveiligde container voor de data/informatie in deze applicaties. Een voorbeeld hiervan zou e-mail kunnen zijn, waarbij de attachments encrypted in een wachtwoord afgeschermde container komen te staan.

Hybride oplossingen verenigen beveiliging en gebruiksgemak

Er is een technologielaag die nog niet nader is toegelicht - data en informatie management. Uiteindelijk zou je als bedrijf wensen dat je enkel beheer en beveiliging doet op data- en informatieniveau en niet op al die andere lagen. Vooralsnog is dit een onderwerp met vele uitdagingen, zeker voor de mobiele markt, en heeft de ervaring geleerd dat als je bijvoorbeeld naar de technologie-roadmaps van de grote ondernemingen kijkt, zij minimaal vijf tot zeven jaar vooruit plannen, waarbij dit onderwerp ook deze tijdslijn doorloopt.

Uiteindelijk beveilig je het liefst de datalaag

In de huidige situatie is de koppeling met dataclassificatie nog productspecifiek, wat kan leiden tot interoperabiliteitsproblemen of erger, een vendor lock-in. Dit terwijl er goede oplossingen nodig zijn voor zowel desktops als voor de mobiele apparaten. De ontwikkeling en adoptie van standaarden op dit vlak zou zowel de klanten als de leveranciers helpen. Bedrijven zullen gaan ondervinden dat HNW pas een echte win-win wordt als zij in staat zijn om kostenbeheersing, duurzaam ondernemen, continuïteit en waarde creatie met elkaar te verenigen. De snelheid waarmee bedrijven in staat zijn zich aan te passen aan de continue veranderende marktomstandigheden, is een belangrijk onderdeel geworden van de hedendaagse bedrijfs-DNA. En hierin past HNW in de breedste zin van het woord met al haar dimensies. HNmW, en dus "Mobiel Werken", is anno 2013 een realiteit en rand-voorwaardelijk en dwingt bedrijven om op een andere manier haar organisatie in te richten en aan te sturen!

GEEN DIGITALISERING ZONDER DIGITALE VEILIGHEID

Drs. Erik Hoorweg MCM, Mr. Patrick de Graaf en Drs. Roeland de Koning zijn respectievelijk vice-president, principal consultant en managing consultant bij Capgemini Consulting en als zodanig actief op het gebied van openbare orde en veiligheid. Specifiek richten zij zich op vraagstukken op het vlak van cybersecurity, crisisbeheersing, beleidsrealisatie en bedrijfsvoering. Voor meer informatie kunt u contact opnemen met Erik Hoorweg, +31306893862 of kijk op www.capgeminiconsulting.nl.

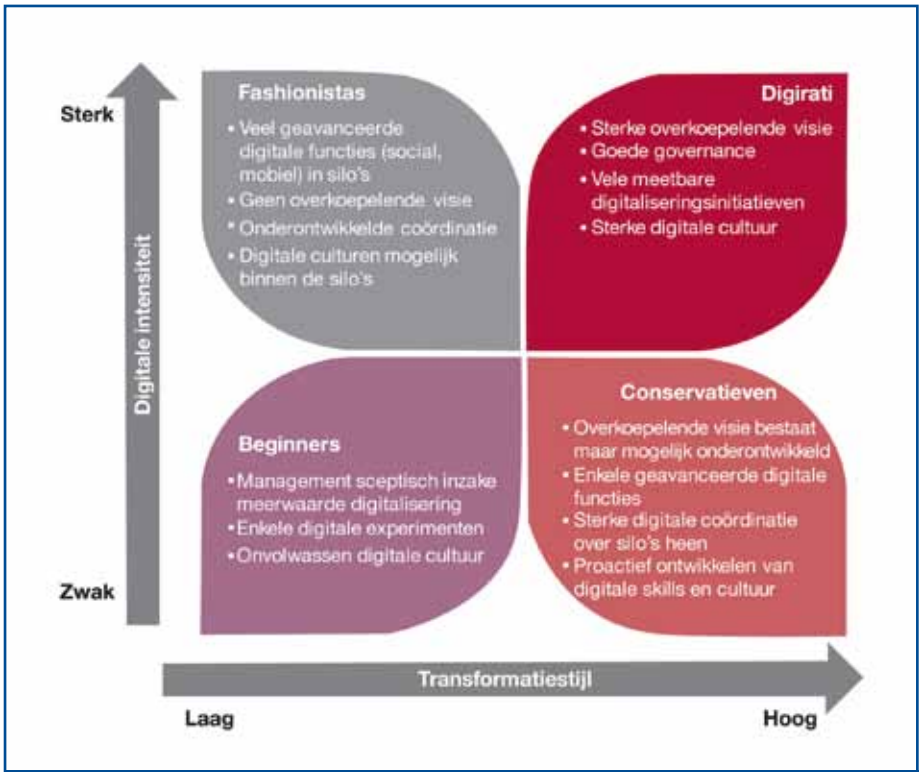
De digitale transformatie van onze maatschappij biedt enorme perspectieven voor de toekomst en is de motor achter de huidige economie. De snelheid van de digitale ontwikkelingen en de mate waarin deze door de maatschappij zijn omarmd, leiden tot vergaande afhankelijkheid van digitale innovaties en dwingt iedereen om mee te gaan in het digitale transformatieproces.

Voor bedrijven en instellingen betreft deze digitale transformatie onder andere het digitaliseren van bedrijfsprocessen. Dit staat internationaal hoog op de agenda, blijkt uit een onderzoek dat Capgemini Consulting en MIT uitvoeren [1]. Mobiele diensten, sociale media, tablets, analytics (big data) en embedded software zijn belangrijke technologische ontwikkelingen die met een ongekende snelheid worden omarmd door zowel organisaties als klanten. De wijze waarop organisaties omgaan met deze digitale transformatie (en de daarmee gepaard gaande digitale risico's) hangt af van twee elementen: de digitale intensiteit (wat) en het transformatiestijl (hoe). Uit het onderzoek blijkt dat organisaties (publiek en privaat) zijn in te delen in vier typen: Beginners, Fashionistas, Conservatieven en Digirati. De organisatie van cybersecurity verschilt per type, dat is een artikel op zich waard.

De druk om te digitaliseren is groot en de wens komt voort uit klanten, het eigen personeel en de concurrentie. Investeringsbeslissingen worden echter veelal vanuit een economische argumentatie genomen, zonder veel oog te hebben voor de risico's [2].

De digitale transformatie kan alleen maar duurzaam plaatsvinden, indien digitale veiligheid simultaan hieraan wordt georganiseerd. De digitale ontwikkelingen geven naast vele mogelijkheden en kansen, namelijk ook ruimte voor kwetsbaarheden en misbruik. Veel informatie die we opslaan, verwerken of uitwisselen of (denken te) verwijderen, heeft door de toegenomen afhankelijkheid steeds meer waarde. De sterke gebondenheid met de hedendaagse digitale ontwikkelingen dringt diep door in ons dagelijks leven. Denk maar aan het gebruik van online bankieren of het gebruik van de ov-chipkaart. Dit zijn digitale omgevingen waarin financiële en persoonsgegevens zijn opgeslagen. De gehele samenleving kan niet meer zonder goed functionerende en veilige ICT-systemen. Storingen (in bijvoorbeeld het betalingsnetwerk) zorgen voor een grote impact in onze maatschappij. Zowel organisaties als individuele gebruikers vertrouwen op de veiligheid en werkzaamheid van digitale systemen. Of in woorden van de Europese Commissie: *"The more we*

> Digitale veiligheid is een randvoorwaarde voor digitalisering



Figuur 1 - Typen organisaties

depend on the internet – the more we depend on its security." [3]

De combinatie van afhankelijkheid, hoge waarde en kwetsbaarheid, trekt kwaadwillende personen. Gedreven door nieuwsgierigheid, persoonlijk gewin, activisme, landsbelang of gewoon voor de kick, kunnen zij veel materiële en immateriële schade veroorzaken. De weinige harde cijfers die er zijn ten aanzien van cybercrime, digitale spionage, hacktivisme, cyberwarfare en cyberterrorisme, laten een stijging zien van digitaal misbruik. Het Cybersecuritybeeld Nederland 2012 geeft aan dat cybercrime en digitale spionage net als vorig jaar de grootste dreiging vormen voor overheden, bedrijven en burgers. Hacktivisten, technisch falen en andere niet-opzettelijke incidenten zijn dat in mindere mate [4]. Banken rapporteren al enkele jaren stijgende cijfers over schade bij internetbankieren [5].

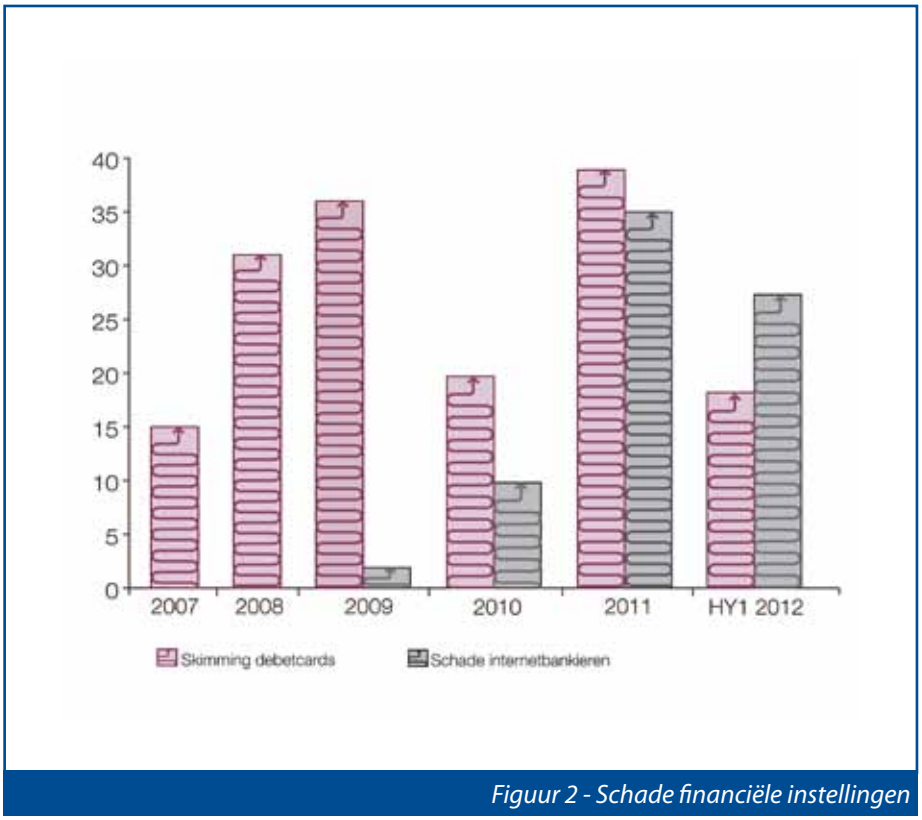
Digitale dreigingen moeten serieus en op alle niveaus in de organisatie worden opgepakt. Digitale dreigingen vormen een relatief nieuwe dimensie van een breed scala aan dreigingen die de organisatie dient te mitigeren. Het vormt daarmee een aanvulling op de set van veiligheidsrisico's van een organisatie. Digitale veiligheid is een normale randvoorwaarde voor de continuïteit van de organisatie en moet onderdeel zijn van een integrale veiligheidsbenadering. Organisaties kunnen digitale veiligheid niet langer onderschatten en zullen hun verantwoordelijkheid moeten nemen. Maar hoe moet de invulling van digitale veiligheid eruit zien en welke nieuwe inzichten zijn daarbij belangrijk?

De traditionele benadering van informatiebeveiliging, waarbij aan de buitenkant van de organisatie (vuur-) muren werden opgetrokken om het kwaad buiten te houden, is niet meer houdbaar. Medewerkers maken immers gebruik van internet, sociale media, mobiele apparaten, tablets, werken ook thuis of brengen hun eigen apparatuur mee naar kantoor [4]. Digitale buitengrenzen van de organisatie vervagen en de kwetsbaarheid voor dreigingen verhoogt. Het bewust of onbewust verspreiden van virussen en andere malware, onvoldoende beveiligde websites en webapplicaties, toegangsbeveiliging die eenvoudig is te omzeilen, niet bijgewerkte software, het gebruik van mobiele apparaten, het gebruik van big data en de effecten daarvan, zijn zaken waar iedere organisatie zich tegen moet bewapenen. Of er wordt toegestaan dat een leverancier onderhoud pleegt en ongemerkt een besmette laptop op het netwerk aansluit, of iemand plugt een besmette USB-stick in waar z'n presentatie op staat.

De nieuwe wereld: ga ervan uit dat je wordt gehackt

Organisaties zullen bij de planning en maatregelen er vanuit moeten gaan dat hun digitale muren doordringbaar zijn, zelfs als de kritische netwerken niet direct met het internet verbonden zijn. Ook afzonderlijke onderdelen van de ICT-omgeving kunnen kwetsbaarheden bevatten en alleen al door de toenemende complexiteit van ICT-systemen en de manier waarop zij in verbinding staan met andere systemen en mensen ontstaat kwetsbaarheid [6]. Dat een organisatie gehackt kan worden, betekent dat het accent van de veiligheidsmaatregelen verschuift van het steeds hoger maken van de digitale muren (*weerbaarheid*) naar de capaciteit veerkrachtig (*'resilient'*) op te kunnen treden. Detectie van, en de respons op incidenten (*'recovery'*) moeten worden georganiseerd. Om de hinder voor klanten en het eigen bedrijfsproces te minimaliseren, is aandacht nodig voor het herstellend vermogen en continuïteitsmanagement.

Als hogere muren niet voldoende zijn, wordt het beveiligen van kleinere delen binnen de muren relevanter. Dergelijke '*defense in depth*' zorgt ervoor dat een aanvaller die eenmaal binnen is, niet overal door kan



Figuur 2 - Schade financiële instellingen

dringen. Dit kan bijvoorbeeld worden gerealiseerd door delen van het netwerk in verschillende, afgescheiden netwerken (*zonering*) of door afzonderlijke ICT-systemen zwaarder te beveiligen dan de rest van de omgeving waarin ze staan. Daarnaast kan de beveiliging nog dieper: op het niveau van de data zelf [7].

