06/2012

INFORMATIE BEVEILIGING

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 6 - 2012

INCIDENT RESPONSE

OH NEE…, EEN ICT-CRISIS!

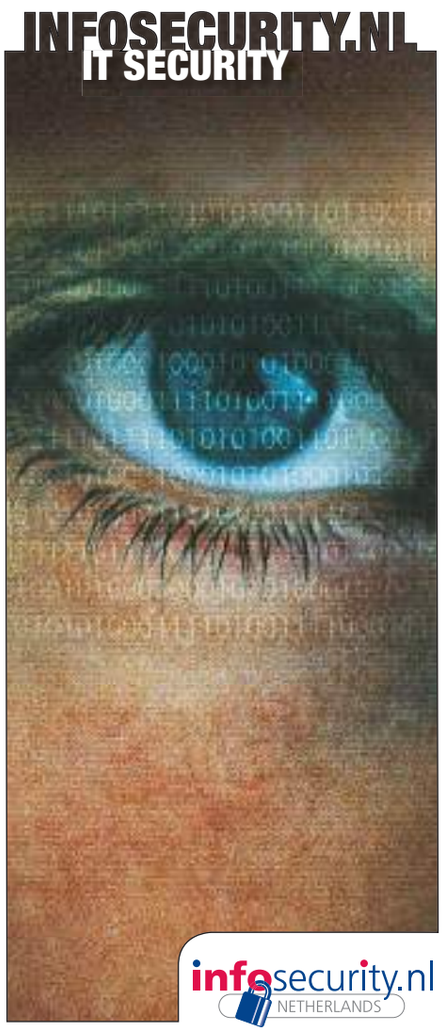
SCHAAP OF HERDER

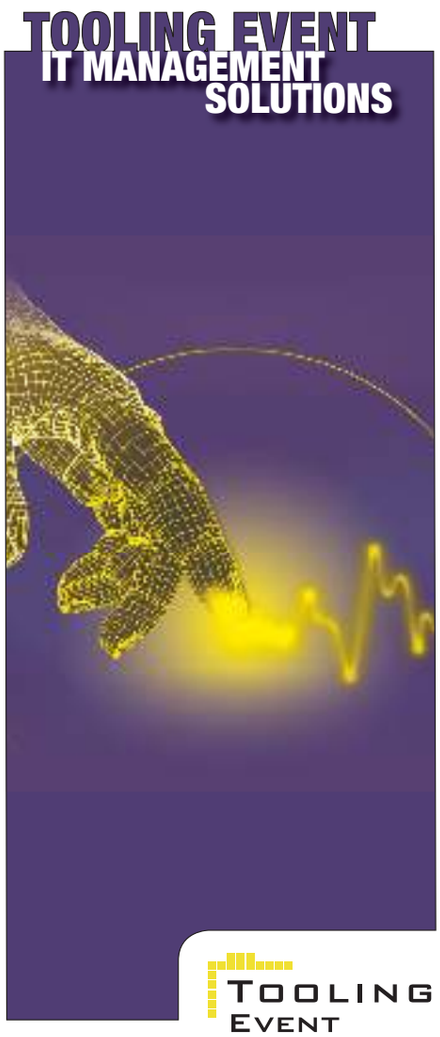
OPEN EINDE

COMMUNICATIE CRUCIAAL TIJDENS CRISIS

31 OKT - 1 NOV 2012 JAARBEURS UTRECHT

VAKBEURZEN, SEMINARS EN ONLINE MATCHMAKING VOOR IT-MANAGERS EN IT-PROFESSIONALS





SCAN OM JE DIRECT AAN TE MELDEN:

REGISTREER NU VOOR GRATIS TOEGANG

TOT ALLE DRIE DE VAKBEURZEN VIA:

WWW.INFOSECURITY.NL | WWW.STORAGE-EXPO.NL | WWW.TOOLINGEVENT.NL

KEYNOTES | SEMINARS | CASE STUDIES | RUIM 150 EXPOSANTEN

Reed Exhibitions

marcit

vnu exhibitions europe

VOORWOORD

In een winkel raakte ik in gesprek met de ondernemer. Hij had het helemaal gehad met de elektronische samenleving. Hij had een virus dat zijn zakelijke computer blokkeerde. Wat hij beschreef was vrij snel te classificeren. Het was ransomware, dus ik gaf het advies om in ieder geval niet te betalen of contact op te nemen. Ik bood aan die avond bij hem langs te komen. Heel snel bleek dat het ging om de trojan.ransom Nederlandse Politie en dat de trojan heel goed is om de gebruikelijke interventies zoals antivirusbewaking en task manager opstarten met ctrl-alt-del effectief afving. Opstarten in veilige modus lukte wel, en dan werkt de computer prima - maar wel traag en met alle beperkingen. Gelukkig, er waren kennelijk geen bestanden verwijderd of verminkt.

Mijn eerste gedachte was dat nu een antivirus scan gedaan kon worden, het probleem wel snel gevonden en opgelost zou zijn. Helaas echter, na twee uur waren alleen 8 tracing cookies gevonden. Ondertussen heb ik ook nog zitten googelen om meer informatie over de trojan te weten te komen. Het is best lastig om het kaf van het koren te scheiden en een diagnose/oplossing te vinden die niet eerst het downloaden van allerlei programmatuur eiste. Verder kwam ik er achter dat er nogal wat varianten van deze trojan zijn en dat ze zich op semi-random plaatsen nestelen op je PC.

Het beste wat ik kon vinden was op een hele lijst registry-keys af te lopen waar de trojan zich zou kunnen verbergen en zoeken naar iets met een onlogische naam. Halverwege had ik beet: een vreemde naam in een vreemde directory. Ik hernoemde het bestand door de extensie ".bad" toe te voegen en startte de PC opnieuw op. Succes! De PC zit niet meer vast in het ransomscherm. Ik verwijder dus het bestand en de registry-key en speur nog even door naar nog andere vreemde bestanden, maar die vind ik niet.

Dan over naar de volgende stap: waarom was een infectie mogelijk? Deze trojan was binnengekomen via een Java vulnerability. "Java houd ik helemaal up-to-date" verzekert de ondernemer mij. En de PC bevat inderdaad de nieuwste versie bij controle. Maar ook nog eens zo'n 20 oude versies, waaronder volledige Java runtimes! Zoveel had ik er nog nooit bij elkaar gezien. Dit vergte behoorlijk wat software de-install acties. Uiteindelijk besluit ik Java helemaal te verwijderen omdat de goede man dit niet nodig heeft.

Adobe Reader en Flash waren redelijk up-to-date, maar Windows Update helemaal niet. Dat laatste verbaasde mij in eerste instantie, juist omdat de PC alleen zakelijk gebruikt werd en geconfigureerd was voor het automatisch ontvangen van updates. Toen ik Windows Update met de hand opstartte kwam meteen een vraag op om een ActiveX control te installeren. Ik gaf daar bijna instinctief een OK op, en de man vroeg waarom ik dat deed. Hij zei dit vaker gezien te hebben en vertrouwde dit niet. Toen begreep ik in een keer waarom de PC zo achter liep op updates. Maar ik kon hem geen voor hem acceptabel antwoord geven waarom dít verzoek tot installatie nu wel OK was en een ander waarschijnlijk malware. Ja, dit komt van Microsoft af, maar dat kunnen ze allemaal zeggen. Ja, het certificaat klopt, maar dat zegt tegenwoordig ook niets meer.

Is het dan waar: Koning Prevention is dood, lang leve Prins Incident Response?

INHOUDSOPGAVE

Foto omslag: CC-By Official U.S. Navy Imagery.

INCIDENT RESPONSE

*Aart Jochem is redacteur van **Informatiebeveiliging** en werkt bij het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie. Het NCSC is naast het expertise-centrum voor cyber security in Nederland ook het incident response team van de Nederlandse overheid. Hij is te bereiken via aart.jochem@ncsc.nl.*

Je ziet ze niet zo veel meer: nieuwe publieke diensten die als gegarandeerd veilig worden aangeprezen. Terwijl veilig is wat we willen als gebruiker. Inmiddels weten dienstaanbieders ook dat een dienst veilig maken en veilig houden geen sinecure is. Daar zijn expertise, planning en een lange adem voor nodig, vaak tegen hogere kosten dan vooraf bedacht. Rekening houden met falende beveiliging is een goede tweede. Vroegtijdige detectie van incidenten en snelle respons kan veel schade beperken. Deze special van Informatiebeveiliging heeft incident response als thema en we zijn blij dat enkele ervaren professionals de pen wilden grijpen en ons meenemen in verschillende aspecten van dit werkveld. De totstandkoming van de special is typisch voor incident response projecten: goed plannen en uitdenken, maar door incidenten komt de uitvoering toch weer op het laatst. Alsof het project zelf een incident is.

Als je een tijdje meeloopt in ons mooie vak, heb je de invoering van vele nieuwe maatregelen meegemaakt. Zoals antivirus, compartimentering van netwerken met firewalls, anti-ddos appliances, IPS, security awareness programma's en als dat niet werkt het blacklisten of juist whitelisten van software en sites. Allemaal hele noodzakelijke maatregelen, die soms gebaseerd zijn op een goede risico analyse en dito security architectuur, maar soms ook op de glimmende folders van de security industrie.

Toch worden we dagelijks geconfronteerd met beveiligingsincidenten en de statistieken laten zien dat het aantal al lang een stijgend verloop kent. Het toont wat mij betreft twee dingen aan. In de eerste plaats is het moeilijk om alle risico's vooraf in te schatten, de maatregelen op een goede manier te implementeren en ook veilig te houden. Maar het laat ook zien dat cyberdreigingen zich snel ontwikkelen. Ook actoren veranderen. Van de onderzoeker die iets wil proberen, via studenten die hunkeren naar aandacht en criminelen die internet op grote schaal gebruiken voor hun praktijken tot overheden die naar digitale wapens grijpen of hackers stimuleren (zie ook ref. [1]).

Cyberdreigingen en actoren veranderen zo snel: preventieve maatregelen moeten worden aangevuld met reactieve

Inmiddels is de term Advanced Persistent Threat (APT) in ons jargon opgenomen (en bekritiseerd). Door de verhalen van grote organisaties als Google, RSA en ook kleinere als DigiNotar weten we dat als een actor genoeg tijd en geld kan investeren, hij altijd wel een manier vindt om binnen te dringen en toegang krijgt tot de kroonjuwelen van de organisatie. De uitspraak van Bruce Schneier over de aanpak van terreur lijkt ook op te gaan voor geavanceerde, gerichte aanvallen op systemen: *"You can't defend. You can't prevent. The only thing you can do is detect and respond."* (ref.[2]). Hoewel preventie noodzakelijk is, ben ik het helemaal met hem eens dat detectie van incidenten en respons vaak onvoldoende aandacht krijgen en dat in organisaties vaak gedacht wordt dat preventieve maatregelen genoeg zijn. Als voorbeeld noem ik hier het vertrouwen op antivirus als

bescherming tegen malware, terwijl al uitgebreid is aangetoond dat het alleen beschermt tegen een deel van de malware (namelijk de bekende malware) en dan alleen nog op de systemen die zijn voorzien van een werkend updatemechanisme.

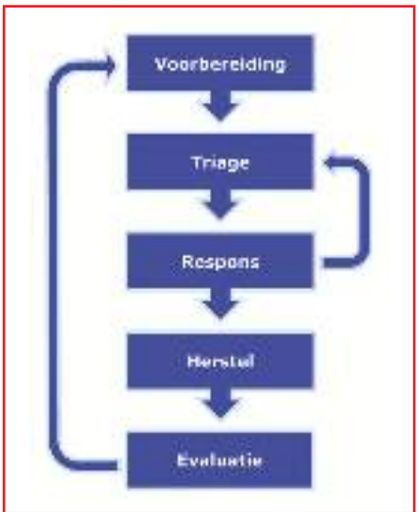
Detectie of monitoring is een boeiend onderwerp, wellicht voor een andere special van *Informatiebeveiliging*. In deze uitgave richten we ons op incident response. En de overtreffende trap crisisbeheersing.

Incident response wordt vaak gedefinieerd als een gestructureerde aanpak van lekken, beveiligingsincidenten of aanvallen, gericht op het beperken van schade en hersteltijd. Het is een reactieve

benadering van informatiebeveiliging, uitgaande van de realiteit dat 100% beveiliging alleen tegen zeer hoge kosten bereikt kan worden.

Incident management is een functie die in de ITIL servicemanagement-aanpak gericht is op het oplossen van alles wat afwijkt van de standaard routines en procedures. Het is een van de processen die een service-management-organisatie op orde moet hebben met plannen en procedures. Incident response in de context van deze uitgave is gericht op het aanpakken van informatiebeveiligingsincidenten, los van de ITMS-aanpak die gekozen wordt. Vaak worden dit soort incidenten opgelost door een gespecialiseerd team en buiten de grenzen van de organisatie of zelfs het land. Maar ook hier valt te plannen en te organiseren.

Veel incident response teams volgen globaal dezelfde aanpak, niet in de minste plaats omdat CERT/CC, de moeder aller incident response teams, al sinds eind jaren tachtig van de vorige eeuw het opzetten van incident response teams in organisaties en landen stimuleert met kennis en ervaring. In Europa speelt ENISA hierin een belangrijke rol. In grote lijnen worden 5 fasen onderkend:



De aanpak van incidenten kent globaal 5 fasen

Voorbereiding

In de voorbereiding worden rollen gedefinieerd en stappenplannen gemaakt voor de aanpak van een incident. Hierbij houdt men rekening met verschillende typen incidenten met een verschillende mate van impact. Vragen die in deze fase worden beantwoord zijn: waar worden incidenten gemeld, hoe wordt de ernst en aanpak bepaald (triage), hoe zijn de verhoudingen tussen incident responder en IT-staf of -business en welke escalatielijn wordt gevolgd? Tegenwoordig moet ook duidelijk zijn welke incidenten gemeld moeten worden bij een toezichthouder en wie dat moet doen.

Ervaren medewerkers verminderen chaos en stress tijdens een incident of crisis

Essentiële onderdelen van de voorbereiding zijn het trainen en oefenen. Als medewerkers de situatie al eens ervaren hebben: het verminderen van chaos en stress tijdens een incident of crisis. Maar ook het opbouwen van relaties die bij een incident nodig zijn, zowel binnen als buiten de organisatie is een belangrijk onderdeel van de voorbereiding. Vaak is het inschakelen van kennis en ervaring uit het netwerk van doorslaggevende betekenis bij het stoppen van een incident.

Vaststellen van een incident en triage

Een incident wordt gedetecteerd, of gemeld van binnen (bijvoorbeeld via de helpdesk) of buiten de organisatie. (Hopelijk via het NCSC, maar houdt er rekening mee dat het ook een journalist kan zijn.) Het eerste dat moet gebeuren is verifiëren of er daadwerkelijk een incident is en of het incident de organisatie of achterban raakt. Daarna moet de ernst en prioriteit bepaald worden. Per organisatie kan dat verschillen. Bij een bedrijf kan dat afhangen van het feit dat klanten betrokken zijn of van het aantal medewerkers dat getroffen is. Bij overheidsorganisaties komen bijvoorbeeld de risico's voor nationale en/of staatsveiligheid, maatschappelijke onrust en volksgezondheid al snel aan bod. Er wordt gekeken of er malware in het spel is, of dat hackers van buitenaf toegang hebben gekregen tot systemen. Direct na de triage zal bepaald moeten worden welk team op een incident gezet wordt en of geëscaleerd moet worden. Tijdens de afhandeling komt deze vraag regelmatig terug. Ook is dit het moment om te bepalen of (of beter wanneer) de communicatieafdeling betrokken moet worden.

Het inschakelen van kennis en ervaring uit het netwerk is vaak van doorslaggevende betekenis bij het stoppen van een incident

Response: afhandelen van het incident

De eerste stap in de afhandeling van een incident is het stoppen van de uitbreiding van de effecten van een incident. De aanpak is afhankelijk van het incident en de situatie. Soms kan het zijn dat publieke communicatie een van de eerste stappen is, met name als vertrouwen in de organisatie in het geding kan komen. Soms worden de eerste stappen zoveel mogelijk in stilte genomen, bijvoorbeeld om een geconstateerd lek te kunnen dichten voordat er massaal misbruik van gemaakt wordt. De aanpak kan per type incident in grote lijnen in procedures beschreven worden, maar het is altijd goed om een ervaren rot in je team te hebben en daar goed naar te luisteren. De tweede stap bij de incidentafhandeling is het verwijderen van de oorzaak van het incident: het opschonen van systemen, het aanbrengen van filters voor netwerkverkeer, het oprollen van een botnet. Soms worden noodverbanden aangebracht om functionaliteit weer terug te geven aan de gebruikers. Deze zullen later worden vervangen door definitieve oplossingen. Het afhandelen van een incident kent ook een einde waarin communicatie wordt afgerond, informatie gearchiveerd, aangifte bij politie wordt gedaan

en bewijsmateriaal overgedragen. Dit is ook het moment voor een hot wash evaluatie.

Herstel

Na de incidentafhandeling volgt het herstel dat vele maanden kan duren. Systeem- en infrastructuurontwikkelaars repareren de gaten in de systemen en implementeren nieuwe maatregelen om herhaling te voorkomen. Vaak is de rol van het incident response team hier afgenomen tot die van adviseur of tester van de oplossing.

Voorbeeld van een incident dat direct zichtbaar is: de defecement van een website

Evaluatie

De lessons learned van de organisatie en het response team zijn erg waardevol. Wat liep goed, wat kan vast beter worden voorbereid voor een volgend incident?

De artikelen in deze uitgave van *Informatiebeveiliging* gaan op enkele van deze aspecten in. Te weinig om de volle omvang van incident response te dekken. De auteurs vallen allemaal in de eerder genoemde categorie 'ervaren rot'. Ook valt er veel te lezen over de aanpak van incident response en het opzetten van een incident response team. Wat vaak ontbreekt in de literatuur zijn de *war stories*, de verhalen. Ik kan van harte aanbevelen om hiervoor naar conferenties te gaan. Je kunt veel leren van de verhalen en tegelijkertijd je netwerk uitbreiden. Altijd handig in tijden van nood.

Referentie

[1] *In het Cyber Security Beeld Nederland wordt een actueel overzicht gegeven van actoren bij cyberdreigingen: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland.html*

[2] *http://www.pcworld.com/article/64824/pc_world_poll_highlights_privacy_concerns.html*

EVEN VOORSTELLEN: NIEUW REDACTIELID BART VAN STAVEREN

Ik ben nieuw voor de redactie, maar niet voor de vereniging. Veel van de leden zullen me kennen als (oud)bestuurslid en trekker van de IBO-bijeenkomsten. Sinds 1 mei ben ik met deeltijdprepensioen bij UWV. Wel ben ik nog adviseur voor CIP, het Centrum voor Informatiebeveiliging en Privacybescherming. CIP is een initiatief van UWV, Belastingdienst, SVB en DUO, maar staat open voor alle organisaties uit de publieke sector. Het adviseurschap geeft me een ideale gelegenheid om actief te blijven in ons vakgebied. De ruimte die ik heb, nu ik geen full time functie meer vervul, wil ik voor een deel gebruiken om PvIB te steunen, onder meer door ons blad op het hoge niveau te houden dat het nu is. Mijn grote interesse ligt de laatste tijd op het terrein van ketens. Nu de informatievoorziening van veel bedrijven en organisaties meer en meer afhankelijk is geworden van collega-organisaties is de informatiebeveiliging van de primaire processen dat ook. Vertrouwen in elkaars informatiebeveiliging is noodzakelijk, maar niet altijd terecht. De incidenten van het afgelopen jaar hebben dat maar al te duidelijk aangetoond. Dit stelt ons als informatiebeveiligers voor een grote uitdaging. Ik nodig met deze introductie dan ook alle lezers uit om wanneer ze ideeën hebben hoe tot veilige informatieketens te komen dit in het blad te publiceren. Als redacteur wil ik ze hierbij graag helpen.
Mijn achtergrond ligt in de IT-Auditwereld, waar ik bij onze zustervereniging Norea nog altijd lid ben van de Vaktechnische Commissie. Vanuit die ervaring is er voor mij een tweede onderwerp dat mijn speciale belangstelling heeft; de verantwoording over de informatiebeveiliging. Speciaal bij uitbesteding heeft dit geleid tot een veelheid van interpretaties van de diverse regelgeving zonder dat de opdrachtgevers nu een goed beeld krijgen van de risico's die ze lopen. Het verminderen van de auditbelasting voor informatiebeveiligers en tegelijk het verstrekken van doeltreffende informatie aan opdrachtgevers, toezichthouders en andere belanghebbenden is een van mijn uitdagingen. Ook op dit onderwerp hoop ik met de lezers van het blad een dialoog te kunnen voeren.

OH NEE…, EEN ICT-CRISIS!

Marijke Stokkel (projectmanager Crisisbeheersing en Oefenen) en Douwe Leguit (afdelingshoofd Ontwikkeling en Programma's), beide werkzaam bij het Nationaal Cyber Security Centrum. Zij zijn bereikbaar via info@nscs.nl.

Met het Dorifel-virus zijn deze zomer Nederlandse gemeenten, overheden, instellingen, bedrijven en particulieren mogelijk gegevens kwijtgeraakt of zijn getroffen in hun bedrijfsvoering. Door de inbraak bij certificaatautoriteit Diginotar in de nazomer van 2011 stond de veiligheid van communicatie met overheidsdiensten tijdelijk onder druk. In februari dit jaar bleek een aantal Nederlandse sluizen en rioleringspompen onvoldoende beveiligd en daardoor kwetsbaar voor cyberaanvallen.

Mede door bovenstaande voorbeelden is de laatste jaren binnen de politiek, bij de (nationale) overheid en in het bedrijfsleven in toenemende mate het besef doorgedrongen dat we als samenleving steeds afhankelijker zijn van ICT. Een aanval op of verstoring van de ICT in onze vitale infrastructuren kan potentieel grootschalige en ontwrichtende gevolgen hebben. ICT-crises zijn op een aantal punten anders dan 'klassieke' crises die we kennen zoals brand en vliegtuigongelukken. Dit artikel gaat hierop in, alsook op de wijze waarop ICT-crises aangepakt kunnen worden en hoe dit nu al in de praktijk gebeurt; binnen de Nederlandse overheid in het algemeen en door het Nationaal Cyber Security Centrum (NCSC) in het bijzonder.

Wat is een ICT-crisis?

Er is sprake van een ICT-crisis wanneer:

- één of meer vitale belangen in het geding zijn en er sprake is van (potentiële) maatschappelijke ontwrichting. Vitale belangen betreffen de territoriale, economische, ecologische en fysieke veiligheid en de sociale en politieke stabiliteit (1) van Nederland.
- de reguliere structuren niet toereikend zijn. Met 'reguliere structuren' worden de reguliere overlegstructuren en hiërarchische lijnen van de nationale overheid bedoeld. Als de situatie zeer ernstig is of als meerdere sectoren geraakt worden, voldoen deze niet meer. Er is gecoördineerd optreden van de rijksoverheid nodig om de dreiging weg te nemen en het effect te beperken: de nationale crisisbesluitvormingsstructuur treedt in werking. Deze bevat een aantal overlegorganen die, afhankelijk van de ernst van de situatie, geactiveerd worden: één voor ambtenaren (adviesteam), één voor hoge ambtenaren (Interdepartementale Commissie Crisisbeheersing -ICCB) en één voor ministers (Ministeriële Commissie Crisisbeheersing -MCCB).
- de bron en/of effect liggen in het ICT-domein. Het kan gaan om netwerken en digitale apparaten die verbonden zijn aan het internet, maar ook die daar los van staan, zoals usb-sticks en meet- en regelsystemen voor de aansturing van industriële processen (zoals ICS en SCADA).

> ICT-crises zijn anders dan 'klassieke' crises

Volgens deze definitie heeft zich voor de Nederlandse overheid vooralsnog één ICT-crisis voorgedaan: de hack bij certificaatautoriteit DigiNotar in het najaar van 2011. In deze situatie is daadwerkelijk de crisisbesluitvormingsstructuur van de Rijksoverheid in werking getreden. Zowel het adviesteam als ICCB en MCCB kwamen bijeen om de situatie te bespreken en maatregelen te treffen. Hierbij werd overleg gevoerd met specialisten, onderzoekspartijen en andere belanghebbenden, zoals KPN, Fox IT, Microsoft, KLPD en OM. Het toenmalige GOVCERT.NL speelde een belangrijke rol in het adviseren van deze overlegorganen, de operationele coördinatie en respons.

Andere incidenten, zoals Dorifel en de KPN inbraak in januari 2012, kunnen gezien worden als grootschalige ICT incidenten, niet als daadwerkelijke crises op basis van de hierboven gehanteerde definitie. Bij grotere incidenten heeft het NCSC de operationele coördinatie en houdt het voortdurend in de gaten of de nationale veiligheid niet in gevaar komt. Een crisis begint vaak als een incident.

