oktober 2010 nummer 6

INFORMATIEBEVEILIGING

Zwichten voor autoriteit

‘Gescoopt’ Risico Management

Rekenen aan Malware

ACTA en netneutraliteit

creative commons

PvIB
Platform voor InformatieBeveiliging

ib

Voorwoord/colofon

Beste lezer,

In mijn rol van informatiemanager, architect en hobbyist hou ik me met meer bezig dan alleen beveiliging. Jaren geleden besloot ik om me te verdiepen in verwerking van gegevens in grote systemen. Gedistribueerde systemen. Ik had geen benul van wat dat inhield, dus besloot ik me te wenden tot de experts. Ik werd lid van IEEE. Interessante club, verantwoordelijk voor de meeste technische standaarden. Technische standaarden die nodig zijn voor interoperabiliteit en integratie. Dat bleek ook voor gedistribueerde databases wenselijk, want ja, als zo'n database op verschillende systemen draait, dan is het wel handig als al die systemen met elkaar kunnen communiceren en interacteren. Latency is zo'n beetje een kernbegrip, maar ook synchronisatie is een probleem. En daar denken de experts van IEEE over na. Leek me leuk. Totdat ik de eerste publicatie in de bus ontving. Dat ging niet over informatie, maar was allemaal hogere wiskunde. Dat was nooit mijn favoriete studieonderwerp. Statistiek vond ik wel leuk, maar iets als integreren kreeg ik nooit onder de knie. En dat hele IEEE-blad stond vol met die integraalhaken. Mijn lidmaatschap duurde maar een jaar. Korter kon niet.

Waarom deze inleiding? Ik kreeg een deja-vu gevoel bij het doorbladeren van dit nummer. Verdikke, wiskunde. En daar heb ik niet veel mee, maar dat schreef ik al. Gelukkig hebben we keigoede auteurs en keigoede redacteuren, dus de kans dat we goede artikelen plaatsen is vrij groot. En we gaan nu een paar keer heel diep.

Om zeker te weten dat ook u van mening bent dat we de goede dingen doen, willen we u trouwens binnenkort lastigvallen. We hebben als redactie eigenlijk nooit gevraagd wat u van het blad vindt. We krijgen wel regelmatig reacties, maar een echt beeld hebben we niet. We willen dus graag even van uw tijd gebruikmaken om ons te informeren over uw leeservaringen. Dat doen we via de mail, dus als u niets van ons hoort, is dat de oorzaak. We hopen op een grote respons, zodat we op basis van uw reacties de koers voor de komende tijd kunnen bepalen.

Uw reactie is dus te vroeg voor dit nummer. Maar we vinden dat we genoeg interessante stof tot nadenken bieden, dit keer met een paar stevige artikelen, die iets dieper graven dan we gewend zijn. We verwachten dat u genoeg te lezen hebt en we wensen u dan ook veel leesplezier.

Groetjes,

André Koot
Hoofdredacteur

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

Redactie
André Koot (hoofdredactie, werkzaam bij Univé-VGZ-IZA-Trias),
e-mail: A.Koot@Unive.nl
Cynthia Kremer (eindredactie, Motivation Office Support bv, Nijkerk)
e-mail: ibmagazine@pvib.nl

Redactieraad
Said El Aoufi (Metapoint)
Tom Bakker (Delta Lloyd)
Lex Borger (Domus Technica)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Rob Greuter
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
Rachel Marbus (BetterID4all)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving en druk
De Drie Poorten, Nijkerk

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
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

Mits niet anders vermeld valt de inhoud van dit tijdschrift onder een Creative Commons licentie.

ISSN 1569-1063

creative commons

PvIB
Platform voor InformatieBeveiliging

Inhoud





Viva Las Vegas

Een bezoek aan de woestijn midden in de zomer

Auteur: Ing. Frank Breedijk CISSP > Frank Breedijk CISSP werkt als Security Engineer voor Schuberg Philis, de leverancier van bedrijfskritische outsourcingsdiensten met een 100% functionele beschikbaarheid. Zijn taken omvatten onder andere het geven van security awareness-trainingen, vulnerability management, interne security consultancy en het uitvoeren van technische audits. Frank is tevens auteur van het open source-project Seccubus (voorheen AutoNessus) en blogt hij voor www.cupfighter.net. Hij is bereikbaar op fbreedijk@schubergphilis.com.

Zelfs als er geen security conferenties gehouden zouden worden, zou ik een aantal redenen kunnen bedenken om naar Las Vegas te gaan. Het moderne Sodom en Gomorra van de Verenigde Staten. Een stad die leeft van glitter, glamour en gokken. Een soort Disneyland voor volwassenen. Een stad waarin je je na een aantal dagen gaat afvragen of de volle maan wel echt is, waar verleiden en misleiden valide manieren zijn om je boterham te verdienen. Maar, laten we eerlijk zijn, geen van die redenen is op welke manier dan ook zakelijk te noemen. Waarom bevind ik me dan op dit moment op 37.941 voet boven de noordelijke Atlantische Oceaan op weg terug van een zakenreis naar ditzelfde Las Vegas?

In mijn geval waren er drie goede redenen te noemen: Black Hat; DefCon; en een relatief kleine conferentie genaamd Security B-Sides Las Vegas. Op uitnodiging van de verschillende conferentieorganisaties bracht ik een bezoek aan deze drie conferenties en verzorgde ik een presentatie.

Black Hat

Black Hat is waarschijnlijk een van de, zo niet de meest professionele security conferenties ter wereld. Al vele jaren weet deze conferentie een groot aantal toeschouwers en bekende namen uit de beveiligingswereld naar het Ceasar's Palace hotel te trekken. Naast de twee dagen durende conferentie op woensdag en donderdag biedt de Black Hat-organisatie trainingen aan op hoog niveau. Deze trainingen beginnen op zaterdag en gaan door tot de dag voor de conferentie. Black Hat is goed in het aantrekken van grote namen als Dan Kaminiski, Felix Lindner en Moxie Marlinspike, maar biedt ook ruimte aan opkomend talent. Zoals bijvoorbeeld de Nederlandse Christiaan Beek, die ons wist bij te praten op het gebied van forensische onderzoeksmethoden met betrekking tot virtualisatie. De conferentie biedt een zeer brede keus aan onderwerpen. Dit jaar is het aantal parallelsessies zelfs opgevoerd tot elf, niet te vergelijken met de drie tracks die Black Hat in Barcelona organiseerde. Het aantal deelnemers is ook duidelijk groter, uitgedrukt in een paar duizend in plaats van een paar honderd. Hoewel de Black Hat-conferentie de meest professionele van de conferenties is, is de sfeer wel informeel. De nadruk van de conferentie ligt op het offensieve vlak. Onderzoek naar kwetsbaarheden en onderzoek door penetratietesters staan hoog op de agenda, maar ook onderwerpen als het beschermen van bijvoorbeeld Scada-infrastructuren staan op de agenda. Al met al is deze conferentie een goede gelegenheid om te netwerken in bijvoorbeeld de vendor area tijdens de conferentie zelf of tijdens de lunch. Maar ook tijdens de vele door leveranciers georganiseerde avondactiviteiten.

Op welke manieren geldautomaten aangevallen kunnen worden

De meest in het oog springende presentatie van deze conferentie was Jackpotting ATMs van IOActive's Director Security Testing Barnaby Jack (http://bit.ly/atKQym). In deze presentatie laat Barnaby zien op welke manieren geldautomaten aangevallen kunnen worden.

B-Sides

De schaal van Black Hat en DefCon staat in schril contrast met die van B-Sides, een privaat georganiseerde conferentie die vorig jaar voor het eerst is gestart. Deze conferentie is door de kleine omvang,

ongeveer 150 deelnemers, bijna anti-conferentie te noemen. B-Sides kent geen bezoekers maar uitsluitend deelnemers en wordt voornamelijk gedreven door vrijwilligers. Maar dit doet niets af aan het niveau van de presentaties. Zo koos de bekende onderzoeker H.D. Moore juist B-Sides uit voor het presenteren van zijn onderzoek naar tot nu toe onbekende kwetsbaarheden in VxWorks. De B-Sides-conferentie heeft sponsors, maar deze bevinden zich voornamelijk op de achtergrond. Zo is er bijvoorbeeld geen vendor area. De conferentie vindt plaats op een privé resort met een zwembad, in een zeer informele sfeer en natuurlijk mag de barbecue met hamburgers en hotdogs niet ontbreken. Al met al een zeer geslaagd en intiem evenement, op dezelfde woensdag en donderdag als de Black Hat-conferentie.

DefCon

Na de professionaliteit van Black Hat en de intimiteit van B-Sides is het even overschakelen naar de massaliteit van DefCon, een hackersconferentie die nu al voor de 18e keer door Jeff Moss, tevens CEO van Black Hat, en zijn team wordt georganiseerd. DefCon is een echte hackersconferentie en dat is aan alles te merken. Aan de sprekers en hun onderwerpen, de kledingstijl van de bezoekers en bijvoorbeeld ook de vendor area. Hier geen leveranciers van beveiligingsproducten en -diensten, maar veel zwarte T-shirts, WiFi en tweedehands Unix-hardware. DefCon is de grootste van de genoemde conferenties en had dit jaar 10.000 betalende bezoekers. Hierbij moet nog een groot aantal vrijwilligers en sprekers opgeteld worden dat het evenement mogelijk maakt. Tijdens DefCon gebeurt er van alles, niet alleen tijdens de vijf parallelsessies, maar ook daarbuiten. Er is een flink aantal wedstrijden: capture the flag (live hacking); scavanger hunt; beverage cooling contest; cannonball run; password cracking; en social engineering contest, om er maar een paar te noemen. Daarnaast is er een lockpicking en hardware hacking village waar je respectievelijk kunt leren sloten ongemerkt open te maken of je naar hartenlust kunt uitleven op het modificeren van hardware. Bijvoorbeeld op die van de elektronische toegangspas van de conferentie.

Apparaten maken het mogelijk gsm-verkeer af te tappen

De meest in het oog springende presentatie is wat mij betreft die van Chris Paget, die voor ongeveer $1.500 een open source-versie van een zogenaamde IMSI-catcher heeft gemaakt. Deze apparaten, waarvan commerciële varianten enkele miljoenen kosten, maken het mogelijk gsm-verkeer af te tappen, wat hij live op het podium demonstreert. Mede door het advies van de Electronic Frontier Foundation (EFF) was het mogelijk dit volkomen legaal te doen. De eerste tien minuten zijn beschikbaar op deze url: http://youtu.be/q8JuYh7Km34.

Wat moet je zien?

Voor mijn eigen bezoek aan alle drie de conferenties heb ik me sterk laten leiden door het feit dat veel van de presentaties worden opgenomen, maar mijn gesprekken in de gang en bij de bar niet. Van veel van de presentaties die ik heb bijgewoond, heb ik voor onze blog CupFighter een verslag getikt. Daarnaast heb ik op Black Hat en DefCon een presentatie gegeven over mijn open source-project Seccubus (voorheen AutoNessus, zie het artikel van mij daarover in IB-magazine 5 van 2009). Informatie hierover is te vinden op www.seccubus.com. Op B-Sides heb ik de presentatie 'The Road to Hell is paved with Best Practises' verzorgd. Deze presentatie zal in Nederland te zien zijn op de NLUUG najaarconferentie.

Zijn deze conferenties het bezoeken van een woestijnstad in het midden van de zomer waard? Wat mij betreft wel, ik heb veel contacten kunnen leggen en onderhouden met nieuwe en oude bekenden uit de internationale securitywereld. Met name DefCon kent zeer veel vaste bezoekers die ieder jaar weer naar dit evenement terugkeren. Ik hoop volgend jaar dan ook weer, als spreker, bezoeker of pers te mogen terugkeren.

Links

Blackhat: www.blackhat.com
DefCon: www.defcon.org
Security B-Sides: www.securitybsides.com
CupFighter blog: www.cupfighter.net
Seccubus: www.seccubus.com
Frank Breedijk op twitter: www.twitter.com/seccubus

De internationale normcommissie voor IT-beveiligingstechnieken

De ISO/IEC 27000-serie

Auteur: Jan Rietveld > Jan Rietveld is secretaris van de NEN-commissie IT-beveiligingstechnieken en is bereikbaar via jan.rietveld@nen.nl.

Dit artikel gaat over de normen in de 270xx-serie van de internationale normcommissie JTC 1/SC 27 'IT Security techniques'. Het sluit aan bij het meer algemene artikel over JTC 1/SC 27 dat is verschenen in IB-magazine 7 van november 2009.

Binnen de normcommissie JTC 1/SC 27 'IT Security techniques' werken de werkgroepen 1 en 4 aan de normen in de 270xx-serie. WG 1 richt zich op de normen bedoeld voor het managen van informatiebeveiliging, informatiebeveiliging op beheerniveau (governance niveau) en WG 4 op normen die organisaties helpen bij het implementeren van '270xx-serie'-normen, 'Security controls and services'. De belangrijkste norm in de serie is ISO/IEC 27001 'Managementsystemen voor informatiebeveiliging - Eisen'. Het zogenaamde Information Security Management System (ISMS) waartegen gecertificeerd kan worden. De ontwikkelingen volgen elkaar snel op en daardoor zijn verschillende normen in de revisie, zoals de 27000, de 27001, de 27002 en de 27005.

Vijf normtypen binnen de 270xx-serie

De normen in de 270xx-serie kunnen in vijf groepen worden verdeeld. Hieronder worden deze besproken waarbij soms aandacht wordt gegeven aan een individuele norm als daar aanleiding voor is.

Groep 1: overzicht en woordenlijst (Vocabulary standard)

In deze categorie valt alleen de norm ISO/IEC 27000:2009 'Information security management systems - Overview and vocabulary'. ISO/IEC 27000 is de basis voor de 270xx-serie en geeft een overzicht van de normen in de 270xx-serie en hoe deze zich tot elkaar verhouden. Ondanks dat deze norm pas vorig jaar is verschenen, wordt al aan een revisie gewerkt. Dit komt door de vele (snelle) ontwikkelingen rond informatiebeveiliging wat zich vertaalt in nieuwe normen en revisies van bestaande normen in de 270XX-serie. Het is gewenst het woordgebruik in de verschillende 270xx-normen te harmoniseren en een consistent woordgebruik te bevorderen. ISO/IEC 27000 moet hier richting aan geven. Verder maken de ontwikkelingen het nodig bepaalde tekstdelen te actualiseren. Gezien de dynamiek en ontwikkelingen rond informatiebeveiliging is het de verwachting dat de 27000 de komende jaren vaker moet worden aangepast. Er zijn dan ook voorstellen om de norm om te zetten naar een Standing Document waardoor het aanpassen eenvoudiger wordt.

Een van de commentaren op de huidige 270xx-serie is dat zij erg heterogeen is zonder duidelijke basis of leidende principes. De normen zijn op basis van behoefte ontstaan. Geprobeerd wordt in de herziene 27000 een duidelijk en eenduidig raamwerk op te nemen dat als basis kan dienen voor de hele 270xx-serie.

ISO/IEC 27000 is gratis te downloaden. Zie de informatie aan het einde van dit artikel.

Groep 2: normen met eisen (Requirements standards)

In deze categorie valt de belangrijkste norm van de serie, ISO/IEC 27001 'Managementsystemen voor informatiebeveiliging - Eisen'. Deze norm is in 2005 gepubliceerd en wordt op het moment herzien. Er zijn tientallen commentaren voor verbeteringen en aanpassingen binnengekomen. Zo ligt er een voorstel om in de norm duidelijk aan te geven wat de relatie is met het Capability Maturity Model (CMM) en dat de norm alleen van belang is voor organisaties die minimaal CMM niveau 3 hebben bereikt. Bepaalde termen moeten duidelijker worden gedefinieerd en sommige termen worden uit deze norm verwijderd om te worden opgenomen in de 27000. Verder wordt nader gekeken naar het gebruik van de termen 'asset' en 'information asset' en naar de termen 'risk evaluation criteria' en 'risk acceptance criteria' die tot verwarring kunnen leiden. Geconstateerde onduidelijkheden worden weggewerkt en er wordt geprobeerd het taal- en woordgebruik te harmoniseren met NEN-EN-ISO 9000 'Kwaliteitsmanagementsystemen -Grondbeginselen en verklarende woordenlijst' en NEN-ISO 31000 'Risicomanagement - Principes en richtlijnen'. Verder liggen er voorstellen om de tekst duidelijker en eenduidiger te maken en verdubbelingen en overbodige toevoegingen te verwijderen. Dit natuurlijk naast het corrigeren van typos. In oktober 2010 wordt in Berlijn vergaderd over de nieuwe versie van deze norm. Het streven is dat de nieuwe versie in 2011 verschijnt.