Digitale veiligheid is onderdeel van strategisch risicomanagement

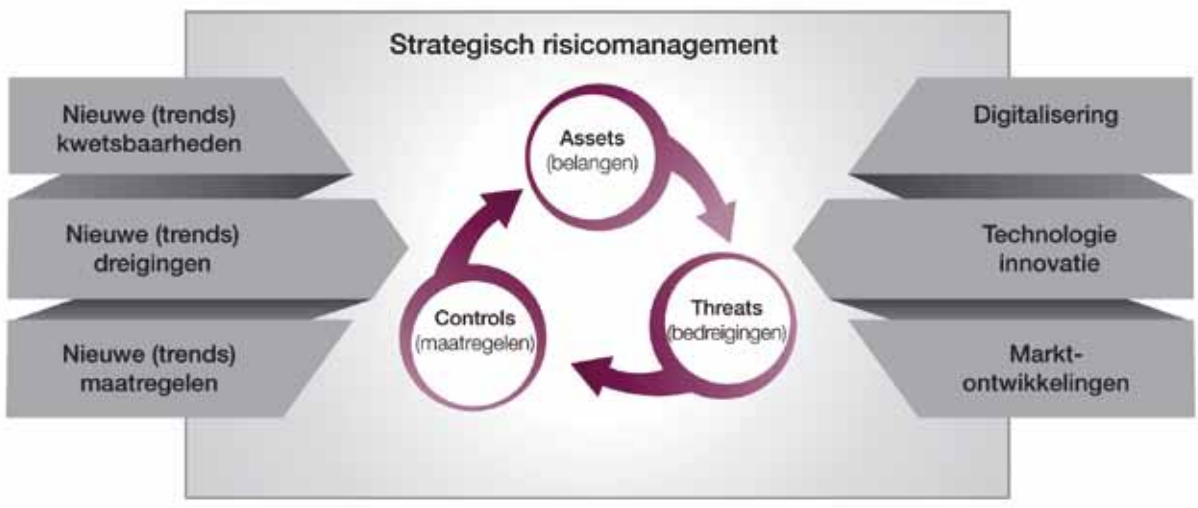
De weerbaarheid kan worden vergroot door zowel aan de binnenkant van de organisatie als aan de poort te monitoren. Echter het is van groot belang dat men ook op de hoogte blijft van ontwikkelingen buiten de organisatie, zoals: in hoeverre heeft de digitale buitenwereld impact op de organisatie? Is er bijvoorbeeld sprake van malware die cruciale elementen uit de ICT tot doelwit heeft? Is de organisatie op de hoogte van hoe er over haar wordt gesproken op (underground) fora? Geeft de informatie op social media inzicht in op handen zijnde aanvallen? Zijn er bij vergelijkbare partijen aanvallen geweest waar organisaties van kunnen leren? Loont het om te investeren in cyber threat intelligence, wanneer digitale belangen (heel) groot zijn? Cyber *threat intelligence* versterkt het omgevingsbewustzijn (ook wel '*situational awareness*') en kan ervoor zorgen dat de organisatie meer tijd krijgt om zich voor te bereiden op een incident.

Aanvullend is versterking van het omgevingsbewustzijn over de digitale wereld ook nodig op *senior management* niveau. Digitale onveiligheid raakt namelijk belangrijke 'assets' van de organisatie, zoals geld, intellectueel eigendom, continuïteit van processen, gegevens van klanten, en imago. Voor de *boardroom* moet daarom duidelijk zijn welke risico's de organisatie loopt en welke maatregelen nodig en gerechtvaardigd zijn op basis van de kritieke assets. Een *cyber dashboard* voor senior management helpt om een goed beeld te krijgen en te houden en daarmee met de juiste informatie sturing te geven, als onderdeel van het totale strategisch risicomanagement. Dit geldt ook voor het nationaal niveau. Het cyber dashboard is geen technisch dashboard, maar een vertaling van digitale trends (zowel positief als negatief) naar actuele en voor de organisatie kritische parameters. Dit voorkomt een focus op incidenten.

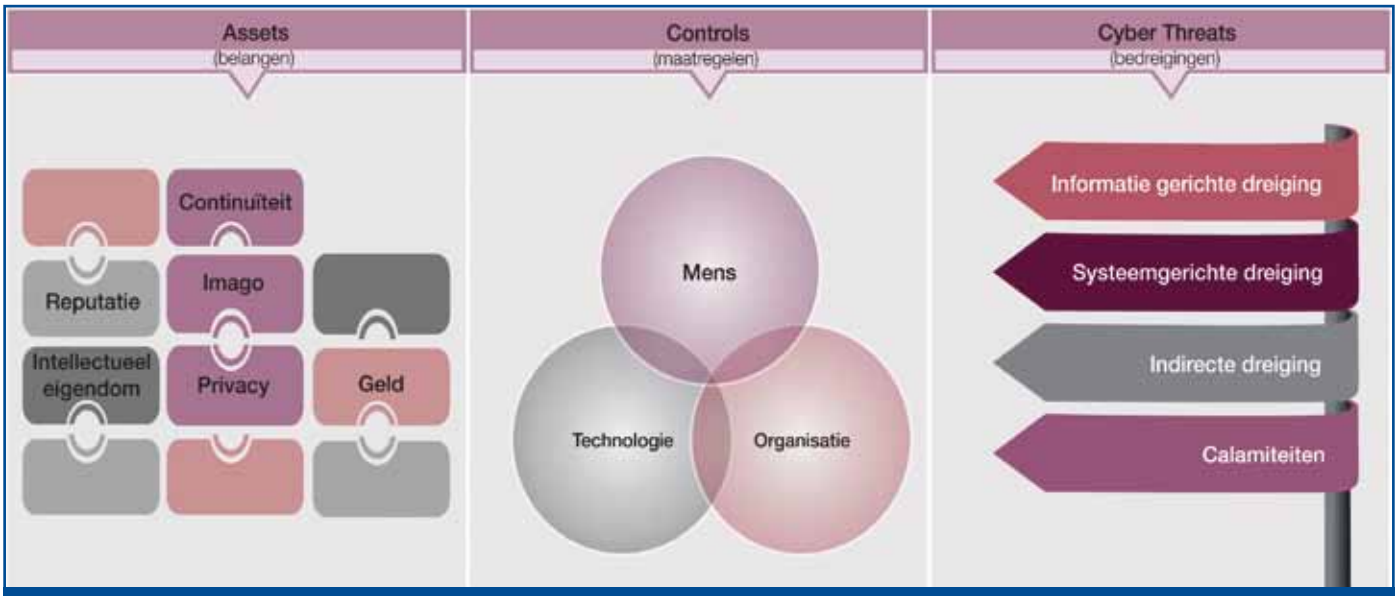
Een integrale aanpak zoekt synergie met andere vakgebieden

Cybersecurity is vanwege het belang van ICT voor de organisatie bij uitstek een onderwerp voor de *boardroom*. Er zijn namelijk genoeg organisaties waarbij uitval van ICT (of de elektriciteit die de ICT draaiende houdt) zal betekenen dat veel werk stil komt te vallen. Denk aan webwinkels of banken, maar ook transport, de elektriciteitsvoorziening of administratieve processen bij overheden en bedrijven. Zo zijn er genoeg voorbeelden waaruit die afhankelijkheid ook blijkt.

Digitale veiligheid verdient meer aandacht in de praktijk. Zoals gezegd vormen digitale dreigingen een aanvulling op de bestaande veiligheidsrisico's van een organisatie. Cyberrisico's moeten onderdeel zijn van het cyclische proces van strategisch risicomanagement, waarbij periodiek, belangen (assets), dreigingen en risico's en maatregelen (*controls*) worden geëvalueerd. Cyberrisico's zijn daarbij slechts één dimensie waar



Figuur 3 - Strategisch Risico Management

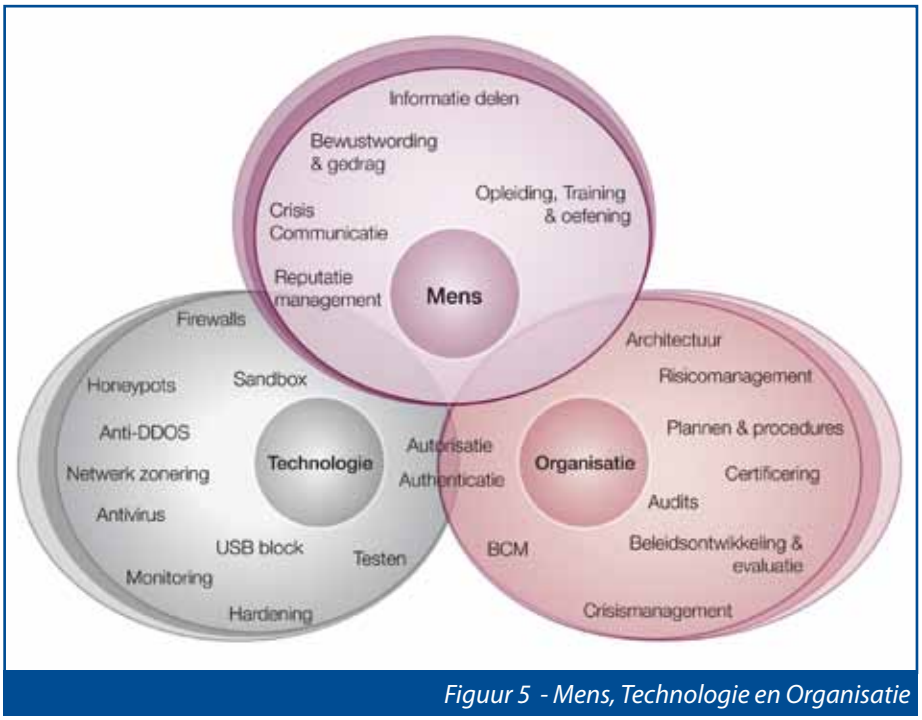


Figuur 4 - Assets, Controls en Cyber Threats

de organisatie rekening mee moet houden. Een integrale aanpak kijkt ook naar dreigingen en kwetsbaarheden vanuit andere dimensies zoals fysieke verstoring (moedwillig of '*acts of God*' c.q. security en safety), milieurisico's, arborisico's en eventueel financiële risico's. Alleen al daarom is een integrale aanpak nodig, waarbij gestreefd wordt naar synergie en samenwerking met disciplines zoals HR, finance, communications, legal en strategy. Alleen door deze integrale aanpak kan de bestuurder '*in control*' zijn over de veiligheid in de organisatie. De uitdaging voor een organisatie is er om, door middel van de juiste maatregelenmix in de dimensies 'mens', 'technologie' en 'organisatie', de belangen te beschermen. Onderstaande figuur geeft een overzicht van de samenhang om als organisatie 'in control' te zijn.

Cybersecurity is mensenwerk

Hoe technisch 'cyber' ook lijkt, cybersecurity omvat veel meer dan technologie. Juist de mens en de organisatie zijn belangrijke dimensies voor een veilige digitale omgeving. In elk van deze drie dimensies bevinden zich kwetsbaarheden, maar ook mogelijkheden om de schade te voorkomen of te beperken.



Figuur 5 - Mens, Technologie en Organisatie

Technologische maatregelen voor het beveiligen van waardevolle assets in de organisatie, zoals hardware, netwerken, besturingssystemen, administratieve bedrijfssystemen, industriële procescontrolesystemen (ICS of PCS) en webapplicaties, is een noodzakelijke stap. Het is daarom goed te blijven investeren in klassieke informatiebeveiligingsmaatregelen, zoals bijvoorbeeld: firewalls, netwerkbeveiliging, identity and access management, monitoring.

Organisatorische maatregelen in de vorm van een beveiligingsbeleid, koppeling aan de organisatiedoelstellingen, financiering, crisismanagement, wet- en regelgeving en eigen richtlijnen en de inrichting van bedrijfsprocessen is essentieel voor cybersecurity en zorgt voor een volwassen en veerkrachtige organisatie die snel weer een normale situatie kan creëren.

In veel opzichten staat echter de mens centraal en wordt deze ook vaak de 'zwakste schakel' genoemd. Maatregelen in de dimensie mens zijn

gericht op bewustwording, gedrag en informatie uitwisseling. Versterking van het omgevingsbewustzijn, over zowel de cyberdreigingen als de ontwikkelingen in de digitale wereld, is noodzakelijk op alle niveaus in de organisatie (strategisch, tactisch en operationeel). Op elk niveau zijn verschillende maatregelen aan te grijpen. Awareness staat of valt dus met de implementatie van maatregelen op alle drie de lagen in de organisatie.

De mens kan vanuit drie rollen te maken krijgen met cybersecurity. Als gebruiker, als besluitvormer en/of zijn adviseur en als expert.

De medewerker/gebruiker (ook thuis): is hij voldoende op de hoogte van de risico's die hij zelf loopt en in staat om maatregelen te treffen om bijvoorbeeld besmetting met een computervirus te voorkomen of te verwijderen? Houdt hij zich aan de spelregels? Bij deze groep zijn bewustwording (of *awareness*) en basiskennis van dreigingen belangrijk.
De besluitvormer en diens adviseurs: is deze doelgroep voldoende geïnformeerd over incidenten en strategische risico's? Is deze doelgroep in staat om bij incidenten effectief te sturen op herstel?
Hoe kan op een effectieve manier worden samengewerkt met ketenpartners, branchegenoten en de overheid? Bewustwording, externe samenwerking en een goede vertaalslag van en naar cyber experts zijn van belang.
De cyber specialist/expert: zijn er kwalitatief en kwantitatief voldoende 'mensen achter de knoppen'?
Hoe werken zij samen met de rest van de organisatie in de koude en warme fase (normale gang van zaken en incidenten)? Onder andere capaciteit, motivatie, opleiding, wijze van aansturing en diepgaande kennis zijn van belang.