Wat is er nodig om een ICT-crisis te lijf te gaan?

De afgelopen jaren heeft het NCSC (en haar voorloper GOVCERT.NL) een (coordinerende) rol gespeeld bij DigiNotar en grootschalige ICT-incidenten, alsme-

de bij diverse grootschalige nationale en internationale oefeningen waarbij ICT-crises werden nagebootst (zoals Cyber Storm III (VS-IWWN) en Cyber Europe (EU) in 2010 en Cyber Coalition II (NATO) in 2011). Uit de evaluatie van deze incidenten en oefeningen blijkt een aantal ingrediënten essentieel om ICT-crises effectief aan te pakken.

Investeren in samenwerkingsverbanden

Het lijkt wellicht een dooddoener, maar het wordt telkens weer bevestigd in evaluaties: sterke samenwerkingsverbanden zowel publiek-publiek, publiek-privaat, als ook nationaal-internationaal zijn van cruciaal belang bij de aanpak van ICT incidenten en –crises. Dit heeft een aantal redenen, gerelateerd aan het specifieke karakter van de ICT component.

- *Verantwoordelijkheid ligt niet bij één partij.*
  Eerdere onderzoeken en incidenten laten zien dat binnen het ICT-domein in hoge mate sprake is van intersectorale afhankelijkheden: organisaties binnen en tussen sectoren zijn steeds meer met elkaar verbonden via ICT-ketens en diensten. De telecomsector is bijvoorbeeld afhankelijk van de energiesector en bijna alle vitale sectoren zijn afhankelijk van telecom en internet. Bijvoorbeeld: het uitvallen van de airconditioning kan ervoor zorgen dat de netwerkapparatuur van een telecombedrijf oververhit raakt en niet meer functioneert. Dit gebeurde bij Vodafone in april dit jaar. Het gevolg was dat miljoenen mensen in de Randstad niet meer konden bellen, inclusief velen binnen de overheid. Zo'n incident kan ook gevolgen hebben voor andere sectoren; een eerdere storing bij KPN zorgde voor uitval van tram en metro in de regio Rotterdam, omdat de medewerkers geen portofoon konden gebruiken. Ook was 112 korte tijd onbereikbaar.
  Dit maakt de aanpak van ICT-crises complex; er is geen sprake van eenduidig bevoegd gezag bij één partij of heldere escalatie-structuren, zoals vaak wel bij klassieke crises van toepassing is. Er is geen 'baas van het internet'; een groot deel van de ICT-netwerken en vitale infrastructuren is in handen van de private sector. Een goede en nauwe samenwerking tussen overheid en private sector is essentieel om effectief te kunnen reageren bij crises.

- *ICT-crises zijn niet gebonden aan geografische grenzen.*
  Terwijl klassieke crises vaak lokaal starten (brand, vliegtuigcrash) en in eerste instantie ook lokaal (kunnen) worden aangepakt, ontwikkelt een ICT-incident of -crisis zich snel over geografische grenzen heen of start zelfs meteen internationaal. Dit vraagt om goede internationale contacten. Zoals de hack bij DigiNotar: als dit een klassieke crisis was, zou deze lokaal opgemerkt zijn en in eerste instantie aangepakt door de burgemeester van Beverwijk (vestigingsplaats DigiNotar). Maar zo is het uiteraard niet gegaan. In werkelijkheid kwam de bal kwam aan het rollen doordat GOVCERT.NL werd geïnformeerd door haar Duitse evenknie. De hack werd direct landelijk, en snel daarna internationaal, opgepakt.

> Sterke samenwerkingsverbanden zijn van cruciaal belang

- *Schaarste aan expertise en capaciteiten.*
  Door de snelle ontwikkeling van de technologie en de brede toepassing ervan, ontstaan ICT-incidenten en –crises uit veel verschillende soorten aanvallen en zijn er verschillende verschijningsvormen te onderscheiden (zoals hacking, virusuitbraken, ddos aanvallen, data manipulatie, uit laten lekken van data). Voor elk subtype is andere expertise nodig, die niet altijd bij één partij te vinden is. Een gezamenlijke aanpak van de crisis is essentieel om tot het juiste inzicht en de passende oplossingsrichtingen te komen.

Focus op flexibiliteit en probleemoplossend vermogen

Het is van te voren lastig te voorspellen op welke wijze een ICT crisis zich zal manifesteren. In het kader van de 'Nationale Risico Beoordeling' zijn en worden scenario's gemaakt, om beelden te verkrijgen van mogelijke risico's voor de nationale veiligheid, maar deze zijn nooit uitputtend. Zo is DigiNotar een voorbeeld van een scenario dat nog niet eerder onderkend en uitgewerkt was. Het ontwikkelen van een standaardaanpak van ICT-crises is daarom niet mogelijk en ook onwenselijk. Het gaat eerder om flexibiliteit en probleemoplossend vermogen: de vaardigheid om snel een overzicht te kunnen creëren in een snel veranderende en onduidelijke situatie en bedenken wie en wat op dat moment nodig zijn om de situatie te verbeteren.

Werken met heldere informatieafspraken en procedures

Tijdens een groot incident of crisis is het creëren van duidelijkheid van groot belang. Wat is er aan de hand? Wie heeft welke informatie? Wie is waarvoor verantwoordelijk en wie kan welke maatregelen nemen? Bij wie kan ik waarvoor terecht en wat wordt er van mij verwacht? Vooraf opgestelde eenduidige en eenvoudige afspraken en procedures rondom informatiedeling, zowel binnen als tussen samenwerkingspartijen, kunnen helpen om tijdens een crisissituatie snel te kunnen acteren en zo te komen tot passende aanpak.
Het is zaak om hierbij niet door te slaan: procedures hebben altijd betrekking op kennis uit het verleden. Wanneer men zich vastklampt aan procedures neigt het naar een standaardaanpak en verliest men de hierboven genoemde flexibiliteit die zo belangrijk is in de aanpak van ICT-crises. Idealiter creëren procedures de randvoorwaarden om op een flexibele manier de crisis aan te kunnen pakken.

CC-SA-BY Alan Stanton

Hoe bereidt de overheid zich voor op ICT-crises?
Met de komst van het Nationaal Cyber Security Centrum wordt ingezet op het versterken van de ICT-crisisbeheersing. Het centrum valt onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) van het Ministerie van Veiligheid en Justitie. Bij (dreiging van) een ICT-crisis verlopen signalering en eerste duiding via het NCSC. Indien nodig activeert het NCSC de ICT response board en schaalt het op naar de nationale crisisstructuur.

Hoe gaat het NCSC verder?
Om haar rol in incident respons en crisisbeheersing goed waar te kunnen blijven maken, voert het centrum voortdurend verbeterslagen uit. Deze staan beschreven in onderstaande acties en sluiten aan bij de eerder genoemde 'ingrediënten' voor de aanpak van ICT-crises.

Doorbouwen op wederzijds vertrouwen
De afgelopen tien jaar heeft GOVCERT.NL, en sinds 2012 NCSC, zich ingezet voor de ontwikkeling van sterke samenwerkingsrelaties. Dat doet de organisatie o.a. door actief deel te nemen aan (inter-) nationale overlegorganen en symposia in binnen- en buitenland en door zelf jaarlijks een symposium te organiseren.

> Het ontwikkelen van een standaardaanpak van ICT-crises is niet mogelijk en ook onwenselijk

Dagelijks plukt het NCSC tijdens (grootschalige) incidenten hier de vruchten van: het weet snel relevante partijen te vinden en omgekeerd. Doordat er veelal sprake is van langdurige, vertrouwde relaties, lukt het NCSC om snel toegang te krijgen tot vertrouwelijke netwerken en informatie, om zo te kunnen werken aan de oplossing van het probleem.

Partijen waar het NCSC mee samenwerkt zijn onder andere:
- overheidsorganisaties zoals de het Ministerie van Defensie en EL&I, het Nationaal Crisiscentrum, de KLPD en de AIVD
- private partijen zoals internet service providers en leveranciers van hard- en software
- vitale organisaties zoals banken, energiebedrijven en telecomproviders
- internationale samenwerkingsverbanden op Europees en globaal niveau
- personen uit de security- of hackerscommunity

Een van de geformaliseerde samenwerkingsverbanden sinds de zomer van 2011 is de ICT Response Board (IRB): dit adviesorgaan bestaat uit afgevaardigden van publieke en private organisaties en komt samen tijdens (dreiging van) een ICT-crisis. De IRB adviseert de crisisbesluitvormingsstructuur van de Rijksoverheid en (indirect) vitale sectoren over de situatie. Tijdens DigiNotar is de IRB drie keer bijeen gekomen. Met positief resultaat: de kennisuitwisseling tussen de verschillende partijen leverde nieuwe inzichten over de aard van het probleem, waardoor de coördinatie en aanpak van de crisis verbeterde.

Versterken expertise
NCSC medewerkers krijgen de ruimte om hun expertise binnen cybersecurity te doorontwikkelen. Ze zetten projecten op met partners uit binnen- en buitenland, bouwen en onderhouden een (inter)nationaal netwerk en geven presentaties voor vakgenoten. NCSC

NCSC
Sinds begin 2012 is het Nationaal Cyber Security Centrum (NCSC of 'centrum') operationeel. Het centrum is een publiek-privaat samenwerkingsverband en heeft als doel om de weerbaarheid van de Nederlandse samenleving in het digitale domein te vergroten. De taakgebieden van het centrum richten zich op het leveren van expertise & advies, monitoring & incident respons en het versterken van de crisisbeheersing, allen op het vlak van cyber security. Het NCSC richt zich primair op de rijksoverheid en de vitale sectoren, met nationale veiligheid als focuspunt. Daarnaast stelt het haar expertise en inzichten online via www.ncsc.nl beschikbaar voor een breder publiek, zoals bedrijfsleven, overheid, burgers en professionals. NCSC is voorgegaan door GOVCERT.NL, dat zich sinds 2002 richtte op cyber security en incident response voor de overheid.

ontwikkelt state-of-the-art kennisproducten en tools die bijdragen aan preventie van en response op ICT-incidenten en –crises. Bijvoorbeeld het Cybersecuritybeeld, een actuele observatie van cybersecurity, dat het NCSC samen met publieke en private partners ontwikkelt. Afgelopen juli is het tweede beeld gepubliceerd. Ook ontwikkelt NCSC monitoringtools om cyberaanvallen snel te kunnen detecteren en analyseren. Een voorbeeld is Honeyspider Network. Deze tool kan vaststellen of url's kwaadaardig zijn of niet, inclusief nog onbekende aanvallen (zero-day attacks).
Daar waar expertise niet aanwezig is binnen het NCSC en snel ontsloten dient te worden bij crises of dreigingen, gaat NCSC inzetten op het opzetten van een publiek-private expertpool, waarbij ook de aansluiting gezocht wordt met de wetenschap.

Duidelijke afspraken en draaiboeken
Aangezien een ICT-crisis een relatief nieuw crisistype is voor de Nederlandse overheid, en ook internationaal, wordt er hard gewerkt aan het ontwikkelen, vastleggen en borgen van informatie-afspraken en procedures. Voorbeelden zijn:

- het Nationaal Crisis Plan ICT (NCP-ICT), waarin beschreven staat welke partijen bij een ICT-crisis betrokken zijn en wat hun rol en verantwoordelijkheid is. Initiators zijn het Nationaal Crisiscentrum (NCC) en het Ministerie van EL&I.
- het formaliseren van samenwerkingsrelaties tussen NCSC en vitale sectoren zoals het bankwezen, telecom en energie;
- het opstellen van zogeheten Standard Operating Procedures (SOPs). Deze maken voor alle partijen duidelijk wie wat wanneer doet en waar men elkaar op aan kan spreken. Zowel in Europees als wereldwijd verband worden dergelijke SOPs geformuleerd en geïmplementeerd.
- Voor de eerder genoemde ICT response board (IRB) is een procesbeschrijving opgesteld die is geoefend met de leden. Deze procesbeschrijving wordt voortdurend geëvalueerd en indien nodig aangepast.
- Binnen het NCSC ontwikkelen van interne procedures en protocollen met betrekking tot crisisbeheersing. Crisisbeheersing is een nieuw taakgebied voor NCSC; het toenmalige GOVCERT.NL had hier geen formele rol in. Dit betekent dat vooraf vastgestelde procedures voor GOVCERT.NL-medewerkers ten tijde van crises ontbraken. Momenteel wordt hieraan gewerkt. De nieuwe procedures sluiten aan bij de bestaande crisisbeheersingsstructuur van de overheid, zoals ontwikkeld door het Nationaal Crisiscentrum (NCC). Het NCSC neemt andere initiatieven op het gebied van ICT-crisisbeheersing, zoals de hierboven genoemde NCP-ICT en de SOPs, mee in de interne procedures en protocollen.

> NCSC ontwikkelt state-of-the-art kennisproducten en tools

Regelmatig oefenen
Het nabootsen van crisissituaties is bij uitstek een manier om bovenstaande elementen verder te ontwikkelen en toetsen. In toenemende mate worden (veelal grootschalige en internationale) oefeningen georganiseerd waar het NCSC aan deelneemt en ook de samenwerkingspartners bij betrokken worden. Om de toegevoegde waarde van deze oefeningen zo groot mogelijk te maken, worden de volgende uitgangspunten gehanteerd:

- Goede voorbereiding geeft een goede oefening en levert vaak al meer inzichten dan de oefening zelf.
- Altijd met meerdere partijen oefenen, om zo inzicht te verkrijgen in de samenwerkingsrelaties en deze te kunnen verbeteren. Hierbij is het ook zaak om niet te overdrijven; in de internationale oefening Cyberstorm III (2010) speelden zoveel nationale en internationale partijen mee, dat het voor de spelers en oefenleiding qua logistiek en scenario wel heel complex werd.
- Focus op de crisisbeheersingsvaardigheden: zijn de medewerkers gezamenlijk in staat om adequaat te reageren op de crisissituatie? Zijn zij flexibel en beschikken zij over het juiste probleemoplossend vermogen? Goed gebruik maken van procedures en informatie-afspraken zijn hierbij een middel, geen doel op zich.
- Neem voldoende ruimte om te evalueren, zowel binnen de eigen organisatie als met partnerorganisaties. Door te reflecteren op het eigen handelen en dat van anderen worden vaak de grootste ontwikkelstappen gezet.

De komende jaren investeert het NCSC actief met haar partners in het verder versterken van de ICT-crisisbeheersing, zodat zij tot een adequate crisisbestrijding komen wanneer dat in de toekomst nodig is.

Noten

[1] *Dit zijn de formele vitale belangen zoals gedefinieerd in het Nationaal Handboek Crisisbesluitvorming van de Rijksoverheid.*
Zie: https://www.nationaalcrisiscentrum.nl/document/nationaal-handboek-crisisbesluitvorming

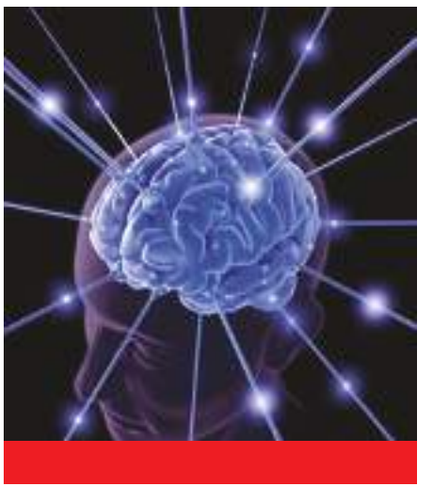
Afkortingen:
ICCb: Interdepartementale Commissie Crisisbeheersing
MCCb: Ministeriële Commissie Crisisbeheersing
ICS: Industrial Control systems
SCADA: Supervisory Control and Data Acqusition
IWWN: International Watch and Warning Network
IRB: ICT Response Board
NCP-ICT: Nationaal Crisisplan ICT
SOP: standard operating procedures
NCC: Nationaal Crisiscentrum

COMMUNICATIE CRUCIAAL TIJDENS CRISIS

VOORBEREIDEN IS HET HALVE WERK

Ella Broos is communicatiestrateeg en gecertificeerd crisismanager (CCMP) en bereikbaar via info@brooscommunicatie.nl.

Uitval van elektriciteit, watervoorziening, betaal- of verkeerssystemen. Maar ook: fraude met PKI-certificaten, het lekken van vertrouwelijke gegevens, stokken van telecomservices. Het zijn stuk voor stuk ernstige crises, waar veel schade mee gemoeid is. Op nationaal niveau is men geprepareerd op dergelijke crises. Geldt hetzelfde op branche- of bedrijfsniveau? Te weinig, weten we. En dat terwijl voorbereiding het halve werk is.



Onder gewone omstandigheden kunnen onze hersenen 7 boodschappen tegelijkertijd verwerken, in stresssituaties zijn dat er 3. De gemiddelde lengte van een citaat in de gedrukte media beslaat 27 woorden, op televisie duurt een quote gemiddeld 9 seconden. In gewone situaties concentreert de luisteraar zich op positieve boodschappen, in gespannen situaties op de negatieve. Triviale informatie? Niet wanneer er sprake is van een crisissituatie. Want dan gelden de gewone wetten van de communicatie niet meer.

Voorziene crisis

We kunnen ons er maar beter op voorbereiden: de kans dat organisaties steeds vaker te maken zullen krijgen met ICT-gerelateerde incidenten en crises is levensgroot. Uitval van systemen door een DDos-aanval, privacygevaar door een databreach, stokken van dienstverlening en faciliteiten, gevaar voor afnemers of klanten: het is allemaal mogelijk. Maar een crisis mag dan altijd plotseling zijn, onverwacht is deze dus niet altijd. Wanneer we een crisis definiëren naar de algehele convictie, spreken we van een plotselinge gebeurtenis, die schade op kan leveren aan medewerkers en klanten van een organisatie, aan de reputatie en aan de continuïteit van de bedrijfsvoering (en daarmee aan de continuïteit van de organisatie). Plotseling inderdaad. Maar ook een brand, een stroomstoring, een pandemie en ICT-uitval (al of niet veroorzaakt door aanval door kwaadwillenden) zijn te voorzien. Niet wanneer, maar wel dat ze kunnen gebeuren. Daarom is voorbereiding het halve werk. Goed voorbereid zijn op een crisis kan de schade, zowel financiële, maatschappelijke, als op gebied van reputatie, beperken.

Scenario

Die voorbereiding bestaat uit het ontwikkelen van scenario's voor het geval de organisatie dit overkomt. Deze krijgen een plek in een Crisishandboek, waarin procedures, checklists, contactpersonen en conceptbrieven en -berichten opgenomen zijn. Dit handboek is leidend voor de crisisorganisatie én -communicatie. Het is niet moeilijk te bedenken dat er bij een ICT-storing persberichtgeving, klantbrieven, websiteberichten, contacten met leveranciers, stakeholders en eventueel burgers geregeld moet worden. Maar dat is allemaal van te voren te bedenken en moet niet op het moment suprême worden uitgevonden. Dan is het te laat.

> Gouden uur: eerste uur communicatie van grootste belang

Gouden uur

Na de uitbraak van een crisis, is het eerste uur communicatief van het grootste belang. Dit wordt ook wel 'het gouden uur' genoemd. We leven niet meer in de tijd dat de woordvoerder een paar uur kon nemen voor een persbericht, dat vervolgens nog eens door een aantal leidinggevende geaccordeerd moest worden. Er moet snel, maar ook doordacht, gehandeld worden. Maxi-

male transparantie - hoe obligaat het ook klinkt - is van belang. Communiceer dat wat bekend is en geef aan wat nog niet bekend is en nog uitgezocht moet worden. Loop niet op de feiten vooruit: is de oorzaak van de uitval niet bekend, speculeer dan niet over een hackersaanval. Bagatelliseer niet, ontken niet: wees feitelijk en zorgvuldig en zorg dat er op een later tijdstip niets weersproken of teruggenomen moet worden. Maak afspraken met medewerkers dat de woordvoering gestroomlijnd wordt via het crisisteam of de woordvoerder, zodat de communicatie consequent en consistent is.

Nieuwe media

Twitter, Facebook, nieuwssites: het nieuws gaat sneller dan ooit. Daar moet in het scenario rekening mee gehouden worden en het is van groot belang dat de organisatie zich daar van bewust is. Zie ze niet als een bedreiging, maar maak er gebruik van in de crisiscommunicatie. Het inschakelen van een webcare-team is cruciaal tijdens crisiscommunicatie. Niet alleen om berichten te plaatsen, maar ook om de berichten die geplaatst worden door derden te monitoren en verzamelen. Er zijn handige tools beschikbaar om dat te doen, waaronder Hootsuite, Tweetdeck en Google Analytics. Daar is in een oogopslag te zien hoe er getweet en gepost wordt. Plaats zelf nieuwsberichten op de site van de organisatie, en link hiernaar door via Twitter en mail. En, mogen we ervan uitgaan dat er uitwijk is geregeld voor de ICT-systemen en eventuele webhosting? Ja toch?

Message mapping

Snelheid is dus belangrijk in het eerste uur van een crisis, de zogenoemde alarmeringsfase. Maar die gaat niet ten koste van bedachtzaamheid. Een eerste reflex van mensen in een crisissituatie is 'in de actie' schieten: het zogenoemde 'Bumble bee effect'.

De risico's daarvan zijn groot, want ondoordacht communiceren zal meer kwaad dan goed doen. Het blijft dus zaak het hoofd koel te houden. Naast vaart en transparantie is het ook goed rekening te houden met de psychologische effecten van mensen tijdens een crisissituatie. De 'normale wetten' van de communicatie gelden niet in een situatie van hoge druk en stress. Hanteer de principes van het zogeheten Message mapping [1]. Deze methodiek, die in Amerika is ontwikkeld en in Nederland (te) weinig bekendheid heeft, helpt om in moeilijke omstandigheden effectief een heldere boodschap over te brengen. En dat is geen luxe in crisissituaties.

77 vragen

Uit wetenschappelijk onderzoek naar crisiscommunicatie in het kader van *message mapping*, blijkt dat de media in crisissituaties 77 vragen het meest stellen. Een hard copy van deze lijst in het Crisishandboek van de organisatie is aan te raden. Te vinden in de uitgave "Effective Risk and Crisis Communication during Water Security Emergencies", door Vincent Covello van het Center for Risk Communication New York. (www.epa.gov)

Maar er zijn meer - wederom in Nederland te weinig gebruikte - technieken, gebaseerd op kennis van de werking van hersenen in moeilijke situaties. De regel van drie houdt er rekening mee dat mensen in tijden van grote stress maar drie kernboodschappen kunnen onthouden, daar waar er in normale tijden zeven onthouden kunnen worden. Negatieve boodschappen blijven in stresssituaties langer hangen en krijgen meer aandacht dan positieve. Dit kan worden gecompenseerd door één negatieve boodschap te laten volgen door een aantal positieve (bijvoorbeeld een oplossing). Ook is het goed om te weten dat mensen de eerste en de laatste boodschap het beste onthouden. Handig bij het opstellen van een verklaring. En dan de 27x9x3 regel. De grootste kans dat een boodschap volledig en helder overkomt in de media wordt behaald door een statement van 27 woorden te formuleren, die in 9 seconden kan worden uitgesproken en zowel empathie, overtuiging en optimisme bevat.

> Een plotselinge crisis hoeft niet onverwacht te zijn

Pity, praise, promise

Rekening houdend met de lessen die we uit het bovenstaande leren: kort en bondig. In het gouden uur beperken we ons tot de feitelijke informatie: dit is er aan de hand, dit zijn de consequenties voor de dienstverlening, dit zijn we aan het doen, dit weten we nog niet, zodra we meer weten communiceren we dat. Vervolgens komt, in de stabilisatiefase van de crisis, meer informatie beschikbaar. Over de gevolgen, de herstelwerkzaamheden en de vervolgmaatregelen. Een uitgangspunt bij crisiscommunicatie is dat het vertrouwen hersteld moet worden. Een manier om dat te doen is de Pity-Praise-Promise [2] formule. Betuig spijt van wat er gebeurd is, bedank degenen die hebben bijgedragen aan de - snelle - oplossing van de crisis en geef zicht op wat de organisatie zal doen om een en ander voortaan te voorkomen.

Geringe tijdsinvestering

Uit onderzoek blijkt telkens weer dat weinig organisaties voorbereid zijn op een crisis. Een handboek ontbreekt, procedures en tools ontbreken, er is geen fysieke noch ICT-uitwijk geregeld, perslijsten zijn niet up-to-date en niemand weet wie eigenlijk in het crisisteam moet zitten. Het nadenken over een eventuele crisis is niet prettig, maar het loont wel. Organisaties kunnen met een geringe tijdsinvestering een goed scenario opzetten en de nodige voorzieningen treffen om zowel de crisis snel te beheersen als de schade te beperken door een adequate communicatiestrategie. Maar dan moet de awareness er zijn dat een crisis iedereen kan overkomen. Ongepland, maar in veel gevallen niet onverwacht.