Zoals misschien bekend, is de 27001 een managementsysteemnorm. In het Engels wordt gesproken van Management System Standard (MSS). Bekende MSS-normen zijn NEN-EN-ISO 9001 'Kwaliteitsmanagementsystemen - Eisen' en NEN-EN-ISO 22000 'Eisen aan een organisatie in de voedselketen'. ISO werkt aan een systeem om alle MSS-normen beter op elkaar af te stemmen door ze op dezelfde wijze te structureren, daar waar mogelijk gelijke tekst te gebruiken en door het gebruik van dezelfde terminologie en definities. De termen moeten aansluiten bij NEN-EN-ISO 19011 'Richtlijnen voor het uitvoeren van kwaliteits- en/of milieumanagementsysteemaudits' en NEN-ISO 31000 'Risicomanagement - Principes en richtlijnen'. Door de MSS-normen te harmoniseren moet een geïntegreerd gebruik ervan worden geoptimaliseerd. De nieuwe structuur heeft als titel meegekregen High Level Structure (HLS).
Voor bedrijven is deze harmonisatie van belang om meer efficiënt en effectief te kunnen werken. Door met de ISO/IEC 27001 aan te sluiten bij de HLS wordt de kwaliteit ervan verhoogd en sluit hij beter aan bij andere managementnormen waardoor bijvoorbeeld

het gecombineerd auditen op de 9001 en 27001 eenvoudiger wordt.
De markt vraagt om geïntegreerde management systemen. De NEN-commissie Informatie- en archiefmanagement kijkt al naar het gezamenlijk toepassen van de MSS-normen NEN-ISO/IEC 27001, NEN-EN-ISO 9001 en ISO NEN-ISO 15489-1 'Informatie- en archiefmanagement - Deel 1: Algemeen'. Binnenkort verschijnt een Nederlandse Praktijk Richtlijn (NPR) waarin beschreven wordt hoe deze drie normen samen toegepast kunnen worden, NPR 2083 'De geïntegreerde toepassing van ISO- en ISO/IEC-normen in de informatiehuishouding'.

ISO/IEC 27006 'Requirements for bodies providing audit and certification of information security management systems' is de norm waarmee organisaties kunnen worden geaccrediteerd zodat ze tegen de 27001 mogen certificeren. De 27006 is gebaseerd op en in lijn met ISO 17021-1 die beschrijft waar certificerende instellingen aan moeten voldoen. Van ISO 17021 is een revisie verschenen en ISO/IEC 27006 moet in overeenstemming worden gebracht met deze nieuwe versie. Echter, hoewel de verantwoordelijke ISO-experts voor een revisie zijn, hebben de normalisatie-instituten van de verschillende landen hier nog geen eenduidig besluit over genomen. Of er een revisie komt wordt waarschijnlijk tijdens de eerder genoemde vergadering in oktober in Berlijn besloten.

Groep 3: richtlijnen (guidelines standards)

Het betreft hier richtlijnen voor het toepassen van de eisen uit de voorgaande groep. Op het moment zijn er acht normdocumenten die onder deze categorie vallen waarvan NEN-ISO/IEC 27002 'Code voor informatiebeveiliging' de bekendste is. Ook deze norm wordt herzien. Er zijn ruim 700 commentaren binnengekomen waarvan meer dan 600 inhoudelijk van karakter. Gepland is dat de nieuwe versie eind 2012 verschijnt.

ISO/IEC 27005 'Information security risk management' wordt ook herzien. Gekozen is voor een korte revisieronde waarin de norm wordt aangepast aan NEN-ISO 31000 'Risicomanagement - Principes en richtlijnen' en aan Guide 73 'Risicomanagement - Verklarende woordenlijst'. Er staan geen grote technische aanpassingen op stapel.

De andere normdocumenten zijn:
NEN-ISO/IEC 27003 'Information security management system implementation guidance', een richtlijn die de 27001 ondersteunt.
NEN-ISO/IEC 27004 'Information security management - Measurement', bedoeld om het effect te meten van de implementatie van de 27001.
Deze beide normen zijn gepubliceerd. Daarnaast zijn nog vier normen in ontwikkeling:
ISO/IEC 27007 'Guidelines for information security management systems auditing', gepland voor eind 2011.
ISO/IEC 27008 'Guidance for auditors on information security management systems controls', gepland voor mei 2012.
ISO/IEC 27013 'Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001', gepland voor eind 2012.
ISO/IEC 27014 'Information security governance framework', gepland voor eind 2012.

Groep 4: sector specifieke eisen en richtlijnen (sector-specific requirements/ guidelines standards)

De hiervoor genoemde normen zijn algemeen toepasbaar. Echter, er zijn normen die zich specifiek richten op informatiebeveiliging binnen een bepaalde sector. Initiatieven voor deze sector specifieke normen zijn soms genomen binnen de normcommissie Informatiebeveiliging en hebben een nummer in de 270xx-serie. Hieronder een overzicht:

ISO/IEC 27010 'Information security management for inter-sector and inter-organisational communications' voor communicatie en samenwerking tussen de publieke en/of private sector. De norm is in ontwikkeling en wordt waarschijnlijk afgerond in november 2012.
NEN-ISO/IEC 27011 'Information security management guidelines for telecommunications organizations based on ISO/IEC 27002'. Deze is reeds gepubliceerd en in 2011 wordt gekeken of hij herzien moet worden.
ISO/IEC 27015 'Information security management guidelines for financial and insurance services'. Deze norm wordt ontwikkeld in samenwerking met de ISO-commissie Financiële diensten (ISO/TC 68). Verwacht wordt dat hij eind 2012 wordt gepubliceerd.

Een sector specifieke richtlijn kan ook zijn oorsprong hebben binnen een sector specifieke ISO-commissie. Echter, bij deze normen is vaak gebruik gemaakt van normen uit de 270xx-serie. Een overzicht:
NEN-EN-ISO 27799 'Informatiebeveiligingsmanagement in de gezondheidszorg volgens ISO/IEC 27002'. Deze norm is ontwikkeld door ISO/TC 215 'Health informatics'. De revisie van NEN 7510 die voorjaar 2011 verschijnt, is gebaseerd op de 27799 en de 27002.

Verder kan genoemd worden NEN-ISO/TR 13569 'Financiële diensten - Leidraad voor de beveiliging van informatie. Deze TR (Technical Report, dus géén norm) is door ÍSO/TC 68 gemaakt.

Groep 5: maatregel-specifieke richtlijnen (control-specific guideline standards)

Op het moment wordt in deze serie aan zes normen gewerkt. Ter informatie, een norm kan uit verschillende delen bestaan. NEN-ISO/IEC 27033 'Network security' is hier een voorbeeld van. Deel 1, 'Overview and concepts' is verschenen. Er zijn drie delen in ontwikkeling. Deel 2,'Guidelines for the design and implementation of network security', deel 3, 'Reference networking scenarios - Threats, design techniques and control issues' en deel 4, 'Securing communications between networks using security gateways - Threats, design techniques and control issues'. Besloten is deze norm met nog drie delen uit te bereiden, voor 'Virtual private networks'. Voor 'IP convergence' en een voor 'Wireless networks'. De komende maanden worden de eerste voorstellen voor deze drie nieuwe delen doorgenomen door de nationale normcommissies.
In de laatste ontwikkelfase is ISO/IEC 27031 'Guidelines for ICT readiness for business continuity'. Verder wordt gewerkt aan ISO/IEC 27034 'Application security', een norm in vijf delen. Verwacht wordt dat deel 1, 'Overview and concepts' eind 2011 wordt gepubliceerd, de vier andere delen in 2013. ISO/IEC 27035 'Information security incident management' wordt ook eind 2011 verwacht.
Tot slot, er wordt onderzocht of er behoefte is aan een norm voor 'ICT Supply chain security'.

Mogelijke toekomstige onderwerpen in de 270xx-serie

Er wordt natuurlijk nagedacht over hoe de 27001 verder te ondersteunen en kracht bij te zetten. Zo wordt er gesproken over een norm voor 'Monitoring and review' van interne procedures, voor 'Continual improvements' en voor een management review norm. Verder wordt gedacht aan een norm voor informatiebeveiliging van het midden- en kleinbedrijf (MKB) en 'home users' op basis van de 27001: hoe kan een MKB-bedrijf een ISMS opzetten en onderhouden? Er is nog geen concreet voorstel maar er is de intentie om er aan te gaan werken.

Tot slot

De commissie 'IT beveiligingstechnieken' van het Nederlands Normalisatie-instituut (NEN) werkt mee aan de normen van JTC 1/SC 27. Heeft u suggesties voor aanvullingen en/of

De internationale normcommissie voor IT-beveiligingstechnieken

commentaar inzake een van de genoemde normen? Neemt u dan contact op met de secretaris van de commissie.

Ter informatie

Voor informatie over de NEN-commissie kunt u contact opnemen met de secretaris van de commissie: Jan Rietveld, e-mail: jan.rietveld@NEN.nl, telefoonnummer (0156) 26 90 376.

Informatie over de documenten van de normcommissie vindt u via Technical Committees op de ISO-website: www.iso.org.

Informatie over de NEN-commissie vindt u op www.nen.nl/IT-beveiligingstechnieken.

Sommige 'ISO/IEC JTC 1/SC 27'-normen zijn kosteloos beschikbaar via: http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm.

Geprinte versies van deze normen kunt u via NEN.nl bestellen.

Het artikel uit IB-magazine 7 (novembernummer van 2009) is te downloaden als PDF op de website van PvIB: https://www.pvib.nl/download/?id=13614545&download=1.

Overzicht van de normen die verschenen zijn en die in ontwikkeling zijn.

ISO/IEC	Publicatie-jaar	Titel	Status
27000	2009	Overview and vocabulary	Gepubliceerd
27001	2005	Requirements	Gepubliceerd
27002	2005	Code of practice for information security management	Gepubliceerd
27003	2010	Information security management system implementation guidance	Gepubliceerd
27004	2009	Information security management - Measurement	Gepubliceerd
27005	2008	Information security risk management	Gepubliceerd
27006	2007	Requirements for bodies providing audit and certification of information security management	Gepubliceerd
27007		Guidelines for information security management systems auditing	In ontwikkeling
27008		Guidelines for auditors on information security management systems controls	In ontwikkeling
27010		Information security management for intersector and inter-organisational communications	In ontwikkeling
27011	2008	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Gepubliceerd
27013		Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001	In ontwikkeling
27014		Information security governance framework	In ontwikkeling
27015		Information security management guidelines for financial and insurance services	In ontwikkeling
27031		Guidelines for ICT readiness for business continuity	In ontwikkeling
27032		Guidelines for cybersecurity	In ontwikkeling
27033-1	2009	Network security - Part 1: Overview and concepts	Gepubliceerd
27033-2		Network security - Part 2: Guidelines for the design and implementation of network security	In ontwikkeling
27033-3		Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues	In ontwikkeling
27033-4		Securing communications between networks using security gateways - Threats, design techniques and control issues	In ontwikkeling
27033-5		Network security - Part 5: Securing communications across networks using Virtual private Network (VPNs) - Threats, design techniques and control issues	In ontwikkeling
27033-6		Network security - Part 6: IP convergence	In ontwikkeling
27033-7		Network security -Part 7: Wireless	In ontwikkeling
27034-1		Application security - Part 1: Overview and concepts	In ontwikkeling
27034-2		Application security - Part 2: Organization normative framework	In ontwikkeling
27034-3		Application security - Part 3: Application security management process	In ontwikkeling
27034-4		Application security - Part 4: Application security validation	In ontwikkeling
27034-5		Application security - Part 5: Protocols and application security controls data structure	In ontwikkeling
27035		Information security incident management	In ontwikkeling
27036		Guidelines for security of outsourcing	In ontwikkeling
27037		Guidelines for identification, collection and/or acquisition and preservation of digital evidence	In ontwikkeling
27038		Specification for digital redaction	In ontwikkeling

Big Brother, Soft Sister... Friendly Foes

In 1948 introduceerde Orwell Big Brother. Het zou nog vele jaren duren voor zijn 'alom aanwezige leider' intrede deed in discussies over privacy. De overheid als Grote Broer waar je als burger toch echt erg voor moet oppassen: hij weet alles van je en kan met gemak achter de voordeur kijken. Hoewel wat gechargeerd gezegd, zit er nog steeds een kern van waarheid in het loerende gevaar van Big Brother die inmiddels steeds vaker wordt omgedoopt tot Soft Sister, 'de liefdevolle zus die alles van je mag weten'. De overheid kan veel gegevens aan elkaar koppelen, heeft inzicht in ons

meest intieme leven en door gebruik te maken van allerlei datamining-technieken kan ze ook profielen samenstellen over verwacht toekomstig gedrag. Wie denkt dat dit futuristisch klinkt en niet gespeend is van enige linksdenkerij, nodig ik uit om eens te beginnen met zoeken naar informatie over de 'Verwijsindex Risicojongeren' en dan vooral de voorgeschiedenis ervan. (In 1998 al startte de gemeente Rotterdam met het zogenaamde risicosignaleringssysteem; het is dus niet nieuw.) Om nog maar te zwijgen over de extreme hoeveelheid taps die onze overheid elk jaar pleegt te 'zetten'. Ook commerciële bedrijven die een wellicht veel sluipender gevaar vormen voor onze privacy, daar zij vaak niet controleerbaar handelen, weten veel over ons. Wat kopen we, waar kijken we naar, hoe betalen we (betalen we überhaupt wel), waar wonen we, wat zijn onze persoonlijke voorkeuren en wat zouden we misschien graag willen gaan kopen? En daar stopt het niet. Ik zou graag nog een relatief nieuwe speler aan deze lijst willen toevoegen: de Friendly Foes.

Friendly Foes, dat zijn mijn eigen vrienden. Ja, echt. Ook die vormen tegenwoordig steeds vaker en steeds indringender een gevaar voor mijn persoonlijke privacy. Ik ben namelijk online allang niet meer de enige die iets over mij zegt, ook mijn vrienden zeggen regelmatig iets over mij. Bedoeld, onbedoeld, per ongeluk of expres. En dat gaat op den duur (hoe vluchtig wellicht) ook onderdeel uitmaken van het beeld dat anderen van mij hebben en dus van mijn identiteit. Ik heb Jochem Meyer zien twitteren dat zijn voorgaande tweet toch echt, oeps, eigenlijk bedoeld was als een sms aan zijn vriendin (twijfelachtig, maar toch). En ook ikzelf heb wel eens een persoonlijk bericht ontvangen met de mededeling dat de tweet die zojuist 'live' gegaan was en in het openbaar verscheen eigenlijk een DM (Direct Message) had moeten zijn. Nu was het nog een vrij onschuldige mededeling (althans zo op het blote oog - gelukkig was de eraan voorafgaande communicatie wel besloten gebleven). Maar, het had net zo goed verstrekkende gevolgen kunnen hebben.

Zo ervoer gerenommeerd journaliste Laurie Garret na het uitlekken van een persoonlijke e-mail aan haar 'vrienden'. In een licht ironisch epistel had zij verslag gedaan van de persoonlijke onderonsjes van grote wereldleiders op een Wereldtop in Davos. Een van de vrienden vond het nodig deze e-mail te forwarden naar zijn volledige adresboek en in een mum van tijd stond het bericht op internet. Laurie Garret's naam erbij, maar alle contextuele informatie verdwenen. Ik geloof dat het nog steeds niet helemaal goed gaat met haar reputatie. Herinnert iemand zich Willibrord Frequin en de schedels nog? Reputatieschade blijft lang aan je kleven en al helemaal in de online-wereld waar 'social forgetfulness' praktisch nihil is.

Friendly Foes. Ze bestaan. Ze zijn echt. En het zijn er steeds meer. Het gaat ook lang niet altijd expres. Wat de een ervaart als een schending van zijn privacy, vindt de ander totaal niet relevant. Dat is tegelijk het lastige van dit vraagstuk. Vaak gaat het toch om vrienden zonder slechte bedoelingen, maar zijn we alleen even niet insync wat betreft onze privacywensen en verwachtingen. En ja, ook ik ben er wel eens op gewezen dat ik een bericht de openbare wijde wereld had ingestuurd wat eigenlijk in het geheel niet op prijs werd gesteld. Vooruit, voor de nieuwsgierigen: ik had gesproken over het feit dat iemand al vroeg onder de wol was gekropen. Deze persoon had echter zeer zorgvuldig de zakelijke reputatie opgebouwd immer 's avonds laat nog hard te werken en was bang dat deze reputatie door mijn bericht schade werd aangedaan. Je kunt ervan denken wat je wilt, voor mij was het een nietszeggend bericht, voor de 'ontvangende' kant had het minder aangename connotaties. Naast kritisch zijn op de informatiedrang van Big Brother alias Soft Sister moeten we dus nu ook steeds vaker naar onze vrienden gaan en onderhandelen met onze Friendly Foes over onze waarden, verlangen en wensen aangaande onze privacy in de online wereld. Friendly Foes hebben echter wel een streepje voor op onze Big Brother alias Soft Sister; doorgaans luisteren ze beter en zullen ze eerder bereid zijn, omwille van de vriendschap, hun gedrag aan te passen.

mr. Rachel Marbus
(@RachelMarbus op Twitter)

Herstel van de zwakste schakel

Zwichten voor autoriteit

Auteur: Jan de Boer MSIT > Jan de Boer MSIT is als managing consultant werkzaam bij Capgemini. Zijn Master Thesis betrof de psychologie in de informatiebeveiliging. Zijn vakgebied is de integrale (informatie)beveiliging. Social Engineering is zijn hobby. Hij is bereikbaar op jan.de.boer@capgemini.com.

Dit is het zesde artikel in een serie van acht waarin wordt ingegaan op de psychologische trucs die door Social Engineers worden gebruikt om slachtoffers te manipuleren. Waarom en hoe werken ze? Hoe zijn ze te herkennen en wat is de beste verdediging? In dit artikel komt het aspect Autoriteit aan de orde.