'No digital transformation without digital security'

Digitale ontwikkelingen in onze maatschappij dwingt iedereen om mee te gaan in het digitale transformatieproces. Investeren in digitale vooruitgang betekent ook investeren in digitale veiligheid, anders kan de continuïteit van de organisatie niet meer gegarandeerd worden. Gezien de grote potentiële impact van digitale dreigingen is versterking van veerkracht nodig om na incidenten schade voor de eigen organisatie en derden te beperken en terug te veren naar de normale bedrijfsvoering.

Alleen een integrale aanpak, waarbij synergie en samenwerking ontstaat met verschillende disciplines in de bedrijfsvoering helpt de bestuurder in control te zijn over de veiligheid van de organisatie. Cybersecurity is hierbij meer dan techniek alleen en 'de mens' heeft een sleutelrol in het vergroten van de veiligheid.

Versterking van het omgevings-bewustzijn over de digitale wereld op senior management niveau is echter essentieel. Digitale veiligheid moet onderdeel zijn van strategisch risicomanagement, wanneer digitale middelen belangrijk zijn voor uw organisatie. Het is een 'gewone' randvoorwaarde voor de bedrijfsvoering, net als mensen, geld en kennis. Door cyber threat intelligence en een sturingsinstrument in de vorm van een cyber dashboard krijgen bestuurders meer zicht en grip op digitale veiligheid. ●

Door gericht aan de buiten- en binnenkant van uw organisatie te investeren in beveiliging (defense in depth), kunt u beter balanceren tussen de mate van veiligheid en de kosten die daarmee samenhangen. Wat is het risico in termen van kans en impact en wat is daartoe een gerechtvaardigde investering? U kunt efficiënter beveiligen wanneer u het opschalen van een hoger beveiligingsniveau weet te beperken tot die onderdelen die dat ook echt nodig hebben.

Kortom:
- Ga ervan uit dat u wordt gehackt;
- accepteer uw kwetsbaarheid;
- focus op 'resilience' en 'recovery';
- pas uw beveiligingsniveau aan op kleinere extra gevoelige onderdelen;
- investeer in cyber threat analysis;
- geef senior management een middel, zoals een cyber dashboard, waarmee ze kunnen sturen.

Digitale Veiligheid

Links

[1] *Digital Transformation Review N° 02, January 2012; Capgemini Consulting, MIT Center for Digital Business; http://ebooks.capgemini-consulting.com/digital-transformation-review-2/*

[2] *Bauer, J.M., Eeten, M.; "Introduction to the economics of Cyber Security", Communications & Strategies, N° 81.Business; http://quello.msu.edu/sites/default/files/pdf/Bauer-VanEeten-CS81_Intro_2011.pdf*

[3] *Eurocommissioner Neelie Kroes, The Digital Agenda two years on: is Europe well-placed?, 12 June 2012 (press release); http://europa.eu/rapid/press-release_SPEECH-12-483_en.htm*

[4] *Nationaal Cyber Security Centrum. (2011) Cybersecuritybeeld Nederland CSBN-2. Den Haag: Ministerie van Veiligheid en Justitie; https://www.nctv.nl/pp/csbn/*

[5] *http://www.nvb.nl/home-nederlands/nieuws/nieuwsberichten/fraude-internetbankieren-stijgt-eerste-half-jaar-met-14_.html*

[6] *Weijnen, M., Bruijne, M.de; "Complexiteit: de nieuwe realiteit van vitale infrastructuren", 3 april 2012.*

[7] *Jericho Forum® Data Protection; https://www2.opengroup.org/ogsys/catalog/W12C*

GEORGANISEERD DOOR MADISON GURKHA

14 mei 2013 | De Reehorst in Ede

Black Hat Sessions XI

Dit jaar organiseert Madison Gurkha alweer de 11e editie van de inmiddels befaamde Black Hat Sessions. Het thema dit jaar is: **Cyber...Security**. Het woord 'cyber' kent nogal wat achtervoegsels, waarmee zaken uit het echte leven te verplaatsen zijn naar de digitale wereld. Denk bijvoorbeeld aan cyberpesten, cybersex, cyberpunk en meer on-topic voor de Black Hat Sessions vooral ook aan cyberwarfare, cyberterrorisme en cybercrime.

CYBER ... SECURITY

#bhspartXI

SPREKERS

Met trots presenteert Madison Gurkha voor de Black Hat Sessions Part XI prominente sprekers die zeer goed aansluiten bij het thema **Cyber...Security**.

'Cyberkolonel' Hans Folmer
Commandant Taskforce Cyber bij de Defensiestaf

Gerben Klein Baltink
Secretaris Cyber Security Raad

Wim Verloop
Managing Partner & Senior Forensic Analist, Digital Investigation B.V.

Eileen Monsma
Advisor, Politie Team High Tech Crime

Rickey Gevers
veroordeeld hacker en tegenwoordig werkzaam bij Digital Investigation B.V.

Alex de Joode
Senior Regulatory Counsel and Liaison Officer, LeaseWeb

INFORMATIE

De Black Hat Sessions Part XI: **Cyber...Security** vindt plaats op dinsdag 14 mei 2013 bij Hotel en Congrescentrum De Reehorst te Ede. Het programma start om 09.25 uur en duurt tot 16.40 uur. Aansluitend wordt nog een borrel georganiseerd. Registratie is mogelijk vanaf 08.30 uur. Meer informatie over het congres is te vinden op: **www.blackhatsessions.com**.

REGISTREER NU!

Speciaal voor leden van het PvIB geldt een aantrekkelijke korting van 35 euro. Zo betaalt u i.p.v. 265 euro maar 230 euro excl. BTW per persoon. Via het inschrijfformulier Via het inschrijfformulier op www.blackhatsessions.com kunt u de kortingscode BHSPVIB-14m opgeven en de korting wordt tijdens het afrekenproces automatisch verwerkt. **Als u zich voor 16 maart a.s. aanmeldt ontvangt u bovendien 10% vroegboekvoordeel!**

SPONSORS

ITSX SCOS DIGITAL Investigation qict TSTC

MEDIA PARTNERS

NOREA winmag PvIB ISACA Netherlands Chapter Ngi

ORGANISATIE

Madison Gurkha
Your Security is Our Business

VEILIG INFORMATIEVERKEER IN EEN BYOD-WERELD

Gavan Egan is Vice President bij Verizon Terremark, dat Cloud/IT en Security Services levert.
Hij is te bereiken via verizonbenelux@axicom.com.

Bedrijven worden steeds vaker geconfronteerd met *digital natives*, medewerkers die hun eigen smartphone, tablet en/of laptop binnen de bedrijfsmuren brengen en gewend zijn aan constante digitale communicatie. Om gelijke tred te houden met deze generatie is het noodzakelijk bedrijfsstructuren, vormen van dienstverlening en veiligheidsprotocollen constant aan te passen. Dit *Bring Your Own Device (BYOD)* fenomeen is dan ook één van de meest belangrijke uitdagingen voor de CIO van vandaag.

Digital natives zijn gewend aan een vrije keuze in het apparaat dat ze gebruiken om te communiceren of toegang te krijgen tot informatie. Zij willen communiceren en (samen) werken waar en wanneer zij dat willen in de vorm die zij wensen. Naarmate het gebruik van mobiele apparaten op de werkvloer toeneemt, stijgt ook de vraag naar intelligente zakelijke applicaties die op meerdere platformen toegankelijk zijn. Dat geldt ook voor de vraag naar data, bandbreedte en rekenkracht om deze applicaties te laten draaien.

Meer gebruik betekent grotere vraag

Organisaties zijn al bezig met het integreren van consument-gedreven IT oplossingen op de werkvloer. Mobiele werknemers worden hierbij uitgerust met cloud-gebaseerde geïntegreerde applicaties die veilig en betrouwbaar werken op zowel draagbare apparaten als desktops. Systemen voor device management en content delivery zijn belangrijke succesfactoren in een dergelijke omgeving.

Als het gaat om volledige mobiele integratie van alle werknemers is het trieste feit dat veel bestaande IT-infrastructuren hier volstrekt ontoereikend voor zijn. De mobiele werknemers vereisen constante en veilige toegang tot tools en back-end systemen om productief samen te werken. In zo'n situatie kunnen cloud services een oplossing bieden, hetzij door een gehele overstap, dan wel door een uitbreiding van de IT-infrastructuur.

> Digital natives zijn gewend aan een vrije keuze in het apparaat dat ze gebruiken

Cloud computing geeft organisaties een flexibele en veilige toegang tot grote hoeveelheden schaalbare rekenkracht, met de vrijheid om de capaciteit op of terug te schalen, om de natuurlijke cycli van het bedrijf te ondersteunen. In de praktijk betekent dit dat de ICT-omgeving in kan spelen op het tempo en de dynamiek van het bedrijf, zodat de technologie in dienst staat van de veranderende zakelijke behoeften.

Het combineren van cloud computing met *High IQ Networks* - een "super" datacenter met ultra-wideband capaciteit voor de cloud en 'slimme' mobiele apparaten met gepersonaliseerde applicaties- is een goede stap naar een efficiënt, effectief en toekomstbestendig platform. Deze netwerken maken het mogelijk applicaties naadloos en veilig te 'mobiliseren', zodat ze niet alleen op de desktop toegankelijk zijn, maar ook op de steeds slimmere mobiele apparaten met behulp van de "thin-client" benadering, waarin applicaties worden opgeslagen en geleverd vanuit de cloud.

Vijf simpele beveiligingsstappen

Om veilig gebruik te maken van dergelijke netwerken zijn er wel een aantal risicofactoren voor het bedrijf wat de mobiele apparaten

Figure 8. VERIS A⁴ Grid depicting the frequency of high-level threat events

		Malware			Hacking			Social			Misuse			Physical			Error			Environmental		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Servers	Confidentiality & Possession	381			518		1				9	8	1					2	1			
	Integrity & Authenticity	397			422		1				6	1	1									
	Availability & Utility	2			6						5											
Networks	Confidentiality & Possession										1											
	Integrity & Authenticity	1									1											
	Availability & Utility	1			1						1											
User Devices	Confidentiality & Possession	356			419						1			86								
	Integrity & Authenticity	355			355						1	1		86								
	Availability & Utility										1			3								
Offline Data	Confidentiality & Possession											23							1			
	Integrity & Authenticity																					
	Availability & Utility																					
People	Confidentiality & Possession							30	1													
	Integrity & Authenticity							59	2													
	Availability & Utility																					

The frequency of high-level threat events

betreft. Deze zijn op te splitsen in drie categorieën: vertrouwelijkheid, integriteit en beschikbaarheid.

Vertrouwelijkheid is alleen haalbaar als het bedrijf beschikt over strikte beveiligingsprotocollen waarmee grenzen worden gesteld aan de informatie die medewerkers mogen kopiëren naar hun mobiele apparaten. Hierin staat ook welke encryptietechnologieën ze hiervoor gebruiken. Het openstellen van communicatie en toegang tot diensten aan de mobiele werknemers vereist niet alleen integriteit en verantwoordelijkheid van de medewerkers, maar ook een gedegen kennis van de risico's die hiermee gepaard gaan, evenals een duidelijke standaard. De beschikbaarheid van mobiele communicatiediensten kan ook een grote zorg zijn voor organisaties die zeer afhankelijk zijn van mobiele werknemers. Een bedrijfscontinuïteitsplan is dan ook essentieel om storingen te minimaliseren.

Als organisaties continu rekening houden met deze risicofactoren naarmate de mobiliteitstrategie evolueert, kunnen ze dit proces in goede banen leiden. Mobiele veiligheid is in vijf maatregelen te bereiken:

1. Inventariseer, categoriseer en wijs gevoeligheidsniveaus toe aan bedrijfsinformatie en bepaal beleidsregels en controles. Zo is er een nulpunt en basis voor toekomstige evaluatie.
2. Evalueer en actualiseer het bestaande mobiele beleid, of creëer nieuw beleid als bedrijfsstandaard voor beveiliging van alle mobiele apparaten en applicaties.
3. Maak een lijst van de mobility tools die werknemers nodig hebben om te kunnen werken op hun pc thuis, persoonlijke mobiele apparaten en publieke internetdiensten. Selecteer een MDM-oplossing waarmee deze applicaties leverbaar zijn, bijvoorbeeld via een Enterprise Appstore of door sandboxing.
4. Gebruik encryptie voor alle data op alle apparaten.
5. Hanteer vaste beveiligings-instellingen - van wachtwoorden tot het bepalen van "lock/wipe" protocollen.

> Eén datalek kan gemakkelijk de kosten van een veiligheidsprogramma in veelvoud overstijgen

Regelmatige evaluatie en controle van de processen voor beveiliging en de veiligheid van publieke diensten blijft uiteraard altijd van belang. Beveiliging is een constant evoluerende vereiste en staat nooit stil. Cybercriminelen zoeken continu naar de zwakke plekken in de beveiliging om waardevolle bedrijfsgegevens te bemachtigen.

Constant trainen van werknemers in veiliger gebruik

Mobiele apparaten maken sociale netwerken altijd beschikbaar - thuis en op het werk. Met dit in het achterhoofd is het belangrijk dat werknemers op de

hoogte zijn van de mogelijke gevolgen van het gebruik van sociale netwerken binnen de organisatie. En dus ook van de veiligheidsrichtlijnen en -procedures voor het gebruik van mobiele apparaten. Sociale netwerken bieden een zeker mate van beveiliging voor de gebruikers tegen malware, spam en phishing, maar geraffineerde cybercriminelen blijven gebruikers verleiden besmette websites te bezoeken of persoonlijke informatie te delen. Welke risico's dit binnen een zakelijke omgeving op kan leveren behoeft geen uitleg.