Scenario's helpen om veerkrachtig met een crisis om te kunnen gaan

Meer lezen:

Crisis Management, chaos in de orde, Hans Slaman. Uitgeverij Boom/Nelissen.
De Kleine Gids, risico- en crisiscommunicatie 2010. Kluwer.
Geen commentaar, communicatie in turbulente tijden, Hugo Marijnissen en Stijn Pieters. Business Contact.

https://www.nationaalcrisiscentrum.nl/bibliotheek

http://www.frankwatching.com/archive/2010/05/11/10-tips-voor-online-crisiscommunicatie-en-issue-management/

Referenties

[1] *http://www.epa.gov/nhsrc/video/rcom.html*

[2] *Lees ook "Drie minuten…" over het schietincident in Alphen aan den Rijn, geschreven door Bas Eenhoorn*

Advertorial

PROEFAUDIT ZET INFORMATIEBEVEILIGING FORMEEL OP AGENDA

Bijna wekelijks zijn de risico's van de geautomatiseerde samenleving in het nieuws. Informatiebeveiliging staat in de schijnwerpers, terwijl menige organisatie het nog nauwelijks formeel op de agenda voert. Een proefaudit kan daar verandering in brengen; niet zelden is objectieve meting dé aanzet tot verdere actie.

De trend die we zien, is dat IT steeds grootschaliger wordt, met een fundamentele invloed op ons dagelijks leven. Steeds meer gegevens over meer mensen zijn opgeslagen in steeds meer systemen met meer doeleinden. Onzekerheidsfactoren zijn er te over. De risico's lopen uiteen van persoonlijke schade voor een enkele betrokkene tot technische, financiële en imagoschade voor bedrijven, overheden en zelfs complete sectoren. Integrale beveiliging is een serieuze zaak. Waarom is informatiebeveiliging dan geen *conditio sine qua non*?

30% Systemen, 70% mensenwerk

"De bewustwording groeit snel", signaleert Mike Wetters, Lead Auditor van DNV Business Assurance. Wetters is één van Nederlands specialisten in *Information Security Management*. Als auditor komt hij dagelijks over de vloer bij bedrijven en overheden. "Het gevaar van informatielekken is reëel", zegt hij. "Zo'n lek wordt dan pijnlijk breed uitgemeten in de media, met alle gevolgen van dien. Het is in het belang van de organisatie én van cliënten om dat te voorkomen. Gelukkig is er steeds meer bereidheid om werk te maken van informatiebeveiliging, bijvoorbeeld door borging met een objectieve norm zoals ISO 27001. Daarbij gaat het overigens meer dan om alleen techniek; 70% van de

veiligheid wordt uitgemaakt door mensenwerk."

"Op het niveau van directie of Raad van bestuur wordt de sense of urgency vaak nog niet gevoeld"

Wetters illustreert zijn betoog met een recente ervaring bij een groot Nederlands bedrijf. Bij de entree vanuit de parkeergarage opende een behulpzame medewerker de deur voor de auditor. Het kostbare toegangssysteem dat kort geleden was geïnstalleerd, werd goedbedoeld omzeild. Wetters: "Informatiebeveiliging valt en staat met het bewustzijn van medewerkers. Meestal gaat het onbewust mis. Zo ook bij medewerkers die het bedrijf verlaten. Men levert de telefoon en de laptop in. Niemand checkt of er nog bestanden op de privé-PC en telefoon staan, het neveneffect van thuiswerken. Zo ontstaan informatielekken, waarover meestal niemand behalve de IT'er zich opwindt. Op het niveau van directie of raad van bestuur wordt de *sense of urgency* vaak nog niet gevoeld."

Proefaudit: de thermometer in de organisatie

Gelukkig zijn er ook positieve 'uitschieters', zoals Riagg Zuid in Roermond. Hier besloot de afdeling Informatievoorziening & Beheer onlangs tot een proefaudit, gevolgd door een consultancydag, uitgevoerd door certificerende instelling DNV Business Assurance in samenwerking met consultancyfirma BMGrip. Opdrachtgever Jan Hendrik van Weelderen: "Een Riagg focust op zorg, zelfs de IT'er of ICT'er. Een onafhankelijke auditor focust op informatiebeveiliging, vanuit specifieke kennis én vanuit specifieke ervaring. De proefaudit was dé manier om informatiebeveiliging serieuze aandacht te geven. Na twee intensieve dagen lag er een heldere rapportage."

ISO 27001 of NEN 7510 certificering ter bevestiging

"Riagg Zuid is goed bezig," concludeert Mike Wetters. Riagg Zuid investeerde kort geleden in een digitaliseringsslag. Van Weelderen: "Die ervaring had ons al bewust gemaakt van de gevoeligheid van cliënteninformatie. Op alle niveaus zijn we alert op de vertrouwelijkheid van gegevens, behandelingen en ook over onze medewerkers/ behandelaars zelf. Toch is het prettig om met een externe, onafhankelijke partij te sparren, om impulsen te krijgen en gescherpt te worden. In no time werden de kaders duidelijk en hebben we het traject naar certificering bepaald. Onze gedachten zijn omgezet in een conceptbeleidsplan, concreet met toetsmomenten. Informatiebeveiliging is geagendeerd. Dat is goed voor ons en voor de buitenwacht."

EERSTE LUSTRUMCONGRES PVIB

AWARENESS EN VERTROUWEN IN EEN WERELD MET CYBERCRIME

Op woensdag 20 juni 2012 vierde het PvIB haar eerste lustrum in de vorm van een congres in het Leerhotel 't Kloos-ter te Amersfoort. Het thema was "Awareness en vertrouwen in een wereld met cybercrime". Wij presenteren hierbij een fotoimpressie van dit congres en het welkomstwoord dat voorzitter Fred van Noord op de avond uitsprak.

Beste collega informatiebeveiligers en andere gasten,

Ik ben blij u hier te mogen te verwelkomen bij de opening van het eerste lustrumcongres van PvIB.

Allereerst wil ik welkom heten de sprekers die bereid zijn om hier hun verhaal te vertellen over waarom zij vinden dat informatiebeveiliging zo'n belangrijk vakgebied is. Dank Sharon Gesthuizen (Tweede Kamerlid), Wil van Gemert (directeur Cyber Security van het ministerie van V&J) en Gigi Tagliapietra, de voorzitter van onze zustervereniging CLUSIT in Italië.
Daarnaast de ereleden die zo'n belangrijke rol hebben gespeeld bij de ontwikkeling van PvIB.
Welkom aan de bestuurders van andere verenigingen met wie we goede banden onderhouden op de grenzen van het vakgebied. Dat zijn Ngi, NOREA, ISACA en EEMA.

Verder de leden van de Commissie Informatiebeveiliging van VNO-NCW en de leden van de Adviesraad, vertegenwoordigers uit de sectoren van onze maatschappij die het bestuur voorzien van wijze raad en daad.
Ik ben blij dat u er allemaal bent.

We vieren vandaag het eerste lustrum van PvIB. Wat mij betreft staan de eerste 5 jaar van PvIB symbool voor de dynamiek van onze beroepsvereniging met een historie van 32 jaar. Vanuit verenigingen als CSA, OTB, Platform Informatiebeveiliging en Genootschap van Informatiebeveiligers. Over de geschiedenis zal ik niet veel zeggen, die vindt u uitgebreid terug in het lustrumboek dat in september verschijnt.

De community van informatiebeveiligers heb ik in de afgelopen 12 jaar ervaren als een groep van zeer bevlogen professionals. Uitingen daarvan zijn de constante groei van de vereniging tot nu met zo'n 1300 leden, de grote groep professionals die zich inzet in commissies en bestuur, en de zeer grote belangstelling van de leden voor de themabijeenkomsten. Met aantallen van 150- 250 deelnemers elke maand weer, zult u begrijpen dat uw collega's op basis van vrijwillige inzet een optimale prestatie leveren om dit allemaal mogelijk te maken, zonder de leden van de andere commissies daarmee tekort te willen doen. Afgelopen weekend nog is bij u de laatste editie van ons vakblad in de bus gevallen en zijn de elektronische versies vanaf de website te downloaden. De afgelopen weken nog ben ik bij twee parels uit ons aanbod aanwezig geweest:
bij de Esmeralda lezing van het IBO, een bijeenkomst voor het management met een meer filosofisch getint karakter over ons vakgebied;
en een themasessie over de ontwikkeling van soft skills in voor ons vakgebied op maat gesneden trainingsessies.
Met wat meer geluk had ik vandaag de bijeenkomst kunnen bijwonen van de Young Professionals waar door ervaren collega's een "Zeur ze de kop van de romp" sessie hadden georganiseerd voor de jonge garde.

Velen zetten zich als aanvulling op hun dagelijks werk, voor een langere periode in voor hun vakgebied. Zij bouwen zelf op die manier veel kennis op en breiden hun netwerk uit met collega's met wie het altijd weer boeiend is elkaar te ontmoeten omdat kennis en competenties vaak aanvullend zijn.
Met elkaar zorgen zij bij onze beroeps-

vereniging voor het ontwikkelen van onze vakgenoten met actuele kennis en ervaring.

De laatste jaren is het vakgebied steeds meer in het nieuws geweest vanwege de vele incidenten die zich hebben voorgedaan. Hierdoor is het bewustzijn gegroeid dat het vakgebied informatiebeveiliging en de beroepsgroep van groot maatschappelijk belang zijn en toegevoegde waarde hebben voor de Nederlandse en Europese economie. Ik refereer nog maar eens aan het interview van twee jaar geleden van bestuursleden met Neelie Kroes over de Digitale Agenda.

En aan het Algemeen Overleg in de Tweede Kamer waar vertegenwoordigers uit de Tweede Kamer gelegenheid hebben om vragen te stellen over het gevoerde beleid aan de verantwoordelijke minister. Regelmatig werd geconstateerd dat er gebrek is aan kennis en gebrek aan capaciteit op ons vakgebied. Parlementariër Jeanine Hennis stelde dan ook de vraag " … hoe de minister staat tegenover de realisatie van een kwalificatieschema dat de kwaliteitsborging van de beroepsgroep informatiebeveiligers eenduidig maakt en bewaakt". Het antwoord van Opstelten was duidelijk: "Het is van belang dat we in Nederland kwalitatief hoogwaardige informatiebeveiligers bezitten. Initiatieven van de beroepsgroep juich ik toe, en we zullen er voor zorgen dat we in gesprek komen en blijven".
Inmiddels heeft een gesprek over kwalificatie met de ministerie van Veiligheid & Justitie en het ministerie Economische Zaken, Landbouw en Innovatie plaatsgevonden.

Voorafgaand aan het Algemeen Overleg is actief gelobbyd met meerdere parlementariërs. Dat parlementariërs het onderwerp nu expliciet op de politieke agenda hebben geplaatst is een stimulans voor ons vakgebied. De overheid heeft in haar eigen Nationale Cyber Security Strategie een paragraaf

opgenomen over de kwalificatie van de beroepsgroep. Het Algemeen Beleid van PvIB sluit op dit punt naadloos aan.

PvIB wordt ook gevraagd om onze mening te geven. Er zijn relaties met het NCSC, VNO-NCW, het Centrum IB & Privacy van de overheid.

Deze ontwikkelingen rechtvaardigen de inspanningen om voor het vakgebied informatiebeveiliging, de vorming te stimuleren van een community van gekwalificeerde professionals. Zoals gekwalificeerde en gecertificeerde werkers in de gezondheid waken over het fysieke en mentale welzijn van burgers, kunnen gekwalificeerde en gecertificeerde informatiebeveiligers meer waarborgen geven over het welzijn in de digitale wereld aan de maatschappij, organisaties en burgers.

Vandaag is een bijeenkomst met sprekers waar ik dan ook trots op ben. Het is een gezelschap dat een afspiegeling is van wat PvIB momenteel graag wil zijn: Internationaal georiënteerd, politiek bewust en een beroepsvereniging van een maatschappelijk relevant vakgebied.

Ik wens u een goede toekomst binnen het vakgebied informatiebeveiliging.

Fred van Noord, voorzitter PvIB

COLUMN

EEN PRIVACY 'RED TEAM': ECHTE RIDDERS OF MOOIE PR-STUNT?

Privacy is weliswaar een heet onderwerp als je de kranten en beleidsmatige initiatieven mag geloven. Toch blijkt het vaak in de praktijk eerst ernstig mis te gaan en wordt pas achteraf met een klein lapje de boel weer opgepoetst. Totdat het eerstvolgende incident zich aandient en de reddingspaniek zijn intrede doet. Echt effectief voorkomen dat zich incidenten voordoen, blijkt lastig. Het verrichten van een Privacy Impact Assessment voorafgaande aan de ontwikkeling van een nieuw product of jaarlijks, ter controle van de algehele stand van privacyzaken binnen een organisatie, is nog steeds geen gemeengoed.

Steeds vaker treden Data Protectie Autoriteiten, zoals het College Bescherming Persoonsgegevens, naar buiten met het nieuws dat het 'ergens' niet op orde is en wordt de publieke schandpaal gebruikt om instanties al doende te dwingen beter voor de privacy van individuen te zorgen. De boetes zijn nog steeds laag en kunnen alleen worden afgedwongen voor het overtreden van de administratieve vereisten van de Wet bescherming persoonsgegevens. Het overtreden van de materiële normen uit de wet kan (nog) niet worden bestraft met een boete. Alhoewel Donner bij de evaluatie van de Wbp nog had gezegd dat gekeken zou worden naar een uitbreiding van de boetebevoegdheid, is daar tot op heden nog niets van gebleken. Die schandpaal werkt dus een stuk effectiever, moeten veel Data Protectie Autoriteiten nu vast denken. Wellicht dat dit heeft meegespeeld in het opvallende nieuws dat Google een red team aan het oprichten is die de privacyzaken van het bedrijf in de gaten moet gaan houden. Het team zou de privacyproblemen van de verschillende producten moeten blootleggen en vervolgens oplossen.

Het idee van red teaming is natuurlijk niet nieuw en is binnen de informatiebeveiliging een steeds frequenter gebruikte methode om de security op orde te houden. Red teams, samengesteld uit informatiebeveiligingsspecialisten, lichten een organisatie door en opereren daarbij 'in het geheim' om zo effectief mogelijk potentiële gevaren te ontdekken. Het idee van een specifiek privacy red team is bij mijn weten echt nieuw. Ik ben ze in ieder geval nog niet eerder tegengekomen. Voor Google zal wellicht ook meegespeeld hebben dat ze de komende twintig jaar onder streng (Amerikaans) overheidstoezicht staat nadat ze net eenmaal te vaak een privacygerelateerd incident voor de kiezen heeft gehad. Google moet dus wel iets verzinnen om te voorkomen dat ze bij de onafhankelijke privacyaudits (zoals afgesproken in de schikking met de FTC) telkens een tik op de vingers krijgt. En, eerlijk is eerlijk, ik vind het een ontzettend mooi idee. Of het in de praktijk ook echt goed zal werken, moet nog blijken en hoe Google een en ander zal willen institutionaliseren in de organisatie vertelt het nieuws me niet.

Maar natuurlijk heb ik daar wel wat ideeën over. Om te beginnen moet je zo'n team een onafhankelijke positie geven die – liefst – juridische bescherming geniet. Denk aan de wettelijke bescherming van de FG (Functionaris Gegevensbescherming). Deze luizen in de bedrijfspels zullen immers best weleens geconfronteerd gaan worden met situaties waarin het privacybelang dient te prevaleren terwijl dit indruist tegen een bedrijfseconomisch belang. Het is dus zaak en taak dat een dergelijk red team echt kan doorpakken en de macht heeft om privacyinvasieve producten tegen te houden totdat een en ander daadwerkelijk op een privacyvriendelijke manier vormgegeven is. Daarnaast moet je er wel wat zwaargewichten in stoppen die een behoorlijke staat van dienst op het gebied van privacy en security hebben. Samenwerken in een multidisciplinair team waarin niet alleen juristen een plaats hebben, maar ook technici en wellicht zelfs wel een ethicus, lijkt mij de beste weg te bewandelen om te garanderen dat je alle noodzakelijke kennis in huis hebt om niet alleen dataprotectie-vragen te beantwoorden, maar om ook werkelijk te garanderen dat geen enkel persoon in zijn grondrechtelijk gegarandeerde recht op privacy wordt getast. Als zo'n team dus echt goed in elkaar wordt gezet door Google, dan wordt een nieuwe generatie ridders geboren; de geïnstitutionaliseerde beschermheren en -dames van de privacy. Ik hoop oprecht dat privacy red teams een trend gaan worden en dat het bij veel andere organisaties - inclusief onze eigen overheid, die heeft immers ook nog wel een paar lesjes te leren op privacygebied - navolging gaat vinden. En wie weet mag ik dan over een paar jaar wel schrijven over die nieuwe beroepsgroep privacyridders die er gezamenlijk voor heeft gezorgd dat de windmolens waartegen de burgerrechtenvoorvechters ageren met de juiste wind meedraaien.

Mr. Rachel Marbus, @RachelMarbus op Twitter

SCHAAP OF HERDER

Ir. drs. Jurgen van der Vlugt RE CISA CRISC is zelfstandig professional onder de naam Maverisk Consultancy, IS Audit and Advisory services. Hiervoor heeft hij zeventien jaar als externe en interne IT- en risk-auditor en -adviseur gewerkt bij onder andere KPMG, ABN AMRO Bank, Noordbeek en Achmea, en recent onder andere 'terug' bij ABN AMRO Bank. Daarnaast is Jurgen actief in de vaktechniek bij diverse beroepsverenigingen en regelmatig docent, spreker en auteur. Jurgen is bereikbaar via jvdvlugt@maverisk.nl.

Wie werkt in de informatiebeveiliging, merkt te werken in een omgeving waar sluipenderwijs allerlei nieuwe ideeën over organisatie-inrichting en -beheersing van concept tot implementatie komen. Dat gebeurt vaak zonder expliciete besluitvorming. Men gaat mee met wat de trend lijkt te zijn of liever, men merkt plotseling te zijn gevangen in verwachtingen die anderen hebben over wat passend is voor de beheersing binnen de eigen organisatie. Daar kleven echter nogal wat bezwaren aan. Zeker wanneer we worden geacht mee te drijven met ontwikkelingen die vanuit verkeerde grondgedachten ingestoken, te weinig of verkeerde resultaten leveren. In dit artikel zal worden ingegaan op twee belangrijke trends van misschien wel het afgelopen decennium waarvan de effecten merkbaar zijn in de informatiebeveiligingswereld. Er zal worden aangegeven wat er mis is met die twee, en zal in houtskoolschets worden aangegeven van wat we wél kunnen doen om informatiebeveiliging effectief te maken. Dit artikel zal voor sommigen wellicht wat weinig positieve kritiek bevatten. Met excuses en met opzet; een koud bad is het best op te warmen met een scheut gloeiend heet water, zoals de Chinese wijsheid luidt. Discussie brengt ons verder…

Te veel schaap

De algemene these is dat veranderingen in de wereld om ons heen en binnen onze (werk)organisaties, aanpassingen nodig maken in de wijze en aanpak van informatiebeveiliging. Of we het nu willen of niet, de organisatie-inrichting is aan verandering onderhevig. Hoe die veranderingen worden in- en doorgevoerd, kan vanaf drie niveaus:

1. Top-down verfijnen van algemene organisatierichtlijnen tot operationele regeltjes;
2. Middle-out modelleren van (het gedrag van) de wereld om ons heen en daarmee risico-analyses doen, vervolgens aan de hand daarvan onze organisatie-inrichting en informatiebeveiliging aanpassen;
3. Bottom-up doen wat nodig is.

De eerste twee gaan meestal samen, de tweede parallel en vaak losstaand van de eerste. Het is het denken van het makke schaap dat zich individu voelt in een kudde. Een kudde die lekker warm is en bescherming biedt, tot de wolf (of de herder…) trek heeft in een willekeurig lapje schapenvlees. Een ongeluk zit in een klein hoekje, en wacht tot de herder en zijn hond (de auditor?) er even niet zijn. Zo zal ook de volgzame informatiebeveiliger worden behandeld als er onverhoeds iets misgaat.

Dit artikel poogt wakker te maken

Command zonder control

Het top-down verfijnen van algemene richtlijnen is een vrij breed bekend fenomeen. Wat we eigenlijk ook weten,

is dat dat verfijnen ergens ophoudt. Op een gegeven moment weet eigenlijk niemand meer waarvoor allerlei details nodig zijn. Er zijn natuurlijk wel allerlei fraaie tabellen, beleidsstukken (soms gewoon fout als 'policies' aangeduid), standaarden, etc. waar men met enig geluk zelf in kan terugpuzzelen wat nou eigenlijk de bedoeling was. Maar dat terugpuzzelen is een klus op zich en wie heeft daar nog tijd voor? Zeker in een tijdsgewricht waarin allerlei middle managers ook niet kunnen worden verdacht van al te diep inzicht in de materie, bestaat vaak een werksfeer waarin het stellen van lastige vragen als "Waarom?" niet wordt gewaardeerd. "Doe nou maar gewoon wat er gezegd wordt…"

Onbegrepen overhead

Het onbegrip wordt versterkt door subtiele maar verwarrende nuanceverschillen in de gehanteerde taal. Veel, heel veel termen waar we zo nonchalant mee strooien, zijn helemaal niet zo scherp gedefinieerd als nodig is en worden in allerlei interpretaties gebruikt. Geef me een definitie van 'risicomanagement' en ik kan die op ieder woord wel onderuithalen. Ga nu eens uw organisatie in en bezie hoeveel mensen zouden hebben durven toegeven dat ze hebben gevraagd naar de exacte betekenis van gangbare termen, toen ze die voor het eerst hoorden. Dat zal best een klein aantal zijn. Men interpreteert naar eigen goeddunken en praat elkaar na, eerst in kleinere kring, waarna men in grotere kring ervan uitgaat dat iedereen wel dezelfde interpretatie zal hanteren. Niet dus. Waardoor de missieven van hogerhand een aantal vertaalslagen en interpretaties ondergaan voor ze operationeel kunnen worden uitgevoerd. Of blijven hangen omdat ze halverwege het proces worden 'weggemasseerd'. Dit alles kost soms járen tijd; in die tijd is de organisatie alweer verder ontwikkeld, de wereld eromheen ook en dus vechten we 'the day-before-yesterday's-war', en soms zijn de regels al veranderd voor ze zijn ingevoerd…
Dit betekent uiteindelijk wel dat er op de werkvloer een hoop maatregelen worden uitgevoerd waarin slechts weinigen nog enig nut kunnen zien. Hetgeen de motivatie en dus de effectiviteit nou niet echt ten goede komen. Integendeel soms, de nieuwe regels moeten in de plaats komen van wat al werkt; op de werkvloer weet men verrassend (?) vaak heus wel wat er moet gebeuren. En dus vervangen we iets wat goed (genoeg) is door iets waarvan we maar moeten afwachten of het gaat werken.
Mét een hoop overhead erbij, want het moet natuurlijk allemaal wel 'aantoonbaar' zijn. Waarom eigenlijk? Omdat een auditor moet kunnen zien dat het werkt? Het is zijn/haar werk om het onderzoek te doen; dat hoeft niet door degenen die uiteindelijk het werk doen op een presenteerblaadje te worden opgelepeld. Het is dus best begrijpelijk dat op de werkvloer een houding ontstaat van murw meeliggen tot het overwaait. Maar juist op de werkvloer heeft men nog besef dat effectiviteit vóór zou moeten gaan, en de overhead van onbegrepen en (met grote kans) onnuttige regeltjes die effectiviteit in de weg kan komen te staan. Met als gevolg dat de organisatie als geheel minder presteert.

> Op een gegeven moment weet eigenlijk niemand meer waarvoor allerlei details nodig zijn

En dat nog afgezien van de overheadkosten van al die (informatiebeveiligings)managers [disclaimer: auteur is er ook zo een] die ook van de opbrengst afgaan. In hedendaagse grotere organisaties is een 'span of control' van vier of minder redelijk normaal, terwijl door de hele organisatie heen dat best vijf tot acht zou kunnen zijn. Vele organisaties zijn, zonder het te beseffen, met allerlei stafafdelingen, matrixstructuren en zeker bezien naar salarissommen op de diverse niveaus, naar feitelijke structuur eerder een ruit dan een driehoek. Op de werkvloer wordt de druk van allerlei kanten dan wel erg hoog. Degenen die nog wat energie besteden aan feitelijke effectiviteit, schieten tekort en vallen weg. Alleen degenen die het meest gespecialiseerd zijn in het onder druk staan en niets anders, blijven over. Doel bereikt?