Social Engineering; een korte terugblik

In de informatiebeveiliging wordt de mens steeds omschreven als de zwakste schakel. Mede door extreme resultaten van security audits in de vorm Social Engineering (SE), zoals het in ontvangst mogen nemen van vijf handvuurwapens, ben ik er steeds meer van overtuigd geraakt dat de beveiliging niet zit in firewalls, hoge hekken, SafeWord tokens en andere technische beveiligingsmaatregelen maar in de mens zelf. De mens is inderdaad de zwakste schakel.

Uit een onderzoek onder 250 CIO's en CISO's van bedrijven en overheden naar (informatie)beveiliging is gebleken dat 60% GEEN aandacht schenkt aan het beveiligingsbewustzijn van de medewerkers. Een opmerkelijk hoog percentage aangezien 16% aangeeft dat er informatie is gestolen met behulp van SE en dat zelfs 23% aangeeft de dreiging van diefstal door SE als serieus ervaart.

Deze artikelserie over het hoe en waarom van menselijk gedrag en hoe daar misbruik van kan worden gemaakt door profiteurs, is bedoeld als bijdrage aan een reeds bestaand bewustwordingsprogramma van een organisatie. Maar het is ook prima primair inzetbaar als zelfstandig bewustwordingsprogramma voor een risicogroep zoals secretaresses of bewakingspersoneel. De artikelen behandelen de psychologische mechanismen die door SE's worden gebruikt om tegenstanders te manipuleren. Er wordt ingegaan op de achtergrond van de werking en er vindt een verduidelijking plaats aan de hand van voorbeelden uit de praktijk. Verder worden maatregelen aangedragen om een aanval te herkennen en af te slaan.

Autoriteit: eigen ervaring (1)

Bij een ministerie was de beveiliging van de kantoren van de minister en zijn directe staf sterk verbeterd. De Plaatsvervangend Secretaris Generaal had mij gevraagd om deze beveiliging te testen. Ik kwam (gekleed in driedelig kostuum) hard aangelopen bij de bewaking van de achteringang en parkeerplaats van de auto's van de hogere ambtenaren. Hijgend zei ik tegen de portier dat ik zojuist bij het verlaten van het complex mijn elektronische toegangspas was vergeten en vroeg hem of ik het pasje even mocht ophalen. Hij aarzelde. Ik zei dat de Plaatsvervangend SG (ik noemde de voor en achternaam) twee straten verder ongeduldig stond te wachten. Er was haast bij en ik moest snel mijn pas hebben. De poort ging open en ik rende snel naar een toegangdeur. Binnen in het gebouw pakte ik twee lege dozen uit het printerhok en deed daar mijn colbertje en vestje in en liep met de twee dozen naar de toegang van het compartiment van de minister. Ik sloot achter een man aan die ook in dezelfde richting liep. Toen hij zijn pas aanbood en het poortje open ging begon ik hoorbaar te mopperen dat ik mijn pas op mijn kantoor vergeten was. Hij was erg vriendelijk en opende het poortje voor me (er was geen anti-pass-back). Mijn visitekaartje heb ik vervolgens op het toetsenbord van mijn opdrachtgever achtergelaten ten teken dat de opdracht was uitgevoerd.

Door te benoemen dat ik in opdracht van een bekende en hooggeplaatste autoriteit handelde (de Plaatsvervangend Secretaris Generaal), voldeed de bewaker aan mijn verzoek en werd ik toegelaten tot het complex.

Autoriteit

Elk mens voert nagenoeg iedere opdracht uit als een autoriteit dit van hem verlangt. Vanaf de geboorte wordt ons geleerd dat gehoorzaamheid aan goede autoriteiten juist is. Die 'goede' autoriteiten variëren van je ouders tot leraren, artsen en de politie. Daarbij maakt het (in het kader van dit artikel) niet uit of de persoon zijn autoriteit ontleent aan bijzondere kennis of aan gezag met een wettelijke grondslag. Natuurlijk kent iedereen wel een periode in zijn leven waarin er verzet werd gepleegd tegen deze autoriteiten maar voor de meesten is dit gedrag ten goede gekeerd.

Het gehoorzamen aan autoriteiten levert ons meestal voordelen op. Doordat zij zoveel kennis of macht hebben, is het vaak verstandig om deze autoriteiten te gehoorzamen. Je verzetten tegen een controle door de politie levert doorgaans alleen nog maar meer vertraging op. Wanneer we dus ontdekken dat gehoorzaamheid vrijwel altijd iets oplevert, bestaat de kans dat we er een automatisme van maken.

Vaak zijn we niet alleen gevoelig voor de autoriteiten zelf, maar ook met de symbolen die we met hen verbinden, zoals titels, kleding en bepaalde voorwerpen. Forse mannen dwingen meer respect af dan kleine. Oplichters dragen daarom vaak verhoogde schoenen. Mensen willigen verzoeken veel gemakkelijker in als de vragers in uniform gekleed zijn of op een andere wijze worden geassocieerd met een autoriteit (door bijvoorbeeld de genoemde symbolen). Ook mensen die in kostuum lopen kunnen op ontzag rekenen. Attributen als dure auto's, merkkleding, laptops, de nieuwste PDA's en juwelen zijn ook prima gezagssymbolen.

Autoriteit: eigen ervaring (2)
In het kader van een korte opleiding over de menselijke aspecten van beveiliging zat een kleine groep collega's te wachten tot ik zou binnen komen. Maar in plaats daarvan had ik me voorgenomen om de groep zelf te laten ervaren hoe zij zouden reageren op gezag. Een vriendin had een hesje aangetrokken met daarop de tekst ONTRUIMER. Zij liep de ruimte binnen en zei kort maar krachtig: "Er is beneden een kleine brand ontdekt. Ik wil dat u uw spullen pakt en direct het pand verlaat via het trappenhuis". Daarna verdween zij weer. Ik stond in het trappenhuis te wachten en ving de verbaasde groep op waarna ik gestart ben met mijn korte opleiding.

Autoriteit: eigen ervaring (3)
Als training 'on the job' was een vrouwelijke collega toegevoegd aan het team van SE's. Zij was gekleed in het werkuniform van de brandweer (blauwe werkbroek en blauw T-shirt). Nadat we ongemerkt het pand waren binnengekomen zijn we omstreeks 18.00 uur langs alle interessante afdelingen gegaan. Er waren nog veel mensen aan het werk maar niemand keek op van zijn werk. Toen we bij de ICT-afdeling aankwamen was deze op slot. Onze trainee heeft daarop haar stoute schoenen aangetrokken en is naar de particuliere bewaker gegaan die dienst had aan de balie bij de ingang. Zonder enige terughoudendheid verstrekte hij de sleutel van de ICT-afdeling waar wij vervolgens grote hoeveelheden laptops aantroffen en de back-up-tapes van het netwerk. Ze was met vlag en wimpel geslaagd.

Autoriteit kun je gewoon aantrekken
Een uniform maakt nog geen autoriteit van een persoon zou je denken, maar toch zijn mensen geneigd om die autoriteit te accepteren alleen al bij het zien van een uniform. Bij een zoektocht op het internet blijkt al heel snel dat je bijna ieder uniform kunt kopen, bij speciale winkels of gewoon tweedehands. Officiële legitimatiebewijzen van politie of brandweer zijn na korte tijd ook op het internet te vinden. En weet de gewone burger eigenlijk wel hoe die er uitzien? Met behulp van een goede kleurenprinter of smartcardprinter heb je al snel een pas op naam van je alias. Het blijkt dat zelfs overheidsinstanties die een legitimatieplicht kennen voor bezoekers, een nagemaakte pas accepteren, zeker als je ook nog een bibliotheekkaart en een giropas op naam van je alias kunt overleggen.

Mensen willigen verzoeken veel gemakkelijker in als de vragers in uniform zijn gekleed.

Verdediging
Vaak zijn we niet voorzichtig genoeg wanneer volgzaamheid gevraagd wordt. Door constant waakzaam te blijven tegenover zogenaamde autoriteiten kunnen we achteraf minder snel voor verrassingen komen te staan. Wanneer we ons bovendien nog eens extra bewust worden van het feit dat gezagssymbolen eenvoudig kunnen worden nagemaakt, zullen we ook waakzamer zijn wanneer autoriteiten ons willen beïnvloeden.
De enige kanttekening is echter dat we liever niet tegen het gezag ingaan. Meestal is het immers juist om autoriteiten te gehoorzamen. Je kunt het beste leren ontdekken wanneer je de richtlijnen van autoriteiten wel en wanneer je deze niet zou moeten opvolgen. Maar voorkom wel dat het een tweede puberteit gaat worden.

Twijfel je over een autoriteit? Stel jezelf dan de volgende twee vragen:
1. Is de autoriteit daadwerkelijk deskundig?
2. Is deze autoriteit ook betrouwbaar?

Samenvatting
'Geen uniform is heilig' maar toch zijn we onbewust geneigd autoriteit te erkennen als er een uniform gedragen wordt of attributen die geassocieerd worden met een functie met status. Aanwijzingen van autoriteit opvolgen is raadzaam want verzet levert doorgaans alleen maar ellende en vertraging op. Maar wees je er van bewust dat zogenaamde autoriteiten niet altijd deskundig en betrouwbaar zijn.

De tendens van de afnemende macht
Het lijkt er op dat autoriteit niet meer als vanzelfsprekend wordt gezien en dat de macht afneemt. Voordat we met een klacht naar een huisarts gaan hebben we vaak op het internet al opgezocht welke ziekte daar mee in verband zou kunnen staan. Doordat medische kennis ook voor ons beschikbaar is neemt de macht van de huisarts af. Geweld tegen geüniformeerden zoals conducteurs en ambulancepersoneel neemt toe. In groepsverband opererende jongeren in het uitgaansleven tarten de politie zonder dat zij daarvoor worden gestraft. Toch lijkt de macht niet af te nemen als mensen op individuele basis plotseling geconfronteerd worden met een dergelijke autoriteit. Dan zijn ze doorgaans gewoon weer volgzaam.

‘Gescoopt’ Risico Management

Auteur: Rieks Joosten > Rieks Joosten doet onderzoek in het Claims-based lab van TNO in Groningen op het gebied van robuuste, op bedrijfsregels gebaseerde processen. Speciale aandacht hierbij heeft het ontwerpen en het beheren van deze regels op basis van risico analyses, alsmede een op information cards gebaseerde infrastructuur hiervoor. Hij is bereikbaar via rieks.joosten@tno.nl.

Vanuit de geschiedenis weten we dat kleine gebeurtenissen en verwaarloosbaar ingeschatte risico’s, grootschalige uitval van dienstverlening tot gevolg kunnen hebben. Daarom is een actueel overzicht van dreigingen en goed ingeschatte risico’s onontbeerlijk. Binnen grote organisaties zoals overheden, telecom operators, energieleveranciers, en ziekenhuizen, is het beheersen en inzichtelijk maken van risico’s geen sinecure. Niet alleen zijn de aantallen risico’s binnen zulke organisaties onoverzichtelijk groot, maar ook de samenhang ertussen is erg complex. Veel methoden voor de analyse en het managen van risico’s werken weliswaar goed voor kleinere organisaties, maar schalen niet goed naar grote organisaties. Dit artikel beschrijft een werkwijze voor risico management die wel schaalbaar is.

Risico management (RM) binnen grote organisaties is om een aantal redenen zeer complex. Grote organisaties kunnen gemakkelijk tientallen of honderden gebouwen hebben, duizenden systemen, en tienduizenden applicaties, processen en registraties. Alleen al voor systemen bevatten standaardlijsten van mogelijke risico’s en dreigingen er al gauw tien- tot honderdtallen. PriceWaterhouseCoopers [PWC08] stelt dat bijna de helft van de organisaties geen kwetsbaarheden kan aanwijzen die geleid hebben tot security-incidenten.

Een verklaring hiervoor is dat de aantallen risico’s en dreigingen voor mensen eenvoudigweg te groot is om te overzien en lastig te inventariseren en dit actueel te houden. Miller [Miller56] merkte meer dan een halve eeuw geleden al op dat de grens waarbij mensen nog informatie kunnen opnemen en verwerken, heel erg beperkt is. Nu schrijven standaarden en guidelines als ISO [ISO31000] en NIST [NIST02] voor dat als eerste stap in het RM-proces de scope en context van het systeem moeten worden vastgesteld. Dat maakt RM overzichtelijk voor organisaties wiens systemen elk afzonderlijk voldoende overzichtelijk zijn.

De echt grote organisaties hebben echter systemen of diensten die onoverzichtelijk zijn. Daar blijven we dus tegen de fysiologische grenzen van ons mens-zijn aanlopen.

Een tweede reden dat RM complex is heeft te maken met de samenhang tussen risico’s onderling, en tussen risico’s en maatregelen. Een oliecrisis kan bijvoorbeeld leiden tot uitval van het elektriciteitsnet, waardoor noodstroomvoorzieningen extra worden belast. Het gevolg is dat het risico op uitval van vitale systemen (bijvoorbeeld beademingsapparatuur) groter wordt. De maatregel om een operatingsysteem te vervangen door een veiligere variant, met als doel het risico van een virusuitbraak te reduceren, ook tot gevolg hebben dat die kleine applicatie waarmee de ‘speciale service’ wordt geleverd die een paar grootzakelijke klanten hebben afgedwongen, niet langer beschikbaar is. Reason [Reason90] beschrijft dit aan de hand van zijn ‘Swiss Cheese’ model. Alleen organisaties die zulke samenhangen beheersen, kunnen voorzien dat deze maatregel het risico van het verlies van een paar grootzakelijke accounts met zich meebrengt.

Naast deze redenen zijn er tal van praktische redenen die RM kunnen bemoeilijken. Als bijvoorbeeld de verantwoordelijkheden voor diensten, processen of systemen niet eenduidig zijn belegd, dan is daarmee ook niet duidelijk wie verantwoordelijk is voor het inventariseren en behandelen van de bijbehorende risico’s. Dat geldt ook als het kan voorkomen dat bij het niet langer beschikbaar zijn van de verantwoordelijke persoon, (ziekte, verandering van werkkring) de verantwoordelijkheid niet opnieuw wordt belegd of de nieuwe verantwoordelijke hiervan niet actief in kennis wordt gesteld.

Afbakenen

Bij risicomanagement moeten alle voorkomende taken behapbaar blijven. Alleen deze taken kunnen consciëntieus en min of meer foutloos worden uitgevoerd. Een kenmerk van goede RM-methodes, is dat met het groeien van het aantal bedrijfsmiddelen (en daarmee het aantal risico’s), het aantal RM-taken evenredig groeit en daarmee het benodigde aantal uitvoerende personen.

ISO [ISO31000], NIST [NIST02] en andere standaarden en guidelines schrijven in het RM-proces als eerste stap voor dat de scope en context moeten worden vastgesteld. Concreet betekent dit dat het bepaalde afbakeningscriterium (‘scopecriterium’) vaststelt wat binnen de scope valt en wat daarbuiten en daarmee deel uitmaakt van de context. Het belang van afbakenen is echter niet alleen om te kunnen onderscheiden wat al dan niet binnen de scope van RM valt. Een goede afbakening beoogt ook het bijbehorende werk behapbaar te houden. Dat maakt dat elk scopecriterium aan twee bruikbaarheidseisen moet voldoen.

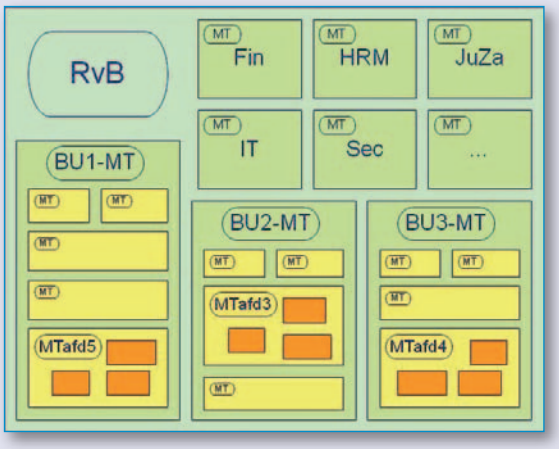


Fig. 1. Scoping met de organieke lijn.

De eerste eis aan scopecriteria, die we de *'behapbaarheidseis'* noemen, moet zijn dat het af te bakenen gebied overzichtelijk is voor mensen. Anderson [Anderson95] stelde al dat mensen op enig tijdstip niet meer dan zeven concepten tegelijk kunnen overzien. Wie dat toch probeert gaat fouten maken. Als RM via de organieke lijn is belegd, heeft deze eis de ogenschijnlijk paradoxale consequentie dat de organisatiebrede RM een scopecriterium moet hebben die zich slechts over een deel van de (hele) organisatie kan uitstrekken. Dit geldt ook voor grote organisatie-eenheden zoals business units. Fig. 1 maakt dit zichtbaar. De buitenste rechthoek stelt een (grote) organisatie voor, met het bijbehorende management team (MT, hier aangegeven als RvB). Binnen de organisatie zitten stafafdelingen (aangegeven met Fin, HRM, JuZa, IT, Sec, enz.) en business units (BU1, BU2 en BU3) die elk een eigen MT hebben. We willen hier benadrukken dat binnen de buitenste rechthoek alleen het lichtstgroene gedeelte de scope vormt waarbinnen zich het organisatiebrede RM zich afspeelt. Alles wat zich binnen de stafafdelingen en BU's afspeelt hoort bij het RM-proces van de betreffende afdeling/BU. De groengekleurde stafafdelingen en BU's bestaan immers om de RvB van zekere taken te ontlasten, en horen dan ook de daarbij behorende risico's zelf te managen. Later gaan we in op hoe dit dan samenhangt met de bedrijfsbrede RM. We merken op dat, aangezien de structuur binnen de BU's dezelfde is als hiervoor beschreven (namelijk dat binnen elke BU (staf)afdelingen zitten met elk hun eigen MT) het RM daarbinnen ook volgens dezelfde principes en samenhangen geregeld kan worden.
De tweede eis, die we de *'eenduidigheidseis'* noemen, is dat scopecriteria zodanig eenduidig moeten zijn dat alle (verschillende) stakeholders het er over eens zijn wat binnen en wat buiten de scope valt. Hierdoor kunnen vaak lange maar nutteloze discussies worden vermeden, wat de efficiency van het werk ten goede komt. Het voldoen aan deze eis faciliteert ook het eenduidig beleggen van verantwoordelijkheden, bijvoorbeeld door voor elke scope personen aan te wijzen die plichtverantwoordelijk en/of taakverantwoordelijk (accountable en/of responsible[1]) zijn voor alles wat binnen de scope gebeurt.