Een gedegen beveiligingsprogramma blijft noodzakelijk

Hoewel sommige organisaties zich verzetten tegen regelmatige evaluaties van veiligheidsregels en niet bereid zijn meer uit te geven dan nodig, kan slechts één datalek - al dan niet opzettelijk - gemakkelijk de kosten van een gedegen veiligheidsprogramma in veelvoud overstijgen. Dit geldt des te meer voor de mobiele werkomgeving.

In het Verizon Data Breach Investigation Report van 2012 (DBIR 2012) zijn 855 datalekken geanalyseerd waarbij 174 miljoen records zijn gestolen. Verrassend genoeg was 97% van de geanalyseerde aanvallen gemakkelijk te vermijden geweest. Bovendien hadden de getroffen bedrijven hiervoor niet eens moeilijke of dure maatregelen hoeven nemen.

2012 DBIR

Sommige beveiligingsexperts voorspellen dat de meest waarschijnlijke datalekken bij organisaties in de toekomst hun herkomst vinden in mobiele apparaten. De onderzoekers van Verizon's DBIR trekken echter andere conclusies, zij zien authenticatie-aanvallen, voortdurende spionage en "hacktivisme", besmette webapplicaties en social engineering als de cybercrime tactieken om voor op te passen.

Met betrekking tot mobiele apparaten verwachten de onderzoekers dat verloren en gestolen mobiele apparaten - veelal niet voorzien van encryptie - het grootste gevaar blijven, dit komt nog veel vaker voor dan hacking en malware. Een toename van aanvallen op mobiele apparaten door cybercriminelen zal nauw verbonden zijn met de groei van mobiele betalingen in de zakelijke en consumentenmarkt. Maar zolang er bij veel organisaties geen standaard is voor beveiliging en gebruik van mobiele apparaten, blijft dit een zwakke plek.

Omhels de vrijheid van mobiliteit in een veilige omgeving

Steeds meer werknemers ontdekken de vrijheid en flexibiliteit van mobiel werken; en organisaties plukken hiervan de vruchten door verhoogde productiviteit en handelingssnelheid. Zakelijke mobiliteit is of wordt hiermee voor veel bedrijven een belangrijke succesfactor. Nieuwe werknemers brengen hun nieuwe apparaten binnen de organisatie en moeten zich bewust zijn van het bedrijfskritische belang van de data die ze bij zich dragen. Met een effectieve controle en regelmatige evaluatie van de veiligheidsprotocollen kunnen bedrijven de kracht van mobiliteit optimaal inzetten en hun merk en vertrouwelijke data beschermen. Nu en in de toekomst. ●

Links

DBIR 2012:
http://www.verizonenterprise.com/DBIR/2012

COLUMN

DE INVAL

"Goedemorgen, wij zijn van het College Bescherming Persoonsgegevens." En dan ineens heb je als bedrijf of instelling een ambtshalve inval van het CBP aan je broek. De receptioniste in paniek, de afdeling Legal staat op zijn kop, de Privacy Officer kamt nog eens netjes de haren en de directie wordt wakker gebeld. Denkt u nu niet, "dat overkomt ons niet", want velen gingen u inmiddels voor. En ja, vaak wordt er echt wel iets gevonden door het College wat niet helemaal in orde lijkt te zijn. Het CBP geeft weliswaar aan dat "De nadruk ligt […] op onderzoek naar ernstige overtredingen die structureel van aard zijn en veel mensen raken", doch dat belet hen niet ook voor minder aan de poort te staan.

Wat mag het CBP dan eigenlijk allemaal? Het College heeft verschillende bevoegdheden onder de Wet bescherming persoonsgegevens. Zo mogen zij een inval doen (inclusief inbeslagname) zonder rechterlijk bevel. Zij kunnen audits verrichten, mogen informatie en documenten opvragen en mogen verzoeken doen voor toegang tot databanken en archiveringssystemen. Overigens is zo'n verzoek niet vrijblijvend.

Maar hoe gaat dat nu eigenlijk zo'n inval? Het CBP komt met een speciaal daarvoor samengesteld team en klopt letterlijk onverwacht aan de deur. Zij verwachten dan dat u uw zaakjes op orde heeft, hoe u hen het beste kunt ontvangen en wat op orde moet zijn, zal ik zo schetsen. Eerst verder met die inval. Het team moet vervolgens naar een ruimte begeleid worden, laat ze alsjeblieft niet rondlopen door het gebouw. Overigens kunt u het team wel heel eventjes laten wachten - de gegevens waarom zij verzoeken, moeten immers bij elkaar vergaard worden - maar neem daarvoor niet teveel tijd, want starten met een ongeduldig invalteam is niet aanbevelenswaardig. Het team geeft dan al aan wat zij precies willen, het is zaak daar snel op door te pakken, want u moet het zo snel mogelijk gereed hebben. Doorgaans verzoeken ze om inzage in de relevante documentatie. Daarna zullen specifieke systemen bekeken worden. Het team weet tevoren wat ze willen zien en zullen dat dan ook melden. Die inzage moet zeer letterlijk genomen worden. Het team staat over de schouder mee te kijken bij degene die de knoppen moet bedienen en vragen gaandeweg precies datgene te laten zien waar ze voor komen. Zo zullen ze willen zien hoe het systeem werkt, welke gegevensstromen daarin zitten, wie dat kan zien, wat ermee gedaan wordt, etc. Vaak volgen daarna nog enkele interviews, waarin specifieke personen binnen het bedrijf aan de tand gevoeld worden. U dient uitleg te verschaffen.

En wat moet u dan op orde hebben? Zorg er allereerst voor dat u een draaiboek heeft. Wat moet de receptioniste doen als het CBP invalt? Wie moeten gebeld worden? Waar mag het team 'neergezet' worden? Waar vindt u de documentatie? Welke personen moeten aanwezig zijn en moeten direct opgeschakeld worden? Weet iedereen dat je vragen alleen maar met de essentiële informatie beantwoord en dat je nooit vrijwillig allerlei extra informatie geeft? Is er geen bedrijfsjurist, is er dan een telefoonnummer van een advocaat paraat?

Daarnaast de inhoud van datgene wat overlegd moet worden bij de inval. Zorg er in ieder geval voor:

- dat het privacybeleid (want dat heeft u natuurlijk) gereed ligt;
- dat eventueel sub-beleid aanwezig is (denk aan specifieke richtlijnen zoals de omgang met datalekken of huisregels over omgang met BYOD);
- vergeet niet dat privacy ook de plicht tot beveiligen behelst, dus heb ook het beveiligingsbeleid klaarliggen;
- verricht u pentesten, audits of andere assurance gerelateerde zaken? Zorg dat de rapportages klaarliggen en ook de follow-ups daarop;
- weet wie er binnen uw bedrijf het beste op toegericht is om het team door de systemen te leiden, vergeet daarbij niet dat veel mensen bloednerveus van een dergelijke inval worden.

Moet u zich nu zorgen gaan maken? Nee. Zeker niet als u bovenstaande zaken goed op orde hebt. De basis van uw privacybeleid moet als een huis door de organisatie heen staan. Is er nog geen Privacy Officer of iemand met een vergelijkbaar takenpakket? Zorg er dan voor dat u iemand die taak toebedeelt. Het is meer dan de moeite waard. Het CBP blaft en bijt soms best even gemeen, maar wees vooral niet bang. Wees voorbereid. ●

Mr. Rachel Marbus, @RachelMarbus op Twitter

IPV6, NIET ALLEEN EEN LANGER ADRES!

Drs. Andor Demarteau CISA CISSP CEH is als Senior IT Security specialist de schakel tussen business en IT met een gefundeerde achtergrond in de techniek. Onderwerpen als PKI, encryptie, privacy, policies en procedures, risico analyses en security architectuur zijn de kernbegrippen binnen zijn vakkennis. In zijn vrije tijd is hij radiozendamateur en sportduiker. Andor is te bereiken via andor.demarteau@capgemini.com

Zeker 10 tot 15 jaar geleden toen het internet in opkomst was in onze business wereld, riepen de wetenschappers en ingewijden al dat de IP adressen eigenlijk al bijna op waren. Niemand geloofde ze natuurlijk.

Feitelijk echter hadden zij gelijk en het feit dat het uiteindelijk nu echt zover is, heeft meer te maken met een aantal kunstgrepen die wij in de industrie hebben uitgehaald, dan dat er daadwerkelijk meer adressen beschikbaar zijn gekomen.
Kunstgrepen als het opknippen van klasse A en B adressen uit de oude IPv4 adres indeling en NAT (network address translation) hebben er voor gezorgd dat de daadwerkelijke uitputting van de IP versie 4 adressen op zich heeft laten wachten. Dit heeft echter wel een heel groot nadeel tot gevolg: nu het daadwerkelijk zover is dat de adressen echt op zijn, lopen we keihard tegen de grenzen van het internet aan.
En dan nog maar niet te spreken over het misbruik van NAT en andere soortgelijke technieken als security maatregel.
In dit artikel zal ik kort ingaan op de risico's die wij in de nabije toekomst tegen zullen komen, wanneer wij gaan overstappen op IP versie 6. Dat dit zal gebeuren staat als een paal boven water, wanneer en hoe precies valt te bezien. Ook het tijdsbestek waarin dit zal gebeuren zal zich uitstrekken over het grootste zo niet het gehele huidige decennium.

Today's latte, World IPv6 Launch (Bron: Yuko Honda, via Flickr)

Wat is IP versie 6?
De naam, of liever de nummering, zou kunnen doen vermoeden dat het hier gaat om een upgrade van het huidige IP protocol (IP versie 4) en dat het puur gaat om alleen langere adressen zodat we weer een tijdje voort kunnen. Als het aan de industrie had gelegen was dat waarschijnlijk wel de uitkomst geweest. Echter, niet 15 maar al ruim 22 jaar geleden, hebben de wetenschappers ingezien dat het gebruik van het toen nog relatief nieuwe IPv4 protocol zijn problemen bezat, waarvan eentje, de lengte en opdeling in klassen van de adres ruimte, de meest urgente leek te gaan

worden richting het einde van de vorige eeuw.
In het steeds maar uitdijende internet bleek de opzet van het huidige IP protocol nog meer haarscheurtjes te vertonen die schreeuwden om een oplossing. Zo werd routering een steeds groter en complexer probleem en kwamen er langzaam ook vormen van misbruik aan het licht waarbij routering, fragmentatie van pakketten halverwege hun transport et cetera werden misbruikt.
De ontwerpers van het nieuwe IP protocol (IP versie 6) gingen met hun kennis en inzicht een flinke stap verder dan zij strikt genomen hadden moeten doen. Ze breidden de adresruimte uit van 32 naar 128 bits per adres, versimpelden de routeringsmechanismen dusdanig, dat aan een adres valt te zien waar dit in de wereld thuishoort, bouwden beveiligingsmechanismen als encryptie en authenticatie in het protocol in, verwijderden mogelijkheden tot het aangeven van routeringspaden en verboden het fragmenteren van IP verkeer en route.
Natuurlijk is er in de 20 jaar nadat de eerste RFCs (request for comments) over IPv6 zijn uitgekomen nog wel het een en ander gewijzigd en aangepast vanwege voortschrijdend inzicht, maar dit is kort gezegd wel waar het hele verhaal om draait.

Loop ik nu al gevaar?
Het korte antwoord daarop is "ja".
Echter dit verdient natuurlijk wel wat meer uitleg en verduidelijking.
De industrie is langzaam wakker aan het worden en zich aan het beseffen dat de IP versie 4 adressen echt op zijn en ze dus iets moeten doen. Er zijn in bijvoorbeeld China al hotels waar je met een IPv4 only machine niet eens meer op het lokale internet kan, omdat zij al volledig IPv6 only omgeschakeld zijn, maar dat terzijde.
Veel apparatuur, firmware, besturingssystemen en andere software die wij in onze business tegenwoordig kopen, is inmiddels IPv6 ready. In vele gevallen zelfs IPv6 enabled by default, zonder enige vorm van beveiliging of policies die de hardware en software moeten beschermen tegen aanvallen en misbruik.

We lopen keihard tegen de grenzen van het internet aan

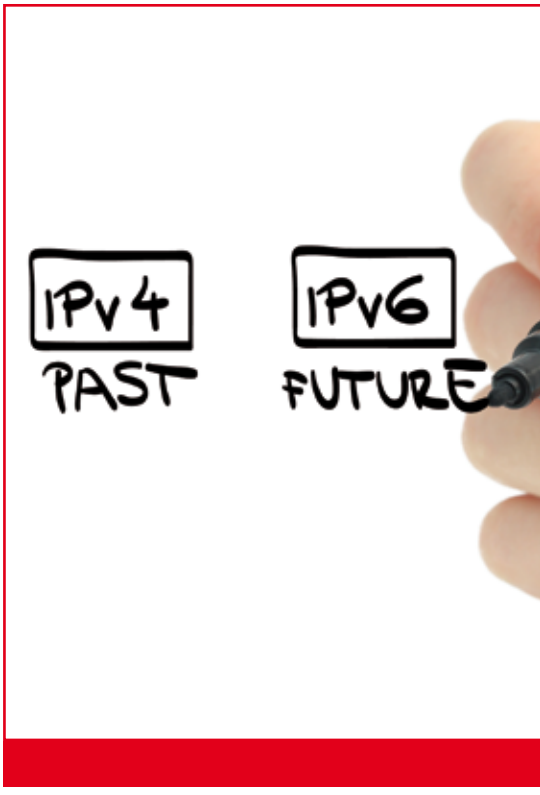
Laat nu dat precies het grootste probleem zijn in de huidige status van IP versie 6.
Het probleem zit hem in het feit dat IPv6 in tegenstelling tot zijn voorganger, het huidige IPv4, niet bepaald een simpele upgrade of uitbreiding is. Niet alleen de adressen zijn langer geworden, maar door de gehele opbouw van de IP protocolstack is er zoveel gewijzigd, dat als je IPv4 en IPv6 tegelijkertijd wilt kunnen gebruiken, je eigenlijk een duale oplossing nodig hebt. Je moet dus beide protocolstacks volledig naast elkaar draaien om beide soorten IP verkeer te kunnen afhandelen.
En dat is nu juist waar hier het probleem, of liever de uitdaging, zit. Beveiligingsmaatregelen genomen op de oude en vertrouwde IPv4 protocolstack gelden niet voor IPv6. Sterker nog, doordat IPv4 netwerken tegenwoordig veelal achter een NAT boundry zitten en deze dus deels worden misbruikt als security maatregel, ligt het IPv6 gedeelte van het netwerk volledig open en bloot.