Zo gaan we de mist in

Veel toekijkende overhead

Effecten, geen effectiviteit

Dat zou allemaal overkomelijk zijn als uiteindelijk zou blijken dat de regels op de werkvloer ook echt effectief zijn *voor het bereiken van het ooit beoogde doel*. Maar het zicht op effectiviteit, laat staan efficiency of volledigheid, is al verdwenen [Power, 1997, 2008; Schneier, 2012]. Ja, de effectiviteit van een individuele maatregel, dat lukt misschien nog. Maar de effectiviteit van het *gehele stelsel* van maatregelen? Wie me zegt dat dat ook niet echt hoeft, die verwijs ik naar een beginnerscursus efficiency. Schrappen, al die regels die kennelijk niet echt nodig zijn en dus niks bijdragen. En wie me zegt dat budgetbeperkingen en risicogebaseerde afwegingen wel moeten leiden tot minder dan honderd procent implementaties, die zegt dat door budgetbeperkingen de doelstelling van een stelsel van maatregelen dus bij voorbaat nooit zal worden gehaald! Nou is dat inderdaad het geval, zie hierna.

Enne, we hebben het over command and control. Control is toch bij*sturen* op basis van informatie? Dat is toch meer dan alleen gebreken die achteraf uit rapportages blijken, herstellen? De op positieve ontwikkelingen aansturende component, hebben we eigenlijk in de informatiebeveiliging nog steeds te veel laten liggen. Het bleef en blijft, lijkt het, bij lippendienst aan het idee ook eens zelf met mogelijkheden te komen voor nieuwe diensten in plaats van alleen maar nee zeggen. Waardoor de nadruk nog steeds ligt op dat nee zeggen en vooral dingen minder doen, beheersen, klein houden, inperken. Maar krimp is geen groei.

Het resultaat is dus, om bij ons vakgebied te blijven, geen beheersing van de informatievoorziening of adequate informatiebeveiliging. Het resultaat was en is compliance met een papieren werkelijkheid. Die papieren werkelijkheid is buitengewoon incompleet, en bovendien zegt het niets over de werkelijke bescherming. Waarom spreekt men van 'three lines of defence' als die three lines maar een beetje langs de zijkant staan te kijken en niet tussen threat en vulnerability staan? Hint: omdat ze verdedigen tegen toezichthouders van buiten, niet tegen threats. Wanneer hebt u voor het laatst een firewall log doorgekeken?

Wanneer hebt u vastgesteld dat *alle* te beschermen informatie daadwerkelijk adequaat *en* effectief was beveiligd?

Kom nou, u weet helemaal niet of de CEO op een borrel zijn mond voorbij praat terwijl er een journalist achter zijn rug staat. Terwijl u wel weet dat daar aanzienlijke risico's voor de organisatie in zitten.

De effectiviteit van informatiebeveiliging die voor 80% uit mensgerichte maatregelen zou moeten komen, vertaalt die zich ook in 80% van uw aandacht en organisatiebudget voor informatiebeveiliging op de HR-control objectives en -maatregelen? Die firewall-beheerder weet heus wel wat hij of zij moet doen om de boel dicht te houden – hooguit krijgt hij er niet de tijd en budget voor – doordat de papieren werkelijkheid zoveel tijd en budget verbruikt. Waar de werkelijke onkunde zit voor wat betreft informatiebeveiliging, tsja, daar hebben we veel minder grip op.

> Dus vechten we 'the day-before-yesterday's-war', en soms zijn de regels al veranderd voor ze zijn ingevoerd

Hetgeen al met al geen prettig plaatje oplevert. 'Gelukkig' zien we wel al een paar jaar een sterke stroming ontstaan die de vertaling van bloemrijke doelstellingen naar concrete maatregelen wil verfijnen door het in het bedrijfsgebeuren tussenschuiven van, liefst kwantitatieve, risicomodellen.

Het falen modelleren

Het middle-out modelleren van het gedrag van de wereld om ons heen begint aan populariteit te winnen. Zeker in de financiële wereld, waar toezichthoudersrichtlijnen zulks vereisen, zien we dat er flinke budgetten worden uitgetrokken om te bezien welke dreigingen op ons afkomen (risico-analyse) en welke controls we daartegenover kunnen stellen om de oh zo kwetsbare (informatie) assets te beschermen. Echter, in modellenland gaat er heel wat mis.

Zo is het nog steeds gebruikelijk om te denken in analyse van enkelvoudige 'events', met vaak enkelvoudige of slechts enkele oorzaken en/of enkelvoudige of slechts enkele gevolgen, alles werkende op zeer discrete tijdsmomenten. Ja, dat vergemakkelijkt de analyse. Maar nee, zo zit de wereld niet in elkaar. De vele, vele factoren die een rol spelen bij incidenten kennen allen in de tijd soms zeer wisselende frequenties van optreden en zeer fluctuerende impacts. Ook is de onderlinge samenhang van oorzaken én gevolgen zeer complex met, in de tijd wisselende en qua sterkte wisselende, positieve en negatieve feedback loops. Onduidelijk is welke loops er zijn, de samenhang onder en tussen oorzaken

en gevolgen is zeer complex en lineariteit van de relaties is een allesbehalve verantwoorde aanname.
In de informatiebeveiliging maken we het ons echter 'gelukkig' (quod non) simpel. We geven een 'systeem' (bedoelt u platform, 'infrastructuur', applicatie(s), database, procedures, of gewoon een CIA-rating) en op basis daarvan werken we de beveiligingsmaatregelen uit, liefst per vaste set bij een classificatie.
Dat lijkt wel fijn, maar betekent natuurlijk wel dat alle mogelijke oorzaken en gevolgen worden platgeslagen in één rating. De koppeling van beschermende maatregelen aan kwetsbaarheden en bedreigingen gaat verloren. Wat we waarvoor doen, dus ook; voor inschatting van de effectiviteit of rationeel budget, niet zo'n goede insteek.

Foute methodologie

Daarnaast hebben we nog steeds geen goede gezamenlijke taal ontwikkeld als het gaat om de classificatie van bedreigingen en impacts in de informatiebeveiliging, die zo belangrijk zijn in de modelvorming in de risico-analyse. Zoals gesteld, de definities zijn onhelder en waar we aan het modelleren slaan, slaan we de plank flink mis:

1. De classificaties die we hanteren, zijn zelden orthagonaal, waardoor ambiguïteit ontstaat die bijvoorbeeld statistische gegevens slecht of (al snel) waardeloos maakt.
2. De feedforward- en feedback-lussen zijn slecht onder te brengen in de modellen; idem voor onderlinge samenhang (versterking of verzwakking) bij diverse maten van optreden van bedreigingen/oorzaken.
3. De variatie in de tijd van de ernst van bedreigingen/oorzaken en gevolgen is niet of slecht in te brengen.
4. De sterkte van 'controls' en de variatie daarvan in de tijd, en de onderling versterkende of verzwakkende, complementaire of vervangende kracht, is niet of slecht in te brengen. Terwijl incidenten juist zo vaak optreden waar 'toevallig nou net op dat moment' controls per ongeluk niet werken, al of niet door de afhankelijkheid van soms minder aandachtige / gemotiveerde 'mensen'.
5. Er is zelden aandacht voor tijdseffecten van het in werking treden van controls na het begin van optreden van een incident. We denken vrijwel alleen in termen van preventieve controls. De schadebeperkende effectiviteit van de detectieve en correctieve controls die we in ogenschouw nemen komt echter pas na enige tijd op gang. Anderzijds hadden we toch al te weinig aandacht voor efficiency, die in heel wat gevallen andere dan alleen preventieve controls rationeel maakt, zie [Schwartau, 1999].
6. De kwantificeringen zijn vaak zeer slecht passend:
   - Puntschattingen in absolute getallen van karakteristieken die slechts ordinaal of zelfs maar nominaal (categorisch) kunnen worden ingeschaald;
   - Andersom, het platslaan van schattingen van reële waarden tot discrete categorieën of zelfs ordinale schalen – om te zwijgen van genoemde tijdvariaties in de waarden. Is een schade van € 900k niet zowat even erg als, zeg, € 105k terwijl de grens tussen Laag en Midden op € 100k ligt? Wie bepaalt dat minder dan € 100k 'Laag' is ..? Ook als die € 100k door de organisatie met dubbeltjes en kwartjes bij elkaar moet worden verdiend? En als een Laag geclassificeerd incident niet adequaat wordt aangepakt, kan die dan niet makkelijk escaleren naar een Zeer Hoog probleem? Waarom dan Hoog/Midden/Laag gebruikt..?
   - Zo er al tijd in acht wordt genomen, een slechte verwerking ervan: Als de kans op een bedreiging 1 op 1000 is; wordt dan bedoeld een kans van 1 op de 1000 dagen, nanoseconden, jaar of …? En dat kan dus ook betekenen dat zowel vandaag nog én morgen de bedreiging toeslaat, zonder dat noodzakelijkerwijs de statistiek verandert;
   - Al met al zullen we toe moeten naar continue niet-lineaire berekeningen en kansrekening, waar we nog veel te weinig kaas van hebben gegeten.
7. De kosten van beheersing en de gebreken daarin, jarenlang doorlopend door het handhaven van controls en ad hoc bij het, onvermijdelijk, optreden van incidenten, schatten we slechts zelden in. Terwijl de ratio van risicomodellering toch was om kosten en baten af te wegen. Ja, incidenteel wordt het gedaan, maar niet structureel. Wie weet wat een nieuw firewallcomplex mag kosten (inclusief jaren aan onderhoud en –personeel) ten opzichte van het huidige, als het nieuwe 'beter' is of beter bij de tijd te houden valt? Of is het allemaal 'cost of doing business'? Dat laatste zou dan eens zo in de reguliere productiekosten van producten c.q. diensten moeten worden vertaald. Wie heeft wel eens de gezamenlijke kosten (gesuperbruteerd) van de informatiebeveiligingsafdeling buiten de 'werkvloer' van de IT-infrastructuur opgeteld? En, hoeveel scheelde dat de organisatie in vermindering van schade door informatiebeveiligingsincidenten? Nee, eerst modelleren en dan pas met kosten komen kan niet want de controls die we op basis van kosten al of niet selecteren, horen in het model (of niet).
8. We hebben nog steeds geen goede methoden om andere dan directe financiële schade te meten. Terwijl bijvoorbeeld reputatieschade zo'n belangrijke factor aan het worden is. Uiteindelijk 'moet' alle schade in geld worden uitgedrukt om in de huidige modellen te kunnen gebruiken. Dus wordt er, (semi-) wetenschappelijk of zelfs maar semi-rationeel, op los geschat.

9. We hebben geen of beperkte cijfers over near misses waar een of meer controls, wellicht door toeval, hebben gewerkt. Dit verstoort dus de cijfers, als we die al hebben, over frequenties van optreden van bedreigingen.
10. We hebben sowieso nauwelijks cijfers. Ja, er zijn initiatieven om over organisaties heen te benchmarken en andere cijfers centraal te administreren om een basis voor statistiek te kunnen hebben. Maar de aangeleverde cijfers lijden aan alle bovenstaande beperkingen. Eigenlijk erger nog, ze krijgen een dubbelslag omdat de verschillen in achterliggende 'modellen' oftewel organisatie-inrichtingen en -culturen, tussen organisaties nog groter zijn dan binnen organisaties tussen afdelingen. Oftewel, de statistieken zijn leuk als bladvulling in rapporten van consultantsbureaus maar zeggen niets over de situatie waar u middenin zit.
    En de weinige cijfer die u wel hebt, … zijn gewoonweg te weinig om statistiek mee te bedrijven. Het blijven incidentele cijfers, die morgen totaal anders kunnen zijn.
11. Statistiek helpt maar we gaan er vrijwel altijd verkeerd mee om [Kahnemann, 2011; Taleb, 2010b].

Met dergelijke 'methoden' zou de gemiddelde (risico)manager nooit door de brugklas hebben mogen komen. En de resultaten zijn pover, zeer pover. Eigenlijk zijn ze alleen bruikbaar om een *kwalitatief* beeld te krijgen van het eigen onvermogen om grip te krijgen op de materie.

Zodra gesmolten, niet (exact) reconstrueerbaar

Als dat de bedoeling is, spendeer dan niet al die kosten! Begin dan met kwalitatieve inschattingen en doe het daarmee. Inderdaad, dat is voor ons onbekend terrein. Dat is dan jammer, als we om ons werk goed te doen moeten toegeven dat we het tot nu toe niet goed deden en eigenlijk ook niet precies weten hoe het moet.

Verkeerde gedachten

Want we kunnen het wel beginnen te leren. We zullen wel moeten. We hebben namelijk nóg een probleem te tackelen met modelleren; van nogal fundamentele aard:
De beperking van het modelleren. Modellen dienen om een situatie te *be*grijpen, niet om in te grijpen. Modellen versimpelen oftewel laten fenomenen die zich in de werkelijkheid voordoen, weg. Maar hoe weten we wat we weg kunnen laten en wat niet ..? Dat weten we niet.
Wel weten we dat, juist in onze leefwereld, de grootste, de break-your-business-gebeurtenissen dermate onwaarschijnlijk zijn dat ze onder de radar blijven. Maar het zijn er zoveel, en de individuele kansen zijn niet nul, dus zal er iets fout gaan. Puur bij toeval gebeurt dat niet om de haverklap maar dat is meer geluk dan wijsheid; we kunnen best klap op klap krijgen en toch binnen de geschatte kansverdelingen blijven.
En als, als we een model zouden hebben dat zowel een goede beschrijving is van de situatie met alle problemen van het te abstract zijn maar niet concreter te maken, én dat bruikbaar is om beslissingen mee te nemen, dan hebben we nog steeds het probleem van een tekortschietend model: Door het gebruik verandert de wereld die het beschrijft. En de wereld van het model en om ons heen verandert toch al, autonoom, zo snel dat we het in ons model nauwelijks of niet kunnen bijbenen.
Zelfs in gevallen waar modellen case-based, dus bottom-up worden opgebouwd, is het lastig niet te vervallen in '*reconstructing the ice cube from the water*'. We weten niet of ons model wel het juiste is en alle elementen omvat die ertoe doen en niet meer, met de juiste onderlinge relaties en de juiste sterkten daarvan. Misschien is een heel ander model wel een betere beschrijving van de situatie. En is het beter om doorheen te exerceren en op basis van de uitkomsten dan besluiten uit te nemen.
Maar wellicht is dat model wel in geheel andere termen dan we gewend zijn. We zien al 'taal'verschillen ontstaan tussen de gewone informatiebeveiliging, nog steeds zeer sterk denkend in termen van perimeterbeveiliging, veilig 'binnen' en onveilig 'buiten', en de nieuwe richtingen van informatiebeveiliging zoals rond cybercrime en cyberwarfare of rond social networking als informatiedelings- en samenwerkingsparadigma.

> Vele organisaties zijn naar feitelijke structuur eerder een ruit dan een driehoek

Dit alles leidt tot het 'Turkey before Thanksgiving' fenomeen: Hoe meer we denken dat we modellen hebben die werken, qua voorspelling, hoe meer we in slaap sukkelen en hoe verrassender een crash is. Op financiële markten is aangetoond dat als de volatiliteit terugloopt, dit wordt gezien als een teken dat men eindelijk de markt(en) 'beheerst' – terwijl dat ook juist een teken is dat een grote klap (omhoog of omlaag – meestal het laatste) aanstaande is. Het konijn dat al bijna een jaar lang goed wordt verzorgd, gelooft dat de wereld er is om hem te verzorgen totdat het plots Kerstmis is. Een feest waar het konijn geen benul van had, en heeft, tot de slager toeslaat.
En zo zal het ook gaan met de modelleerders.
Ja maar … Al deze argumenten leiden tot nog toe niet tot het verlaten van modelleerpogingen. Rationeel zien we wel dat die een futiele poging zijn het universum in formules te vangen, maar een irrationele angst drijft ons kennelijk toch

tot pogingen nog wat te redden [Beck, 1997]. Helaas! Misschien zitten we nog te veel vast in de evolutionaire drijfveer van het proberen onze leefomgeving te kunnen voorspellen om preventief de negatieve dingen te kunnen ontwijken en de positieve te kunnen grijpen. Dat lukt om kleine schaal, maar niet op de schaal van complexe en snel veranderende samenlevingen waarin moderne organisaties moeten opereren.

Ja maar … We moeten toch wát …!? Misschien. Maar dan niet met modellen conform de argumenten vóór modelleren zoals weergegeven in het kader. Let ook op argument (quod non) nummer 12. Inderdaad, als we niet oppassen met onze modellen, *mis*leiden we onze interne en externe klanten, door te veel zekerheid en vertrouwen in onze beheersing voor te spiegelen en doordat de uitkomsten van risicomanagement tot de verkeerde beslissingen leidt. We zullen aansprakelijk zijn of in ieder geval worden gesteld voor de gevolgen.

De koppeling van beschermende maatregelen aan kwetsbaarheden en bedreigingen gaat verloren

Meer herder

De conclusie is duidelijk; ook de *middle-out* modelleeraanpak zal niet werken. Laten we daarom als beroepsgroep zelf de zaak ter hand nemen en, omdat ons hart toch ingeeft dat we goed willen doen, informatiebeveiliging bottom-up invullen en organiseren. Meer de herder dus, die zelfstandig de woestenij ingaat, wakend en sturend over de in zijn beheer gegeven informatiekudde. In ons geval ook: Terug naar de kern van de zaak en oplossingen bedenken en maken voor acute problemen, we zijn op onszelf aangewezen. Vooral principles-based denken en praktisch doen dus; de on-

Argument vóór modelleren	**Tegenwerping**
Niets is perfect	Inderdaad, maar weinig is zo imperfect als uw modellen.
De aannames zijn reëel	Nee, een aap met dartspijltjes maakt minder bevooroordeelde aannames
De aannames doen er niet zo toe	Waarom de aannames dan neergezet? En ze doen ertoe anders was er geen model.
De aannames zijn conservatief	Conservatief, ten opzichte van wat? En als de modellen enige realiteitswaarde moeten hebben kunnen de aannames toch beter neutraal zijn? Anders leidt het model tot de verkeerde conclusies.
Dat de aannames fout zijn, is niet te bewijzen	Het is ontstellend veel makkelijker om te bewijzen dat de aannames niet kloppen dan dat te bewijzen (!) is dat ze wel kloppen. Dat geldt ook voor aannemelijkheid. Conform de stelregel: wie stelt, bewijst; dat geldt ook voor aannames.
We doen alleen maar wat iedereen doet	Dus als iedereen in de sloot springt, volgt u?
De beslisser is beter af met ons dan zonder ons	Oh, dus de beslisser is beter af als die wordt misleid..?
De modellen zijn niet helemaal waardeloos	Jawel, want ze misleiden maar onduidelijk is hoe en waar. Of, als wel duidelijk is hoe en waar, dan kan het foute deel van het model worden weggegooid. Horoscopen geven mensen ook een goed gevoel, waarom die dan niet gebruikt?
We moeten ons best doen met de gegevens die we hebben	Garbage in, garbage out. Je best doen kan onvoldoende zijn, zelfs als de gegevens correct zijn. Het universum van inputs is oneindig; hoe bepalen we dan volledigheid?
Men moet aannames doen om vooruit te komen	Ja, maar kies dan de juiste aannames, test rücksichtslos of ze kloppen en bepaal de impact van variatie in de aannames. Ooit gedaan?
De modellen verdienen het voordeel van de twijfel	Hoezo? Het zijn geen babies, het zijn hulpmiddelen. Onvoldoende goed, dan weg ermee, uithuilen en een andere weg inslaan.
Wat is er mis met het gebruik van modellen?	Wat er mis is, is dat ze (zowat) iedereen het bos insturen met des keizers nieuwe kleren. Waarom niet vliegen van Schiphol naar Chicago O'Hare met alleen een kaart van Eelde aan boord? Wie koopt er een auto waarvan alle onderdelen voor de individuele klant zijn herontworpen en de remmen niet zijn getest? Er zijn nog zo veel analogieën…

Argumenten tegen het verwerpen van modellen en hun verwerping (naar: [Taleb, 2008, 2010a])

bruikbare regels zijn formaliteiten die 'moeten' worden genegeerd wanneer het algemeen belang dat eist!

Beginnen bij de basis

Dat begint met ons werk goed doen. Gewoon, eerst doen, en dan anderen laten opschrijven wat we doen. Hoe is het mogelijk dat we na decennia nog steeds blijven hangen in telkens opnieuw geprobeerde 'implementaties' van ITIL en CObIT. Als we dat in één keer goed hadden gedaan, zouden we met wat eenvoudige aanpassingen de stelsel-adepten op afstand (van de werkvloer) hebben kunnen houden. Dan zouden we niet in een situatie zijn beland waarin door anderen top-down processen worden ontworpen en de werkvloer vervolgens, murw van de auditbevindingen, gewoon de procedures volgt die *pennywise and poundfoolish* zorgen voor aardig gevulde dossiers vol aantoonbaarheid en bewijs van procedurevolgen – maar ondertussen vierkante wielen en betonnen zwemvesten opleveren. Maar werken zoals we op basis van decennia aan informatiebeveiligingservaring hebben geleerd effectief te zijn.

En als dat niet kan of mag, laat dan vooral bestuurders maar letterlijk zwart op wit aftekenen dat ze compliance boven effectiviteit stellen. Als de budgetten geen ruimte geven voor en-en, dan is het of-of (hopelijk niet nog minder…), maar zorg dan dat de aansprakelijkheid ligt waar die moet liggen namelijk bij de bestuurder(s) die de keuze maakt.

We hebben nog steeds geen goede methoden om andere dan directe financiële schade te meten

Dat begint ook met een kritische analyse van waar we willen uitkomen. Zoals gesteld, de toekomst is nogal onzeker. We kúnnen gewoonweg niet weten welke problemen we in de al of niet nabije toekomst het hoofd zullen moeten bieden. We kunnen alleen trendlijnen voor de *nabije* toekomst doortrekken en tegelijkertijd zorgen dat we die ombuigen of aftoppen. Waarna we een en ander doorgeven aan dagelijks operations-risicomanagement. (Operational risk management houdt zich bezig met de dagelijkse gang van zaken in risk management; operations-risicomanagement doet het risk management in Operations).

Oppassen niet te veel te goed willen doen

Onderdeel van dit trendspotten en, liefst, pre-emptief in de hand houden, is natuurlijk een goed ontwikkeld gevoel voor 'early warning signals' op basis van goede intel. Oftewel, weten wat er speelt in de wereld, ook al zijn het maar vage kleine signaaltjes in de uithoeken van ons werkterrein. We kunnen onze expertise tonen, en benutten, door al vroeg de signalen op te pikken, voor de massa uit, en hopelijk redelijk accuraat de werkelijke bedreigingen tussen de ruis uit te kunnen pikken. Als we dan maar oppassen niet te veel te goed willen doen:

Het begint ook met beseffen dat we voor informatiebeveiliging helemaal niet te maken hebben met een nieuw probleem. Overtredingen en misdrijven zijn van alle tijden. De vorm lijkt (sic) wellicht nieuw, het optimale resultaat zal dat niet zijn. In de 'gewone' beveiligingssector heeft men al eeuwen ervaring met beveiliging en beheersing van incidenten omdat 100% veiligheid een naïeve fata morgana is. Waarom gaan we daar niet in de leer?

Statistiek helpt maar we gaan er vrijwel altijd verkeerd mee om

Ondanks pogingen, is het nog steeds niet tot 'integrated security' gekomen. Misschien doordat we een andere taal spraken, vanuit andere grondgedachten (totale of totalitaire beheersing in plaats van 'containment' en inperking), misschien ook omdat we dachten te speciaal te zijn. Dat zou ten onrechte zijn. We worden beter in ons eigen vak door toe te geven dat we nog niet goed genoeg zijn.

Op weg naar huis

Nodig is dus vooral inzicht in wat we nog niet goed doen en in welke richting we het moeten zoeken. Dit artikel wil daartoe een aanzet geven. Maar er zal nog heel wat out of the box denken nodig zijn om oplossingen te bedenken. En we zullen met z'n allen nog heel wat aan onze communicatieve vaardigheden moeten doen om aan te sluiten bij (niet op) de anderen, onze klanten, om effectief te kunnen zijn en dat uit te kunnen leggen.

Vanaf de werkvloer de control op-bouwen

Dat betekent dus een terugkeer naar de basis. Daar kan het best goed toeven zijn! Laten we dus weer de gewone problemen gewoon oplossen zonder zo nodig eerst te pogen al ons werk in processen of zo te gieten. Laten we van wat we doen, case-based, bottom-up processen bouwen, om de eeuwige problemen aan te pakken met een goeie mix van preventieve én andere, vaak vergeten maatregelen [Schwartau, 1999]. Laten we, in dit tijdsgewricht waarin de nadruk ligt op de veroudering van het denken in grote command-and-control bureaucratieën met het opgroeien van veel kleinere netwerkorganisaties, vooral de focus houden op het bottom-up vorm geven, niet top-down afdwingen, van onze eigen toekomst.