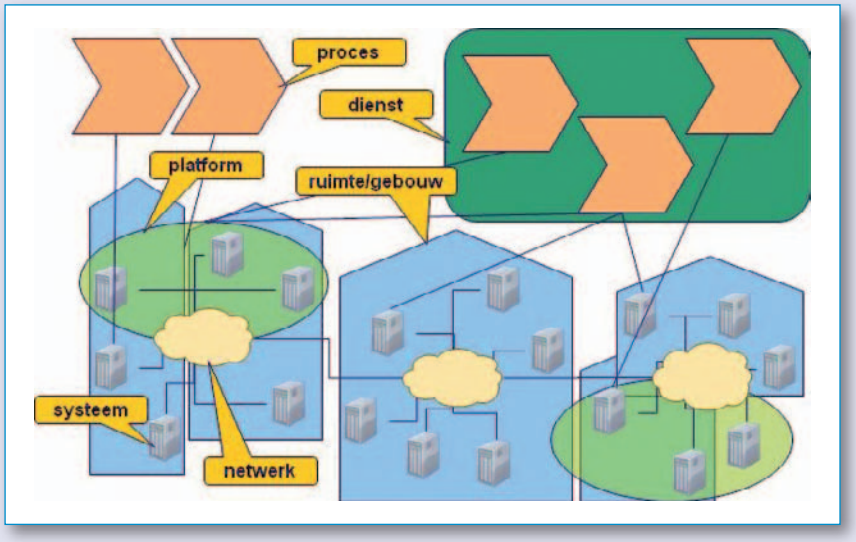


Fig. 2. Samenhang tussen bedrijfsmiddelen.

Het hebben van goede scopecriteria is niet alleen van belang voor 'de lijn', maar ook in de organisatie waar operationeel werk plaatsvindt waarbij werk over afdelingen heen loopt. Als een organisatie bijvoorbeeld specifiek haar HRM-risico's wil managen, moet als eerste een goede afbakening plaatsvinden van wat dit behelst. Een afbakeningscriterium 'HRM' volstaat alleen als alle betrokkenen binnen de organisatie dezelfde antwoorden geven op vragen als: 'Valt het beheer van mobiele telefoons voor werknemers hieronder?' of 'Valt de Peoplesoft-applicatie ook binnen de scope?' Eenduidigheid verkrijgen voor dit type afbakeningen is moeilijker dat voor de organieke lijn.

Fig laat schematisch zien hoe verschillende soorten bedrijfsmiddelen met elkaar samenhangen. De figuur toont bijvoorbeeld dat systemen via netwerken aan andere systemen gekoppeld zijn, zich in ruimtes (gebouwen) bevinden, en onderdeel kunnen zijn van een (service)platform. Ook zien we dat diensten bestaan uit processen die weer van systemen en/of platformen gebruikmaken. De figuur laat zien dat bedrijfsmiddelen getypeerd kunnen worden, bijvoorbeeld als dienst, proces, platform, applicatie, systeem, gebouw, ruimte, enzovoort. Ook andere typeringen zijn mogelijk zoals bijvoorbeeld applicatie, registratie en meer. De figuur toont ook dat individuele bedrijfsmiddelen onderling een samenhang vertonen en het moge duidelijk zijn dat die samenhang onoverzichtelijker wordt naarmate het aantal bedrijfsmiddelen groeit. Eerder is al opgemerkt dat een compleet en courant zicht op deze samenhang noodzakelijk is om risico's goed in kaart te kunnen brengen.

Met behulp van een bedrijfsmiddelen-inventarisatie kunnen scopes als 'HRM' concreet worden gemaakt. Als bijvoorbeeld 'HRM' wordt voorgesteld door het groene vlak in Fig, dan zien we drie processen die afhankelijk zijn van één platform (links) en enkele systemen. Echter, als de scope 'HRM' al deze systemen, platformen en processen zou omvatten, dan is weliswaar aan de eenduidigheidseis voldaan (het is immers duidelijk wat wel en wat niet tot 'HRM' behoort), maar niet aan de behapbaarheidseis. Immers, er zitten niet alleen meer dan zeven onderdelen in 'HRM, maar ze zijn bovendien van verschillende soort, wat het overzicht belemmert.

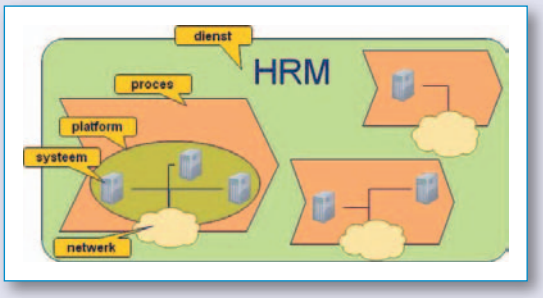


Fig. 3. Scoping met bedrijfsmiddelen.

Fig. 3 laat zien dat we 'behapbaarheid' op vrijwel dezelfde manier kunnen krijgen als we dat (in Fig. 1) met de organieke lijn hebben gedaan. Als we het lichtgroene vlak als de scope 'HRM' zien, en de drie

1 Hiermee past wat we doen binnen het RA(S)CI besturingsmodel.

Voorbeeld

Stel, een organisatie beschikt over een gebouw dat we GN3 noemen. Op de computerzaal staat server S4711, waarop de applicatie DOCA draait. Deze applicatie draait ook op system S1234 die in gebouw AMS1 staat en met server S4711 verbonden is via netwerk NW5. Dat DOCA het documentenarchief is maakt dat voor het opslaan van digitale documenten vrijwel alle bedrijfsprocessen ervan gebruikmaken. Fig. 3 toont deze opzet schematisch, waarbij de gestippelde lijnen de afhankelijkheden aangeven tussen de verschillende scopes.

Als de organisatie gescoopt RM inricht, betekent dit dat de beheerders van beide gebouwen, beide systemen, het netwerk, DOCA, en de processen, allemaal een RM-proces hebben voor dezelfde scope als waarvoor ze beheerder zijn. Zo zal de beheerder van S1234 een risico-analyse (RA) moeten uitvoeren voor dit systeem. Als hij de dreigingen inventariseert, zal daar 'stroomtoevoer naar S1234 valt uit' onder vallen. Dat is een goede dreiging omdat het geheel is geformuleerd in termen die zinvol zijn binnen de eigen scope. Een tekst als 'stroomuitval door bliksemінslag' zal niet worden geaccepteerd als dreiging, omdat (het op orde hebben van) de stroomvoorziening buiten de scope valt. Dit zou weer wel een goede dreiging zijn voor de scopes AMS1 en GN3, omdat de stroomvoorziening voor wat zich in die gebouwen afspeelt binnen deze scopes valt. De beheerder van AMS1 zal in de RA voor zijn scope deze dreiging opnemen en koppelen aan het risico 'stroomtoevoer naar alle (niet van noodstroom voorziene) elektronische apparatuur (binnen AMS1) valt uit'. Als de beheerder van AMS1 dit risico doorgeeft aan de beheerder van S1234, dan kan die dat als dreiging interpreteren en nagaan wat het risico is dat hij daarbij loopt vanuit S1234. Hij moet dit risico dan weer doorgeven aan de beheerder van DOCA die dit weer ziet als een dreiging, enz. Op deze manier propageren alle risico's en dreigingen door de verschillende scopes zodat binnen elke scope een kundige risicoinschatting[2] kan worden gemaakt. Elk RM-proces dat in een scope draait zorgt vervolgens dat de risico's binnen die scope niet uit de hand lopen. Dat kan onder meer door te besluiten maatregelen te nemen die deze risico's reduceren. Dat heeft dan niet alleen effect op de hoogte van het risico, maar ook op de dreigingen van scopes die van de eerste scope afhankelijk zijn. Bilateraal overleg tussen scopebeheerders van onderling afhankelijke scopes is essentieel om de maatregelen af te stemmen zoals bijvoorbeeld in de vorm van een SLA.

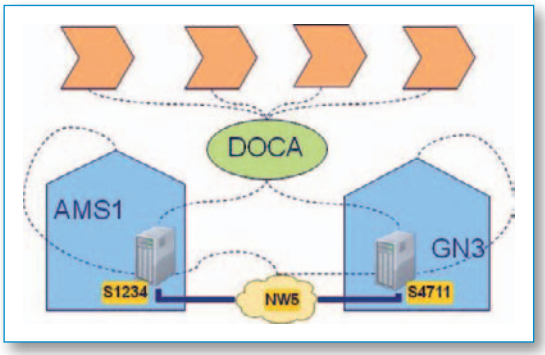


Fig. 4. Voorbeeld van samenhangende scopes.

processen als subscopes daarvan, dan is de taak van 'HRM' om te organiseren en te bewaken dat deze processen in de bedoelde onderlinge samenhang werken. Dat wil zeggen: zorgen dat (1) de processen gezamenlijk de HRM-dienstverlening adequaat vormgeven, (2) de processen daartoe alle benodigde gegevens van/naar andere processen krijgen/sturen en (3) ze onderling resultaten uitwisselen waar nodig. Op soortgelijke wijze kunnen we van elk proces zeggen dat de afbakening wordt weergegeven door de betreffende kleur in het vlak. Dus zonder de platformen, systemen en netwerken die voor de procesondersteuning zorgen, die immers weer eigen scopes zijn en waarbij zodanig de regie wordt gevoerd over de onderliggende scopes dat de resultaten waarvoor het proces verantwoordelijk is, worden geleverd.

Gescoopt Risico Management

Een organisatie die afbakeningscriteria gebruikt die aan beide bruikbaarheidseisen voldoen, ziet zich geconfronteerd met een veelheid aan scopes, waarbij binnen elke scope een RM-taak ligt. Deze waarneming leidt gemakkelijk tot het idee dat overall, RM een welhaast onbegonnen taak zou zijn. Om dit te voorkomen moet consciëntieus met de verschillende RM-taken worden omgegaan.

Criteria

Onder 'gescoopt RM' verstaan we een RM-werkwijze waarbij binnen elke scope:

a) een RM proces[3] draait voor het beheersbaar houden van de risico's binnen deze scope;
b) elke dreiging en elk risico is geformuleerd in termen die horen binnen de eigen scope;
c) elk geïdentificeerd (en gekwalificeerd of gekwantificeerd) risico wordt doorgegeven aan elke scope die van de eigen scope afhankelijk is;
d) elk risico dat naar de eigen scope wordt doorgegeven vanuit scopes waarvan de eigen scope afhankelijk is, wordt behandeld als een dreiging binnen de eigen scope.

Met betrekking tot a) kan een willekeurig RM-proces dienst doen die binnen de kaders van ISO [ISO31000] valt. Denk hier bijvoorbeeld aan ITIL, SEI [SEI93], NIST [NIST02], AS/NZS [AS/NZS4360] en dergelijke. De eigenschap onder b) is een noodzakelijke voorwaarde om aan c) en d) te kunnen voldoen. De eigenschappen c) en d) maken dat risico's als het ware kunnen 'propageren' door verschillende scopes.
Een organisatie (of bedrijfsonderdeel) heeft gescoopt RM ingericht als daarbinnen de volgende criteria[4] worden nageleefd:

a) elk van diens bedrijfsmiddellen is ondergebracht in één scope;
b) voor elk bedrijfsmiddel en elke scope is vastgesteld van welke andere bedrijfsmiddelen c.q. scopes het afhankelijk is voor diens goede functioneren;
c) voor elke scope is één persoon (functionaris) verantwoordelijk voor de RM;
d) binnen elke afbakening is aan de criteria voor gescoopt RM voldaan.

Het werkt eenvoudiger als de afbakening voor bedrijfsmiddelen ook wordt gebruikt

2 Het ligt voor de hand om deze propagatie-eigenschap te gebruiken voor het construeren van Fault Trees IEC [IEC61025]. Daar hebben we echter niet naar gekeken.
3 Dit houdt dus in dat daar dreigingen en risico's worden geïnventariseerd en ingeschat, maatregelen gedefinieerd en geïmplementeerd, etc., zoals dat gebruikelijk is voor een RM proces.
4 Deze criteria zouden deel uit kunnen maken van de organisatie brede risico management policy.

als scope voor RM, zodat de verantwoordelijke voor het bedrijfsmiddel ook voor de scope verantwoordelijk kan worden gemaakt. Deze persoon weet immers al van welke andere bedrijfsmiddelen zijn bedrijfsmiddel afhankelijk is, en welke bedrijfsmiddelen van het zijne afhankelijk zijn. Zo weet hij ook van welke bedrijfsmiddelen hij zijn dreigingen kan verwachten en naar welke bedrijfsmiddelen hij zijn risico's moet exporteren. Daarnaast hoeft hij alleen maar de dreigingen en risico's in kaart te brengen die vanuit zijn eigen bedrijfsmiddel stammen.
Een organisatieonderdeel kan ook als een bedrijfsmiddel worden gezien, dat bijvoorbeeld nodig is om werkkracht (bijvoorbeeld operators) te leveren aan andere bedrijfsmiddelen. Omdat managers van een organisatieonderdeel vaak accountable zijn voor bedrijfsmiddelen, kun je ook zeggen dat de goede werking van dat onderdeel afhankelijk is van die bedrijfsmiddelen. Daarmee kunnen organisatieonderdelen en bedrijfsmiddelen wederzijds van elkaar afhankelijk zijn.

Afspraken tussen scopes

Gescoopt RM helpt bij het maken van afspraken tussen organisaties en/of onderdelen daarvan door de term **'risico'** te definiëren als de inschatting van de waarschijnlijkheid dat een zekere verplichting die op de scope rust, niet waargemaakt gaat worden. **'Verplichtingen'** van een scope zijn dus zaken waarvoor binnen die scope werk moet worden verzet. Verplichtingen zijn er niet alleen ten aanzien van externe partijen (in contracten), maar kunnen ook door wet- of regelgeving zijn opgelegd, of kunnen targets zijn. Het **risico-overzicht** van een scope bestaat dan uit een overzicht van al haar verplichtingen, waarbij voor elk daarvan een inschatting is gegeven van de waarschijnlijkheid dat de verplichting niet kan worden nagekomen: het risico (zie figuur 5).
Fig. **4** geeft een voorbeeld van een risico-overzicht van een scope op een hoog organiek niveau, gezien het strategische karakter van de erin genoemde verplichtingen. Voor scopes lager in de organisatie, zullen de verplichtingen veel specifieker en dus ook veel toetsbaarder zijn.

Met behulp van zo'n risico-overzicht kan een scopeverantwoordelijke besluiten het te accepteren, reduceren, op te heffen of af te wentelen. Afwentelen kan bijvoorbeeld door de boete van het niet nakomen te

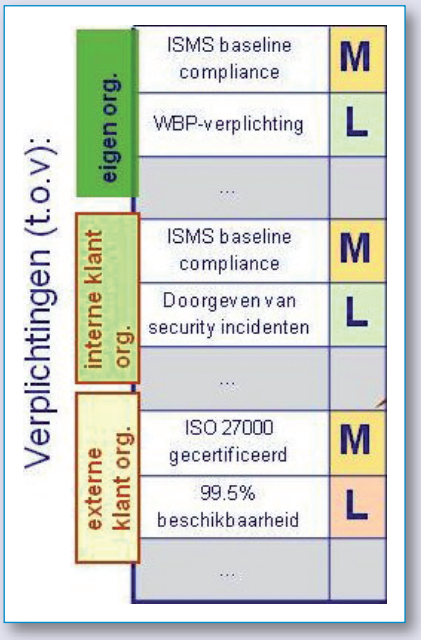


Fig. 5. Risicolijst.

verzekeren, opheffen door na te gaan of de verplichting kan worden verzacht en reduceren betekent doorgaans het specificeren van 'controls'.
Specificaties van controls kunnen we zien als **verwachtingen** die een scope heeft, en wel zo dat als er aan wordt voldaan, risico's worden gereduceerd. Als aan alle verwachtingen is voldaan, dan zijn de resterende risico's acceptabel. Zo worden controls geselecteerd. Daarom is het van belang dat verwachtingen toetsbaar zijn. Dat kan met prestatie-indicatoren (PI's). Als een verwachting van een scope niet wordt waargemaakt, dit een **dreiging** omdat het betekent dat de scope mogelijk niet meer aan (alle) verplichtingen kan voldoen.
Door verwachtingen uit te zetten bij andere scopes (bijvoorbeeld via een SLA of een contract waarin de PI's zijn opgenomen), of binnen de eigen scope (bijvoorbeeld door middel van targets, die eigenlijk al PI's zijn) wordt duidelijk wie vanuit de scope moet worden aangesproken mocht niet aan de verwachting zijn voldaan. Verwachtingen die uitgezet zijn bij een andere scope, worden voor die andere scope verplichtingen op het moment dat deze ze accepteert. Verwachtingen die binnen de eigen scope worden uitgezet worden voor de eigen scope (ook) verplichtingen, en moeten in het risico-overzicht worden opgenomen. Er zijn ook nog verwachtingen die niet kunnen worden uitgezet zoals bijvoorbeeld ten aanzien van het weer of andere niet toe te rekenen verwachtingen die, als ze als dreiging worden geformuleerd, onder de noemer 'acts of God' vallen.