Het IPv6 gedeelte van het netwerk ligt volledig open

Impact en risico
Zoals gezegd is veel van onze nieuwe apparatuur al IPv6 enabled en houden onze security policies, controls en maatregelen daar geen rekening mee. Dit gekoppeld aan het misbruik van NAT als security maatregel en het feit dat veel IPv6 enabled software zijn eigen lokale adressen al auto-configureert, zorgt voor een nogal gevaarlijke mix voor onze netwerk- en data beveiliging. Immers, als een hacker binnen wil dringen, komt hij niet langs de NAT firewall, want connecties naar binnen zijn niet mogelijk. Feitelijk correct.

Echter, gezien het feit dat uw firewall en routers inmiddels ook IPv6 praten, local-link adressen auto-configureren en je ook een IPv4 adres in IPv6 kan schrijven en daarmee je verkeer via de IPv6 stack kan laten lopen, is er een mooie en vooral "onzichtbare" route rond uw zo goed opgestelde firewall. Daar komt dan nog bij dat de meeste besturingssystemen, zoals Windows 7 en hoger, maar ook Mac OSX en Linux, precies hetzelfde doen. Nu hebben we een perfecte verbinding via het IPv6 enabled internet vanaf de hacker rechtstreeks tot in het hart van uw organisatie.
En voor wie denkt dat dit niet misbruikt kan worden of actief misbruikt wordt, zoek gerust zelf even op internet en je weet dat je al achterhaald bent.

Hoe is dit ontstaan?
Heel simpel, we zien dat de industrie eigenlijk nog steeds dezelfde fouten maakt die zij in het begin bij IPv4 ook maakten. "Och, leuke feature, maar daar is toch geen beveiliging voor



nodig?" Dezelfde fout die de industrie ook blijft maken voor consumenten en klein-zakelijke apparatuur zoals printers, scanners, multi-functionals, NAS en SAN storage drives, beveiligingscamera's etc. Security-by-design bestaat niet, kost geld en onze klanten willen er toch niet voor betalen als mijn concurrent het ook niet heeft en daardoor goedkoper is.
Deze wijze van werken strekt verder dan alleen netwerkbeveiliging, maar dat valt buiten de scope van dit artikel.
Het is belangrijk te onthouden dat uw leverancier van hardware en software uw veiligheid niet waarborgt, dat zult u als organisatie zelf moeten doen.
Dat geldt eens en temeer voor het hier aangegeven risico rond IP versie 6.

De oplossing

Echter er is niet echt een "de" oplossing, maar is het een traject met eerdere zijpaden die u kunt bewandelen. Dit heeft alles te maken met de keuze die u nu zult moeten maken: ga ik nu al investeren en kijken in hoeverre ik kan overstappen naar IPv6 of doe ik dat later. Het zal sterk van deze keuze afhangen wat uw verdere traject zal inhouden.

Ga ik nu al overstappen naar IPv6 of doe ik dat later?

Wat u echter te allen tijde zult moeten uitvoeren, is een risicoscan op uw huidige infrastructuur waarin u bepaalt wat er al wel en niet IPv6 enabled is, wat het beveiligingsniveau van uw systemen is als deze via IPv6 worden benaderd en wat u dient te doen om de beveiliging van deze systemen terug te krijgen op het door u gewenste niveau.
Dit is natuurlijk niet een eenmalige actie, maar zal moeten worden herhaald bij updates, upgrades en aanschaf van nieuwe hardware en software. Dit zal een integraal onderdeel van uw bedrijfsbeveiligingsstrategie moeten worden zolang u bezig bent of wacht op de transitie naar het IPv6 protocol. Immers, zolang die transitie nog niet is voltooid, zult u beide protocolstacks naast elkaar blijven gebruiken.

Hoe nu verder

De transitie naar IP versie 6 zal niet van de ene op de andere dag voltooid zijn, daarvoor zijn er teveel zaken die wijzigen en moeten worden aangepakt. Gedurende het hele traject blijft het risico dat de dualstack operation van IPv4 en IPv6 met zich meebrengt actief en vereist dit dus een verdeelde en dubbele aandacht op het gebied van infrastructuurbeveiliging.

Kunnen uw klanten u straks nog wel bereiken?

Wat de beste wijze van transitie is, zal sterk afhangen van uw organisatie. Als u veel oude apparatuur in uw infrastructuur heeft die het nieuwe IPv6 protocol niet aankan of over 5 tot 10 jaar toch zal worden vervangen door apparatuur die dat wel zou moeten kunnen (bijvoorbeeld SCADA systemen) dan maakt u waarschijnlijk nu de keuze de transitie voor die apparatuur nog niet te maken.

Daarnaast speelt mee in hoeverre straks het internet zelf, en uw service provider in het bijzonder, klaar zijn voor de toekomst.
En kunnen uw klanten u straks nog wel bereiken als u de switch wel maakt als een van de early adopters? Ook hierin zullen belangrijke keuzes moeten worden gemaakt en zal een dualstack oplossing in eerste instantie de enige mogelijkheid zijn.
Een aantal andere vragen die u zich zeker moet stellen zijn:

- hoe ga ik om met IPv6 only apparatuur in een IPv4 netwerk segment en vice versa
- wat doe ik met IPv6 verkeer van buiten mijn organisatie op mijn interne IPv4 intranet en vice versa
- hoe regel ik het huidige niveau van beveiliging in IPv6, zodat dit gelijk komt te staan of beter is dan mijn huidige IPv4 beveiliging?
- welke type van adressering ga ik gebruiken, en waarom en waar?
- welke apparatuur gebruikt welke klassen van adressering? (let op: meervoud)

In het algemeen kan worden gesteld dat IP versie 6 niet alleen als protocol een transitie heeft doorgemaakt, maar dat uw netwerk en uw beveiliging diezelfde transitie zullen moeten voltooien. Uw beheerders zullen niet meer hun systemen kunnen benaderen op basis van het IP adres dat ze altijd konden onthouden. Beveiliging en correcte adres resolving via DNS worden nog belangrijker en ongewenste gasten op uw netwerk, die hun "eigen" IP adres kunnen "kiezen", zullen nog lastiger op te sporen zijn.
En dan heb ik het nog maar even niet over alle mogelijke aanvalspaden en privacy issues die gerelateerd zijn aan deze nieuwe en toch oude technologische vooruitgang.
Kortom, werk genoeg. De vraag is namelijk niet of maar wanneer deze transitie zal worden ingezet, we kunnen niet anders en staan met de rug tegen de grenzen van het Internet gedrukt. ●

INTERVIEW MET KALLE PALOMÄKI

Kalle Palomäki, de CEO van RM5, een voor het grootste deel van onze lezersgroep onbekende, leverancier van een softwareproduct voor identiteitenbeheer en access control. RM5 is een Fins bedrijf dat op dit moment probeert om buiten Scandinavië voet aan de grond te krijgen. Opmerkingen of vragen naar aanleiding van dit interview kunnen worden gestuurd naar André Koot, info@i3advies.nl.

Kalle Palomäki was onlangs in Nederland en we kregen uitgebreid de kans om hem te spreken over het bedrijf RM5, de visie en het product.

'Vertel, wie is je vader, wie is je moeder?' Nee, dat is niet de beste vraag om aan iemand die Tante Es niet kent te stellen, maar we komen wel in de buurt. Kalle is afkomstig uit Tampere in Finland en heeft daar zijn Msc in techniek gehaald. Daarna haalde hij z'n MBA aan de universiteit in Helsinki. Die combinatie leverde hem, na een eerdere baan, de functie van CEO bij RM5 op. RM5 was op zoek naar een Marketing en Sales persoon met technische achtergrond, dat lijkt wel geslaagd.

Kalle is sinds anderhalf jaar de CEO van het bedrijf dat rond 2005 is ontstaan. Het bedrijf is een afsplitsing van de ontwikkeltak van het Finse consultancybedrijf Panorama.
RM5 staat voor het 5e generatie Representation Management systeem. Waarom 5? Kalle heeft niet echt een idee, waarschijnlijk bekt het gewoon lekker. Over Representation Management komen we nog uitgebreid te spreken.

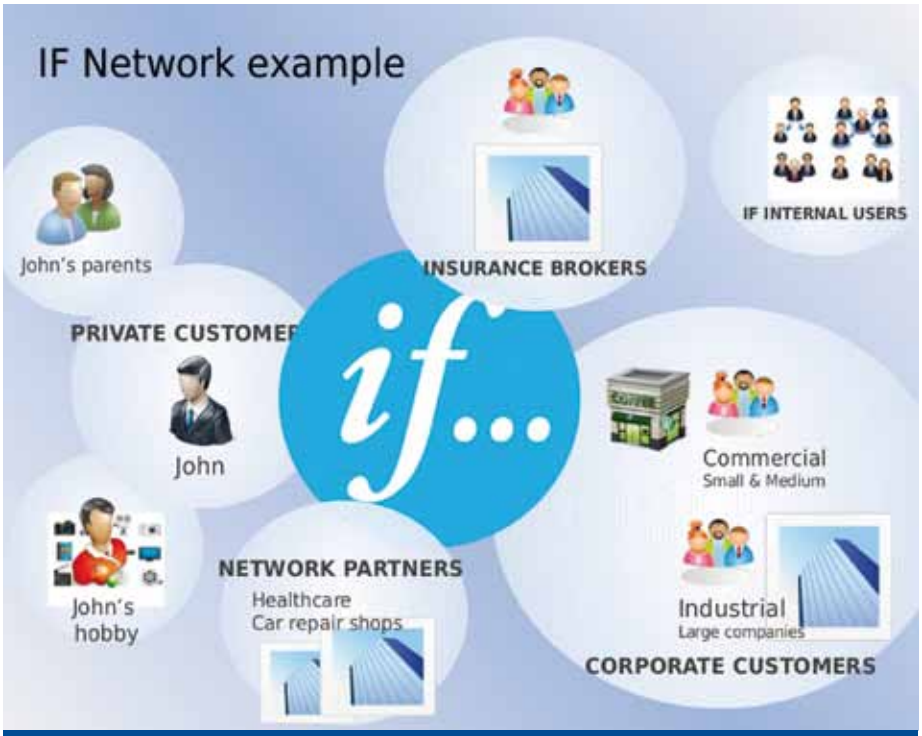
Waarom probeert RM5 via Nederland de grens over te gaan?
Kalle noemt een aantal overwegingen om het hier te proberen. 'Simple logic' volgens hem:
Kalle kende Aexus, de Nederlandse agent, al vanuit een vorige betrekking, en dat helpt. Daarnaast zijn er enkele problemen om andere landen te betreden: Duitsland vereist feitelijk het oprichten van een vestiging of een alliantie met een Duits bedrijf, Frankrijk is redelijk chauvinistisch, waardoor een buitenlands bedrijf weinig kansen krijgt en in Engeland geldt een heftige concurrentiestrijd met de grote vendors. Nederland is van oudsher een land van ondernemers en heeft een open cultuur. Dat we onze talen spreken helpt mee.

RM5 is als een product ontstaan uit een ontwikkeling bij de Finse spoorwegen (VR). Consultancybedrijf Panorama werd in 2003 gevraagd om het probleem van e-business identiteiten op te lossen. Met name het beheren van externe identiteiten, zoals agenten van reisbureaus en verladers, moesten via het portaal transacties verrichten, maar VR wilde dat niet zelf doen. Uit een marktonderzoek bleek dat de beschikbare standaardoplossingen prima in staat zijn intern identiteitenbeheer te realiseren, maar dat er voor het beheer van externe identiteiten niet een standaardoplossing is. Maatwerk was dus de oplossing. Panorama heeft de oplossing ontwikkeld, maar vastgesteld dat de eisen van VR niet uniek zijn. De software is als een standaardoplossing ontwikkeld en uitgerold. Na VR werden ook andere Scandinavische klanten voorzien van de software.
Om een vendor lock-in te voorkomen (het verplicht afnemen van de consultancydiensten bij Panorama als een bedrijf alleen RM5 wilde hebben) werd het product en de ontwikkeling afgesplitst van Panorama. Hierdoor konden ook andere systeemintegrators en consultancypartijen het product aanbieden. Inmiddels zijn er verschillende implementatiepartners in Scandinavië en nu ook in Nederland.

> Voor het beheer van externe identiteiten bestaan geen standaardoplossingen

Waarin verschilt RM5 van de concurrentie?
RM5 is niet een IAM suite zoals andere systemen. De kracht van RM5 ligt vooral in het concept van Representation Management. RepMgt is te beschouwen als een vorm van Volmachtenbeheer. Binnen RM5 heet het principe wel Power of Attorney. Het principe werd uitgedacht om het autoriseren van derden mogelijk te maken.

De crux is dat ieder individu die binnen RM5 wordt beheerd, zelf autorisaties



If Case Presentation

kan krijgen op alle andere beheerde objecten in RM5, dat kunnen ook autorisaties in volmacht zijn. Een volmacht, dus een door een eigenaar van een object toegekende autorisatie, kan ook worden overgedragen naar een andere identiteit. Dit lijkt een nogal filosofische beschouwing, misschien kan een voorbeeld van RM5 zelf het duidelijk maken:

Een verzekeringsmaatschappij heeft grote zakelijke klanten. Elke zakelijke klant bestaat zelf weer uit meerdere min of meer autonome onderdelen.