Bovenstaande kan sommigen provocatief en kort door de bocht overkomen. Dan is de opzet geslaagd. En bedenkt: Met alleen brave verhalen komen we niet verder. En/of vindt de lezer het lastig te worden gewezen op het falen van bewusteloze volgzaamheid? Auteur ontvangt zeer gaarne opbouwende (!) kritiek, toevoegingen en aanvullingen. Zo kunnen we gezamenlijk helderheid geven. Alleen gezamenlijk kunnen we na de these van meehobbelen met de massa richting ravijn en de antithese van betrokken actievoerders, komen tot een synthese die de informatiemaatschappij mede vormgeeft.

Ondanks pogingen, is het nog steeds niet tot 'integrated security' gekomen

Literatuur

U. Beck, U., De wereld als risicomaatschappij, De Balie Amsterdam 1997

Kahnemann, D., Thinking, Fast and Slow, Penguin London 2012

Power, M., The Audit Society, Rituals of Verification, Oxford University Press 1997

Power, M., Organized Uncertainty, Oxford University Press 2008

Schneier, B., Liars & Outliers, Wiley, Indianapolis 2012

Schwartau, W., Time Based Security, Interpact press, Seminole 1999

Taleb, N.N., Fooled by Randomness, Random House, New York 2008

Taleb, N.N., The Black Swan, Random House, New York 2nd edition 2010

Taleb, N.N., The Bed of Procrustes, Random House, New York 2010

OPEN EINDE

Henk-Jan van der Molen is als docent verbonden aan de Hogeschool Wageningen. Hij doceert binnen de opleiding Bedrijfskundige Informatica onder meer: Business Intelligence, Informatiebeveiliging en Verandermanagement. Vanuit zijn praktijkervaringen heeft hij diverse artikelen gepubliceerd in bladen zoals Computable, Informatiebeveiliging, ISACA Journal en het NRC. Hij is te bereiken via hjvdmolen@gmail.com.

Alles in deze tekst is fictie, behalve de feiten over Open Standaarden.

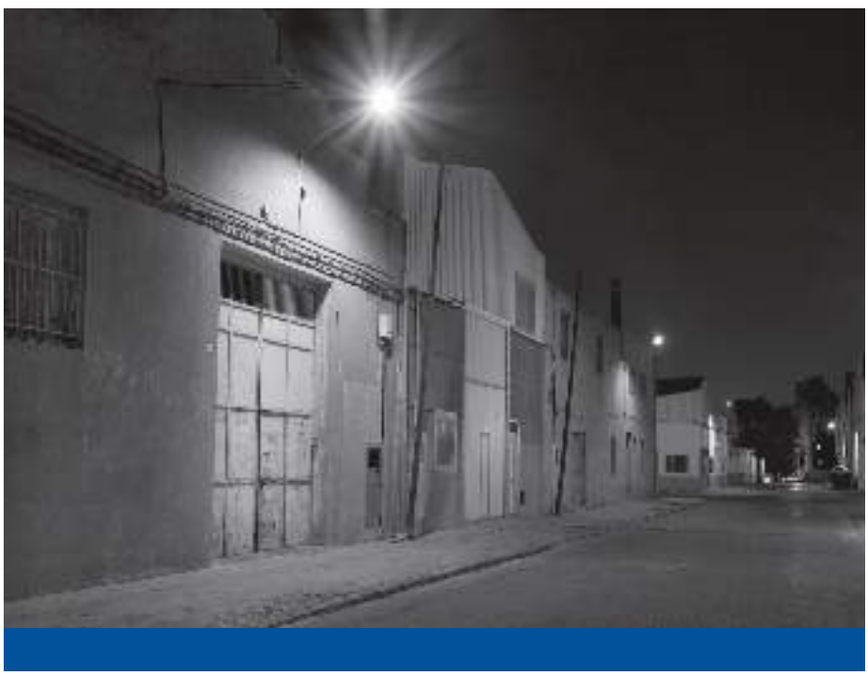
2016, 19 december 05:25
Van Woustraat, Amsterdam
"AT in positie" klinkt het blikkerig in de beveiligde intercom. De springstofexpert van het arrestatieteam kruipt behoedzaam onder het raam door en plakt snel het slagkoord vast aan het deurkozijn. De twee agenten aan weerskanten van de deur pakken elk een flashbang. Het is pikdonker in de straat, vanwege het door de politie 'geplande' onderhoud aan de straatverlichting. Met hun *Enhanced Vision* brillen zien de teamleden hun leider drie vingers opsteken, dan twee, één en dan zwaait zijn arm omlaag. Bijna tegelijkertijd valt met een droge knal de deur, inclusief kozijn, plat op het trottoir. "Go, Go, GO!" Met hun Heckler & Koch wapens in aanslag golft het arrestatieteam als een waterval naar binnen. Twee oogverblindende flitsen met harde knallen volgen. Uit de woning klinkt op verschillende plaatsen "Police! Show me your hands!" en kreten van woede en angst. In één kamer gaat het schreeuwen door, totdat er twee schoten klinken.
"Onder controle", hoort de leider AT in zijn oor. "Gewonden?" vraagt hij gespannen. "Eén arrestant licht gewond, geen ambulance nodig". In verschillende woningen in de buurt gaan de lichten aan. De leider geeft opdracht de arrestanten geboeid en geblinddoekt af te voeren naar separate locaties. "Opschieten! Ik wil weg voor de pers er is. En geen fouten, de politiek kijkt vandaag mee."

2016, 20 december 09:24, op een geheime locatie in Amsterdam Zuidoost
Buiten waait de sneeuw tegen de geblindeerde ramen. Binnen hangt een kale gloeilamp aan het plafond en tikt de oude verwarming. Commissaris Peter Both van het Korps Nationale Politie wacht op de laatste verdachte. De arrestatie gisteren was de kroon op het lange onderzoek van het Team High Tech Crime binnen het KNP. Het Nationaal Cyber Security Centrum had overigens het leeuwendeel bijgedragen aan de arrestatie van de bende gisteren. Maar er waren ook dingen grandioos misgegaan.
De politie kreeg begin vorig jaar een tip dat de cyberbende elke week in Amsterdam steeds in een ander Indiaas restaurant ging eten. Na een streng geheim gehouden onderzoek volgde een spectaculaire inval in het restaurant Taj Mahal. Toen bleek dat de 'tip' niet waar was, had de pers de bende daarna "Cash & Curry" genoemd. Kort daarna had Peter onverwacht het commando gekregen over de cybercrime unit en de leiding over het onderzoek naar deze bende.
"Peter!" Hij schrikt op uit zijn mijmeringen en kijkt Chris de Vries aan, die als digitaal rechercheur deels werkt bij het Nationaal Cyber Security Centrum. Ze knipoogt. "Nachtje doorgehaald? Wil je zo meteen zijn dossier erbij?"
Peter rekt zich geeuwend uit. "Nog niet. Tot dusver heeft geen enkele verdachte iets losgelaten. Deze arrestant heeft speciaal naar de leider van het onderzoek gevraagd. Ik wil eerst horen wat hij te zeggen heeft."
De arrestant wordt binnengereden in een rolstoel, snurkend met een raspend geluid. Met handboeien om zijn polsen en een provisorisch verband om zijn linker kuit, waar hij werd getroffen door een politiekogel. De leider van het arrestatieteam had verklaard dat de man

weigerde zijn wapen neer te leggen. Chris maakt aanstalten om de verdachte te wekken. "Voorzichtig!" zegt Peter. Chris antwoordt rustig: "Zwarte band judo" en schudt aan zijn schouder. Geen reactie, zelfs na nog een keer schudden gaat het snurken door. De lachrimpels van Peter verdiepen zich. "Chris, als jij eens een emmer water gaat halen". Even later komt ze terug met een prullenbak half gevuld met water. Op dat moment houdt het snurken abrupt op en gaat de man recht in zijn rolstoel zitten. Hij opent zijn ogen en kijkt Peter direct aan.
Peter start de recorder, zegt de datum en tijd en vraagt "Who are you? Wie ben je?" De man antwoordt in vlekkeloos Nederlands. "Later zal ik mezelf identificeren, maar voorlopig wil ik anoniem blijven."
De man gaat verder: "Voordat we beginnen, wil ik in Nederland politiek asiel aanvragen. Binnen enkele uren verwacht ik dat de Bulgaarse regering Nederland zal vragen mij uit te leveren. Daar zit de leider van de bende achter, die ik jullie gisteren in handen heb gegeven. Hij heeft veel invloed in Bulgarije. Tijdens mijn proces wordt de rechter omgekocht en krijg ik de doodstraf – als ik geluk heb."
Peter fronst zijn wenkbrauwen: "Je bent een informant? Ik neem aan dat je dat kunt bewijzen. Ik zal je asielaanvraag straks doorgeven aan de Immigratiedienst. Eerst moet je ons het complete verhaal vertellen. Als ik merk dat je liegt, zorg ik er voor dat je Nederland uit wordt gezet."
De man knikt kort en begint te vertellen.

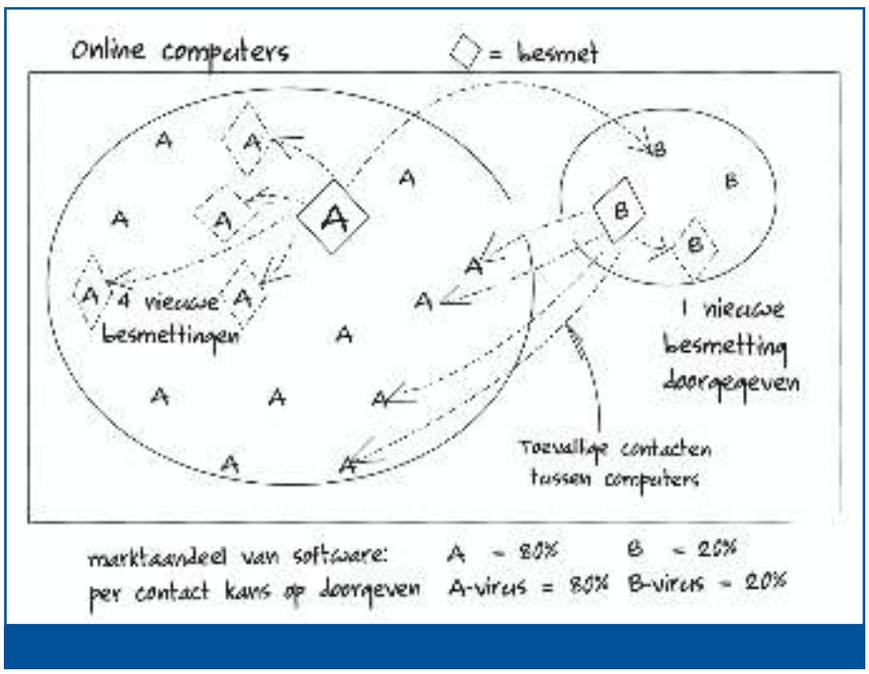
2016, 20 december 10:13, Den Haag
"Spreek ik met de ambassadeur?"
"Daar spreekt u mee. Waarmee -"
"Luister goed. Ergens in Amsterdam wordt een voormalig lid van onze Geheime Dienst vastgehouden. Die persoon moet onmiddellijk terug naar Bulgarije, hij mag geen gevoelige informatie doorspelen naar de Nederlandse autoriteiten."
"Duidelijk. En als Nederland die persoon niet wil uitleveren?"
"Voor die situatie sturen we iemand van ons mee. We weten binnen één uur waar onze landgenoot wordt vastgehouden. Zorg dat er dan een diplomaat klaar staat om hem op te halen."

2016, 20 december 10:14, op de geheime locatie in Amsterdam Zuidoost
Enkele jaren geleden is de man bij de bende gekomen toen de Bulgaarse geheime dienst werd afgeslankt. Met zijn universitaire IT-kennis en zijn cybertools kon hij de toenmalige leider van bende snel imponeren door in 30 minuten het e-mailaccount en de voicemailbox van een Amsterdamse officier van Justitie te kraken.
"We gingen naar Nederland omdat er veel computers met breedbandverbindingen in gebruik zijn, die bovendien bijna allemaal werken met dezelfde software. De meeste organisaties standaardiseren op de marktleidende software, omdat ze denken dat ze door schaalvergroting kosten kunnen besparen. Ze negeren daarbij de kosten van cyber incidenten. Veel computers met dezelfde software is gunstig voor ons, omdat we dan met één virus alle machines kunnen besmetten. We verdienden veel geld met het versturen van spam, computervirussen en afpersing van organisaties en personen, bijv. met bedrijfsgeheimen of buitenechtelijke relaties. Zoals met die politicus vlak voor de verkiezingen van 2010, daar hebben we aardig aan verdiend. Zelfs als er geen gênante informatie op een computer staat, dan kunnen we altijd gevoelig materiaal uploaden en dreigen de politie te tippen, dan wordt er meestal grif betaald."
"De computers van mensen thuis lijken me gemakkelijk te hacken. Maar bedrijven hebben toch meestal een goede beveiliging?", vraagt Peter.
"Beveiliging wordt minder effectief door de enorme groei van cybercrime. Antiviruspakketten lopen steeds meer achter en detecteren nog maar maximaal 70% van de nieuwste virussen. Dergelijke standaard beveiligingsmaatregelen maken het hooguit ietsje moeilijker om computers te besmetten. We testen nieuwe virussen uitgebreid om te voorkomen dat ze snel worden gedetecteerd, anders genereert zo'n virus voor ons geen inkomsten meer. In 2011 is in een Europees onderzoek vastgesteld dat bijna alle Nederlandse computers dat soort beveiligingsmaatregelen had, maar dat Nederland met 23% besmettingen toen nog middelmatig scoorde. Maar onze inkomsten verminderden doordat het gebruik van Open Standaarden in 2012 binnen Nederland een grote vlucht nam."



"Open Stand... Wat heeft dat er nou mee te maken?", valt Peter hem geïrriteerd in de rede.
De man knipoogt naar Chris. "Hieruit blijkt dat jouw gebrek aan visie op IT-gebied gecompenseerd moet worden… door je collega?"
Chris glimlacht en Peter wordt rood in zijn gezicht: "Zegt de visionair die door de politie is neergeschoten en gearresteerd!"
"Dat heb ik zelf zo opgezet, maar dat vertel ik later. Laat ik het simpel uitleggen. Alle software bevat kwetsbaarheden die inbreken mogelijk maakt. Waarom denk je dat er veel meer virussen in omloop zijn voor bijvoorbeeld het Windows platform en minder voor Linux?"
"Waarom Windows de meeste virussen heeft? Da's makkelijk, dat komt natuurlijk door het grote marktaandeel. Maar ook al is Linux beter dan Windows, als Linux net zoveel marktaandeel krijgt als Windows, volgen de virussen vanzelf."
"Met dat rookgordijn vliegen veel mensen uit de bocht", merkt de man op. "Het gaat namelijk helemaal niet over Windows versus Linux, of de Mac. Het gaat om keuzevrijheid. Of liever gezegd, het GEBREK aan keuzevrijheid."
Peter kijkt hoopvol naar Chris, die kucht: "Vandaar die Open Standaarden?"
De man verzet zijn gewonde been en trekt een grimas. "Precies! Computergebruikers zullen pas veranderen van software, als ze zich niet druk meer hoeven te maken over uitwisseling van data en vertrouwen hebben in de alternatieve software. Hoe meer verschillende software wordt gebruikt, hoe meer het risico van cybercrime wordt gespreid. In Nederland gaf de overheid in 2012 het goede voorbeeld door zoveel mogelijk voor Open Standaarden te kiezen en op het gebruik daarvan actief te sturen. Bovendien zorgde de bezuinigingen ervoor dat de overheid waar mogelijk overschakelde naar gratis Open Source software. Leveranciers van betaalde software schreeuwden natuurlijk moord en brand, maar het viel politiek niet te verkopen veel ambtenaren te ontslaan, terwijl er miljoenen voor software wordt uitgegeven als gratis software ook voldoet.
Na dit voorbeeld van de rijksoverheid volgden de vitale sectoren en het bedrijfsleven op enige afstand. Daardoor verminderde de software monocultuur in Nederland langzamerhand."
Peter leunt achterover. "Net zei je dat er in Nederland op zoveel computers dezelfde software draait. De marktaandelen van software in Nederland zijn de afgelopen jaren nauwelijks veranderd. Moet ik geloven dat zoveel mensen in zo'n korte tijd allemaal van software zijn veranderd?"
"Met een wiskundig model voor de verspreiding van virussen kun je uitrekenen dat iets meer softwarediversiteit de verspreiding van virussen al effectief verhindert. Als meer mensen migreren naar niet marktleidende software dan er virusbesmettingen zijn, dan sterven volgens de theorie alle virusbesmettingen uit."
"Ja, dat zou kunnen. En wat dan nog? Zelf al veranderen sommige mensen van bijvoorbeeld Windows naar de Mac, dan kun je daar nog steeds virussen voor ontwikkelen?"
De man rolt zijn rolstoel dichter naar de tafel en zegt: "Dat kan wel, maar OF dat ook gebeurt is afhankelijk van het marktaandeel van die software. Ik kan het voor je uittekenen."

Peter haalt een plastic pen uit zijn colbert en schuift die met een vel papier over de tafel naar de man. De man begint te tekenen en legt tegelijkertijd uit. "Kijk, het kopen of ontwikkelen van een virus kost ongeveer evenveel geld, welk platform je ook kiest. Dat geld kan je terugverdienen als het virus niet voortijdig uitsterft. Hoe groter het marktaandeel is van het platform dat het virus aanvalt, hoe kleiner die kans is."
"De computers binnen dezelfde cirkel gebruiken dezelfde software. Andere cirkel betekent andere software. Stel, software A heeft in de grote cirkel een marktaandeel van 80% en software B in de kleine cirkel 20% marktaandeel."
De man wijst op het papier. "In principe kan een besmette A-computer geen B-computers besmetten en vice versa. Alleen als een besmette computer toevallig contact maakt met andere computers in dezelfde cirkel, kan het virus zich vermenigvuldigen. Daarnaast heeft elke besmette PC een bepaalde kans om zijn besmetting kwijt te raken, bijvoorbeeld met antivirussoftware. Als je aanneemt dat bij een contact tussen A-computers de kans op besmetting en ontsmetting even groot is als voor B-computers, dan…"



2016, 20 december 10:45
Amsterdam, de Beurs van Berlage
De woordvoerder van het Korps Nationale Politie opent de persconferentie en geeft aan dat er eerst een korte verklaring zal volgen over het oprollen van de bende die bekend staat als "Cash & Curry". Daarna is er ruimte voor vragen.
Gisterochtend vroeg is de bende ingerekend, na een gecombineerde actie van het KNP en de Politie Regio Amsterdam. Deze bende hield zich sinds 2010 in Nederland bezig met het verspreiden van computervirussen en het versturen van spam. Daarnaast verkochten ze gevoelige informatie van de computers die ze met virussen hadden besmet en werden mensen en bedrijven daarmee afgeperst.
In een bijna twee jaar durend politieonderzoek zijn diverse tips gecombineerd met digitale recherche, wat uiteindelijk tot de arrestatie gisteren heeft geleid. Vooralsnog bekend zijn alle vijf de bendeleden ingerekend, die voornamelijk van Oost Europese afkomst zijn. Bij de arrestatie van de bende zijn enkele pc's, verschillende wapens met munitie en ca. 3,3 miljoen euro aan contant geld in beslag genomen.

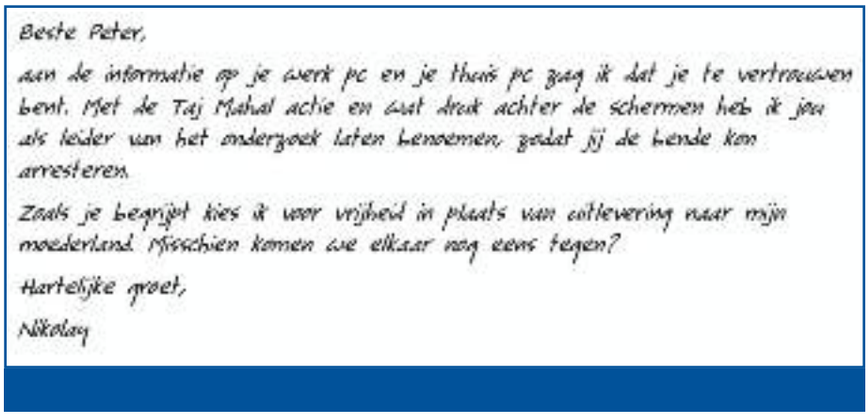
2016, 20 december 11:03, op de geheime locatie in Amsterdam Zuidoost
Nadat ze de uitleg een poosje nadenkend had gevolgd, brak Chris in: "Ik snap het! Van elke 5 contacten tussen computers zijn er 4 met 'A' en maar één met 'B'. Omdat de kans op ontsmetting voor 'A' en 'B' even groot is, maar er veel minder besmettingen voor 'B' worden doorgegeven, zal het B-virus dus veel sneller uitsterven. Omgekeerd is de kans veel groter dat een 'A'-besmetting wordt doorgegeven."
De man kijkt Chris goedkeurend aan. "Juist. Het maximale aantal besmettingen is een evenwicht tussen de kansen voor besmetting en ontsmetting. Daarom maximaliseert een monocultuur het risico van cybercrime: als het merendeel van de mensen marktleidende software gebruikt, is de kans dat je een virus oppikt maximaal. De kans is groot dat deze besmetting vervolgens kan worden doorgegeven aan alle computers met dezelfde software. Dus kans maal impact is maximaal, waardoor een samenleving kwetsbaar wordt."
Peter merkt op: "Dat inzicht bestaat in de landbouw al veel langer. Percelen met hetzelfde gewas mogen niet te groot zijn en niet met elkaar verbonden zijn om ziektes en plagen tegen te gaan. Maar volgens mij is in Nederland de schade door cybercrime van 2012 tot 2016 niet gedaald."
De man schudt zijn hoofd. "Als je de Nederlandse cijfers over de groei en de omvang van cybercrime vergelijkt met de rest van Europa, dan zie je dat veel andere landen jaloers zijn op de Nederlandse situatie. Bijna overal groeit de schade door cybercrime veel sneller."
De man vervolgt: "Doordat in Nederland het rendement van virussen relatief minder werd, gingen we ons steeds meer richten op Engelstalige landen. Maar we moesten steeds harder concurreren met andere cyberbendes. Ongeveer een jaar geleden was er een bende die onze gehackte computers probeerde over te nemen. Ze bleken zich ook bezig te houden met mensenhandel en het verspreiden van porno... ook van jonge kinderen."
"Hoeveel ellende een dergelijke uitbuiting veroorzaakt, heb ik van dichtbij gezien." Met een donkere blik in zijn ogen wrijft de man langzaam in zijn handen. "Misschien loop ik er nog eens eentje tegen het lijf... Ik heb de computers van die bende gekraakt en kwam zo achter

hun locatie en alle wachtwoorden van hun computers. Daarna heb ik die per brief doorgegeven aan de politie."
Peter herinnerde zich dat deze tip in het dossier zat. Op basis hiervan had zijn team vorig jaar verschillende computers in beslag genomen en meegenomen voor onderzoek. Met een geheime, Europees gecoördineerde actie waren veel criminelen en 'klanten' gearresteerd, waarvan een groot aantal kon worden vervolgd met het bewijsmateriaal op deze computers.
"Om meer inkomsten te genereren wilde onze bendeleider daarna de mensenhandel van deze bende overnemen. Afscheid nemen van de bende bleek voor mij geen optie. Toen heb ik besloten de bende in handen van Justitie te geven. Sinds een jaar heb ik de politie e-mails gestuurd met daarin verborgen boodschappen. In mijn laatste boodschap gaf ik aan dat alle bendeleden gisteren in de Van Woustraat verbleven, zodat jullie iedereen konden arresteren."
Peter wist dat de politie sinds een jaar spottende e-mails van een niet-bestaand afzenderadres ontving die waren 'ondertekend' met steeds een andere afbeelding van een curry-gerecht. Net begonnen aan haar stage bij het Nationaal Cyber Security Centrum, had Chris na drie mailberichten de verborgen boodschappen in die afbeeldingen gevonden. De boodschappen bevatten bewijzen over de criminele activiteiten van de bende, waarbij een aantal transporten van mensenhandelaren kon worden onderschept. Het verhaal van de man zou kunnen kloppen, maar zijn verhaal vormt nog geen bewijs. Zijn medewerking is echter essentieel om het hele verhaal boven water te krijgen.

2016, 20 december 11:09
Amsterdam, de Beurs van Berlage
Na de verklaring van de politie is de beurt nu aan de verzamelde pers.
De eerste vraag: "De bende was al sinds 2010 operationeel in Nederland en de aanwijzing die leidde tot aanhouding van de bende was gevonden in een e-mail van twee weken terug. Waarom duurde het zo lang voordat de bende kon worden opgerold?"
De woordvoerder geeft aan dat het KNP jaren nodig heeft gehad om de bende op te sporen en de zaak qua bewijsvoering sluitend te krijgen, omdat de bende met professionele beveiligingskennis hun sporen wiste. Zo werd de communicatiestandaard vercijferd en werden de gehackte computers bestuurd via snel wisselende servers in het buitenland. Pas na diverse tips van een infiltrant het afgelopen jaar is de zaak in een stroomversnelling geraakt.
De volgende vraag vanuit de zaal. "Had de infiltrant de boodschappen ook ondertekend?" Het antwoord: "Ja, met de naam Nikolay, wat zo goed als zeker een schuilnaam is."