Risicomatrix

Het analyseren van de risico's kan eenvoudig worden gedaan met behulp van een risicomatrix. Eén as van de matrix gaat over de verplichtingen die binnen de scope waargemaakt moeten worden, met (per verplichting) het risico dat niet aan die verplichting wordt voldaan in termen van 'L', 'M' of 'H', precies als de risicolijst uit Fig. **4**. De andere as betreft de verwachtingen (controls) die binnen de scope leven, op grond waarvan de verplichtingen van die scope waargemaakt kunnen worden (en die zijn uitgezet bij een andere of de eigen scope). Voor elke verwachting is de kans ingeschat dat *niet* aan de verwachting (zoals die is uitgezet) zal worden voldaan in termen van L(aag), M(idden) of H(oog). De matrix coëfficiënten bevatten de symbolen '0', '+', '++', '+++' die de mate aangeven

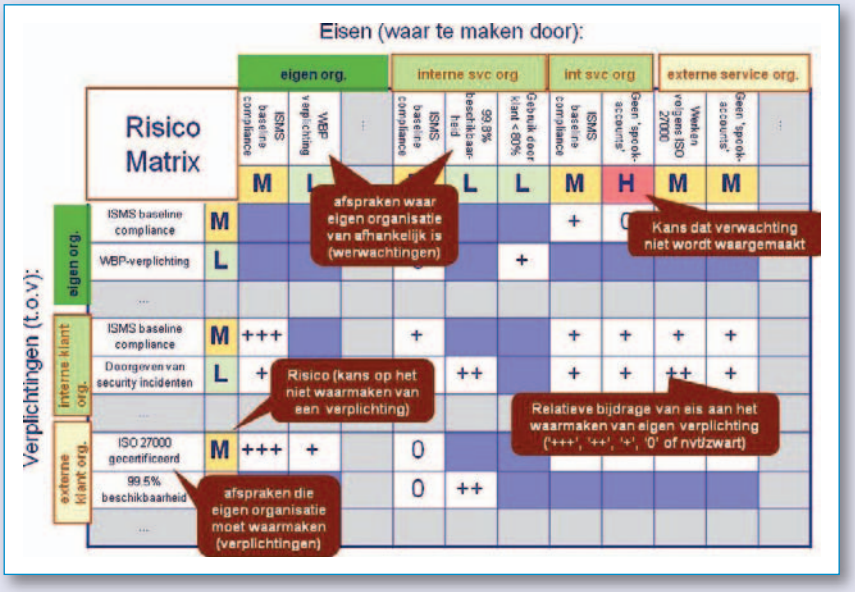


Fig. 6. Risicomatrix van één scope.

waarin de betreffende verwachting en verplichting van elkaar afhankelijk zijn (donkerblauw gekleurde velden geven aan dat er geen afhankelijkheid van toepassing is). Fig. 6 laat een voorbeeldmatrix zien.

Als we deze matrix bekijken, zien we bijvoorbeeld dat de verplichting '99.5% beschikbaarheid' (die door een externe klant wordt geëist) erg (++) afhankelijk is van de verwachting '99,8% beschikbaarheid' (uitgezet aan de interne serviceorganisatie), en niet ('0') afhankelijk is van de verwachting 'ISMS baseline compliance' (uitgezet aan diezelfde serviceorganisatie) en dat de andere afhankelijkheden niet van toepassing zijn. Ook zien we dat alleen de verplichtingen 'Doorgeven security-incidenten' en '99.5% beschikbaarheid' afhankelijk zijn van de verwachting '99,8% beschikbaarheid', en beide in sterke mate (++).
Als we voor één verplichting kijken naar alle verwachtingen waarvan deze afhankelijk is, en we zien bij elke verwachting de kans dat niet aan die verwachting wordt voldaan, dan kunnen we, rekening houdend met de afhankelijkheidscoëfficiënten, een schatting maken voor de kans dat niet aan de verplichting wordt voldaan. Neem bijvoorbeeld de verplichting 'ISMS baseline compliance' (naar de interne klantorganisatie. Deze is van (op één na) alle verwachtingen in dezelfde mate afhankelijk, en (op één na) zijn de kansen dat niet aan de verwachtingen is voldaan, ingeschat als 'M'. Het risico is dan 'M' als we de hiervoor gebruikelijke formule R = K * I (Risico = Kans * Impact) hanteren en aannemen dat de Impact ook 'M' is. Als we dus voor elke verplichting de Impact (= max. hoeveelheid schade die kan ontstaan door niet aan de verplichting te voldoen) inschatten, kunnen met behulp van deze matrix risico's uitrekenen.

Risicomanagement

We beginnen het risicomanagement voor een scope met het opzetten van de risicomatrix. We maken eerst een lijst van verplichtingen en schatten per verplichting de maximale schade (Impact) die voor de scope ontstaat als deze de verplichting niet nakomt, in termen van L, M of H en sorteren deze lijst, waarbij de verplichtingen met de hoogste impact vooraan staan. Dit wordt ook weleens Business Impact Assessment (BIA) genoemd.
Vervolgens gaan we per verplichting (eerst die met impact H, dan die met impact M en die met impact L doen we niet omdat er toch geen bloed uit vloeit) na aan welke verwachtingen moet zijn voldaan om erop te kunnen vertrouwen dat de verplichting kan worden nagekomen. Hiermee vullen we de bovenkant van de matrix en we vullen ook de afhankelijkheidscoëfficiënten in tussen de betreffende verplichting en de ingevulde verwachtingen. Dit is de dreigingeninventarisatie.
In de volgende stap (kansinschatting en risicoberekening) geven we per verwachting met L, M, of H aan of we denken dat *niet* aan de verwachting wordt voldaan. Aan de hand van de afhankelijkheidscoëfficiënten en deze kansinschattingen kunnen we per verplichting bepalen wat de kans is dat de verplichting niet wordt nagekomen (ook weer in L, M of H). Vervolgens bepalen we per verplichting het risico door deze kans te 'vermenigvuldigen' met de bij de verplichting behorende impact. Dat is de bekende formule R = K * I.
Als er 'H'-gescoorde risico's zijn, ligt het voor de hand om een of meer voorstellen te maken die elk betrekking hebben op aanpassingen aan de verplichtingen aan en/of verwachtingen van de scope, zodanig dat als met deze wijzigingen de risicomatrix zou worden gevuld, er geen H-risico's meer in zouden staan. Voor zover het afspraken binnen de eigen scope betreft moeten die worden voorzien van een kostenplaatje en/of andere zaken die het MT nodig heeft om de voorstellen af te kunnen wegen en er over te besluiten. Voor zover het afspraken met andere scopes betreft moeten die met de betreffende eigenaren worden uitonderhandeld - dit is buiten de scope van dit document.

We zien dus dat een scopeverantwoordelijke zijn scope kan besturen met behulp van de risicomatrix, en van elk risico kan bepalen wat ermee te doen. Maar dat hadden we in het begin van dit hoofdstuk al opgeschreven, zodat daarmee de (PDCA)cyclus rond is.

Bedrijfsbreed RM

Omdat RM een gewoon (maar wel bedrijfskritisch) proces is en processen bedrijfsmiddelen zijn, ligt het voor de hand om op het RM-proces zelf ook een RM-proces in te richten. Om dit te kunnen doen zal de RvB zichzelf verplichten dat alle risico's in kaart zijn gebracht, controls zijn gedefinieerd, enz. Als voorbeeld gebruiken we hier de verplichting van de RvB aan zichzelf dat 'hoogstens 3% van alle risico's binnen de organisatie als 'H' mag zijn gekwalificeerd'. Gescoopt RM maakt het mogelijk om deze verplichting 'door te vertalen' naar verwachtingen ten aanzien van de business units of BU's (scopes van het type organisatie-eenheid). De verwachting dat 'hoogstens 3% van alle risico's als 'H' mag zijn gekwalificeerd' hoeft niet voor elke BU met dezelfde tekst te worden doorvertaald: als bijvoorbeeld een (grote) BU 'hoogstens 1%' kan halen, dan zou de bijbehorende verplichting van de RvB ook zijn gehaald als een andere BU 4% scoort. Het doorvertalen van verplichtingen naar verwachtingen levert dus mogelijkheden terwijl je overall toch in control blijft. De keerzijde ervan is dat je wel even moet nadenken over hoe je verwachtingen zodanig doorvertaalt dat als de rapportages terugkomen, jijzelf aan jouw verplichtingen hebt voldaan.

Zijn de verplichtingen (van de RvB) eenmaal doorvertaald naar verwachtingen (van de RvB) voor de BU's, dan moeten de BU's daaraan voldoen. Een verwachting van de RvB ten aanzien van een BU is voor die BU een verplichting. Zo begint het spel opnieuw, maar nu voor de (verschillende) BU(s). Dat levert weer per BU verwachtingen op, die voor de onderliggende bedrijfsonderdelen die weer verplichtingen zijn. Het doorvertalen blijft langs de organieke lijn plaatsvinden, totdat er een bedrijfsonderdeel is dat ook accountable is voor diensten, bedrijfsmiddelen of andersoortige scopes waarop RM plaatsvindt. Dan vindt doorvertaling naar die scopes plaats, en - omgekeerd - wordt vanuit die scopes gerapporteerd en dit weer geaggregeerd tot de rapportage van het bedrijfsonderdeel omhoog de organieke lijn in. Omdat elke scope heeft nagedacht hoe de rapportages die betrekking hebben op haar verwachtingen moeten worden geaggregeerd tot rapportages over de eigen verplichtingen, kan uiteindelijk voor het bedrijf als geheel over alle verplichtingen worden gerapporteerd, en kan bovendien worden onderbouwd met rapportages uit alle hoeken en gaten van de organisatie, waarop de rapportage is gebaseerd.

Discussie

Doordat de voorgestelde werkwijze werkt met meerdere scopes wordt het mogelijk om taken aan scopes te binden en daardoor overzichtelijk en behapbaar te maken. Zowel in onderzoek als in de praktijk zoeken we nog naar een scopetypologie - dat zijn generieke afbakeningen voor systemen, applicaties, gebouwen en dergelijke. Voor elk type scope die we goed kunnen karakteriseren, moet het mogelijk zijn om lijsten van verplichtingen (risico's) en verwachtingen (dreigingen) te maken die voor elke scope van zo'n type relevant zouden kunnen zijn Het hebben van zulke lijsten zou niet alleen RM, maar ook contractmanagement vergemakkelijken. Ook zijn zulke lijsten uitermate nuttig om gebruikt te worden in geautomatiseerde ondersteuning daarvan. In de praktijk lukt dit tot nog toe slechts gedeeltelijk. Een verklaring hiervoor kan zijn dat deze werkwijze toch een heel ander denk- en werkpatroon vereist en de ervaring leert dat zulk soort veranderingen lastig zijn te realiseren binnen organisaties.

We zien dat mensen het lastig vinden hun gedachten, ideeën en zorgen te begrenzen tot één scope. Vanuit de geschiedenis is dit te verklaren doordat niemand goed overzicht had en wie zijn risico's wilde managen dus heel goed moest weten wat al die anderen aan het doen waren. Dat deze scepsis niet zonder meer zal worden afgelegd is dan ook heel begrijpelijk. Geautomatiseerde ondersteuning kan op verschillende manieren nuttig zijn. Zo kan het in de gaten houden dat risico's uit de scopes automatisch worden gepropageerd

als dreigingen binnen afhankelijke scopes. Er kan in de gaten gehouden worden welke geïdentificeerde dreigingen nog niet van een risico-inschatting zijn voorzien, hetgeen bij de scope-eigenaar op een 'to-do' lijst terecht komt. Ook kunnen automatisch managementrapportages worden gegenereerd. Door die als webservices te ontsluiten kan een manager niet alleen op elk moment zien wat de overallstatus van zijn risico's is (groen-geel-rood), maar ook wat de onderbouwing hiervoor is. Tenslotte kunnen managers ook in de gaten houden of de hoeveelheid 'onaf werk' binnen de perken blijft. Mocht de hoeveelheid 'onaf werk' te groot worden, dan kan gericht worden bijgestuurd omdat duidelijk is waar het werk gedaan moet worden. Geautomatiseerde ondersteuning kan ook helpen bij de risico-inventarisatie door voor vaak voorkomende scopes standaard dreigingenlijsten en samenhangen tussen risico's te definiëren zodat deze niet steeds opnieuw bedacht hoeven worden. Dit kan ook helpen bij het onderbouwen van voorstellen voor managementbesluiten.

Conclusies

We hebben een werkwijze voorgesteld voor schaalbaar risicomanagement dat zich kenmerkt door de overzichtelijke en heldere scope-afbakeningen, waarbij de scopes niet groter zijn dan menselijkerwijs is te overzien. Door risicomanagement per scope in te richten blijven de uit te voeren taken overzichtelijk en dus behapbaar. Door de samenhang tussen de scopes expliciet te maken kan risicomanagement over ketens heen, dat wil zeggen bedrijfsbreed (of zelfs over bedrijfsgrenzen heen) zodanig worden gerealiseerd dat niet alleen steeds kan worden nagegaan hoe groot risico's zijn, maar ook wat daar de grondslagen van zijn. Voor het hanteren van deze samenhangen is geautomatiseerde ondersteuning nodig (en mogelijk) waarmee het bovendien mogelijk wordt om (near) real-time aan betrokkenen te signaleren welk werk hij of zij nog moet doen en om soortgelijk overzichten te genereren die management de mogelijkheid bieden erop te sturen dat dit werk ook daadwerkelijk wordt gedaan.

Referenties

[Anderson95] J.R. Anderson: *"Learning and Memory: an integrated approach"*, John Wiley & Sons, 1995, ISBN 0-471-11596-7

[AS/NZS4360] Standards Australia and Standards New Zealand (2004): AS/NZS 4360:2004, *"Risk Management"*, Sydney, NSW.

[IEC61025] Fault Tree Analysis. Edition 2.0. International Electrotechnical Commission. 2006. IEC 61025. ISBN 2-8318-8918-9.

[ISO31000] ISO 31000:2009: *"Risk Management - Principles and Guidelines"*,

[Miller56] George A. Miller: *"The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information"* The Psychological Review, 1956, vol. 63, pp. 81-97

[NIST02] Gary Stoneburner, Alice Goguen, and Alexis Feringa: *"Risk Management Guide for Information Technology Systems"*, National Institute of Standards and Technology, Special Publication 800-30, July 2002

[PWC08] CIO - PriceWaterhouseCoopers (Kim S. Nash): *"The Global State of Information Security 2008"* www.csoonline.com/article/454939/the-global-state-of-information-security-2008

[Reason90] Reason, J. *"Human error"* New York: Cambridge University Press, 1990

[SEI93] Marvin J. Carr e.a.: *"Taxonomy-Based Risk Identification"*, Technical Report CMU/SEI-93-TR-6, ESC-TR-93-183, Software Engineering Institute, Juni 1993

Rekenen aan Malware

Auteur: Henk-Jan van der Molen > Henk-Jan van der Molen is binnen de opleiding Bedrijfskundige Informatica van de Hogeschool Wageningen docent voor o.a. de modules Business Intelligence, Informatiebeveiliging en Verandermanagement. Hij is bereikbaar via henk.jan.van.der.molen@hswageningen.nl

Met dank aan Prof. Dr. ir. Robert Kooij, Faculteit Elektrotechniek, Wiskunde & Informatica TU Delft

In een research document over computer virussen[1], concludeert IBM eind 1998 dat de antivirustechnologie de afgelopen tien jaar zeer succesvol is geweest bij bekende virussen, maar dat er toch nog een paar belangrijke problemen overblijven voor nader onderzoek. Een daarvan is dat het gangbare model voor de verspreiding van computervirussen niet leek te kloppen met de praktijk.

We beschrijven een eenvoudig netwerkmodel dat de verspreiding van malware over het internet beschrijft. De termen *exploit* en malware beschouwen we als synoniemen, hoewel een exploit meestal een kwetsbaarheid in software misbruikt en daardoor op de computer malware kan downloaden en installeren.
Het netwerkmodel verklaart globaal het effect van maatregelen die tegen malware kunnen worden ingezet, zoals antivirussoftware, procedures voor Incident- en Change Management inclusief een *Incident Response Plan*, kennis en bewustzijn op veiligheidsgebied, regels en voorwaarden voor thuiswerken, periodieke vervanging van software en het inrichten van softwarecompartimenten.
Het doel van het artikel is de discussie te bevorderen hoe de aanpak het malwareprobleem kan worden verbeterd. Het malwareprobleem is nu al ernstig en het is waarschijnlijk dat de situatie nog zal verslechteren.