In deze afbeelding staat John als tussenpersoon van de Finse 'if' verzekeringsmaatschappij die voor alle partijen geautoriseerd kan worden. Hij kan zowel als tussenpersoon worden geautoriseerd voor zijn eigen klanten, als ook als vertegenwoordiger van zijn ouders of als administrateur voor zijn voetbalclub die rechtstreeks bij 'if' zijn verzekerd. En natuurlijk als privé persoon die zelf een verzekering bij 'if' heeft afgesloten.

Voor de klant als geheel is één tussenpersoon, die niet bij de verzekeringsmaatschappij of bij de klant werkzaam is, verantwoordelijk. Die tussenpersoon kan voor de klant bij de verzekeringsmaatschappij transacties uitvoeren. Ook kan de tussenpersoon voor een autonoom onderdeel iemand anders mandateren om transacties voor dat onderdeel uit te voeren. Dus feitelijk is er, naast de organisatorische structuur, ook een autorisatie hiërarchie. Als een onderdeel van de klant wordt verkocht, dan kan de autorisatie voor dat onderdeel aan iemand anders worden toegekend.
Maar het concept is nog verder uitgebreid. De betreffende medewerker die voor het onderdeel verantwoordelijk is, kan ook voor anderen optreden. Hij zou bijvoorbeeld ook de verzekerings-administratie ten behoeve van partner en kinderen, maar ook voor weer andere organisaties kunnen uitvoeren, alles binnen de services waarvan de betreffende subjecten gebruikmaken van de diensten van de verzekeringsmaatschappij. De verschillende autorisaties zijn echter ook weer te specificeren in deel-autorisaties of te verplaatsen naar anderen.

> E-services are nowhere from where they will be

Dit wijkt in aanzienlijke mate af van de meeste IAM suites, al zien we in de markt ook daar vernieuwing. Traditioneel richten IAM suites zich op het beheer van identiteiten en autorisaties voor interne, eigen, medewerkers en interne systemen. Met de toename van portaalsystemen zien we echter ook een toename van het beheer van externe identiteiten die gebruik maken van portaalfuncties. En daar waar portaalfuncties rechtstreeks aansluiten op back-office systemen of externe clouddiensten, fungeren de IAM systemen, die identiteiten en autorisaties voor portaalfuncties verstrekken, daarmee net als traditionele IAM suites. Het portaal wordt het enige systeem waar externe gebruikers toegang toe hebben. Maar de complicatie ontstaat wel dat er gebruikersbeheer op het portaal moet plaatsvinden en dat er een koppeling van interne en externe gebruikers ontwikkeld moet worden, met ook weer een gedifferentieerd autorisatiemodel.

RM5 is echter gebouwd vanuit de optiek van het tot interne systemen toegang bieden voor niet beheerde gebruikers. En dat maakt de oplossing wel erg boeiend. Met name organisaties die externe gebruikers toegang willen verlenen aan klanten en volmachten, kunnen baat hebben bij de structuur die RM5 biedt.

Volgens Kalle onderscheidt RM5 zich met name hierin, dat RM5 'scales from the big thing to internal' en dat daarmee cloud models beter ondersteund worden: 'e-services are nowhere from where they will be'.

Hoe groot is RM5 op dit moment?
RM5 is feitelijk alleen een ontwikkel-club. Er zijn 8 medewerkers en het hele bedrijf is zelfstandig. Het bedrijf wordt binnen Nederland vertegenwoordigd door Aexus en Everett fungeert als implementatiepartner. ●

FILE-COLLABORATION OP DE ZAAK

Cyril Vonken, CTO en mede-eigenaar van Tasman Solutions BV. Tasman Solutions, dochteronderneming van mITE, is specialist op het gebied van zakelijke mobiele apps. Zij biedt implementatie, advies en consultancy voor mobiele (maatwerk)oplossingen voor o.a. iPad, iPhone, Android en Windows Phone. Cyril is bereikbaar via cvonken@tasmansolutions.nl of kijk op tasmansolutions.nl.

Hedendaags wordt er door de medewerkers steeds meer verwacht van de ICT-afdeling. Dit geldt ook voor de gebruikers van mobiele toestellen. Er moet e-mail gelezen kunnen worden op het toestel, applicaties benaderd worden die ook op de normale computer benaderd kunnen worden, men moet toegang hebben tot de documenten en tenslotte wil men de vrijheid hebben om het toestel ook te kunnen gebruiken voor privé zaken zoals Facebook, Twitter en eigen foto's. Dat stelt veel eisen aan een toestel welke ook zakelijke data bevat.

Hiermee introduceert zich een potentieel groot gevaar: er is in eerste instantie weinig tot geen grip op de privé applicaties en -data of het gebruik ervan en dus óók niet op de zakelijke content op datzelfde toestel. Gevoelige bedrijfsdocumenten kunnen binnen een paar seconden openlijk gedeeld zijn met de gehele wereld, zonder dat de gebruiker hier bewust voor heeft gekozen.
Om dit te voorkomen zijn er verschillende vormen van bescherming, waar hieronder dieper op wordt ingegaan.

Mobile Device Management
Voor het beheren en beveiligen van mobiele toestellen is er door verschillende toeleveranciers Mobile Device Management (MDM) software ontwikkeld. MDM kan gezien worden als een platform dat het mogelijk maakt om inzicht te krijgen in welke toestellen toegang krijgen tot zakelijke gegevens. Daarnaast is het een platform dat ervoor zorgt dat er voor de (zakelijke)toestellen een bepaald beveiligingsbeleid wordt afgedwongen. Een functionaliteit binnen MDM die nu sterk in opkomst is, is het delen van zakelijke bestanden die gelezen of bewerkt kunnen worden op het mobiele toestel. Wanneer er toegang gegeven wordt tot file-shares of Sharepoint omgevingen, moet er gewaarborgd worden dat de documenten goed en veilig worden opgeslagen en dat er geen mogelijkheden aanwezig zijn om deze documenten te verspreiden naar niet toegestane locaties.
Een oplossing is het bieden van een afgeschermd gedeelte op het toestel waar andere software of andere gebruikers niet bij kunnen. Dit gedeelte is versleuteld en beveiligd met een wachtwoord. Het is vervolgens aan de organisatie om een beleid op te stellen waarin is vastgelegd wat de gebruiker met de documenten mag doen en in welke toepassingen deze geopend mogen worden, zonder dat de organisatie hier schade van kan ondervinden. MDM biedt organisaties de mogelijkheid om het beleid dat betrekking heeft op het mobiele werken met bedrijfsdocumenten, vervolgens technisch vorm te geven.

> File collaboration vraagt om goede beveiliging en controle

Volwassen Enterprise oplossingen
Naast de MDM-leveranciers die file-collaboration als module bieden om bijvoorbeeld Sharepoint bestanden veilig te kunnen ontsluiten, zijn er ook een aantal serieuze aanbieders die zich primair focussen op file-collaboration en security en controle hoog in het vaandel hebben staan.
Deze file-collaboration oplossingen kenmerken zich in het kunnen bieden van veel meer mogelijkheden, de totale controle over elke handeling én het daadwerkelijk kunnen delen van informatie met gebruikers die geen gebruik maken van een MDM oplossing.
Zonder te willen degraderen, behoren diensten als Dropbox, Box of Skydrive duidelijk niet tot deze groep, omdat ze bedrijven onvoldoende grip en controle bieden en daarnaast geen mogelijkheid bieden om de dienst on-premise (lokaal) te draaien.
Een aantal van deze native file-collaboration leveranciers die de zwaardere wensen en eisen van Enterprises wél respecteren, zijn Accellion, Egnyte, RES' Hyperdrive en het door Vmware beloofde Octopus. Uiteraard verschillen de nu beschikbare file-collaboration producten qua features. Bij de keuze voor een product dienen onderstaande zaken zeker de revue te passeren:

- Betreft het een cloud-only, on-premise of hybride oplossing?
- Worden de gebruikte mobiele platvormen ondersteund door een native app?
- Zijn bestanden ook offline beschikbaar?
- Integreert de oplossing met bestaande AD's en/of Sharepoint?
- Zijn gebruikers van buiten de

organisatie in het systeem op te nemen?
- Wordt versie-beheer ondersteund?
- Kunnen gebruikers een notificatie ontvangen bij een wijziging of toevoeging?
- Is het mogelijk om een houdbaarheidsdatum of maximaal aantal downloads in te stellen?
- Geschiedt synchronisatie op de achtergrond of betreft dit een handmatige handeling?

Wie, wat en wanneer

Het delen van informatie valt of staat met de mogelijkheid voor gebruikers om eenvoudig de juiste ontvangers te kunnen kiezen. Wie deze juiste ontvangers zijn, kan middels authenticatie en domein-Whitelists domeininstellingen afgedwongen worden. Het registratieproces binnen veel file-collaboration oplossingen werkt op basis van e-mailadres en een verificatiebericht.

De meeste organisaties werken veel met externe partners, die ook inzicht nodig hebben in documenten die enkel voor projectdeelnemers toegankelijk dienen te zijn.

Het uitnodigen van externen gaat op dezelfde wijze, waarna deze gebruikers als iedere andere gebruiker worden gezien, mits de beheerder geen restricties heeft vastgelegd.

Interne en externe gebruikers kunnen dus - afhankelijk van de gekozen file-collaboration oplossing - tot de groep van stakeholders behoren, waarbij externe partners wellicht enkel leesrechten krijgen.

Het is dus van belang dat de gekozen oplossing ook autorisaties op groepsniveau ondersteunt, waarbij er bijvoorbeeld een map met documenten aan deze groep gekoppeld kan worden. Dit maakt toevoegingen, wijzigingen of verwijderingen van documenten direct voor alle groepsleden inzichtelijk. Bij veel file-collaboration oplossingen zien we dat ze de mogelijkheid bieden om gebruik te maken van Active Directory groepen. Dit vergemakkelijkt het toekennen van autorisaties, omdat de Active Directory groepen binnen een organisatie meestal vaak al groepsleden hebben die vergelijkbare autorisaties nodig hebben.

Autorisatiegroepen die aansluiten op AD maken bestandsdeling erg eenvoudig

Wanneer er nieuwe content binnen een groep of folder beschikbaar komt, zijn notificaties een efficiënt middel om een ieder hiervan op de hoogte te stellen. Dit kan voor nieuwe bestanden of voor wijzigingen van bestaande bestanden. Het abonneren hierop kan - afhankelijk van de oplossing - individueel en per map of zelfs bestand.

Controle

Een van de grote verschillen met de Dropbox-achtige oplossingen, is het niveau van controle en grip op het systeem. Zo biedt een beheerscherm, organisaties zelf de mogelijkheid om functionele- en beheersmatige keuzes te maken. Van registratie tot uploads, van foutieve inlogpogingen tot het delen van bestanden en, afhankelijk van de gekozen oplossing, kan alles gelogd worden. Sommige mogelijkheden lijken een hoog Big Brother gehalte te hebben. Maar op het moment dat bedrijfsgevoelige gegevens toch in verkeerde handen vallen, wil je als IT-organisatie op een afgewogen wijze alles hebben gedaan om dit te voorkomen.

Daarbij is het wenselijk dat de beheerder diverse rollen kan definiëren die - desgewenst automatisch - aan gebruikers gekoppeld kunnen worden, waarbij er een onderscheid gemaakt wordt tussen interne- en externe gebruikers of per groep. Denk hierbij aan het geven van lees- of schrijf rechten, het wel of niet mogen aanmaken van gedeelde mappen en/of het kunnen delen van bestanden met externen en het limiteren van het aantal gebruikte MB's of GB's aan schijfruimte.

Informatie heeft een houdbaarheidsdatum; gegevens zijn enkel relevant voor een bepaalde periode en ook hier kan op worden ingesprongen. Zo kan er bij enkele oplossingen per bestand of zelfs per map een verloopdatum worden opgegeven. Na deze datum is de informatie niet meer bereikbaar; veelal wordt deze niet permanent gewist, maar gearchiveerd, maar ook dit is instelbaar afhankelijk van de gekozen oplossing. Een andere vorm van houdbaarheid is het kunnen delen van een bestand via een link, waar een beperking op het aantal 'clicks' kan worden gelegd om wildgroei te voorkomen.

Als informatie verandert, levert dat op bestandsniveau een andere versie op. De volwassen oplossingen bieden de mogelijkheid om vorige versies in stand te houden, met een bepaald maximum hiervan. Per versie kan men dan tevens terugzien wie het bestand bijgewerkt heeft en mogelijk een oude versie weer inzien.

Integratie

Daar waar file-collaboration oplossingen worden ingezet, zijn altijd reeds opslaglocaties aanwezig. Denk hierbij aan netwerk-shares, Sharepoint en FTP. Deze informatie wil men uiteraard niet nogmaals als kopie gaan ontsluiten; het ontsluiten kan hier middels verwijzing gebeuren. Zo kan een gedeelde map gekoppeld worden aan een bestaande netwerk-share of Sharepoint folder. Merk hierbij op dat deze externe bronnen dan niet versleuteld worden.

Een koppeling met een Active Directory is ook een veel geziene integratie; hergebruik van groep-definities is nuttig met betrekking tot herkenning en het hieraan kunnen koppelen van rollen.

Organisaties waar een MDM oplossing operationeel is of wordt overwogen, kunnen nog een stap verder gaan qua beveiliging. Enkele file-collaboration oplossingen werken nauw samen met MDM producten zoals MobileIron, waardoor het mogelijk wordt om een zakelijk-data-wipe af te dwingen zonder het gehele toestel te hoeven wissen.

Vertrouwen

De file-collaboration oplossingen waarover dit document gaat, worden veelal gekozen vanwege de beveiligingsmogelijkheden.

Zo staan veel organisaties niet toe dat bedrijfsgevoelige informatie buiten de deur wordt opgeslagen. Discussies met betrekking tot de Amerikaanse Patriot-act zijn er legio, en niemand kan hier 100% helderheid over geven. Beter safe than sorry, en dus kiezen bedrijven regelmatig eieren voor hun geld door een on-premise/behind the firewall oplossing te implementeren. Maar ook bij een on-premise oplossing doen bedrijven er verstandig aan om goed te controleren of data niet ongeautoriseerd in handen van derden komt. Een product als Egnyte biedt bijvoorbeeld een on-premise oplossing, maar synct altijd via een cloud server op het moment dat je als organisatie met externe partners wilt samenwerken. Egnyte heeft hun Europese cloud server in Amsterdam staan, maar dit vrijwaart men er niet 100% van dat de Patriot act geen invloed heeft. Onbewust vindt de opslag van backups wellicht in de States plaats en wie garandeert dat iedereen zich aan deze wet houdt?