Gelijktijdig, op de geheime locatie in Amsterdam Zuidoost
"Waarom wilde je tijdens de arrestatie je wapen niet neerleggen?" vroeg Chris.
"Drie maanden geleden betrapte de bendeleider mij toen ik zo'n e-mail naar de politie stuurde. Hij wilde dat ik daarmee stopte. Met jullie inval zag de bendeleider zijn eerdere wantrouwen tegen mij in één klap bevestigd. Omdat hij gewapend was, moest ik hem onder schot houden totdat hij zijn pistool had losgelaten. Hij had me anders neergeschoten."
Peter doet zijn armen over elkaar. "Ik heb nog geen snipper bewijs gezien dat jij de rol van infiltrant hebt ingevuld. Als je inderdaad infiltrant bent, leidt dat mogelijk tot strafvermindering en misschien wel tot politiek asiel. Zonder dat bewijs word je veroordeeld als lid van een criminele organisatie. Wat kun je ons nog meer vertellen?"
Op dat moment worden de persoonlijke bezittingen van de man de verhoorruimte ingebracht: een portefeuille met een afgescheurd stuk papier erin, waarop de naam Nikolay staat geschreven. Chris pakt fronsend het papier op en legt dat naast het bewijsstuk uit de zaak van een jaar geleden waarop de wachtwoorden van de computers waren geschreven. De scheurranden blijken perfect aan te sluiten. Daarnaast is het handschrift op het bewijsstuk en de toelichting van de man identiek. Chris neem Peter apart en zegt zachtjes: "Hij moet Nikolay zijn."
Veel tijd om hierover na te denken krijgen Peter en Chris niet. De gsm van Peter gaat over. Er is een team van de Bulgaarse ambassade gearriveerd en wil de arrestant direct meenemen. Met een wrang gevoel loopt Peter naar de ingang en ziet dat het team bestaat uit een dunne man gekleed als een diplomaat en een breedgeschouderde man met

gemillimeterd haar en indringende ogen. "De verdachte wordt momenteel nog verhoord. U kunt deze persoon dus nog niet meekrijgen", probeert Peter. De diplomaat glimlacht flauwtjes en geeft hem een briefje. "Belt u dat nummer alstublieft. We hebben haast." Peter belt en heeft daarop vrijwel direct de directeur-generaal Internationale Samenwerking aan de lijn. Hij geeft Peter opdracht de arrestant onmiddellijk over te dragen aan het team voor uitlevering aan Bulgarije, vanwege misdaden daar gepleegd. Peter werpt tegen dat de arrestant zojuist politiek asiel heeft aangevraagd. Bovendien lijkt de man kennis te bezitten die zeer waardevol is in het politieonderzoek. Na drie minuten heen en weer gepraat wordt het gesprek geforceerd beëindigd, terwijl het team steeds ongeduldiger wordt. "De uitlevering is al afgestemd met uw baas en het OM. Als u niet meewerkt, dan laat ik de zaak binnen een kwartier overdragen aan iemand anders."


Beste Peter,

aan de informatie op je werk pc en je thuis pc zag ik dat je te vertrouwen bent. Met de Taj Mahal actie en wat druk achter de schermen heb ik jou als leider van het onderzoek laten benoemen, zodat jij de bende kon arresteren.

Zoals je begrijpt kies ik voor vrijheid in plaats van uitlevering naar mijn moederland. Misschien komen we elkaar nog eens tegen?

Hartelijke groet,

Nikolay

Als Peter het overdrachtsdocument wil tekenen, merkt hij dat hij zijn pen mist. Hij ondertekent met een geleende pen en loopt met het team van de diplomatieke dienst terug naar de verhoorruimte. Als ze de deur openen, hangt Chris happend naar adem met handboeien vastgeketend aan de verwarmingsbuis. Ze fluistert hees: "… Slag tegen mijn keel... Nikolay… Handboeien los…" Op tafel ligt de pen waar de metalen clip van is afgebroken. Peter ziet uit zijn ooghoeken op zijn stoel de volgende boodschap, geschreven op de achterkant van het papier.

Terwijl hij de boodschap camoufleert door erop te gaan zitten, tuimelen allerlei gedachten door Peters hoofd. Was de Nikolay indertijd wel ontslagen bij de Bulgaarse Geheime Dienst? Heeft hij zich misschien schuldig gemaakt aan spionage in Nederland? En ... Door het open raam waait sneeuw de kamer in, de voetstappen buiten al bijna gewist.

DE TRUST AUDIT VOOR KWALITEITSBEHEERSING VAN UW ICT-KETEN

Dr. Ir. Harrie Bastiaansen is senior consultant bij TNO op het gebied van IT-besturing en enterprise architectuur. Daarnaast is hij opgeleid IT-Auditor (EUR). Hij is gastdocent aan de Technische Universiteit Delft. Hij is te bereiken via harrie.bastiaansen@tno.nl.

Bij ICT-ketens is het een utopie om kwaliteitsbeheersing uit te oefenen door controle en inspectie van de implementatie van alle ketenpartners in de gehele keten. Als alternatief komt 'vertrouwen in ketenpartners' dan om de hoek kijken. Dit artikel gaat daarom in op de trust audit voor het vaststellen van de mate waarin vertrouwen in ketenpartners kan worden gesteld. De trust audit geeft ketenpartners, toezichthouders en auditors een alternatief en extra instrument om de kwaliteitsbeheersing van ICT-ketens te beoordelen.

Bij ICT-ketens gaan ICT-diensten en -infrastructuren over de grenzen van bedrijven en bedrijfsonderdelen heen. Niet alleen neemt het aantal ICT-ketens sterk toe, ook worden ze steeds complexer: ze ondersteunen meer functionaliteit en er zijn steeds meer partijen (ketenpartners) betrokken. Met het toenemend belang van ICT-ketens neemt ook het belang toe van de kwaliteitsbeheersing daarvan. Echter, bij ICT-ketens kan controle en inspectie van de implementatie van alle ketenpartners in de gehele keten praktisch onuitvoerbaar zijn. Een (strikte) 'line of command' is namelijk niet een gegeven, de span of control voor individuele organisaties is beperkt tot slechts een aantal schakels in de keten en de ketens zijn te uitgebreid om (in doorlooptijd en budget) alles te controleren. Het is nodig om te grijpen naar alternatieve aanpakken. De trust audit is zo'n potentieel alternatief.
De trust audit is een instrument voor het vaststellen van de mate waarin vertrouwen in ketenpartners kan worden gesteld. Met haar resultaten kan de verdere controle-aanpak worden aangepast (en hopelijk, qua belasting voor de betrokkenen, ingeperkt) en kunnen uitspraken worden gedaan over de kwaliteitsbeheersing van ICT-ketens.

In dit artikel wordt de normatiek van trust audits geïdentificeerd (hoofdstuk 2) en worden potentiele rollen ervan bij de kwaliteitsbeheersing van ICT-ketens benoemd (hoofdstuk 3).

Wat is een trust audit?
Zoals in de inleiding toegelicht speelt vertrouwen een steeds grotere rol in de kwaliteitsbeheersing van ICT-ketens.

> Het aantal ICT-ketens neemt sterk toe, ook worden ze steeds complexer: ze ondersteunen meer functionaliteit en er zijn steeds meer partijen (ketenpartners) betrokken

In dit artikel bedoelen we hiermee het vertrouwen dat organisaties in elkaar hebben dat ze de in hun gestelde kwaliteitsverwachting nakomen; het zogenaamde inter-organisatorisch vertrouwen, of kortweg 'trust', met als definitie:

"Inter-organisatorisch vertrouwen ('trust') is de (subjectieve) mate waarin organisaties in de keten worden beoordeeld op de verwachting dat ze zullen voldoen aan de kwalitatieve verplichtingen van hun dienstverlening, onafhankelijk van de omstandigheden."

Een trust audit is het instrument om de mate van inter-organisatorisch vertrouwen volgens deze definitie vast te stellen. Deze definities sluiten goed aan bij de definities van 'Organizational Trust' zoals door het IIA (het Institute of Internal Auditors) gebezigd [IIAResearch]. Zoals de definitie weergeeft, heeft vertrouwen ('trust') per definitie iets subjectiefs in zich. Het heeft betrekking op aspecten die niet objectief vastgesteld kunnen worden, en die niet volledig voorspelbaar zijn. Trust en vertrouwen beginnen daarbij waar de kennis ophoudt. Dit lijkt daarom slecht verenigbaar met het instrument van een trust audit met als doel de betrouwbaarheid van ketenpartners op een zo objectief mogelijke manier vast te stellen en de gevoelsmatige beleving uit te schakelen.
De trust audit kan daarom bij eerste aanblik op gespannen voet lijken te staan met de aanpak in de traditionele auditing wereld waar het beeld heerst dat beheersing en zekerheid ('assurance") strikt gebaseerd zijn op objectieve vaststelling met als adagium 'Vertrouwen is goed, controle is beter'. Zoals in de inleiding aangegeven en verder toegelicht in het volgende hoofdstuk, heeft de trust audit wel degelijk een rol te vervullen in de kwaliteitsbeheersing van ICT-ketens.

Normatiek voor trust audits
In de literatuur wordt al veel aandacht besteed aan het belang van onderling vertrouwen voor het onderhouden van inter-organisatorische samenwerking. Er is echter nog geen eenduidig beeld over

de wijze waarop dit vertrouwen gemodelleerd, geoperationaliseerd en gemeten kan worden [SEPPANEN]. Normatiek voor een trust audit is beperkt, alhoewel [ROSIELLE] een initiele aanzet hiervoor. De kwaliteit van de normatiek wordt bepaald door haar volledigheid en de mate waarin ze subjectiviteit in de beoordeling van de betrouwbaarheid van ketenpartners weghaalt. Voor de normatiek van trust audits sluiten we aan bij een aanpak die oorspronkelijk gericht is op vertrouwen binnen voedselketens [CANAVARI]. De aanpak gaat uit van het perspectief van de afnemer van een ICT-dienst bij een ketenpartner, omdat deze afnemer te maken heeft met informatie asymmetrie over de af te nemen ICT-dienst.

Trust en vertrouwen beginnen waar de kennis ophoudt

De normatiek voor trust audit onderscheidt drie 'aspecten':
- de ICT-dienst;
- de dienstaanbieder;
- het marktsegment.

Het is op dit punt goed even stil te staan bij deze driedeling. Eigenlijk zou kwaliteitsbeheersing van 'alleen maar' de aangeleverde ICT-dienst volstaan. Maar, omdat je dit bij ICT-ketens niet door controle op de implementatie bij ketenpartners kunt vaststellen, vervullen hiervoor de aspecten 'dienstaanbieder' en 'marktsegment' een indirecte rol.
Voor het identificeren van de normen is een twee-staps aanpak gevolgd. In de eerste stap ('bottom-up') zijn bestaande normen voor inter-organisatorisch en interpersoonlijk vertrouwen beschouwd op toepasbaarheid voor ICT-ketens. Ten behoeve van volledigheid van de normatiek zijn in de tweede stap ('top-down') aanvullende normen per aspect geïdentificeerd.

De kwaliteit van de normatiek wordt bepaald door haar volledigheid en de mate waarin ze subjectiviteit in de beoordeling van de betrouwbaarheid van ketenpartners weghaalt

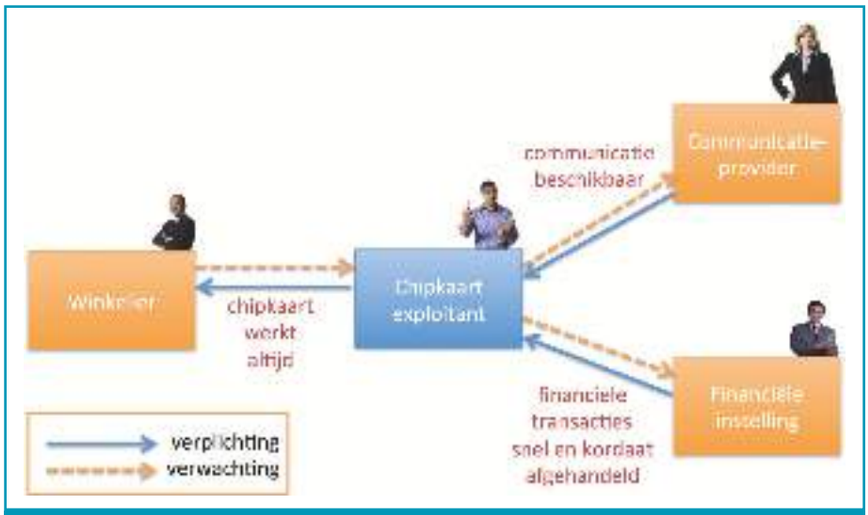
Tabel 1 geeft als resultaat de onderwerpen waarop normen zijn benoemd, met een verdere categorisering per aspect. De omvang hiervan laat niet toe dit in dit artikel over te nemen. Hiervoor verwijzen we naar [BASTIAANSEN1].

Een natuurlijke en voor de hand liggende rol voor de trust audit is om als onderdeel van een reguliere risicoanalyse in de ICT-keten de vraag te beantwoorden of een ketenpartner in voldoende mate kan worden vertrouwen op de geleverde kwaliteit van zijn toeleveranciers om de verwachtingen aan zijn deel van de dienstverlening waar te kunnen maken. Dergelijke risico-analyses maken bijvoorbeeld deel uit van het procuratieproces en het proces van kwaliteitsmanagement (met als vraagstelling of aanvullende

De ICT-dienst	De dienstaanbieder
Dienstaanbod • kwaliteit dienstbeschrijving • wijze van afspraakvorming **Dienstafhankelijkheid** waarde van de dienst voor afnemer financiële compensatie aan afnemer bij niet nakomen van verplichtingen **Beoordeling van dienst** historische reputatie van de dienst onafhankelijke beoordelingen en audits op ICT-dienst	**Leveranciersafhankelijkheid** • functionele symmetrie: in afhankelijkheid van de dienstverlening tussen leverancier en afnemer • financiële afhankelijkheid: van de toeleverancier aan de afnemer van het volgens afspraak leveren van de dienst. • typologie: open (ad hoc en vluchtige) of gesloten (langdurige en stabiele) relatie **Openheid** • transparantie m.b.t. operationele processen en incidenten • invloed van de afnemer op de dienstaanbieder • realistische communicatie door dienstaanbieder • gericht op verbetering van dienstaanbieder
Het marktsegment	**Omvang van de infrastructuur** • aantal componenten in de infrastructuur • aantal 'achterliggende' toeleveranciers van de infrastructuur • kwetsbaarheid van de infrastructuur • Beoordeling van dienstaanbieder • historische reputatie van dienstaanbieder • beoordelingen en audits op dienstaanbieder • afspraken over geschakeld vertrouwen
Toezicht • extern toezicht op marktsegment • intern toezicht binnen marktsegment **Beoordeling van marktsegment** • historische reputatie van marktsegment • transparantie in marktsegment	

Tabel 1

interne compenserende maatregelen nodig zijn).
Aanvullend hieraan beschrijven de volgende paragrafen van dit hoofdstuk een aantal specifiekere rollen voor de trust audit bij de beoordeling van kwaliteitsbeheersing van ICT-ketens, te weten: geschakeld vertrouwen, risicobeheer en kwantificatie van ketenkwaliteit.



Figuur 1 - Verwachtingen en verplichtingen voor een chipkaartexploitant

Geschakelde keten van vertrouwen
Voor een partij in de ICT-keten is het optimaal als hij kan vertrouwen op de kwaliteitsafspraken met zijn directe ketenpartners en dat deze het benodigde niveau van compenserende maatregelen hebben genomen tegen eventuele onbetrouwbaarheid van hun achterliggende toeleveranciers. Deze 'achterliggende' toeleveranciers kunnen dan verder buiten de scope van de ketenpartner worden gehouden.
Er ontstaat dan een geschakelde keten van vertrouwen. Geschakeld vertrouwen kan op diverse manieren worden gerealiseerd.
Als eerste kan dit op basis van controle of certificatie. De betrouwbaarheid van de ketenpartner wordt door een onafhankelijke bevoegde partij gecontroleerd en (eventueel) door certificatie bevestigd. Dit principe wordt bijvoorbeeld toegepast voor eind-tot-eind risico assessments van internationale logistieke ketens. Partijen in de keten kunnen worden gecertificeerd als 'AEO' (Authorized Economic Operator), hetgeen voor douane of toezichthouder voldoende is om verdergaande eigen controle van hen (en al hun eventueel toeleverende ketenpartners ('predecessors')) achterwege te laten.
Ten tweede kan dit op basis van gelijkwaardigheid en afspraken. Betrouwbaarheid van ketenpartner wordt daarbij niet afgedwongen door een gezagsrelatie, maar wordt bestendigd op basis van gelijkwaardigheid door vrijwillige afspraken, bijvoorbeeld als convenant. Het initiatief van 'Horizontaal Toezicht' door de Nederlandse belastingdienst is hiervan een voorbeeld.
Tot slot kan dit op basis van eigen vaststelling van de betrouwbaarheid van een ketenpartner in het voldoen aan de eis van geschakeld vertrouwen. Dit is bijvoorbeeld van toepassing op de ICT-ketens waarbij er geen sprake is van overkoepelend toezicht of gezamenlijke afspraakvorming.

> .....de vraag te beantwoorden of een ketenpartner in voldoende mate kan vertrouwen op de geleverde kwaliteit van zijn toeleveranciers om de verwachtingen aan zijn deel van de dienstverlening waar te kunnen maken

De trust audit met haar normatiek kan worden gebruikt om vast te stellen of (en welke vorm van en voor welke ketenpartners) geschakeld vertrouwen voor een specifieke ICT-keten gerechtvaardigd is. Daar waar als uitkomst van de trust audit geschakeld vertrouwen gerechtvaardigd blijkt, kunnen verdere controle maatregelen worden ingeperkt.

Risicobeheer in ICT-ketens
De trust audit kan een rol spelen in de methodiek van gescoopt risico management voor het bepalen van de (mate van) controle over de robuustheid van ICT-ketens. Deze methodiek ('El Metodo' [JOOSTEN] [BASTIAANSEN2]) heeft als uitgangspunt dat de mate van controle over de robuustheid van een ICT-keten wordt bepaald vanuit de scope van de ketenverantwoordelijke.
Ter illustratie hiervan beschouwen we de keten van een chipkaart exploitant, waarin winkeliers zijn klant zijn. De winkeliers verwachten van de exploitant dat de chipkaart terminals, de achterliggende systemen en de communicatie daartussen altijd werkt. De exploitant heeft zich hiertoe (contractueel) verplicht en zal om aan die verplichtingen te voldoen, zelf weer verwachtingen koesteren ten aan zien van zijn toeleveranciers (voor bijvoorbeeld de communicatie, het gestolen chipkaart register en financiële functies).

Figuur 1 laat zien dat de verwachting van de ene partij (ten aanzien van een andere partij), verplichtingen voor die andere partij worden (ten aanzien van de ene partij). De chipkaart exploitant (ketenverantwoordelijke) is verantwoordelijk voor het maken van afspraken met toeleverende partijen (communicatie provider en financiële instelling) voor de benodigde functionaliteit en het regisseren van alle interne en externe afspraken die maken dat hij zijn eigen functionaliteiten kan leveren en zijn verplichtingen nakomen.

Vanuit de klanten (de winkeliers) gezien is de chipkaart exploitant verantwoordelijk voor het voldoen aan de verwachtingen. Klanten zullen geen genoegen nemen met een verwijzing naar de toeleverancier als hij in gebreke blijft. Om in controle te blijven over de robuustheid van de keten, zal de chipkaart exploitant daarom moeten bepalen:
hoe belangrijk elk van de toegeleverde functionaliteiten is voor de gehele dienst; d.w.z. wat is bijvoorbeeld de impact bij uitval, en
in welke mate hij erop vertrouwt dat de toeleverende partij haar afspraken nakomt, i.e., wat de 'trustscore' is voor de toeleverende partij,
in welke mate hij zelf aanvullende contingentiemaatregelen moet nemen zoals het plaatsen van mobiele chipkaart terminals als back-up.
Bij de 'El Metodo' methodiek met gescoopt risico management vult de ketenverantwoordelijke een risicomatrix in, zie Figuur 2. Deze matrix bevat een overzicht van de verplichtingen (kolommen) en verwachtingen (rijen), gegroepeerd volgens de partijen tegenover wie deze verplichtingen en verwachtingen gelden. Per verplichting O wordt de impact van het niet nakomen van deze verplichting weergegeven met scores 'L', 'M' en 'H' in de kolom Impact[i]. In een cel geeft de afhankelijkheidscoëfficiënt aan in welke mate de verwachting (kolom) van belang is voor het waarmaken van de verplichting (rij). Verder geeft de ketenverantwoordelijke per verwachting E aan in hoeverre hij erop vertrouwt dat de toeleverancier deze verwachting (die voor de toeleverancier een verplichting is), gaat nakomen door trustscores 'L', 'M' en 'H' voor elke verwachting.

> Daar waar als uitkomst van de trust audit geschakeld vertrouwen gerechtvaardigd blijkt, kunnen verdere controlemaatregelen worden ingeperkt

Per verplichting wordt op basis van de afhankelijkheidscoëfficiënten en trustscores de kans op het niet nakomen van deze verplichting berekend in termen van de scores 'L', 'M' en 'H', zie kolom Kans[i]. Nu kan per verplichting het risico worden berekend op basis van kans en impact. De figuur toont dit door scores 'L', 'M' en 'H' in de kolom Risico[i]. Indien een risico hoog uitkomt, heeft de ketenverantwoordelijk te weinig controle en zal hij contingentiemaatregelen moeten nemen. Zo geeft 'El Metodo' meteen een instrument waarmee de ketenverantwoordelijke (onacceptabel grote) risico's kan beheren en mitigeren [HOEVE].

'El Metodo' maakt gebruik van trust scores, i.e. de mate van vertrouwen van de ketenverantwoordelijke (per verwachting) dat de toeleverancier deze verwachting gaat nakomen.
Voor het (kwantitatief) bepalen van deze trust score is er een natuurlijke rol weggelegd voor de trust audit zoals beschreven in dit artikel. Door weging van de normen en toetsen van de trust audit, kan de trustscore benodigd in 'El Metodo' worden vastgesteld.

Kwantificatie van ketenkwaliteit
Voor het kwantitatief bepalen van de kwaliteit (bijvoorbeeld in termen van

Figuur 2 – Risicomatrix vanuit één scope

beschikbaarheid of response tijden) van complexe ICT-ketens zijn wiskundige modellen nodig. In deze modellen wordt de kwaliteit van de gehele ICT keten bepaald op basis van de kwaliteit van de individuele schakels, in combinatie met de topologie van de ICT-keten. Hieraan wordt in de huidige Nederlandse onderzoeksprojecten SEQUAL [SEQUAL] en TTISC [TTISC] gewerkt.

Dergelijke wiskundige modellen houden voor de kwaliteit niet alleen rekening met de kwantitatieve waarden voor de kwaliteitsparameters van een ICT-dienst zoals weergegeven in de SLA (beschikbaarheid, response tijd...) maar ook met de betrouwbaarheid van deze SLA-waarden [WANG]. Het moge duidelijk zijn dat de trust audit ook hier weer een goede rol kan vervullen in het kwantificeren van deze betrouwbaarheid.

Deze modellen worden gebruikt om het ontwerp van een ICT-keten vorm te geven, door dynamisch dienstcompositie door een 'orchestrator'. Hierbij worden zowel de topologie van de ICT-keten als de keuze voor specifieke dienstleveranciers als schakel afgewogen. De modellen doen daarbij een statistische doorberekening van de kwaliteit en tolerantie van individuele schakels naar de kwaliteit van de ICT-keten in zijn geheel.

De trust audit is dan ook niet een instrument waarmee een redelijke mate van zekerheid ('positieve assurance') kan worden verkregen met betrekking tot de robuustheid van ICT-ketens, hooguit een bijdrage aan een beperkte mate van zekerheid ('negative assurance')

In dit artikel hebben we zowel de normatiek voor het uitvoeren van trust audits beschreven als een aantal rollen die trust audits kunnen vervullen voor kwaliteitsbeheersing in ICT-ketens.

Trust audits kennen ook hun beperkingen. Een trust audit doet geen strikte controle op de implementatie van de ICT-omgeving binnen individuele ketenpartners. De trust audit is dan ook niet een instrument waarmee een redelijke mate van zekerheid ('positieve assurance') kan worden verkregen met betrekking tot de robuustheid van ICT-ketens, hooguit een bijdrage aan een beperkte mate van zekerheid ('negative assurance').