Soorten netwerken
Een netwerk is een set van knooppunten die onderling verbonden kunnen zijn (zie illustratie). Dergelijke netwerken worden soms ook aangeduid als 'grafen'.
Het gedrag van informatienetwerken (bijv. verwijzingen op webpagina's), biologische netwerken (zoals roofdier-prooi relaties) en sociale netwerken (bijv. belgedrag), kan ook relevant zijn voor technologische netwerken, zoals het internet met zijn miljarden knooppunten (servers, clients en routers). Het internet is opgezet om robuust te zijn tegen uitval van willekeurig gekozen knooppunten. Wel is het internet zeer kwetsbaar als de knooppunten in aflopende volgorde van het aantal verbindingen gericht worden aangevallen.

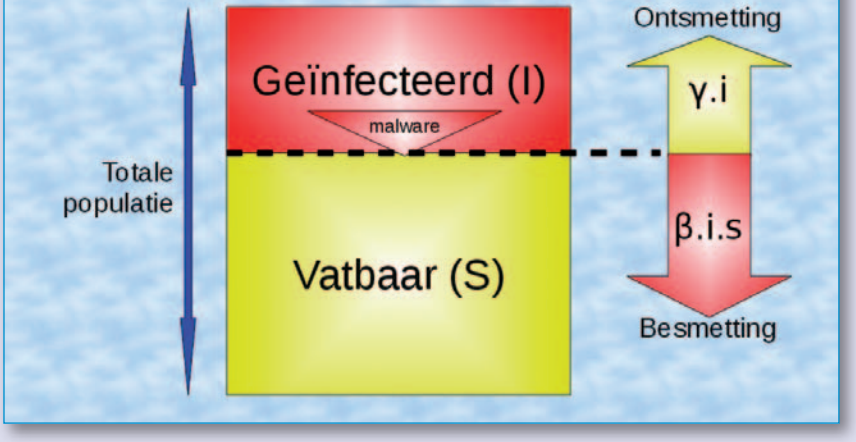
Het individuele gebruik van e-mail, P2P en webbrowser vormt een sociaal netwerk. De grootte van een sociaal netwerk is moeilijker te schatten, maar het concept *'six degrees of separation'*[2], ook wel bekend als het *'Small World Effect'*, bewijst dat de interconnectiviteit ervan hoog is.

Malware kan zich zowel via internet als via sociale netwerken verspreiden. Een internetworm kan zonder interactie van de gebruiker een online server of werkstation besmetten. Daarnaast kan een gebruiker zelf zijn computer besmetten met malware, bijvoorbeeld door het downloaden en gebruiken van een besmet bestand.

Verschillende procesmodellen
Vanuit de literatuur[3] worden drie eenvoudige netwerkmodellen met elkaar vergeleken. Deze modellen zijn niet helemaal realistisch, omdat ervan wordt uitgegaan dat een besmetting 'egaal verdeeld' is over het netwerk, terwijl in werkelijkheid de topologie van een netwerk bepaalt welke knooppunten contact met elkaar kunnen hebben en zo besmettingen kunnen overdragen. De paragraaf 'injectie van malware' gaat hier nader op in. De netwerkmodellen houden daarnaast geen rekening met malware die ontwikkeld is om gericht individuele organisaties aan te vallen.

Percolation theory: in dit model kunnen knooppunten en verbindingen 'vrij' (uitgevallen) zijn of 'bezet' (operationeel). Zo kan bijvoorbeeld worden berekend hoeveel elektriciteitscentrales moeten uitvallen voordat de rest van de centrales de

Figuur 1 – Besmetting en ontsmetting in het SIS model



gevraagde capaciteit niet meer kan leveren. Voor malware is dit model niet geschikt, omdat een computer door meerdere exploits tegelijk kan worden besmet en toch niet hoeft uit te vallen.

Het SIR-model: in dit simpelste model voor de verspreiding van een ziekte wordt uitgegaan van drie toestanden *(Susceptible, Infected, Recovered)* die een knooppunt eenmalig achter elkaar kan doorlopen. Dit model is geschikt om de verspreiding van een individueel Zero-day computervirus te beschrijven als de kwetsbaarheid in de software na besmetting werd gepatcht en het virus werd opgeruimd. Ondanks patching zullen er echter altijd kwetsbaarheden in de gebruikte software aanwezig blijven. Doordat standaard beveiligingsmaatregelen steeds slechter besmettingen kunnen voorkomen, kan een computer meerdere keren achter elkaar door dezelfde malware of gelijktijdig door verschillende malware worden besmet. Daarom is dit model minder geschikt om de verspreiding te beschrijven van malware.

Het SIS-model kent twee toestanden *(S = Susceptible, I = Infected)*, zie figuur 1. Niet alle ziekten resulteren in immuniteit voor overlevenden, zodat zij na genezing vatbaar blijven voor de ziekte. Dit geldt bijvoorbeeld voor tuberculose en malware, omdat sommige kwetsbaarheden die exploits misbruiken niet (kunnen) worden gepatcht, zoals bij *social engineering.*[4] Daarom wordt hier het SIS model gekozen om de verspreiding van malware te beschrijven.

Beschrijving SIS-model

Het SIS-model verdeelt de populatie in twee delen, een deel dat is besmet (i) en de rest dat voor deze besmetting vatbaar is (s). Het model geeft aan dat in het beginstadium een besmetting langzaam groeit, omdat er nog weinig besmette computers zijn die de besmetting kunnen doorgeven. Ook in de eindfase groeit de besmetting langzaam naar de maximale waarde, omdat de kans daalt dat er nog contacten tussen besmette en onbesmette computers plaatsvinden. De besmetting groeit dus evenredig met het product (i.s). Het aantal besmette computers neemt aan de andere kant af door detectie en opruiming van malware. Deze afname is evenredig met het aantal besmette computers (i). De volgende vergelijkingen beschrijven het SIS-model:

Formules

[1] $\partial i/\partial t = \beta is - \gamma i;\ i + s = 1$
[2] $\partial i/\partial t = \beta is - \gamma i = \gamma i(R0s - 1) = 0 \rightarrow \quad R0(1 - imax) = 1 \rightarrow\ imax = 1 - 1/R0$
[3] $\partial s/\partial t = -\beta is + i\gamma + \mu - \mu s = -\beta is + i(\gamma + \mu);\qquad \partial i/\partial t = \beta is - i(\gamma + \mu)$
[4] $\partial i/\partial t = \beta is - \gamma i = \beta i(1 - i - q) - \gamma i$
[5] $R0smin = 1 = R0(1 - imax - q) \rightarrow \quad imax = 1 - q - 1/R0$
[6] $Fmax = \beta imax/(1 - q) = (\beta - \gamma - \beta q)/(1 - q) = \beta - \gamma - \gamma q/(1 - q)$
[7] $pj(1e\ besmetting) = \beta j\Sigma mkm/n \rightarrow \quad pj(GEEN\ 1^{e}\ besmetting) = (1 - \beta j\Sigma mkm/n)$
[8] $\partial ic/\partial t = 1 - \Pi c(1 - \beta j\Sigma mkm/n)$
[9] $\partial i/\partial t = dib/\partial t + dic/\partial t = \beta i(1 - i - q) - \gamma i + \beta cv(1 - q)$

$\partial i/\partial t = \beta is - \gamma i;\ i + s = 1$ (formule 1).
De uitdrukking $(\partial i/\partial t)$ staat voor de toename van (i) in de tijd (t). De besmettelijkheidsfactor (β) bepaalt de kans op overdracht van de besmetting per contact tussen een vatbaar en een besmet persoon. De hoogte van (β) hangt af van de effectiviteit van de preventieve veiligheidsmaatregelen.
De kans op 'genezing' van de besmetting (γ) bepaalt de gemiddelde besmettingsduur ($D = 1/\gamma$) en geeft de effectiviteit van de detectieve en correctieve maatregelen aan. Uit formule 1 blijkt dat zogenaamde logistische functie[5] of S-kromme de oplossing is van het SIS-model (figuur 2).
Een belangrijke indicator is de parameter R0 ($= \beta/\gamma$), de groeifactor van het aantal besmettingen. Door (R0) in te vullen in [1], kan het maximale aantal besmette computers (imax) worden bepaald in de eindfase waarbij $(\partial i/\partial t)$ daalt naar nul (formule 2).
Uit onderzoek van het SIS-model is gebleken dat er altijd besmettingsgevaar blijft bestaan, onafhankelijk van de hoogte van (β). In de eindsituatie is de besmettingsdruk ($F = \beta imax$) maximaal en gelijk aan ($\beta - \gamma$). Als het product (R0.s) kleiner blijft dan 1, dan sterft de besmetting uit. Maar zolang (R0.s) groter is dan 1, groeit de besmetting in de populatie.

Het malwareprobleem

De wedloop tussen cybercriminelen en leveranciers van beveiligingsoplossingen is in volle gang. Uit verschillende onderzoeken blijkt dat met actuele malwarehandtekeningen nog maar tussen de 11% en de 61% van moderne malware kan worden gedetecteerd.[6] Pas na vier weken wordt de meeste malware herkend. Hoewel antivirussoftware tegenwoordig ook via heuristiek sommige malware kan detecteren zonder dat daarvan handtekeningen bekend zijn, is de toegevoegde waarde daarvan beperkt. Dat komt omdat antivirussoftware niet teveel valse positieven mag geven, anders haken gebruikers snel af. Bovendien wordt zowel gesloten source software als malware vaak verpakt in vercijferde zip-bestanden, wat malwaredetectie veel moeilijker maakt. Doordat alle antivirusproducten ongeveer evenveel achterlopen op moderne malware, verbetert de detectie van malware maar marginaal door tegelijk meerdere virusscanners in te zetten. Met meerdere virusscanners groeit bovendien het aantal valse positieven. Antivirussoftwareleverancier Kaspersky meldde hierover al in 2006: *'We're losing this game. There are just too many criminals active on the internet underground, in China, in Latin America, right here in Russia. We have to work all day and all night just to keep up'.*[7]
Soms hebben softwarebedrijven een zodanige onderhoudsachterstand, dat er al maanden zogenaamde *Zero day exploits* circuleren voordat de kwetsbaarheid wordt gepatcht.[8] Daarnaast zijn er aanwijzingen dat cybercriminelen patches automatisch kunnen omvormen tot malware[9], wat langzaam patchen nog gevaarlijker maakt. Toch hebben sommige organisaties een achterstand in het doorvoeren van patches, waardoor er in de praktijk soms computers worden besmet via kwetsbaarheden waarvoor allang patches zijn uitgegeven. Goede Change Management-procedures hebben dus een positief effect op de veiligheid. Het snel produceren en doorvoeren van patches is dus absolute noodzaak, maar patches geven tevens aan dat de ontwikkeling van software niet volwassen is. Zo kan de kwaliteit van software onder andere worden uitgedrukt in de aantal-fouten-per-10.000-regels-code. Door de steeds toenemende computercapaciteit kunnen steeds complexere toepassingen van tientallen-miljoenen-regels-code worden ontwikkeld. Maar omdat producten steeds sneller op de markt moeten komen, neemt de tijd om te testen af. Zelfs na veel patches blijven er in de meeste software daardoor genoeg kwetsbaarheden over die malware kan misbruiken.

	Beveiligingsmaatregelen tegen malware (verkleinen R0)	Tegenacties Cybercriminelen (vergroten R0)
β	Besmettingskans verlagen door preventie met: *Intrusion Prevention System,* firewall; antivirussoftware (on access scan) met patroonherkenning; legale, *white list* software; beperkte gebruikersrechten, *hardening;* software compartimenten; goede procedures voor changes / updates; vergroten kennis en bewustzijn, preventieve security audits.	Verhogen besmettingskans malware door: meerdere aanvalspatronen in malware; social engineering; delen van kennis en malwarecode; testen malware, o.a. met antivirussoftware; *'fuzz'* testen software op kwetsbaarheden; website levert malware op maat; massaal en snel malware verspreiden; encryptie, *code obfuscation* in malware; gerichte malware *('precision ammo')*.
γ	Verbeter ontsmetting (detectie, correctie) door: meerdere antivirussoftware pakketten (voor geplande scans); *Intrusion Detection System,* logging; Management procedures voor incidenten en changes, incl. *Incident Response Plan;* vergroten kennis en bewustzijn, follow-up security audits.	Verlagen uitval van besmette computers door: rootkits, stealth malware, encryptie van communicatie; malware sneller updaten dan antivirussoftware; imitatiegedrag legitieme software; malware activeert zichzelf bij bepaalde condities; patchen van besmette computers (!)

Tabel 1: wedloop tussen cyberaanval en verdediging

Per maand worden er circa 300.000 nieuwe malwarepakketten gedistribueerd.[10] Het aantal nieuwe exploits kan zo groot zijn omdat op internet *'one click'* viruskits voorhanden zijn en dezelfde malware in zelf uitpakkende zip-files met unieke sleutels wordt vercijferd. Door de grote hoeveelheid malware die in omloop is, kan een computer al zijn besmet met verschillende exploits voordat de besmetting wordt opgemerkt. Als een ontsmettingsactie niet alle malware verwijdert, verlaagt dat de waarde van (γ). Incident Management procedures moeten daarom voorzien in een beproefd *Incident Response Plan*. Dat verbetert de effectiviteit van een ontsmetting en voorkomt dat onder stress het wiel moet worden uitgevonden.[11] Het optimaliseren van procedures voor Incident- en Changemanagement vertaalt zich dus in een vermindering van het aantal en de impact van malware-incidenten.

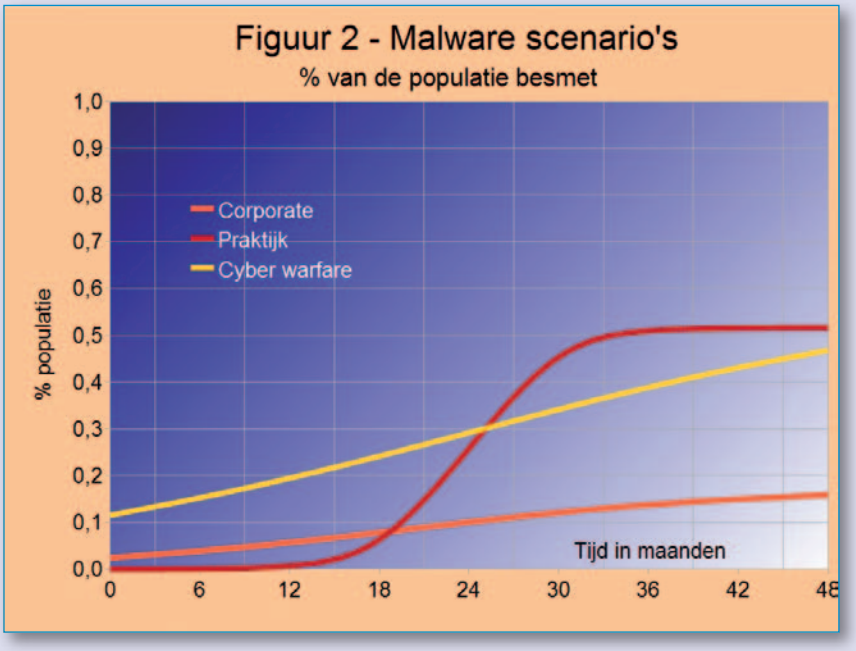
Cybercriminelen verdienen meer geld als (β) hoog is en (γ) laag, zie tabel 1. Op die manier worden meer computers besmet (imax) en duurt de besmetting langer. Een botnet levert bij verkoop direct geld op, maar kan ook per uur worden verhuurd. Zowel de hoogte van de 'huur' als de economische schade door malware is evenredig met (i/γ).

Toch kan het voor cybercriminelen ook voordelig zijn om het aantal besmettingen niet te opvallend laten groeien, omdat snel groeiende malwarebesmettingen op de radar verschijnen van de leveranciers van antivirussoftware. Door per contact niet elke vatbare computer te besmetten, zijn verschillende scenario's denkbaar, waarvan er drie hieronder worden toegelicht (zie figuur 2).

Het *'corporate'* scenario is gebaseerd op beschikbare statistieken over malwarebesmettingen bij organisaties. Uitgaande van de gemeten effectiviteit van antivirussoftware voor nieuwe malware en uit twee opeenvolgende jaarlijkse onderzoeken over cybercrime,[12] kunnen de parameters van het SIS-model (β, γ) worden berekend[13]. Omdat de scope van het onderzoek beperkt is tot organisaties, is dit scenario niet representatief voor de hele populatie.

Het 'praktijk'scenario is erop gericht snel een grote groep computers te besmetten.[14] Voor dit scenario zijn weinig betrouwbare statistieken bekend. Grootschalige besmettingen verschijnen weliswaar op de radar van de leveranciers van antivirussoftware, maar dat betekent niet dat elke besmetting daarna snel kan worden uitgeroeid. Dat laten de ervaringen met de Conficker worm zien.[15]

In het onwaarschijnlijke *'cyber warfare'* scenario zijn de (fictieve) parameters zeer laag gekozen, waardoor langzaam en ongemerkt veel computers kunnen worden besmet.[16] Dit scenario kan eigenlijk alleen werkelijkheid worden als de gekozen kwetsbaarheden langdurig kunnen worden misbruikt, bijvoorbeeld als voor misbruik van de gebruikte kwetsbaarheden kennis van gesloten broncode nodig is. Het is dus essentieel dat de besmette computers niet massaal worden ingezet, zodat de gebruikte kwetsbaarheden niet worden opgepikt door andere cybercriminelen, of worden gepatched.