> Voer goede regie op de opslaglocatie van de bedrijfsdata

Verder is het goed om te weten dat vrijwel alle volwassen oplossingen voldoen aan de strengste normen qua fysieke veiligheid. Data-centra dienen te voldoen aan Tier II, SSAE 16 standaarden, waarbij er eisen worden gesteld aan gebruikte hardware en fysieke toegang door beheerders.

Uiteindelijk draait het om vertrouwen. Wie kan er met 100% zekerheid zeggen wat de impact van de Patriot act is of hoe veilig de hosting van de cloud partner is? Informatie is zo veilig als de zwakste schakel. Organisaties die hoge eisen aan vertrouwelijkheid stellen, doen er verstandig aan om de data achter de eigen firewall op te slaan.

Platformen

Hoe documenten worden gebruikt, is sterk afhankelijk van het platform. Werkt men op een desktop, dan verwacht de eindgebruiker dezelfde eenvoud en werking van het bekende Dropbox. Transparante synchronisatie is hier een must, waarbij de bestanden ook offline zijn in te zien.

Bij de meeste file-sharing oplossingen is het gebruikelijk dat er een web interface beschikbaar is, waarbij de gebruiker alle functies tot zijn of haar beschikking heeft via een browser. Zo wordt er voor de beheerder(s) meestal een beheerportal geboden, zodat management hiervan remote kan plaatsvinden.

80% van de gebruikers ziet een smartphone hoofdzakelijk als middel om informatie tot zich te nemen, waarbij ze slechts een fractie van het totale gebodene bekijken. Belangrijk hierbij is dat smartphones niet altijd online zijn (bijvoorbeeld geen dekking of tijdens roaming) en men juist de content wil kunnen inzien als men offline is. Ook hier verschillen de file-sharing oplossingen sterk. Neem nu Dropbox: men kan een 'live' bestandslijst opvragen, maar de daadwerkelijke content staat op de server en hiervoor moet de gebruiker expliciet aangeven dat deze offline beschikbaar moet worden gemaakt, voordat deze zonder dataverbinding beschikbaar blijft.

Kies dus een oplossing die bestanden lokaal kan opslaan/syncen, zodat gebruikers bij offline gebruik niet naast de benodigde informatie grijpen.

Veelal wordt naast een Windows desktopapplicatie ook een Mac variant geboden. Voor de mobiele platforms zijn apps voor iOS en Android een must, maar ook voor Windows Phone/8 en Blackberry worden apps geboden om ook de organisaties met een BYOD beleid te kunnen ondersteunen. Het is in ieder geval belangrijk om bij de keuze van file-collaboration oplossing rekening te houden met de gebruikte platforms.

Document ontsluiting

File-collaboration draait in beginsel om het kunnen inzien van documenten door de gebruiker. Maar vaak zijn de wensen breder en willen gebruikers ook de mogelijkheid om bestanden te wijzigen of er in te kunnen annoteren. Op het moment dat we hiervoor van een traditionele mobiele werkplek gebruik maken, zijn we het gewend dat we bestanden ook als 'gewone' bestanden kunnen openen. Bijvoorbeeld in Word,

Powerpoint of Excel. Wijzigingen synchroniseren we vervolgens met de centrale server. Hier vindt veilige opslag plaats en hebben andere gebruikers weer toegang tot de bijgewerkte versie. Een onbeveiligde laptop zonder wachtwoord zet voor kwaadwillenden echter de deur wagenwijd open.
Alle security en encryptie van de centrale oplossing ten spijt.
Ontsluiting op een mobile-device werkt technisch op een andere manier, aangezien security hier een veel grotere rol speelt. Bestanden worden altijd versleuteld opgeslagen door de file-collaboration app en door diezelfde app weer ontsleuteld als het document ingezien wordt. De app zelf kent meestal de ingebouwde mogelijkheid om bestanden in te zien, zij het dat dit dan vaak beperkt is tot de gebruikelijke Office formaten (doc/xls/ppt/pdf) en afbeeldingen/foto's.
De app biedt bij de meeste leveranciers de mogelijkheid tot het toevoegen van annotaties en het terughalen van vorige versies, indien file-versioning tot de mogelijkheid behoort.
Wil men het bestand inzien of muteren in een andere externe app, dan dient dit bestand overgedragen te worden, waarbij er in de meeste gevallen een onbeveiligde kopie ontstaat of nog erger: binnen 5 seconden wordt het bestand door de app gesynct met een cloud-dienst. Diverse file-collaboration oplossingen kunnen deze 'open in' functie beperken, waarbij men bijvoorbeeld een Whitelist van vertrouwde externe apps kan definiëren.

"Open in" functionaliteit groot gevaar voor vertrouwelijke data

Ook hier geldt, net als op een traditionele laptop, dat indien de beveiliging en risico's niet in acht wordt genomen, de totale oplossing als een kluis is, waarbij de sleutel nog in het slot steekt.
Het is een uitdaging om beveiliging en productiviteit hand in hand te laten gaan.

Conclusie

Organisaties willen uiteraard dat bedrijfsgevoelige gegevens niet in verkeerde handen vallen. Los van concurrentiegevoelige informatie kan een totaal onbelangrijk uitgelekt document via de media veel imagoschade aanrichten.
Het lekken van documenten via mobiele toestellen is nooit voor de volle 100% te voorkomen, maar mocht het toch zover komen, dan dient een IT-afdeling aan te kunnen tonen dat alle middelen binnen de macht gebruikt zijn om dit te voorkomen.
MDM biedt hiervoor een goede basis en in combinatie met de juiste professionele file-sharing producten die nog een stap verder gaan, bieden deze samen uitstekende oplossingen voor zowel de functionele als de beveiligingsbehoeftes - op alle niveaus - van organisaties. ●

Overheid &ict

www.overheid-en-ict.nl

23 t/m 25 april 2013
Jaarbeurs Utrecht

Overheid & ICT is hét platform voor ICT-toepassingen en -diensten voor de overheid

Vraag nu gratis uw toegangsbadge aan via overheid-en-ict.nl

MEDE MOGELIJK GEMAAKT DOOR

ETTU the art of sharing
Decos Information Solutions
BlackBerry

KENNISPARTNER

VNG Vereniging van Nederlandse Gemeenten

BRANCHEORGANISATIES

KING Kwaliteitsinstituut Nederlandse Gemeenten
Logius
GBO provincies
HetWaterschapshuis
GIN

HOOFDMEDIAPARTNERS

BB
Kluwer a Wolters Kluwer business

MEDIAPARTNERS

GIS Magazine
infosecurity.nl Magazine
Cloud Works
ambtenarennieuws
Gemeente.nu

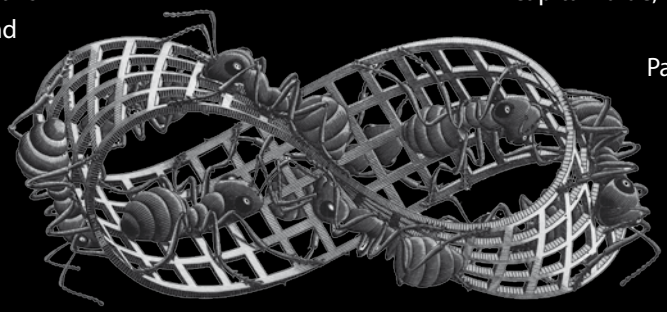
vnu exhibitions europe

COLUMN

ADAPTIVE

Here we take another Business Attribute from the SABSA Business Attributes Taxonomy, looking this time towards the lessons we can learn from the history of the human race. We refer the reader to some research on a number of related topics: see link [1] for an article on Panarchy by Molinari and link [2] on Complex Adaptive Systems (CAS). We shall also engage with some more familiar concepts: evolution, ecosystems, entropy and the second law of thermodynamics.

So how, you asking yourself, are these six concepts inter-related? Our starting point is the Attributer article from IB 2012 Issue 8 on the attribute 'collaborative' – how humans need to find ways to collaborate and exchange value so as to build a society for the benefit of all. To do this they need to work hard. The second law of thermodynamics tells us that the entropy (the level of chaos and disorder) of an isolated system will tend to increase over time. If you've ever kept a garden you will have experienced this in action. You pull the weeds, cut the grass and trim the hedges – a few weeks later it's back to chaos. To build and maintain orderliness you need to input 'work' from outside the system to reduce the entropy and increase the energy of the system.



Now look at the other key concepts. We often mistakenly talk of ecosystems as being in fine balance, as though they will maintain this balance over time. The reality is that whilst in a snapshot moment an ecosystem appears balanced, the balance is continuously changing as time passes. This process is known as evolution. Evolution can be very slow (as in the evolution of new life species), medium pace (as in climate changes) or very quick (as in the evolution of our modern technocratic society and the technologies that drive it). It is with regard to this latter example that we focus our attention in this article. Our human society is a complex ecosystem with many socio-economic and technological characteristics that are in a constant state of change. The rate of change of opportunities and threats becomes ever quicker – so what strategy can we adopt to manage these emerging and evolving risks?

Panarchy is a theory all about the need for government in society and can best be described as 'the rise and fall of empires'. The theory proposes a socio-ecological system lifecycle that follows four phases (also see the model at [3]):

1. An opportunity gives rise to exploitation and the build up of capital value and an increase in the connectedness of the ecosystem.
2. The capital value is conserved and enjoyed as more and more elements become connected.
3. The system degrades (entropy increases) as increased connectedness presents more threats and challenges and it becomes too much work to maintain the socio-economic value. Eventually the value collapses, sometimes catastrophically, sometimes gradually.
4. Usually something new emerges, during a renewal and regeneration phase, moving on to the first phase again, taking advantage of new opportunities to build new capital value, but often with new stakeholders.

Panarchy provides a credible theory for modeling society, but where shall we find the means to apply controls? This is where we might draw on the research done on 'complex adaptive systems'. A CAS is both complex and has the capability to self-adapt to a changing environment. The science of CAS is immature and not widely applied, but with several pundits in the cyber crime world predicting a catastrophic collapse in the current approach to cyber security, maybe we should be paying more attention to how these concepts might be applied in the cyber world. If the 'bad guys' are adapting and evolving more quickly than the 'good guys', then we must explore ways to reverse that tide in the interests of society as whole. Traditional fixed frames of reference such as standard controls libraries are continually degrading in their usefulness. SABSA thinking opens up a completely different approach – one in which risk (both opportunity and threat) is constantly being re-assessed and addressed with innovation. Thus the attribute 'adaptive' may be a critical success factor for the future of business. ●

The Attributer

Links

[1] On the Production of Security, Molinari (1849): http://www.panarchy.org/molinari/security.html

[2] Complex Adaptive System, Wikipedia: http://en.wikipedia.org/wiki/Complex_adaptive_system

[3] Panarchy model: http://www.sustainablescale.org/ConceptualFramework/UnderstandingScale/MeasuringScale/Panarchy.aspx

ACHTER HET NIEUWS

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever, of van PvIB. Vragen en/of opmerkingen kunt u sturen naar ibmagazine@pvib.nl.

"KLOPT HET OF IS HET OPGEKLOPT?"

Op de recente NCSC conferentie werd door William Hagestad II, een oud US militair, een huiveringwekkend verhaal vertelt over de spionage activiteiten van China. William is eigenaar van een bedrijf met de naam "Red Dragon Rising", en als je op zijn LinkedIn profiel kijkt, zie je een indrukwekkende lijst van spreekbeurten over dit onderwerp. Zijn voornaamste (maar ook enige) boodschap: het is niet meer de vraag of je gehackt bent door de Chinezen, het is de vraag wat ze van je weten. Enige tijd later kwam de firma Mandiant met een intelligence rapport over "APT1", een groep hackers die zij, op basis van het door hun aangedragen bewijs, terugvoeren op Unit 61398 van het Chinese volksleger. Grootschalige spionage vanuit China? De Amerikaanse overheid gelooft kennelijk van wel, want de dag na het verschijnen van het Mandiant rapport kwam de Department of Homeland Security met een adviesbulletin voor overheidsinstanties en bedrijfsleven met maatregelen tegen cyberspionage. Inmiddels zijn er ook hier in Nederland in de Tweede Kamer vragen over gesteld. Maar: is dit allemaal wel zo erg als het wordt voorgesteld? Hebben we hier te maken met "China bashing" gestimuleerd/gesubsidieerd door de Amerikaanse overheid? De Chinese regering ontkent uiteraard in alle toonaarden dat ze hier wat mee te maken hebben. Hieronder wat denkbeelden van enkele van onze redactieleden (zoals altijd zijn dit persoonlijke gedachten, en niet noodzakelijkerwijs het standpunt van het bedrijf of organisatie waarvoor zij werkzaam zijn).

André Koot

Heel bijzonder aan dit verhaal is dat het eigenlijk niet is opgeklopt. Ik ben er heilig van overtuigd dat er inderdaad enorm veel gegevens ongewild richting China verdwijnen. Of liever gezegd, ongemerkt gekopieerd worden. Dat is beslist niet opgeklopt. Maar als je dan even door de stapel bewijs bladert, dan zie je eigenlijk ook al even snel dat er eigenlijk niet veel nieuws onder de zon is. De inbraken vinden plaats op dezelfde manier als waarop dat al jaren gebeurt, namelijk via de zwakste schakel, de mens. De mens achter het toetsenbord en de mens die (zonder voldoende kennis en middelen) de techniek beheert. Dus we zien weer phishing en trojans, drive-by attacks, ontbrekende patches en heel veel stilzwijgen. Echt, volgens mij is er niets nieuws, wat niet door traditionele informatiebeveiligingsmaatregelen beperkt zou kunnen worden. Van de enige echte nieuwe dreiging, de embedded backdoors in routers van Huawei en ZTE, hebben we eigenlijk nog niets gevonden. Dat wil natuurlijk niet zeggen dat die er niet ook zijn, maar ja, vindt ze maar.