Wij roepen hierbij organisaties tevens op om tezamen met ons het concept van de trust audits verder door te ontwikkelen, bijvoorbeeld in de uitwerking van het toetsingskader en validatie in representatieve ICT-ketens.

Dit artikel is een beknopte samenvatting van het referaat van de auteur ter afronding van de opleiding tot IT-Auditor aan de Erasmus Universiteit Rotterdam. Het werk is uitgevoerd in het kader van het Nederlandse onderzoeksproject TTSC [TTISC]. Het referaat kan bij de auteur worden opgevraagd.

Referenties

[ROSIELLE] C. Rosielle: "Trust Audits", Informatiebeveiliging, blz. 19-22, November 2010.

[IIARESEARCH] IIA Research Report: "Viewing Organizational Trust and Internal Auditing", 2003-2004

[SEPPANEN] R. Seppänen, e.a.: "Measuring inter-organizational trust—a critical review of the empirical research in 1990–2003", Industrial Marketing Management 36, 2007, pp. 249– 265.

[CANAVARI] M. Canavari, e.a.: "The role of trust in the transition from traditional to electronic B2B relationships in agri-food chains", Computers and Electronics in Agriculture 70, 2010, pp. 321–327.

[BASTIAANSEN1] H. Bastiaansen: "Trust audits en hun rol in het beoordelen van de robuustheid van ICT-ketens", Referaat IT-Auditing opleiding, Erasmus Universiteit Rotterdam, verkrijgbaar via de auteur.

[JOOSTEN] R. Joosten: "'Gescoopt' Risico Management", Informatiebeveiliging, Oktober 2010, pp. 12 – 17.

[BASTIAANSEN2] H. Bastiaansen, e.a.: "Hoe goed bent U in control over de robuustheid van uw ICT-keten?", Informatie, Maart 2011, pp. 24 – 30.

[HOEVE] M. Hoeve, e.a.: "El Metodo – Managing Risks in Value Chains", Securing electronic business processes: highlights of the information security solutions Europe 2011 conference / ISSE 2011, Norbert Pohlmann (ed.) e.a., pp 214-223.

[SEQUAL] IOP GenCom onderzoeksproject: "SEQUAL (Service optimization and QUALity)", http://www.agentschapnl.nl/content/project-service-optimization-and-quality-sequal.

[TTISC] IIP onderzoeksproject: "TTISC (Towards Trustworthy ICT Service Chains)", ICT-regie innovatieplatform. http://www.ict2030.nl/IIP-Cooperation-Challenge.html.

[WANG] S. Wang, e.a.: "A measurement approach of trust relations in web services", Journal of Communication and Computer, Aug. 2009, Volume 6, No.8, pp. 9– 17.

FOX IT

for a more secure society

FOX-IT voorkomt, onderzoekt en beperkt de meest serieuze cyberdreigingen met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. Onze aanpak combineert slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. We ontwikkelen producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.

FOX-IT.COM

Fox zoekt nieuwe Foxers

FOX-IT groeit en bloeit. Om deze reden zijn wij over de volle breedte van ons werk op zoek naar hackers, Forensic Experts, Pentesters, Developers (Python / C++), Hardware Engineers en Fraude analisten. Een Foxer is nieuwsgierig, kritisch en talentvol.
Je draagt bij aan de missie van FOX-IT: having fun in making technical and innovative contributions for a more secure society

Interesse om bij ons te komen werken?
Bel of mail Walter Doorduin 06 41901011 of doorduin@fox-it.com.

IT IN CONTROL VANUIT DE SECURITYCOCKPIT

Gerard Klop (gerard.klop@motiv.nl) is als Business Developer bij Motiv belast met 'IT in Control'-vraagstukken.

Compliancy vereist dat u uw informatietechnologie en -beveiliging aantoonbaar onder controle heeft. Gerard Klop van Motiv legt aan de hand van RSA Archer uit hoe u met een applicatie voor Governance, Risk & Compliancy niet alleen grip krijgt op uw IT, maar ook een helder beeld van de risico's voor uw bedrijfsvoering.

De in ons vakgebied gevleugelde uitdrukking 'IT in Control' betekent letterlijk dat uw 'informatietechnologie onder controle' is. Uw organisatie stelt de norm en het beleid op voor het beveiligen van informatie en het voorkomen van incidenten. Bij een afwijking ten opzichte van de norm worden direct maatregelen genomen. Policy-compliancyrapportages geven volledig inzicht in de kwaliteit van de beveiliging. Op deze manier ontstaat een totale security-cockpit. Vanuit deze cockpit heeft u uw 'IT in Control'.

Norm bepalen

Om een schending van de norm te kunnen waarnemen, is het wel noodzakelijk dat eerst de norm wordt bepaald. Een Governance, Risk & Compliancy (GRC)-applicatie zoals RSA Archer – dat fungeert als security-cockpit – biedt diverse tools die hierbij helpen. Een risico-analyse is bij voorkeur de eerste stap bij het vaststellen van de norm. Tijdens deze analyse kijkt u naar de bedrijfsbrede risico's voor uw bedrijfsvoering en probeert u inzichtelijk te krijgen hoe zwaar de risico's wegen. Welke informatie is écht belangrijk en mag aan geen enkel risico blootstaan? En welke informatie is van iets minder belang waardoor u een (klein) risico durft te nemen? Vervolgens is het zaak om te kijken welke maatregelen noodzakelijk zijn vanuit het oogpunt van compliancy. Voldoet u aan de geldende wet- en regelgeving? Wie de omgekeerde weg bewandelt en bij het stellen van de norm begint bij compliancy, loopt het risico zaken over het hoofd te zien. Met een GRC-applicatie is het vervolgens mogelijk om het door u vastgestelde normenkader te borgen binnen de organisatie. De controles die nodig zijn om te weten dat alle activiteiten binnen het normenkader plaatsvinden, kunnen in handen worden gegeven van een medewerker.

> De GRC-applicatie vormt een solide platform voor het in control krijgen van Governance, Risk en Compliancy

Controles

Een GRC-pakket biedt, zoals gezegd, diverse tooling voor het vaststellen van de norm, maar ook voor het controleren of alle activiteiten binnen het normenkader plaatsvinden. Voorbeelden van die tools zijn:

- Compliancy Assessments. Gebaseerd op nationale of internationale (security-)standaarden kunnen assessments worden uitgevoerd, met een focus op de organisatie van informatiebeveiliging. Op basis hiervan wordt bepaald waar de organisatie staat ten opzichte van de betreffende standaard. De output wordt tevens gebruikt bij het vaststellen van de juiste maatregelen.
- Business Continuity. Hier wordt gekeken naar de potentiële bedreigingen voor de organisatie en wat de gevolgen zijn als de bedreigingen daadwerkelijk manifest worden. Binnen deze discipline worden ook de maatregelen gedefinieerd die nodig zijn om na een 'ramp' zo snel als mogelijk weer 'back-in-business' te zijn.
- Business Impact Analyse, waarmee op basis van de eisen van de businesseigenaren wordt vastgesteld welke informatiesystemen bedrijfskritisch zijn.
- Awareness. Medewerkers bewust maken van de dreigingen die de bedrijfscontinuïteit in gevaar kunnen brengen.
- Risk Management. Het identificeren en kwantificeren van de risico's en het vaststellen van de beheersmaatregelen en mogelijk restrisico.
- Een Information Security Management Systeem (ISMS) conform de strenge eisen van ISO 27001.

De GRC-applicatie, in ons voorbeeld RSA Archer, is de verbindende factor tussen deze diensten, waardoor samenhang en synergie wordt bereikt. De GRC-applicatie vormt daarmee een solide platform voor het in control krijgen van Governance, Risk en Compliancy en daarmee uw complete IT.

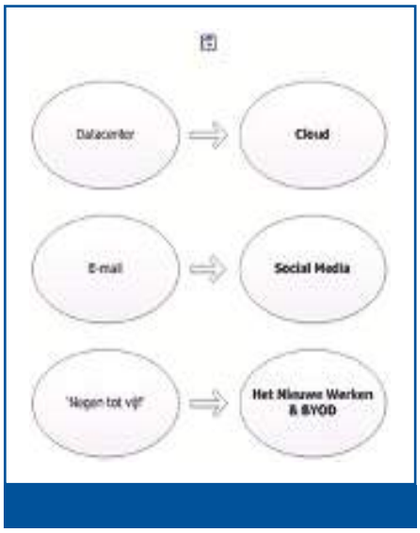
AWARENESS VOOR INFORMATIEBEVEILIGERS, IS HARD NODIG !

Ing. Marc Hullegie is directeur van Vest, een onafhankelijk, gecertificeerd adviesbureau voor informatiebeveiliging. Marc is bereikbaar via info@vest.nl

BUSINESS INFORMATION GOVERNANCE

Vakbroeders en zusters, ons vak kent al jarenlang talloze uitdagingen, waarover we regelmatig klagen dat we onvoldoende ondersteuning van het management krijgen. En dat "gebruikers" al helemaal geen besef hebben van het belang. Ik constateer echter regelmatig dat wij zelf behoorlijk boter op ons hoofd hebben, want we kijken en luisteren niet echt, omdat we te druk zijn om hen te overtuigen van ons credo. Hoog tijd voor een awareness-sessie voor ons zelf!

Er zijn weinig vakgebieden te bedenken waarbij ontwikkelingen en technologieën elkaar zo snel opvolgen als binnen de IT. De snelheid waarmee bedrijven klanten bedienen is een belangrijke succesfactor. Organisaties maken voortdurend strategische keuzes om hun concurrenten voor te blijven. Zij adopteren daarbij nieuwe, zogeheten 'disruptive technologies'. Enkele voorbeelden hiervan zijn mobiel werken, altijd en overal, cloud-applicaties en social media. De meeste security managers hebben moeite met het adopteren van dergelijke technologie die zo vernieuwend is dat de traditionele manier van beveiligen geen oplossing meer biedt. Je kunt je overigens de vraag stellen of veel van de 'nieuwe technologieën' echt zo nieuw zijn als ze worden gepresenteerd ? Kijk maar eens goed naar de volgende illustratie.



Houding en gedrag

Jammer genoeg wordt de inzet van nieuwe technologieën meestal alleen vanuit de business geïnitieerd. Informatiebeveiligers, security managers, weten als geen ander welke trends er spelen en welke voordelen dit voor de organisatie kan hebben, maar zijn van nature behoudend in de adoptie van nieuwe technieken, trends en oplossingen. Een vorm van beroepsdeformatie, die ervoor zorgt dat risico's de boventoon voeren bij de introductie van veranderingen. De voordelen voor de business verdwijnen naar de achtergrond. De business voelt zich gehinderd in de bedrijfsvoering en innovatie. Niet alleen IT- en security-afdelingen hebben het stempel 'business prevention department'. Ook andere faciliterende afdelingen zoals HR, met zijn veelvoud aan procedures, worden gezien als blokkade opwerpende afdelingen.

Een veelgehoorde klacht bij Information Security Managers is dat er te weinig commitment bestaat bij directie en management. Informatiebeveiligers hebben dit voor een groot gedeelte aan zichzelf te danken, het hindert de organisatie in het uitvoeren van hun werkzaamheden.

Uitdaging

Slechts weinig bedrijven kunnen het zich veroorloven om niet mee te gaan met nieuwe ontwikkelingen. En de security manager kan ze hierbij helpen. Hoe veel prettiger zou het zijn als er vanuit de IT- en security-afdeling vooraf al is gekeken naar ontwikkelingen die er aankomen, deze te evalueren en aan te kaarten bij het management. De voordelen van de toepassing van nieuwe technologieën biedt de business nieuwe kansen en wellicht concurrentievoordelen. De business ziet de security-afdeling meewerken en het verkrijgen van commitment voor initiatieven is makkelijker.

Moeten we dan al onze kennis en ervaring op het gebied van security- en risicomanagement, security- architectuur, -technologie, actuele bedreigingen overboord zetten ? Nee, die bagage is onontbeerlijk om de business te helpen om zonder struikelen hun doelen te verwezenlijken.

Kom uit je ivoren toren! Stap op hen af, luister, kijk, begrijp de uitdagingen. Durf ja te zeggen tegen de ideeën van de business. Zeg: "Ja! We gaan het samen realiseren. Ik help je om de gewenste vernieuwing veilig te implementeren." Creëer draagvlak voor beveiliging en maak van de security-afdeling de business enablement department.

Vest daagt de collega-informatiebeveiligers uit om kritisch naar eenieders houding en gedrag te kijken en zich af te vragen in welke mate zij met de organisatie meedenken in het realiseren van missie, visie en doelstellingen, en (nieuwe) technologieën ten voordele van de organisatie.

FEIT OF FICTIE – DE REALITEIT VAN CYBER WAR

Don Eijndhoven heeft meer dan een decennium aan professionele ervaring met het ontwerpen en beveiligen van grote IT- infrastructuren. Hij is de oprichter en tevens directeur van Argent Consulting. Don spreekt regelmatig op conferenties over Cyber Warfare, werkt voor CSFI (www.csfi.us) en schrijft artikelen voor diverse technische sites en bladen over de staat van Cyber Security. Hij is een oprichtend bestuurslid van het Nederlands Cyber Doctrine Instituut. Tevens is hij de oprichter van de Dutch Cyber Warfare Community groep op LinkedIn. Don is per email bereikbaar via donnye@gmail.com.

Cyber War. Twee woorden die u inmiddels vast wel eens in het nieuws gehoord hebt. De afgelopen twee jaar heeft u het wellicht steeds vaker gehoord, misschien wel langer als u enigszins geïnteresseerd bent in het onderwerp, of sites bezoekt die verslag doen over Cyber Warfare. Zeker als je in de VS woont hoor je behoorlijk angstaanjagende verhalen. En niet zomaar van iemand: Richard Clarke (adviseur van de Amerikaanse president, voormalig Hoofd Antiterreur) geeft aan dat Cyber War de grootste bedreiging is voor nationale veiligheid. Hier in Nederland is dit sentiment ook aan het groeien. Clarke had het uiteraard over de nationale veiligheid van de VS, maar zijn kritiek is evengoed steekhoudend voor andere landen, inclusief Nederland. Wat u wellicht verrast is dat hij - hoewel hij misschien wat paniekerig overkomt - het tamelijk bij het rechte eind heeft, ook al is hij waarschijnlijk bang voor de verkeerde vijand.

Laat me beginnen met proberen uit te leggen wat Cyber Warfare nu eigenlijk precies is. Ik zeg "proberen" omdat het vrij lastig te bepalen is wat nu de exacte definitie is. Gelukkig ben ik met dit definitieprobleem in goed gezelschap. Tijdens een hoorzitting ter gelegenheid van zijn bevestiging als allereerste Cyber Generaal in de Amerikaanse geschiedenis, kon 4-ster Generaal Keith Alexander niet aan de commissie uitleggen wat nu precies de juiste definitie is. Er is namelijk een behoorlijk aantal definities. Welke is nu juist? Het niet kunnen definiëren heeft waarschijnlijk ook te maken met het feit dat wij nog steeds aan het ondervinden zijn wat het nu precies betekent (cultureel) om *al* onze collectieve kennis *altijd* tot onze beschikking hebben. We maken ook nog eens zulke snelle technologische veranderingen door, dat het moeilijk is om te zien waar we heen gaan. Voeg hier nog eens aan toe dat zeer weinig mensen (*als* die er überhaupt al zijn) weten of begrijpen waar internettechnologie nu eigenlijk overal gebruikt wordt, en de verwarring is compleet. Internettechnologie is namelijk zo gewoon geworden dat we geheel nieuwe gebieden ontdekken

Bron: wikimedia.org

Richard Clark, cyber-czar

qua kwetsbaarheden, ook al zijn diezelfde kwetsbaarheden al tientallen jaren aanwezig. SCADA-systemen zijn hier een uitstekend voorbeeld van; tot STUXNET wisten eigenlijk alleen de experts van het bestaan en beseften alleen zij dat een aanval op dergelijke systemen ons zwaar kon raken.

> Tot STUXNET wisten eigenlijk alleen de experts van SCADA

Maar wat is dan Cyber Warfare?

Voor een heel algemene definitie van Cyber Warfare zal ik een stukje hergebruiken van Wikipedia's stukje over "Aerial Warfare": *Cyber Warfare is het gebruik van zowel militaire als andere netwerken en systemen om het nationale politieke belang te behartigen op het cyberspace slagveld.*

Ik besef me dat dit zo'n brede definitie is dat het bijna nietszeggend wordt, maar iedere verdere vernauwing van het begrip maakt het feitelijk onjuist. Wikipedia's beschrijving van Cyber Warfare refereert aan politiek gemotiveerd hacken, maar dat is in mijn optiek onjuist omdat hoewel hacking er zeker een deel van is, is het niet de *hele* inhoud van het begrip. De definitie die Richard Clarke gebruikt in zijn boek "Cyber War" vind ik ook te nauw omdat hij het beperkt tot een activiteit die enkel ondernomen wordt door overheden. Hiermee schuift hij alle "non-staat" elementen aan de kant en ik beschouw dit als een vergissing.

Ongeacht de exacte definities, behelst Cyber Warfare het gebruik van computersystemen en netwerken met als doel om vijandelijke informatie te corrumperen, ontzeggen of vernietigen, terwijl je je eigen informatie beschermt.

Wat eigenlijk over het algemeen een cyberaanval genoemd wordt, is in werkelijkheid een aanval op een bestaand netwerk of systeem. In veel gevallen wordt er een (al dan niet natuurlijke) kwetsbaarheid geëxploiteerd in een programma

of systeem. Omdat software geschreven wordt door mensen, en menselijke fouten in het programmeren als onvermijdelijk beschouwd worden (ook al kun je ze wel verminderen door goede kwaliteitscontrole), betekent dit dat er voorlopig nog wel kwetsbaarheden zullen blijven bestaan in de systemen die we gebruiken, en we dus kwetsbaar zullen blijven.

Stuxnet in cyberspace

Bron: http://searchengine.tvo.org/blog/search-engine-blog/audio-podcast-140-last-look-cyberwar

Cyber War – een tijdlijn

Ondanks alles wat je zojuist gelezen hebt, is Cyber Warfare geen nieuw concept. Het bestaat al zo'n twintig jaar en daadwerkelijk politiek gemotiveerde cyberaanvallen vinden al ruim een decennium plaats, misschien zelfs wel langer:

1998: Zware cyberinfiltraties vinden plaats tegen de netwerken en systemen van overheidsdepartementen in de VS, het Pentagon, NASA, verschillende researchlaboratoria en universiteiten, en duurt ongeveer 2 jaar. Rusland wordt verdacht maar ontkent in alle toonaarden. De aanvallen krijgen de codenaam Moonlight Maze.

Maart 1999: Servische hackers vallen NAVO-systemen aan als represaille tegen de militaire interventie van de NAVO in Kosovo.

May 1999: Een golf cyberaanvallen uit China overspoelt Amerikaanse overheidswebsites na een onbedoeld bombardement van de NAVO op een Chinese ambassade in Belgrado.

April 2001: Na een incident met een Amerikaans spionage vliegtuig boven Hainan (China), vallen Chinese hackergroepen Amerikaanse overheidssites aan.

2003: Een serie succesvolle inbraken in Amerikaanse overheidsnetwerken en systemen begint, en wordt pas ongeveer drie jaar later ontdekt. De VS geeft de aanval de codenaam Titan Rain en herleidt de aanvallen uiteindelijk terug naar China.

2006: De VS starten een nieuw militair commando om om te kunnen gaan met cyberdreigingen. Het commando krijgt de naam US Cyber Command (USCYBERCOM).

April-Mei 2007: Cyberaanvallen, zeer waarschijnlijk afkomstig van de Russische overheid, vallen websites van de overheid van Estland aan. Banken, ministeries, kranten en televisiezenders moeten het ontgelden nadat een standbeeld die de Russische Gevallen Soldaat eert, verplaatst wordt naar een plek buiten het stadscentrum.

> Menselijke fouten bij het programmeren zijn onvermijdelijk

Juni-Juli 2008: Honderden websites van de Litouwse overheid en bedrijven worden gekraakt en besmeurd met Sovjettijdperk digitale graffiti, hetgeen Russisch nationalisme impliceert.

August 2008: Massale DDoS-aanvallen op de Georgische overheid, evenals enkele commerciële websites, op hetzelfde moment dat er Russische tanks over de grens rollen voor een invasie.

November 2008: Systemen in het Pentagon worden aangevallen. De daders zijn vermoedelijk Russisch.

December 2008: De grootste bank in India wordt aangevallen door een hackergroep uit Pakistan, met wie India al jarenlang een verhoogde politieke spanning heeft.

Januari 2009: Zware DDoS-aanvallen vallen ISP's aan in Kirgizië tijdens een periode van politieke spanning met Rusland.

Maart 2009: Een grootschalige cyberspionage-operatie wordt ontdekt met zijn voornaamste command- en controlservers in China. De Information Warfare Monitor geeft de operatie de naam GhostNet.

April 2009: Een cyberaanval op een populaire nieuwssite in Kazachstan slaagt erin om de reguliere content te vervangen met politiek beladen berichten.

Zomer 2009: Verzetsstrijders compromitteren onbemande UAV-drones met vrij verkrijgbare software ter waarde van $ 26 en weten de live camerabeelden daarmee te onderscheppen.

Oktober 2009: USCYBERCOM begint met het coördineren van de bescherming van Amerikaanse militaire netwerken tegen cyberaanvallen.

Januari 2010: Melding van cyberaanvallen tegen Google in de tweede helft van 2009. China is de meest waarschijnlijke dader. De aanvallen worden beter bekend als Operation Aurora.

Quote Keith Alexander: "In war, information about your own capabilities and your opponents capabilities is the ultimate force multiplier. That was true in the time of Hannibal as it is today. In war, communication is another force multiplier. Communication and Information are critical conditions for Command. In the end, it is Command that decides the outcome of war. This was also true at the time of Hannibal and holds true today. Now, information and communication are interwoven and inseparable in what we call cyber. Therefore, Cyber War is attacking your opponent's information and communication multipliers, while defending your own."

Juni 2010: Een grote cyberaanval vindt plaats tegen Iran's nucleaire verrijkingsfaciliteit in Natanz. De verantwoordelijke software wordt STUXNET genoemd. Er bestaat een sterk vermoeden dat er overheden betrokken zijn bij het schrijven van de aanvalscode.
December 2010: Anonymous voert grote aanvallen uit tegen Mastercard, Paypal, VISA en PostFinance door Anonymous, als teken van steun voor Wikileaks oprichter Julian Assange.
Voorjaar 2012: Cyberaanvallen en dreigingen door Flare.
Bovenstaande lijst is verre van compleet. Wat belangrijk is, is dat we vanaf ongeveer 2009 jaarlijks een sterk opwaartse beweging zien in de hoeveelheid aanvallen, en de kracht van de individuele aanvallen. In 2011 zagen we bijna wekelijks zware aanvallen zoals die op internationaal beveiligingsbedrijf RSA. Tevens zagen we meerdere flinke aanvallen van de Anonymous-splintergroep LulzSec, waaronder die op Sony's Playstation Network, Fox Networks, de Amerikaanse Senaat en PBS. Google wordt ook weer aangevallen, evenals Citigroup en Lockheed Martin. Zelfs de website van de CIA.

Cyber Warfare – De Oorlog van de Toekomst

Wat Cyber Warfare zo effectief maakt, is dat internettechnologie erg veel computernetwerken en systemen binnen handbereik brengt van mensen die normaliter fysiek zouden moeten reizen om het aan te kunnen vallen. Soms per ongeluk (beheerders weten of controleren niet of een systeem aan internet verbonden is) en soms bewust (beheerders beseffen niet hoe gevaarlijk internetaansluiting kan zijn en vinden het makkelijk om vanuit huis te verbinden). Vandaag de dag kunnen deze zelfde aanvallers je bereiken van achter hun PC in hun eigen woonkamer. Nog een ander voordeel is dat ze vrij eenvoudig hun sporen dusdanig kunnen verbergen dat ze niet bang hoeven te zijn voor vergelding. En internettechnologie wordt iedere dag meer gebruikt. Dit zijn aanzienlijke veranderingen ten opzichte van hoe het altijd was, en we moeten hier hoognodig de consequenties van gaan inzien. We kunnen op dit moment slechts concluderen dat Cyber Warfare een bijzonder goede toekomst tegemoet gaat. Gezien de hoeveelheid overheden die actief Cyber Warfare mogelijkheden aan het ontwikkelen zijn, hebben zij waarschijnlijk dezelfde conclusie getrokken.