Dit theoretische scenario is niet bedoeld om speculaties te voeden zoals waarom de Chinese overheid het gebruik van hun 'Red Flag' besturingssysteem wil verplichten[17], het gevolg van de inzage in de broncode van Windows die Microsoft de Russische geheime dienst biedt,[18] waarom een grote softwareleverancier in 2002 is vrijgesproken in een federale antitrustzaak of dat er in Roswell vliegende schotels zijn geland.

Periodieke vervanging van alle software

Vanuit de netwerktheorie is bekend dat als knooppunten met de meeste verbindingen worden uitgeschakeld, de functie van het netwerk snel verslechtert. Zo wordt de verspreiding van spam en malware het beste belemmerd door de bron aan te pakken. Het uitschakelen van bronnen is echter moeilijk, omdat cybercriminelen vaak in het buitenland opereren en voor de verspreiding van spam of malware roulerende webservers inzetten.

Als malwarebronnen niet effectief kunnen worden aangepakt, is het mogelijk om preventief op computers regelmatig de (schone) software opnieuw te installeren. Hierbij worden mogelijk besmette computers vervangen door onbesmette exemplaren. Het veiligheidseffect van zo'n periodieke vervanging van software kan worden bepaald door het SIS-model aan te passen. Hierbij is (μ) het gedeelte van de populatie dat gemiddeld per maand wordt vervangen. De instroom bedraagt (μ) onbesmette computers, de uitstroom (μi + μs) (besmet en onbesmet). (Zie formule 3). Deze maatregel verkleint weliswaar de factor (R0), maar de bijdrage van deze vervanging aan (γ) is gering als (μ) veel kleiner is, zoals bij de gebruikelijke vierjaarlijkse vervanging van hardware. Het automatisch vervangen van alle software op alle computers past sowieso als maatregel in een *Incident Response Plan*. Een dergelijke arbeidsintensieve actie is echter alleen efficiënt uit te voeren als dat kan worden geautomatiseerd.

Verbeteren thuiswerkvoorzieningen en beveiligingskennis

Het is bekend dat de oorzaak van veel incidenten ligt bij de eigen medewerkers. Als een medewerker op zijn besmette pc thuis verder werkt aan een zakelijk document, kan bedrijfsinformatie op straat komen te liggen. Nu zijn zakelijke computers en de privécomputers van medewerkers thuis vaak direct gekoppeld via e-mail en USB-stick. Dergelijke koppelingen kunnen malware overdragen. Sommige organisaties stellen daarom regels voor thuiswerken en verstrekken hun medewerkers gratis de zakelijke software voor thuisgebruik, inclusief beveiligingssoftware. Organisaties die hiervoor geen licentiekosten willen maken, kunnen gebruikmaken van freeware of open source-software. Deze voorzorgen verminderen tevens de kans dat medewerkers met illegale, besmette software op hun eigen pc hun zakelijke computer besmetten. Daarnaast kunnen deskundige auditors de getroffen beveiligingsmaatregelen beoordelen op effectiviteit en efficiency.

De populatie van computergebruikers kan worden verdeeld in een deel met veel en een deel met weinig beveiligingskennis. Omdat het SIS-model complex wordt bij heterogene populaties, is het kwantitatieve beeld niet volledig.[19]

Kwalitatief is voor securitydeskundigen het besmettingsgevaar van malware (β) lager en de kans op een succesvolle ontsmetting (γ) groter dan voor ondeskundigen omdat ze veiliger werken en beschikken over een betere technische beveiliging.

Nu is de groep ondeskundigen groter dan de groep deskundigen, omdat lang niet alle zakelijke computers goed worden beveiligd (bijv. in het MKB) en er meer computers privé worden gebruikt dan zakelijk. In de praktijk weet de gemiddelde computergebruiker weinig over beveiliging. Als bij computers van ondeskundigen besmettingen vaker voorkomen en langer duren, is dat ook nadelig voor die deskundigen of organisaties die dezelfde software gebruiken. Dat komt omdat in onderlinge communicatie malware kan worden uitgewisseld. De kans op een 'vruchtbaar' contact is het grootst bij marktleidende software.

Daardoor blijft het malwarerisico hoog voor de deskundigen die marktleidende software blijven gebruiken en migreren sommige deskundigen naar niet-marktleidende software.

Aan de andere kant vertaalt het verbeteren van kennis en bewustzijn op veiligheidsgebied van ondeskundige computergebruikers zich dus naar een verlaging van de effectiviteit van malware en een snellere opruiming ervan voor de hele populatie. Dat betekent niet dat het nodig is iedereen op te leiden tot security-expert. Met een beperkte inspanning is mogelijk het aantal incidenten terug te dringen, bijvoorbeeld met een voorlichting bij de instroom en een periodieke opfriscursus over beveiliging. *Do's* en *don'ts* kunnen medewerkers snel streetwise op internet maken. Een goede vuistregel voor veilig internetten: 'als iets te mooi is om waar te zijn, dan is het dat ook'. Ook een simpele stelregel is om programmatuur na download niet direct te gebruiken. Als na vier weken de antivirussoftware daar geen malware in vindt, is de kans veel groter dat dit inderdaad zo is. Als de beveiliging goed is ingericht, zijn er maatregelen getroffen waardoor ondeskundige gebruikers hun pc niet zomaar kunnen besmetten. Als werknemers weten waarom hun rechten beperkt zijn, de zakelijke *white list* software thuis mogen gebruiken en de *'lessons learned'* van incidenten breed worden gecommuniceerd, bevordert dat het draagvlak én het veiligheidsbewustzijn.

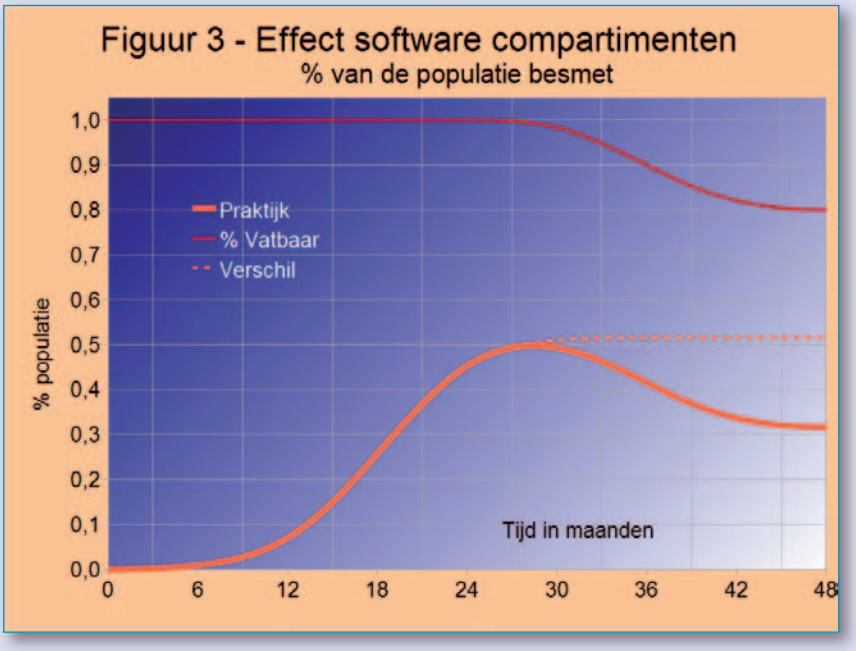
Software compartimenten

Voor malware vormt elk codecompartiment een aparte populatie, zoals bijvoorbeeld alle Windows pc's een eigen compartiment vormen naast Macs en Linux pc's. Hoewel softwarecompartimenten verbonden kunnen zijn door gemeenschappelijk code in hardware drivers en netwerkfuncties, is het in de praktijk zeer onwaarschijnlijk dat Windows malware een Mac kan besmetten. Alle software bevat kwetsbaarheden en computers die dezelfde software gebruiken, bevatten dezelfde kwetsbaarheden. Om hun winst te maximaliseren, richten cybercriminelen hun malware bij voorkeur op de marktleidende software.[20] Het is dus wel mogelijk een virus te schrijven voor een Mac of een Linux pc, maar tegen dezelfde kosten levert Windows malware veel meer winst op.

Software monopolies zijn kwetsbaar, omdat voor malware de kans om een vatbare pc te besmetten het grootst is. Het ligt dus voor de hand om het economisch rendement van malware te verminderen door meer softwarediversiteit te creëren. Om dat mogelijk te maken, moeten organisaties het idee loslaten dat de uitwisselbaarheid van informatie afhangt van het gebruik van dezelfde software. In plaats daarvan moeten organisaties durven te vertrouwen op gegevensstandaarden. Het gebruik van open standaarden garandeert bovendien dat elektronisch gearchiveerde gegevens in de toekomst opnieuw kunnen worden verwerkt.

Het SIS-model kan voorspellen wat het effect is op de verspreiding van malware als de softwarepopulatie meer divers wordt gemaakt. Stel dat het gedeelte (q) van de populatie immuun wordt gemaakt voor de huidige exploits die gericht zijn op de

marktleidende software, bijvoorbeeld door te migreren naar alternatieve software. Als de hoogte van (q) de positie van de marktleidende software niet aantast, blijft verreweg de meeste malware daarop gericht. Dat betekent dat de rest van de populatie (1 - q) marktleidende producten blijft gebruiken en vatbaar blijft voor het gros van de exploits. Door het vervangen van (i + s = 1) met (i + s + q = 1) in formule 1, verandert de besmettingssnelheid (zie formule 4).
Door de diversiteit aan software te vergroten, zullen exploits gericht op de marktleidende software zich dus langzamer verspreiden, omdat het aantal 'vruchtbare' contacten in de populatie vermindert met (βiq). Dit creëert meer reactietijd voor de softwarebranche om op nieuwe malware te reageren. Voor de eindtoestand uit formule 2 geldt dan formule 5.
In de eindsituatie neemt dus zowel het aantal vatbare computers als het aantal besmettingen af met (q). Als (q) groter of gelijk is aan de (imax) van een malwarevariant, dan sterft deze malware gegarandeerd uit. Ook als (q < imax) is de nieuwe waarde van imax verhoudingsgewijs lager dan de afname van het aantal vatbare computers (1 - q). Het effect van softwarecompartimenten is grafisch weergegeven in figuur 3.



Als (q < imax) daalt de besmettingsdruk (Fmax = βimax = β - γ - βq) voor de hele populatie met (-βq). In de oude situatie [2] was Fmax = (β - γ), dus zelfs binnen de vatbare populatie (1 - q) daalt de besmettingsdruk (formule 6).

Stel dat de populatie verdeeld is tussen twee typen software, A met 80% marktaandeel en B met 20%. Het is eenvoudig in te zien dat (q = 0,8) voor het compartiment B. Met andere woorden, een besmetting gericht op dat compartiment B kan zich maar moeilijk verspreiden en dooft hoogstwaarschijnlijk snel uit. Besmetting van computers met software B gebeurt in de praktijk alleen via injectie van malware, nauwelijks door onderlinge sociale contacten.
Met deze berekening is meteen het effect van meer standaardisatie op marktleidende software bekend. Door in [5] en [6] de term (-q) te vervangen door (+q) wordt duidelijk dat daardoor (imax) en de besmettingsdruk (F) toe zullen nemen.

Injectie van malware
Het hier gebruikte SIS-model neemt aan dat de besmettingen al egaal verdeel zijn over het netwerk, maar dat geldt alleen voor malware die zich al enige tijd aan het verspreiden is. Daarom kan het model niet worden gebruikt voor de beschrijving van de injectie van nieuwe malware in de populatie, omdat daarvoor de topologie van de bron-knooppunten van essentieel belang is. Dit geldt ook voor wormen en de distributie van malware via webservers *(drive-by exploit)*. Hoe meer contacten een malwarebron heeft, des te groter is de kans dat een besmetting kan worden overgedragen. Het aantal knooppunten dat een directe relatie heeft met de bron(nen) is gelijk aan de som van het aantal verbindingen (k) van het aantal ingezette malware bronnen. Als (n) het totaal aantal vatbare computers is, dan is de kans (p) dat een malwarebron een nieuwe exploit (j) kan overdragen het resultaat van formule 7. Hierbij staat km voor het aantal verbindingen van bron-knooppunt (m) dat ingezet wordt voor de verspreiding van een exploit. De index (m) geeft aan dat cybercriminelen gelijktijdig meerdere bronnen kunnen inzetten voor de verspreiding van exploit (j).
De kans dat een bron de besmetting kan overdragen is overigens gelijk aan het verwachte deel van de populatie dat direct vanuit de bron wordt besmet. Het deel van de populatie dat door GEEN van de exploits wordt besmet, is het product van alle kansen dat elke individuele exploit de besmetting niet kan overdragen.
Stel dat er elke maand (c) nieuwe exploits bijkomen. Het deel van de populatie dat als eerste wordt besmet door een of meer van deze nieuwe exploits bedraagt daarom (nogmaals overgaan op complementaire kans) formule 8.

Formule 8 kan worden vereenvoudigd tot (βcv) met de volgende aannames:
stel dat β en het aantal verbindingen van de bron-knooppunten voor alle exploits gelijk is, stel dat de spreidingsfactor (v = Σmkm/n) voor alle exploits gelijk is en << 1.

Om zo veel mogelijk computers te besmetten, verspreiden cybercriminelen hun malware via populaire (gehackte) websites, die een hoge waarde hebben voor Σmkm. Hoewel ca. 300.000 nieuwe exploits per maand (= c) gering is ten opzichte van de miljarden internetknooppunten (n), kunnen zo toch veel computers snel worden besmet.
Daarnaast is het mogelijk malware te verspreiden via een tweetraps raket. Besmette computers in een botnet spamberichten laten versturen met malware. Omdat zo langzamerhand 90% van alle e-mails uit spam bestaat, krijgt vrijwel elke e-mailgebruiker regelmatig spam. Als twee op de 100.000 ontvangers van een spambericht ingaan op de 'aanbieding'[21], kan met circa 100 miljard malwareberichten per dag twee miljoen computers worden besmet. En de hoeveelheid spam stijgt nog steeds.
Het effect van diversificatie is dat het (1 - q) gedeelte van de populatie vatbaar is voor een exploit met marktleidende software. Door dit te combineren met [4] en [5], wordt de totale groei van de infecties

van bestaande (b) en nieuwe (c) malware dan: zie formule 9.
Zowel bij de initiële besmetting als bij het verder verspreiden van malware is software diversificatie dus zinvol, omdat de term (q) rechtstreeks terugkomt in de snelheid en omvang van de besmetting.

Conclusie

Binnen de aangegeven restricties biedt het uitgebreide SIS-model inzicht in de effectiviteit van beveiligingsmaatregelen. Voor organisaties is het bijvoorbeeld zinvol om veilig thuiswerken te bevorderen door gedragsregels op te leggen en medewerkers de zakelijk gebruikte software te verstrekken. Het toepassen van freeware en open source-software elimineert de extra licentiekosten daarvoor. Daarnaast is het aan te bevelen op zakelijke computers met een *white list* het gebruik van vreemde software van internet, USB of disk te blokkeren. Dat vermindert de kans dat malware op privécomputers zakelijke computers kan besmetten. Meer beveiligingskennis bij ondeskundige gebruikers vermindert het besmettingsgevaar in de volle breedte van de populatie, dus ook voor de partijen die op dit vlak wel deskundig zijn.

Gezien de ontwikkelingen zal het malwareprobleem in de nabije toekomst nog toenemen, zeker als cybercriminelen automatisch malware gaan genereren uit patches. Dergelijke aanvallen zal met name de veiligheid van organisaties onder grote druk zetten die patches eerst willen testen. Omdat malware besmettingen met gangbare beveiligingsmaatregelen daardoor steeds minder te voorkomen zijn, doen organisaties er goed aan in hun procedures een *Incident Response Plan* op te nemen en hiermee te oefenen. In Nederland wordt gelukkig al uitgebreid geoefend met cyberaanvallen. Bedrijven die periodiek de software van (mogelijk besmette) computers geautomatiseerd terugzetten, verminderen daarmee hun malware risico.

Een software monopolie maximaliseert het economisch rendement van malware. Het gebruik van niet-marktleidende software vermindert het besmettingsgevaar, omdat voor malware het aantal 'vruchtbare contacten' afneemt. Bedrijven kunnen natuurlijk standaardsoftware kiezen, maar vanuit het oogpunt van cybercrime is het onwenselijk dat alle bedrijven dezelfde software gebruiken. Een voldoende hoog percentage computers met alternatieve software kan malwarebesmettingen uit laten sterven. Deze alternatieve software moet dan bij voorkeur Open Standaarden gebruiken om de uitwisselbaarheid en duurzame ontsluiting van informatie te garanderen.