Maar hoe zou het eigenlijk zijn met de verkeersstromen naar het westen? Embedded backdoors in de Cisco en Juniper doosjes? Hoe zou het zijn met de ingrepen in onze tapstations? Dat zijn vaak zaken waar we met traditionele security al niets meer mee kunnen. Dat zijn overheidszaken die er voor ons eigen bestwil zijn. Toch? Het boeiende aan het verhaal van William Hagestad II is, dat hij aangaf dat in de traditionele Chinese gedachtegang eventuele aanvallen pure verdedigingstechnieken zijn. En dat is dan weer voor het bestwil van de Chinezen zelf. Toch?

Ronald van Erven

Dat er veel informatie gelekt wordt, is bekend. Uiteraard naar China maar ook naar de Verenigde Staten, Engeland, Australia, New Zeeland en Canada. Dit alles onder de titel Echelon.

In deze tijd waren er ook Arabische klanten die telefooncentrales wilden hebben met de garantie dat er geen Israëlische Chipset werd gebruikt. Maar het is nog eenvoudiger tegenwoordig. Je geeft iets gratis weg, als een app, in ruil voor informatie. En vervolgens pas je continu de algemene voorwaarden aan, zodat jij als leverancier alles met de informatie mag doen. Zo past Apple regelmatig de gebruikersvoorwaarden aan omdat ze een zg "embedded service entrance" op hun apparatuur hebben. Alles staat en valt bij het alertheidsniveau (bewustzijnsniveau) van de gebruikers. En of deze informatie nu naar het Oosten, het Westen of Brussel gaat, (persoons)informatie is het nieuwe goud.

Maarten Hartsuijker

Als ik alle berichtgeving over malware, botnets, cyberlegers, bundestrojaners en hackende overheden lees, bekruipt mij het gevoel dat het hier al lang niet meer om "wie hackt wie" gaat. Iedereen hackt blijkbaar iedereen! Er is alleen sprake van veel verschillende motieven.

De stelling zal dus ongetwijfeld kloppen. De Chinezen zijn een wereldmacht en het is dus niet vreemd dat ze zich op dit toneel begeven. Maar bij dit soort berichtgeving moet je je naar mijn mening ook altijd afvragen wie er baat bij heeft om dit nieuws te brengen.

Als het nieuws als terechtwijzing moet dienen, dan heeft het naar mijn gevoel een hoog "pot <-> ketel" gehalte. Maar vanuit een awareness perspectief kan ik de berichtgeving persoonlijk wel waarderen. Veel bedrijven zijn geneigd om pas naar informatiebeveiliging om te kijken op het moment dat er incidenten optreden. Denk aan een datalek, vertragingen in het netwerk of instabiliteit van een besmet systeem. Diefstal van gegevens is over het

Mandiant Report

algemeen erg onzichtbaar. Dat merk je pas op het moment dat je concurrent eerder met een productinnovatie op de markt komt dan jij. Of op het moment dat jouw anonieme bron achter een primeur toch ineens niet zo anoniem meer blijkt te zijn. En in die gevallen is de relatie met een computerinbraak lang niet altijd vanzelfsprekend.

Zo bezien kan het wat mij betreft helemaal niet zoveel kwaad om dit soort berichtgeving ook in de algemene media af en toe langs te zien komen. Het herinnert ons eraan dat we ook op dit vlak onze bedrijfsrisico's goed moeten beoordelen.

Lex Borger

Het rapport van Mandiant bevat veel informatie wat op het eerste gezicht wijst op de belangrijkste conclusie van het document: APT1 is Unit 61398, een level 4 afdeling van de Communistische partij in China.

Ik heb in het verleden rapporten gelezen over een sectie op buitenaardse wezens in Area 51, de moord op Kennedy door anderen, de maanlanding die in een studio opgenomen is en de aanval op de Twin Towers die niet door Al Quaeda uitgevoerd zou zijn. Ik geloof niet in deze "conspiracy theories", maar het laat wel zien hoeveel moeite gestoken kan worden in het schetsen van een alternatieve realiteit, met bewijs. En deze theorieën hebben één ding gemeen: ze stellen dat de Amerikaanse overheid geheime en soms onwettige activiteiten uitvoert die hun burgers afleiden en een ander beeld van de werkelijkheid geven.

En juist dat laatste gegeven maakt dat ik toch nog het bewijs uit het Mandiant Intelligence Center Report kritisch tegen het licht wil houden. Staat hier een alternatieve realiteit beschreven? Wie heeft belang bij dit alternatief? Het rapport kreeg gelijk een officiële reactie van de Amerikaanse overheid. Bedenk dat zij middels de NSA/CIA/FBI deze informatie ook allang hebben. Voor Israël of Rusland zou het best goed uitkomen als China stevig in het verdachtenbankje blijft zitten.

Twee vragen:
Zijn deze Chinezen zo naïef en arrogant geworden dat ze gewoon slordig zijn geweest en zich niet goed genoeg verborgen hebben in cyberspace?
En als we collectief met dit soort bewijs geloven dat de Chinese overheid de westerse wereld hackt, waarom geloven zoveel mensen niet dat er een ongekende klimaatverandering aan de gang is en de mensheid daarvoor verantwoordelijk is? Dat laatste is buiten de scope van deze discussie, dus zal ik het hier maar bij laten. ●

Links

https://www.ncsc.nl/conference/conference-2013/speakers/william-hagestad-ii.html

http://intelreport.mandiant.com/

https://www.security.nl/artikel/45307/1/VS_verspreidt_actieplan_tegen_cyberspionage.html

https://www.security.nl/artikel/45326/1/Kamervragen_over_Chinese_hackers_in_Nederland.html

COLOFON

Informatiebeveiliging is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

Redactie
Lex Borger (hoofdredacteur, werkzaam bij Ideas to Interconnect), e-mail: hr@pvib.nl
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Redactieraad
Tom Bakker (Allianz)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Maarten Hartsuijker (ANWB)
Aart Jochem (NCSC)
André Koot (i3advies)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl;
of neem contact op met MOS (Motivation Office Support)
T (033) 247 34 00
ibmagazine@pvib.nl

Vormgeving en druk
VdR druk & print, Nijkerk
www.vdr.nl

Uitgever
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
E-mail: secretariaat@pvib.nl
Website: www.pvib.nl

Abonnementen 2013
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

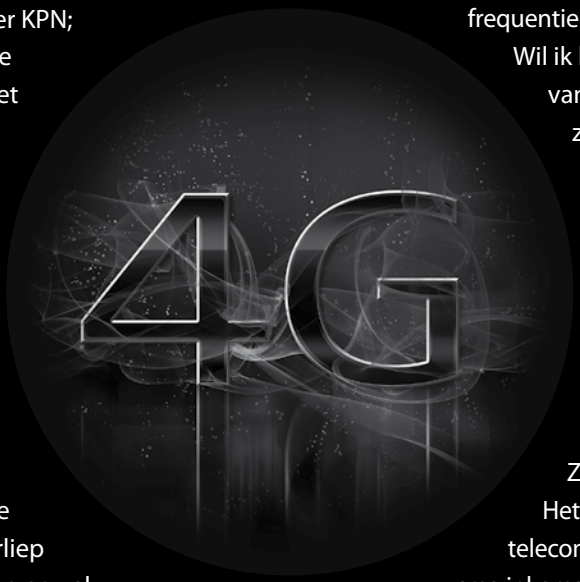
PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

COLUMN

WIE DOET ER MEE MET 4G?

In maart mocht ik weer eens genieten van een korte, maar geweldige vakantie en nu zit ik weer achter mijn bureau met de melding dat ik mijn column moet inleveren. Peinzend over het onderwerp dwalen mijn gedachten weer af naar de periode hiervoor, maar ook naar een bericht dat ik kortgeleden las over KPN; deze club wil 4 miljard ophalen om de liquiditeit wat op te krikken. Onder het bericht werd aangegeven dat KPN in de veiling voor het supersnelle 4G netwerk 1,3 miljard euro heeft betaald. 1,3 miljard euro om het te mogen gebruiken, dus exclusief alle kosten die KPN moet maken om 4G bereikbaar te maken voor hun klanten.



Terug naar mijn vakantie.
Mijn vakanties waren in vroegere jaren heel anders als nu, met name de communicatie naar het thuisfront verliep op een hele andere wijze. GSM's waren er wel, maar het bellen met Nederland was in het buitenland een kostbare zaak en ook het sms-verkeer was extreem duur. Dus sloot je vaak aan in de rij voor de telefooncel om het thuisfront wederom gerust te stellen. Voor de jongeren onder ons, een telefooncel is een (veelal glazen) hokje met een vaste telefoon erin. Die tijden zijn voorbij, de telefooncel is verdwenen, mede omdat de Europese Unie strakke eisen is gaan opleggen om de prijzen van de telefoonproviders een beetje in te dammen. Dat is gelukt, maar er zijn ook andere ontwikkelingen.
Wifi heeft een grote opkomst gemaakt, een camping of hotel zonder Wifi is op dit moment niet denkbaar en die tendens zal doorzetten. Café's, eettenten en andere openbare gelegenheden bieden gratis Wifi en over een jaar of vijf zal Wifi overal te vinden zijn. Ziggo en ook KPN doen inmiddels proeven om Wifi breder beschikbaar te krijgen. Het voordeel van Wifi is natuurlijk de grotere bandbreedte. Daardoor doen zich dan andere mogelijkheden voor zoals Skype, Facetime, VOIP en andere communicatiekanalen. Geweldig, helemaal gratis communiceren met het thuisfront. Nog mooier is de enorme groei van smartphones, waardoor meer dan 60% van de Nederlandse bevolking gebruik kan maken van gratis berichtendiensten als WhatsApp en social media. Ik heb tijdens mijn laatste vakantie dan ook geen enkel telefoontje gepleegd en mijn thuisfront was toch altijd geïnformeerd waar we zaten, wat het weer was en dat werd nog eens opgeleukt met mooie foto's die ter plaatse waren genomen. Omdat ik een fervent smartphone gebruiker ben, had ik bij mijn telefoonprovider voor slechts 15 euro een week lang 3G in het buitenland met een onbeperkte download. Helemaal geweldig, ik hoefde niet eens meer het terras op om te communiceren met het thuisfront, wat overigens geen effect had op de frequentie van terrasbezoek.
Wil ik later dit jaar gebruik gaan maken van 4G? Nee, eigenlijk niet, waarom zou ik dat willen als ik (bijna) overal Wifi beschikbaar heb? Moeten de telefoonproviders dan gaan investeren in 4G? Ze willen dat misschien niet, maar de concurrenten doen het wel en er zijn altijd mensen die overal razendsnel internet ter beschikking willen hebben. Ze kunnen dus niet achterblijven.
Het hele verdienmodel van de telecomproviders is onderuit gegaan, geen sms-inkomsten meer, veel minder belinkomsten en prijzen die voortdurend onder druk staan. Waar moeten ze dan hun inkomsten vandaan halen? Ik zal u naar beste weten mijn antwoord geven: ik weet het werkelijk niet meer. Vaste telefonie is bijna allemaal vervangen door VOIP, ADSL, kabel en liggen in bijna ieder huis, waardoor ook de telefoontikken niet echt meer iets toevoegen. Het kopernetwerk van KPN leek een aantal jaren geleden de goudschat, maar helaas voor KPN is die schat ook bijna leeg gehaald.
Het is een wonderlijke wereld waarvan wij vroeger dachten gebonden te zijn aan telefoonproviders die zuigend onze portemonnee leegtrokken, terwijl de situatie vandaag de dag helemaal gewijzigd is. Er wordt geworsteld om de laatste klanten over te halen naar hen te komen. Een (bijna) gratis telefoon als beloning en ze hebben weer 2 jaar lang een klant. Gaan de telefoonproviders dan failliet? Nee hoor, ze zullen wel iets bedenken om het hoofd boven water te houden en de aandeelhouders gelukkig te houden. Paar duizend man de organisatie uitwerken, nog meer beknibbelen op de continuïteit en veiligheid, en ze houden het nog heel lang vol. Ik ben net op vakantie geweest en toch stromen al weer de meest negatieve woorden uit mijn toetsenbord. Ik geef toe dat ik wel eens met een heel sombere blik de wereld in tuur, maar uiteindelijk wordt hier niemand beter van. Als individu kunnen wij de huidige tendensen niet keren, we zien ze en hebben er zo onze gedachten bij. ●

Berry

Data Leakage

Bring Your Own Device

Security As A Service

Compliance & Auditing

SECURITY

geen keuze, maar noodzaak!

De toepassingsmogelijkheden van Bring Your Own Device, Security As A Service, Data Leakage en Compliance & Auditing ontwikkelen zich in hoog tempo. Daarmee nemen ook bedreigingen toe in de vorm van Cybercrime, Hacking en Identiteitsfraude. Ook worden deze bedreigingen steeds geavanceerder. Adequate beveiliging van werkomgevingen, data en identiteitsgevens zijn inmiddels geen keuze, maar noodzaak geworden. Security vereist nu ervaren, betrouwbare en loyale partners. CRYPSYS is toonaangevend op het gebied van security analyse, advies en installatie bij overheden, semi-overheden, gemeenten, grote bedrijven en organisaties.

CRYPSYS
secure computing

CRYPSYS Data Security BV Edisonweg 4 4207 HG Gorinchem **tel** +31 (0)183 62 44 44 **fax** +31 (0)183 62 28 48 **mail** sales@crypsys.nl **web** www.crypsys.nl

CRYPSYS is officieel distributeur van: Sophos. Lumension. Norman. Cryptzone. Cryptshare. Adyton. Tenable. Kanguru