Scepsis

Helaas is er, ondanks het overweldigende bewijs voor het tegendeel, nog steeds een aantal mensen (waaronder mensen die als expert gezien worden in de informatiebeveiligingssector) die beweren dat de dreiging van Cyber Warfare overdreven wordt. Deze mensen geloven dat de dreiging uit proportie getrokken wordt door de mensen die geld verdienen aan ons beschermen tegen deze dreiging. Na de ontdekking van de veelbesproken en zeer succesvolle cyberaanval genaamd STUXNET, die de nucleaire verrijkingscentrale in Natanz te Iran aanviel, zijn veel van deze mensen terug gekomen op hun standpunt en geven ze toe dat de dreiging reëel is, maar dat we het vooral niet moeten beschrijven in militaire termen. Wederom wijzen ze naar de belangen van het militair industrieel complex, die volgens hen onnodig munt zou slaan uit de militarisering van het internet. Hiermee slaan deze mensen de plank in mijn optiek mis, en ik zal toelichten waarom.

> Angst verkoopt bijna net zo goed als seks

Bron: designyoutrust.com

Playstation

Semantiek

Er zijn meerdere redenen waarom ik vind dat een debat over semantiek nutteloos is. Allereerst: de pers is *gek* op militaire taal. Heel veel mensen zien het graag. Het is doorgaans krachtige en descriptieve taal, en 'cyberwapen' klinkt een stuk beter dan 'computerprogramma'. Militaire taal is doorgaans kort, helder en soms zelfs ronduit agressief. Het wil ook wel eens angstaanjagend klinken, en angst verkoopt bijna net zo goed als seks. Het is ongeveer dezelfde discussie als het aloude verschil tussen een hacker en een cracker. Een hacker was vroeger gewoon iemand die graag alles wilde weten over een bepaald systeem of programma en een cracker iemand die minder positieve intenties had. De pers bleef echter de term hacker gebruiken waar ze eigenlijk cracker had moeten gebruiken, en het gevolg is dat we nu de termen "White Hat" en "Black Hat" gebruiken om het wettelijke spectrum aan te duiden waarin de hacker in kwestie zich bevindt. Het algemene publiek kent nu alleen de term hacker, en slechts de puristen onder ons zullen nog deze kansloze hacker/cracker discussie voeren. Hetzelfde gaat ook gebeuren met Cyber Warfare. De militaire taal rondom Cyber Warfare is sexy en de pers gaat deze terminologie echt niet meer loslaten. We zouden allemaal beter af zijn als we dit gewoon accepteren en onze energie nuttiger besteden.

Gebruik Waar Toepasbaar

Een ander punt is dat, binnen beperkte context, militaire terminologie uitstekend toepasbaar is. Ja, militairen *kunnen* cyberspace - en computertechnologie in het algemeen - gebruiken en misbruiken om de politieke wil van hun respectievelijke land te bevorderen. De kunst van het oorlogvoeren is *altijd* al sterk beïnvloed geweest door technologische ontwikkelingen. In cyberspace is de militaire toepassing misschien niet onmiddellijk zichtbaar voor iedereen. Ook dat is niets nieuws: wellicht verbaast het je om te leren dat vliegtuigen ook niet meteen gebruikt werden op het slagveld. Vandaag de dag is "superioriteit in het luchtruim" vrijwel niet meer weg te denken op het moderne slagveld. Cyber Warfare draait om het vernietigen, ontzeggen of

corrumperen van de informatiestromen van de vijand, terwijl je je eigen informatiestromen beschermt. Informatie is een van de meest belangrijke (zoniet de *meest* belangrijke) factor in de uitkomst van ieder conflict. Carl von Clausewitz, Pruisisch generaal, militair theoreticus en de auteur van "Vom Kriege", beschreef in zijn boek al een fenomeen met de naam "mist van de oorlog". Deze Fog of War is een term die de onzekerheden in situationeel bewustzijn beschrijft die deelnemers ervaren tijdens militaire operaties. Het is in essentie een gebrek aan informatie, en dit is precies het gebied waarin Cyber Warfare opereert.
De meeste legers in de wereld hebben inmiddels verschillende vormen van internettechnologie toegepast om te kunnen communiceren; niet slechts van de ene soldaat met de ander, maar ook op andere gebieden zoals logistiek, radarinstallaties, raketdoelwitsystemen, navigatiesystemen, GPS- en satellietsystemen. Uiteraard zijn niet al deze systemen rechtstreeks verbonden met internet, maar dit hoeft niet per se een onoverkomelijk probleem te zijn voor een aanvaller, zoals we hebben kunnen zien met STUXNET. Twee grote onderdelen van het netwerk van de Amerikaanse Ministerie van Defensie (NIPRNET en SIPRNET), die kritiek zijn voor Command and Control van het Amerikaanse leger, zijn herhaaldelijk met succes aangevallen en geen van beide zijn rechtstreeks verbonden met internet. De mogelijkheid om dergelijke militaire systemen en netwerken aan te kunnen vallen en zo een of meerdere functies van een heel leger te kunnen verlammen of vernietigen, zou een zeer wenselijk wapen zijn voor ieder leger. Dit is ook de reden dat meer dan 120 legers van over de hele wereld momenteel cyber 'mogelijkheden' aan het ontwikkelen zijn. Deze legers zullen hun activiteiten in cyberspace blijven uitleggen met militair jargon. Termen die conflicten in de lucht, op het land of in de zee beschrijven zijn volkomen geaccepteerd en het lijkt mij niet meer dan normaal dat Cyber Warfare dezelfde plaats verdient.

Waarom Richard Clarke zowel gelijk als ongelijk heeft

Eerder stelde ik dat Clarke gelijk had om Cyber Warfare een groot nationaal risico te noemen. Deze stelling zou ik graag even willen nuanceren, omdat hij *in theorie* gelijk heeft. Er zijn namelijk zeer veel netwerken en systemen kwets-

Van Clausewitz On War

Bron: http://www.quotecounterquote.com/2010/08/war-is-continuation-of-politics-by.html

baar tegen aanvallen, maar lang niet al deze systemen zijn automatisch een geschikt doelwit voor militairen. Conflicten ontstaan niet zomaar en escaleren over het algemeen niet meteen tot een totale oorlog. In conflicten tussen landen is er een fenomeen wat men Conflict Escalatie of De-escalatie noemt. Een enkele soldaat die een enkel schot lost, is doorgaans niet genoeg om uit wraak meteen een heel bombardement op de vijandelijke hoofdstad uit te voeren en daar zijn goede redenen voor. Zeker vandaag de dag is er vrijwel niets wat de internationale pers ontgaat. Er zijn overal camera's en dankzij het internet reist nieuws met lichtsnelheid de hele wereld over. Indien een land zonder reden wordt aangevallen, zal dit land veel sympathie ontvangen van de internationale gemeenschap. Slaan ze direct keihard terug, dan is die sympathie evengoed weer direct verdwenen. Tevens signaleer je naar je vijand dat je beiden in een totale oorlog zit en dat geen doelwit te gek is. Een dergelijke uitkomst is voor niemand positief en daarom gebeurt dit ook niet snel. De ongeschreven regel van "ik doe wat jij mij aandoet" geldt meestal wel. Cyber Warfare zou absoluut uitstekend zijn om in een gemoderniseerd land complete chaos te veroorzaken. Stel je voor dat je een land compleet kunt destabiliseren door de financiële markt omver te trekken, het nationale stroomnet uit te schakelen, de olie-industrie lam te leggen of nooddiensten te overspoelen met meerdere grote problemen tegelijk? Geen van deze voorbeelden is militair van aard, maar heeft wel een enorm effect op een land. Je zou hiermee direct je vijand signaleren dat dergelijke (civiele) doelen aangevallen mogen worden. Kortom: het risico is er wel, maar het is een onwaarschijnlijk militair scenario voor overheden om te bezigen.

Fog of War

Dat betekent echter niet dat we automatisch veilig zijn. Ik heb het hier nu slechts gehad over overheden, maar dit is niet de enige groep die geïnteresseerd is in Cyber Warfare. Terroristische groeperingen en criminele organisaties hebben hele andere motieven en zouden wel eens exact dit soort chaos willen veroorzaken. Tot nu toe zijn vooral terroristische organisaties meer bezig geweest met het plegen van aanslagen met bommen, maar gezien het potentieel voor schade is het goed mogelijk dat dit nog eens gaat veranderen. Het internet is voor 90% in commerciële handen en valt dus niet onder de verantwoordelijkheid van de overheid of het leger. Zowel de overheid als het leger kunnen de bescherming van deze netwerken dan ook niet voor hun rekening nemen, al zou je je al af kunnen vragen of je dit zelfs wel zou willen. De beste oplossing voor dit enorme probleem is dat iedereen zijn eigen verantwoordelijkheden neemt, en begint met het beveiligen van het eigen netwerk en het eigen systeem. Het internet is een uitstekend voorbeeld van wereldwijde samenwerking, en dit zou zo moeten blijven.

CONTINUOUS

We started this column, the editor and I, back in issue 4 of this publication. It was to be an experiment to see whether this new piece would appeal to the readership. Its goal was to examine Business Attributes from the SABSA Business Attributes Taxonomy one by one, looking at them from new perspectives and especially looking for topical applications of each attribute as we meet it. For those of you who missed it, you might find it useful to go back to issue and look up the first article. Anyway, it seems that the editor is happy with the outcome of our experiment and he has asked for it to become a regular feature (thank you, Sir). In this issue we shall look at the attribute 'continuous'.

Although the maturity of 'business continuity' thinking has advanced greatly over the past two decades, it is timely now to go back to re-examine what might be meant by 'IT disaster recovery', because the threat landscape of today differs considerably from that of twenty years ago. Cyber-terrorism, hacktivism, malware and industrial espionage and sabotage are part of what we face today on a regular basis. The threat agents have become more sophisticated, well tooled-up, determined and have strong motivation for succeeding in disrupting our businesses through attacking our IT. Added to that, IT is now thoroughly pervasive in modern business, all IT shares common open standards and IT dependency is almost total. All businesses are potential targets, some if only to be pawns in a greater power game (such as has been speculated about the demise of Diginotar – why and by whom was that firm attacked?).

Take for example a pharmaceutical firm that has a database of clinical data that supports the licensing of a drug in which large sums have been invested. There may be competitive reasons why this data is confidential, but much more to the point, its integrity must be beyond question, for if the data cannot be trusted, neither can the product, and an untrusted pharmaceutical product cannot be licensed – game over! It may be sufficient for an opponent merely to claim that they have hacked into the database and changed some data. Even if they haven't actually done that, if you cannot prove that they haven't then the damage is already done. The credibility of your business is destroyed – not unlike the problem faced by Diginotar who could not prove what damage had or had not been done. Consider another example in which an auditor is conducting a due diligence review on behalf of a new customer or new potential owner. She discovers traces of a hacking that occurred just over two years ago. The question arises as to what damage may or may not have been inflicted by that hacker. Can the integrity of your systems and data now be guaranteed? Or is it the case that anything you may now recover is already compromised? How will you show proof one way or the other? This raises the issue of 'forensic readiness', which is a whole topic in itself, but you see the point – proof of integrity is essential in most cases for recovery from a disaster inflicted by a malicious attacker.

The common strategy for defending and protecting our information 'crown jewels' from compromise is usually to surround them with the strongest possible physical and logical security in multiple layers. We build the 'best in class' and relax on the basis that this will be sufficient. The problem is that what is deemed strong today may become weak in the future, submitting to new exploits of unseen vulnerabilities and new technical tools that render our current defences useless. Experience tells us that we will never be able to predict all the attack modes of the future, and therefore we are making a mistake in assuming that doing our best today will avoid future disasters.

So, shall we wring our hands and scream in despair? No! We need to change the paradigm for IT recovery planning. Instead of assuming that the 'crown jewels' will always be safe enough to recover them, we must turn that assumption on its head and assume that they will not. What shall we do then? We need to plan on the basis that at some future unforeseen point, all defences will be broken. This leads to a completely new type of thinking that will lead to entirely new types of recovery plans. It is time now to make this leap in maturity to recognize that our current approaches to IT security are not necessarily going to be the whole solution to providing 'continuous' business. That's what 'SABSA thinking' is about – looking holistically at business risk problems and creating true end-to-end lifecycle solutions.

The Attributer

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.

DORIFEL: HET EINDE VAN DE PREVENTIEDROOM?

In augustus van dit jaar werden tientallen organisaties getroffen door het XDocCrypt/Dorifel-virus. De mate waarin Nederland getroffen werd door dit virus - dat zich via netwerkshares verspreidde en de nationale nieuwsvoorziening dagenlang beheerste - zou je verbazingwekkend kunnen noemen. De periode van de luidruchtig verspreidende virussen ligt bijna een decennium achter ons, de lessen uit het verleden zijn allang doorgesijpeld in onze beveiligingsproducten en -diensten. Wat is hier aan de hand? Vertrouwen we teveel op antivirusproducten en het beveiligingsbewustzijn van de gebruikers in onze organisaties? De vraag aan onze redacteuren is dan ook: hadden we dit kunnen voorkomen of moeten we altijd rekening houden met dit soort incidenten?

Maarten Hartsuijker

"Maar we hebben toch antivirus?" Het is een opmerking die ik bij klanten regelmatig te horen krijg als ik wijs op de noodzaak van het updaten van software als Adobe Reader, Flash, Shockwave, Java, Quicktime en andere browser plugins. Dat we niet meer ontkomen aan antivirus- en Windows-updates hebben we met virussen als Blaster en Conficker wel geleerd. Maar de realiteit is dat alle software, waarmee content uit een e-mail of website wordt geopend, aantrekkelijk is voor hackers. En dat kwetsbaarheden in die software daardoor graag misbruikt worden voor het inbreken in systemen en het creëren van botnets.

Tegelijkertijd richten kwaadwillende hackers zich ook steeds meer op de gebruiker. Want waarom zou je naar kwetsbaarheden in software zoeken als je de gebruiker via een phishingmail ook vriendelijk kunt vragen om zijn eigen PC te besmetten? Veel gebruikers blijken hier uiterst toeschietelijk in te zijn.

Verdedigingsmiddelen als antivirussoftware zijn niet nutteloos, maar ook niet zaligmakend. Het blijft belangrijk om aanvullende maatregelen te treffen, waar ook zeker de bewustwording van gebruikers onder valt.

Een geïnfecteerde werkplek zal over het algemeen proberen om contact met het commandocentrum van de hacker op te nemen. Dit soort verbindingen zijn goed te detecteren met een netwerkgebaseerd Intrusion Detection Systeem als Snort. Op deze manier kan een virus dat alle beschermingsmaatregelen weet te passeren veelal toch gedetecteerd worden.

Ik ben er van overtuigd dat organisaties die het met preventieve en detectieve maatregelen beter doen dan de middenmoot, zich tegen een Dorifel kunnen beschermen. Maar tegelijk moeten we ons beseffen dat hackers ook agressiever zullen worden als we de lat met elkaar succesvol hoger weten te leggen. Het is daarom verstandig om in de Business Continuity Planning ook ruimte te maken voor een Security Incident Response Plan.

Rachel Marbus

Kunnen we incidenten voorkomen? Ja, sommige wel. Nee, echt niet allemaal. Ik besef me terdege dat dit vast moet overkomen als een heel flauw juristenantwoord, maar laten we eerlijk zijn: de wereld is niet zwart-wit. Preventie en awareness liggen in het hart van een veilige online wereld. Als het daarmee niet op orde is, dan zul je zien dat we nog veel meer en veel grotere incidenten zullen krijgen dan we nu gezien hebben. Diginotar en Dorifel zijn dan nog slechts het begin.

Natuurlijk moet er gedegen aandacht zijn voor detectie en respons, niet voor niets vormen zij onderdeel van de driehoek waarbinnen de incident respons dient te opereren. Maar laten we vooral ook geen boter op ons hoofd hebben. De bad guys zijn nog steeds vaak beter dan de good guys. Ze beschikken over meer tijd, meer middelen en vaak ook over meer kennis. De bad guy kan bij wijze van spreken jaren werken aan zijn aanval en alles tot in de puntjes uitwerken, de good guy moet reactief te werk gaan. Dat is altijd een lastigere positie waarin gewerkt moet worden op het scherpst van de snede tegen een tijdsdruk waar je u tegen zegt.

Moet er dus meer aandacht komen voor detectie en respons? Ja, dat lijkt me duidelijk. Daarmee koop je tijd en vergaar je kennis om de bad guy sneller te kunnen pareren. Hebben we daarmee dan ook direct een einde

gebracht aan incidenten? Nee, natuurlijk niet, maar hopelijk is daarmee wel de weg ingezet om de bad guys in ieder geval vaker voor te kunnen zijn en schade te voorkomen in plaats van te repareren.

Aart Jochem
Natuurlijk ben ik voor meer aandacht voor detectie en goede respons, ik verdien mijn boterham ermee. Maar in vorige levens heb ik bij verschillende organisaties gewerkt aan maatregelen om incidenten te voorkomen en heb gemerkt hoeveel investeringen en inzet het kost om met maatregelen de beveiliging waterdicht te maken. En waterdicht te houden over een langere tijd.
Hiervoor is een strakke discipline en een diepe buidel nodig, meer dan veel organisaties en gebruikers bereid zijn te leveren. Daarnaast zijn veel maatregelen gebaseerd op bescherming tegen bekende patronen, zoals antivirus en blacklisting. Digitale bedreigingen ontwikkelen zich juist snel, criminelen zoeken steeds nieuwe manieren om maatregelen te omzeilen. Snelle detectie en adequate respons op incidenten blijft nodig.

Hoe zit dat in Nederland? De afgelopen jaren is bij verschillende organisaties en bij de overheid voorzichtig geïnvesteerd in kleine teams die de omgeving in de gaten houden en het voortouw nemen bij een incident.
Voor het eerst in 1992, toen Surfnet SurfCERT oprichtte. Ook in de markt worden al jaren diensten aangeboden voor monitoring en respons. Deze teams hebben zich langzaam kunnen professionaliseren, met beperkte budgetten en vaak te weinig tijd om te doen wat er moet gebeuren. Enkele grote incidenten in binnen- en buitenland hebben het besef gebracht dat er veel op het spel kan staan als er ondanks alle voorzorgsmaatregelen toch iets misgaat. Ook de druk van actiegroepen, de ontwikkeling van krachtige actoren en de risico's van grote verzamelingen persoonlijke gegevens zorgen ervoor dat momenteel bij bedrijven en de overheid flink wordt geïnvesteerd. Hopelijk op tijd en voldoende. En hopelijk niet ten koste van goede preventieve maatregelen.

Lex Borger
Ik denk dat we hier altijd wel rekening mee moeten houden. Het is niet te voorkomen, omdat we als maatschappij een bepaalde tolerantie hebben voor dit soort incidenten voordat we tot actie overgaan. Lees *Liars & Outliers* maar van *Bruce Schneier*. Dat wil niet zeggen dat er niets aan te doen is. Ik onderscheid hierbij de verschillende rollen:
Als gebruiker: niet erg hoopvol - je moet je echt bewust zijn van een aantal technische zaken, zoals wat file-extensions zijn en hoe die gemaskeerd kunnen zijn; wat wél een software update is of wat malware is die er op probeert te lijken. En dat zijn we echt niet allemaal. Ook moeten we nu eens echt stoppen met het klikken op links in onverwachte e-mail… Al met al blijven we kwetsbaar voor social engineering.
Als IT beheerder: gemengd - er is weinig dat je eenvoudig kunt doen. Bestanden delen middels netwerkshares of e-mail moet je ondersteunen. Systemen blijven hardenen dus en segmenteren: gevoelige data apart houden of versleutelen. Verder kun je je richten op het detecteren van de botnet-activiteit, een geavanceerde bezigheid.
Als software ontwikkelaar: hier ligt de grootste kans - ontwikkel software met beveiligde functionaliteit op een veilige manier en stop met het constant uitbreiden van mogelijkheden, maar beperk je juist tot het realiseren van duidelijke use-cases en het afschermen van misuse-cases.

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 Domus Technica),
e-mail: lex.borger@domustechnica.com
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 (KPMG, IT Advisory)
Gerrit Post (G & I Beheer BV)
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 2012
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

VAKANTIE-IRRITATIES

Net weer teruggekomen van een vakantie in Frankrijk waar ik mij heerlijk vermaakt heb. Voor het eerst in mijn leven heb ik mij laten verleiden om een data-abonnement te nemen want we willen natuurlijk wel graag weten wat er allemaal gebeurt in Nederland. Op zich heerlijk want mijn smartphone verliest wel heel erg veel functionaliteit zodra ik het bordje België ben gepasseerd. Op deze manier kon ik dagelijks de nieuwssites lezen en natuurlijk is het plezierig om bij te blijven met betrekking tot de nieuwsberichten. Maar van wat je zoal tegenkomt word je toch niet heel erg blij en dan doel ik alleen nog op de berichtgeving in ons vakgebied. Tienduizenden wireless netwerken van KPN blijken lek als een mandje omdat de - bij het SSID behorende - wachtwoord eenvoudig te berekenen is. Philips lekt een groot aantal wachtwoorden en Simpel.nl lekt emailadressen. De e.dentifier van ABN-AMRO blijkt lek te zijn waardoor het elektronische betalingsverkeer onveilig lijkt te zijn. De Piratenpartij (wat een toepasselijke naam) maakt emailadressen van aanhangers onbedoeld bekend. De universiteit van Nijmegen is het gelukt om autosleutels te hacken, hotelkamersleutels zijn eenvoudig te hacken, Android-telefoons zijn eenvoudiger te kraken, LinkedIn verliest inloggegevens. Moet ik nog meer noemen? Nee, ik hoef niet meer te noemen! (Toch te lang naar Mart Smeets gekeken de afgelopen zomer.)

Het lijkt er zo langzamerhand op dat alle gegevens die ik ergens heb opgeslagen, blijkbaar zo voor het grijpen liggen. Philips stuurt mij nog een email of ik een review wil schrijven over het nieuwe scheerapparaat dat ik een maand geleden kocht. Ik ontving de mail op een moment dat ik een beetje chagrijnig was en ik heb direct maar een mail terug gezonden met het verzoek om al mijn gegevens uit alle databases te verwijderen die binnen Philips aangemaakt zijn. Dit omdat ze niet goed op hun spulletjes passen. De reactie was voorspelbaar en natuurlijk zeer teleurstellend: nee, daar konden ze niet aan beginnen en ze verzochten me nogmaals de review te schrijven.

Mijn vrouw komt binnen met een kop koffie en zij vraagt of ik mij weer eens ergens aan irriteer. Ik probeer te ontkennen maar ik weet het: mijn vrouw ziet dat aan mij. Ik leg haar uit over mijn scheerapparaat en over KPN maar dat verklaart mijn irritatie nog niet, zegt haar gezicht. Ik leg haar uit dat ze niet raar moet staan te kijken als haar auto ineens weg is terwijl de sleutels en reservesleutels gewoon aan het rekje hangen. Gelukkig, dit voorbeeld verandert haar gezicht. Ik vertel haar dat het inderdaad raar is dat je ruim 150 euro voor een sleutel moet betalen als je er één kwijt bent maar dat het niet zo moeilijk is deze sleutels gewoon na te maken en de elektronica te omzeilen. Verwonderd kijkt ze mij aan en zegt dat ik maar eens met de garage moet bellen. Bij mijzelf denk ik dat ik wederom aan een mission impossible ga beginnen, hetgeen al vrij snel duidelijk wordt. Mij wordt verteld dat het onmogelijk is de sleutels te kopiëren. Eerst moeten namelijk de originele sleutels worden ingelezen in de computer die de code voor de startonderbreker kan vaststellen. Vervolgens kun je inderdaad de auto starten. Ik leg de man uit dat in mijn woordenboek een hele andere betekenis van het woord onmogelijk staat maar de man is blijkbaar al weer met hele andere zaken bezig. Ik onderbreek het gesprek en leg mijn kin vermoeid in de handpalm. Ik denk dat ik aan beroepsdeformatie lijd, ik denk dat het allemaal niet zo ernstig is en dat onze data eigenlijk overal heel veilig liggen opgeborgen. Ik denk dat het elektronisch betalen best wel veilig is ondanks alle spookverhalen dat virussen inloggegevens hebben gestolen. Dat ik mijn wachtwoord op Gmail onmiddellijk moest vervangen zal wel een grap zijn. Ik heb gelukkig niets met de Piratenpartij en heb ook niks met de KPN. Nee, mijn gegevens zijn wel veilig. Mijn telefoon gaat, ik schrik wakker. Het blijkt de autodealer van mijn vrouw te zijn. Of ik net gebeld had. Ik zeg ja, terwijl ik mij in mijn ogen wrijf. Hij wilde mij nogmaals benadrukken dat de auto van mijn vrouw niet te stelen is zonder de originele sleutels. Ik wil wat antwoorden maar besluit hem alleen te bedanken voor de informatie. Ik druk het gesprek weg en drink mijn koude koffie op.

Berry

SHARE INFORMATION

MINIMIZE RISK

Secured eCollaboration

A unique add-in for Microsoft SharePoint® providing document encryption and enhanced access control.

ASK FOR A FREE TRIAL!

SC MAGAZINE

Verdict: "A very nice encryption solution. Priced in the middle of the group, but it delivers protection very well."

cryptzone

www.cryptzone.com

CRYPSYS secure computing

sales@crypsys.nl | www.crypsys.nl | 0183 - 62 44 44