1 *Open Problems in Computer Virus Research (IBM, 1998) http://www.research.ibm.com/antivirus/ SciPapers/White/Problems/Problems.html*
2 *http://nl.wikipedia.org/wiki/Six_degrees_of_separation*
3 *The structure and function of complex networks (Newman) http://www-personal.umich.edu/~mejn/courses/2004/cscs535/review.pdf*
Mathematical modelling of infectious disease, Wikipedia, mei 2010, http:// en.wikipedia.org/wiki/Mathematical_modelling_of_infectious_disease
Virus Spread in Networks, Piet Van Mieghem, Jasmina Omic and Rob Kooij, feb 2009, http://www.nas.ewi.tudelft.nl/people/Piet/papers/IEEEToN_virusspread.pdf
4 *http://en.wikipedia.org/wiki/Social_engineering_%28security%29*
5 *Logistische functie, Wikipedia, mei 2010, http:// en.wikipedia.org/wiki/Logistic_function*
6 *Zie hiervoor de volgende 3 bronnen: FireEye Malware Intelligence Lab, 'Do AntiVirus Products Detect Bots?', 20 November 2008,*
http:// blog.fireeye.com/research/2008/11/does-antivirus-stop-bots.html Proactive / retrospective test, Anti-Virus Comparative, mei 2010
http://www.av-comparatives.org/images/stories/test/ondret/avc_report26.pdf 'Virusscanners detecteren slechts 19% malware', Security.nl, 5 aug 2010
http://www.security.nl/artikel/34081/1/%22Virusscanners_detecteren_slechts_19%25_malware%22.html
7 *Naraine, Ryan; 'The Zero-Day Dilemma', eWeek.com, 24 January 2007, www.eweek.com/article2/0,1759,2087034,00.asp*
8 *http://www.theregister.co.uk/2010/01/22/aurora_exploit_known_months/*
9 *http://www.cs.cmu.edu/~dbrumley/pubs/apeg.html*
10 *F-Secure, 'F-Secure IT Security Threat Summary for the Second Half of 2008',*
www.f-secure.com/en_EMEA/security/security-lab/latest-threats/security-threat-summaries/2008-4.html
11 *'Incident management broodnodig' www.computable.nl/artikel/ict_topics/security/1681630/1276896/incident-management-broodnodig.html*
12 *Ernst & Young, 'Resultaten ICT Barometer over Cybercrime', februari 2010, www.ict-barometer.nl/files-cms/File/Onderzoekresultaten%20ICT%20*
Barometer%20over%20cybercrime%20op%2024%20februari%202010.pdf
Ernst & Young, 'Resultaten ICT Barometer over ICT-beveiliging en Cybercrime', 28 January 2009, www.ict-barometer.nl/files-cms/File/Rapport%20
ICT%20Barometer%20over%20ICT-beveiliging%20en%20cybercrime%20%2028%20%20januari%202009.pdf
13 *Uit onderzoek AV software: Ð = 0,435 (zie voetnoot 8); uit de (∂i/∂t) kan Ð = 0,52 worden berekend*
14 *Uit onderzoek AV software: Ð = 0,435 (zie voetnoot 8); Ð = 0,9 (schatting)*
15 *http://en.wikipedia.org/wiki/Conficker*
16 *Gekozen parameters voor het 'cyber warfare' scenario: Ð = 0,1 en Ð = 0,04*
17 *http://archives.cnn.com/2000/TECH/computing/02/23/microsoft.china.idg/*
18 *http://www.zdnet.co.uk/news/security/2010/07/08/microsoft-opens-source-code-to-russian-secret-service-40089481/*
19 *Heterogeneous Protection in Regular and Complete Bi-partite Networks (Work in Progress), Omic, J.S., R.E. Kooij, and P. Van Mieghem, 2009,*
http://www.nas.its.tudelft.nl/people/Rob/telecom/netw_het.pdf
20 *Aanpak cybercriminaliteit: Verdeel en heers www.computable.nl/artikel/ict_topics/security/2357426/1276896/aanpak-cybercriminaliteit-verdeel-en-heers.html*
21 *http://www.newyorker.com/reporting/2007/08/06/070806fa_fact_specter?currentPage=1*

Kennismaking met....

Maarten Hartsuijker

Wat mij altijd heeft aangetrokken aan Informatiebeveiliging is de grote diversiteit aan onderwerpen die er in het blad voorbij komen. De artikelen van vakgenoten bieden je de mogelijkheid om eens een kijkje in de keuken te nemen van een onderwerp waarin je zelf minder thuis bent. Omdat ik zelf Informatiebeveiliging altijd met veel plezier lees, hoefde ik niet lang na te denken toen mij werd gevraagd of ik interesse had om mij bij het redactieteam aan te sluiten: natuurlijk, leuk!

Iets over mijzelf...

Ik ben mijn loopbaan begonnen bij Getronics. Al heette dat destijds nog het Rijks Computer Centrum. Na wat ITIL- en projectmanagement-omzwervingen kreeg ik daar het beveiligingsvirus te pakken. En hoewel virussen bij ICT'ers over het algemeen een nare bijsmaak hebben, heb ik dat -inmiddels werkzaam als zelfstandig adviseur- tot op heden zelf nog niet zo ervaren. Binnen ons vakgebied heb ik mij gespecialiseerd in infrastructuur- (datacenter en webhosting) beveiliging en daarnaast ondersteun ik regelmatig organisaties met algemeen beveiligingsadvies of security management.

Pak eens een pen...

Toen ik eind jaren 90 mijn studie bedrijfkundige informatica afrondde ben ik afgestudeerd op kennismanagement. Een onderwerp dat mij deed beseffen dat kennisdeling geen eenrichtingsverkeer is, maar zowel de zender als de ontvanger een hoop kan brengen. Dit zie ik ook terug in het schrijven voor informatiebeveiliging. Met het werken aan een artikel breng je niet alleen kennis naar je vakgenoten, je dwingt jezelf ook om een onderwerp nog eens rustig van verschillende kanten te beschouwen en hiermee je eigen kennis te structureren. Ik zou dan ook af willen sluiten met een oproep aan alle lezers van dit blad: pak eens een boeiend onderwerp waar je veel van weet en zet het om in een leuk artikel.

(Advertentie)

woensdag 13 oktober Security-Congres 2010

RISK MANAGEMENT & SECURITY

Een ***file omzeilend*** congres, georganiseerd door ISACA, NOREA en PvIB

Locatie
Hotel Theater Figi
Het Rond 2
3700 AA Zeist
www.figi.nl

Dit congres is mede mogelijk gemaakt door:

Deloitte.

FOX-IT EXPERTS IN IT SECURITY

IT sec

Al ingeschreven op dit succesvol terugkerend congres?
Mis het niet en schrijf u nu in!

Het inspirerende programma vindt u op www.security-congres.nl

Een tipje van de sluier:

- Key note sprekers
  - Paul Overbeek, OIS Information Risk & Security Management: Ruimte voor Information Security Management
  - Wim van Grembergen, Universiteit Antwerpen Management School: From IT Governance to Enterprise Governance of IT
- Uitreiking Joop Bautz Information Security Award

Wij ontmoeten u graag op 13 oktober!

Organisatie: ISACA Netherlands Chapter | NOREA de beroepsorganisatie van IT-auditors | PvIB Platform voor Informatie Beveiliging

Meer informatie
www.security-congres.nl

SecureLink Networking Security Solutions

Mag ik mijn gegevens terug?

Auteur: Maarten Hartsuijker > Maarten Hartsuijker is security consultant bij Classity Informatiebeveiliging. Hij helpt organisaties met security management, security audits en website penetratietesten. Volg Maarten via @classityinfosec.

Wie heeft er nog geen? De smartphone. Als we onderzoekers mogen geloven groeide de markt voor deze telefoons afgelopen maand maar liefst met 64%. En dat is niet verwonderlijk. De apparaten stellen ons in staat om op elk moment alles op te zoeken, met iedereen in contact te staan, te bloggen, met social media te werken en al onze vrienden te laten weten waar we ons op welk moment bevinden. Maar hoe gemakkelijk deze functies ook lijken, voor privacy bewuste mensen hebben ze ook een grote keerzijde. De controle over de eigen privacy neemt erdoor met enorme snelheid af. En dat vaak zonder dat je het zelf in de gaten hebt.

Met de ingebouwde GPS en op basis van WIFI/GSM-toegangspunten kunnen we op onze smartphone eenvoudig zien waar we ons bevinden. Door deze locatiefunctie kunnen we inmiddels met onze smartphone navigeren, zien welke huizen er in de buurt te koop staan of waar we in onze onmiddellijke omgeving lekker kunnen eten. Erg handig, maar dat geldt niet alleen voor onszelf. Ook de smartphone-leveranciers zijn erg graag op de hoogte van waar wij ons begeven en wat onze interesse trekt. Zowel Google als Apple geven toe deze gegevens over ons te verzamelen en soms zelfs door te verkopen aan derden. De telefoon bevat helaas geen knop die je wél toegang geeft tot de handige functies, maar tegelijkertijd voorkomt dat de gegevens bij Google of Apple worden opgeslagen. Waarom kennen we hiervoor eigenlijk geen opt-in/opt-out-wetgeving?

Leuk, al die apps

Zowel de iPhone als Android kennen een marktplaats voor het downloaden van extra applicaties. De marktplaatsen zijn echter niet te bezoeken zonder je eerst aan te melden. Apple heeft hiervoor een iTunes store account en Google biedt je de mogelijkheid om je met een Gmail-account aan te melden. Erg handig, vooral voor Google. Want zodra je je vanaf je telefoon met een Gmail-account aanmeldt, kunnen ze alle gegevens die ze vanuit het gebruik van je mailbox en het zoekscherm al hebben, verrijken met de gegevens die van je telefoon afkomstig zijn. Zo kunnen ze op basis van je online gedrag niet alleen vaststellen welk klanttype je bent, maar is door de locatiedienstverlening van je telefoon ook inzichtelijk op welke locaties je veel te vinden bent. Een droom voor direct marketeers.

Opletten met aanmelden dus?

Eenmaal in het bezit van een smartphone wil je als gebruiker natuurlijk een aantal extra applicaties installeren. Kijken we naar de Android telefoons, dan maakt de privacy bewuste gebruiker hiervoor een apart Google/Gmail-account aan. Deze geeft wel toegang tot de applicaties, maar staat verder overal los van. Maar is dat wel zo? Na het aanmaken van een Gmail-account voor toegang tot de applicaties koppelt Google ook automatisch de telefoon aan de Gmail-agenda, de e-mail en het adresboek. Het gebruiken van deze functies is standaard geactiveerd. De telefoon zal daardoor alle persoonlijke afspraken en contactgegevens naar Google versturen. Op dat moment is Google in het bezit van je dagelijkse leefpatroon en iedereen die zich in je sociale netwerk bevindt. Deze gegevens verdwijnen de Google cloud in, zonder dat je hier als gebruiker expliciet (goed, ongetwijfeld ergens diep verborgen in de voorwaarden van Android, Gmail of Market) voor heb gekozen. Omdat Google geen Nederlands bedrijf is en dus te maken heeft met hele andere (privacy) wetgeving, mag je je afvragen waar deze gegevens vervolgens allemaal terecht komen.

En dan de apps zelf

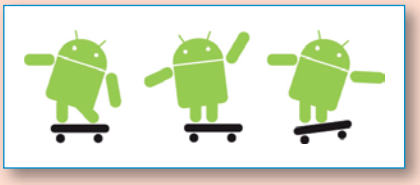
Tijdens de Blackhat-beveiligingsconferentie in Las Vegas gaven Amerikaanse onderzoekers diverse voorbeelden van smartphone-applicaties die persoonlijke informatie over de telefooneigenaar verzamelen. Zo bleek er een Chinese applicatie met achtergronden voor je telefoon te zijn die onder andere het telefoonnummer van de gebruiker naar de Chinese website verzond. Iets wat voor het succesvol tonen van een plaatje op je telefoon uiteraard compleet overbodig is.

Maar ik heb geen smartphone...

Natuurlijk kun je besluiten om bewust niet mee te doen met al dit smartphonegeweld. Als je zorgvuldig met je gegevens omgaat hoef je je over privacyschending geen zorgen te

maken, toch? Dat is maar de vraag. Op het moment dat je voor komt in het adresboek van vrienden of relaties die wel een smartphone hebben, kunnen zij je gegevens verstrekken aan Google, Apple of bijvoorbeeld Microsoft (leverancier van onder andere MSN, Hotmail en Windows Mobile). En op deze manier komen de bedrijven alsnog in het bezit van tenminste jouw persoonlijke gegevens, zoals e-mail, telefoon, adres, geboortedatum, foto, IM-adres en wat er maar is opgeslagen in de telefoons van bekenden. De kans dat ze deze gegevens nimmer meer zullen verwijderen is erg groot.

Is het iemand al eens opgevallen hoe Facebook na het aanmaken van een nieuw account met een al enige tijd gebruikt e-mail adres meteen diverse vriendensuggesties kan doen?



Dit is mogelijk doordat deze vrienden in het verleden hun adresboek naar Facebook hebben verzonden om te controleren of er bekenden lid zijn. De verstrekte gegevens worden niet enkel voor deze koppelacties ingezet, maar permanent opgeslagen en ook voor andere doeleinden gebruikt. Bijvoorbeeld om ook jou een vriendensuggestie te doen. Op dezelfde wijze kan Google ook met de door derden over mij verstrekte gegevens activiteiten ontplooien zonder dat ik hier zelf ook maar enige controle over heb.

En wat als ik binnen Android mijn gmail ontkoppel en de locatiefunctie deactiveer?

Kan ik me dan vrij bewegen zonder hierover iets aan Google bekend te maken?

Helaas niet. Elke keer als je je telefoon aan een datanetwerk koppelt, neemt hij contact op met Google. Hiervoor gebruikt Google het domein '1e100.net'. 1e100 staat voor 1 googol (een 1 met 100 nullen). In het contact met Google wordt het MAC-adres van je telefoon doorgegeven.

10:51:37.728154 arp reply 192.168.0.115 is-at **38:fe:ac:61:09:6a** (oui Unknown)
...
10:54:38.144820 IP 192.168.0.115.35101 > **ww-in-f118.1e100.net.**5228: S 3007542161:3007542161(0) win 64240
0x0000: 000c 29c7 56d8 **38fe ac61 096a** 0800 4500

Maak je gebruik van Wifi, dan kan Google deze gegevens in veel gevallen in combinatie met Streetviewdata alsnog tot een locatie correleren. En weet men in elk geval op welke locaties je je regelmatig ophoudt. Of Google dit daadwerkelijk doet is natuurlijk niet met zekerheid te stellen.

Is hier niets tegen te doen?

Grote bedrijven als Google, Apple en Microsoft weten dus veel van je. Zoveel dat dit te correleren is tot conclusies die je vermoedelijk over jezelf nog niet had getrokken. Geweldig voor marketeers of bijvoorbeeld justitie. Met datamining-programmatuur en vorderingen kan er heerlijk in dit soort informatie worden rondgesnuffeld.

Als individu is hier voor een groot deel weinig aan te doen. Je bent te afhankelijk van de wijze waarop je netwerk met jouw privacy omgaat. Daarnaast zijn de interessante functies voor velen zo aantrekkelijk dat ze ondanks enige huiver toch overstag gaan om hiervoor een stuk privacy op te geven.

Het zou daarom goed zijn als van overheidswege hiertegen strenger zou worden opgetreden. Met name op de onderdelen waar standaardinstellingen ervoor zorgen dat de smartphones direct en zonder hier expliciet voor te hebben gekozen gegevens aan derden aanleveren. Een opt-in zou hier al helpen. Daarnaast zou het goed zijn als leveranciers verplicht zouden worden om eenvoudige functies in te bouwen die het mogelijk maken om alle aan een account gekoppelde gegevens (en historie) volledig te verwijderen. Dus wil je na enige tijd al je gegevens terug en de gedeelde informatie verwijderen, dan zou dit mogelijk moeten zijn. Maar helaas loopt de regelgeving hier over het algemeen ruim achter de techniek aan...

Achter het nieuws

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

Responsible disclosure

Begin juli publiceerde een medewerker van Google op internet details over inbraakmogelijkheden die betrekking hadden op Windows XP. Met de details kunnen hackers die gebruikers over weten te halen een bepaalde internetpagina te bezoeken inbreken op de pc van die gebruiker. De details werden kort nadat Microsoft was geïnformeerd bekendgemaakt aan het grote publiek. Afgelopen maand vielen op internet de experts over elkaar heen met een mening over dit incident. We vroegen drie redacteuren van dit blad om op dit incident te reageren.

Lex Borger: Hackers zijn er op uit om 'zero-days' te vinden. Responsible disclosure vergt dat onderzoekers op zoek gaan naar kwetsbaarheden. Dit gaat ze steeds moeilijker af. De software-industrie heeft nog steeds weinig geld over om dit te steunen. Een onderzoeker moet dus vrij idealistisch bezig zijn om tot responsible disclosure te komen.
Als een vulnerability te vroeg openbaar gemaakt wordt, moet een leverancier daar meteen op reageren. Dit gaat ten koste van andere ontwikkelingen en het goed ontwerpen van de patch. Het systeem van het incidenteel ontdekken en repareren van kwetsbaarheden is de meest kostbare en minst duurzame manier.
Kwetsbaarheden vergen tegenwoordig vaker meer dan een leverancier voor een oplossing, kijk maar naar het DLL-preloading attack wat nu speelt en Dan Kaminski's DNS-probleem.
Responsible disclosure moet zero-day vulnerabilities voorkomen. Dit is echter het minst roemvolle scenario voor de onderzoeker. Die heeft bijvoorbeeld een deadline om te spreken op Black Hat.
Windowsgebruikers hebben nu na tien jaar pas profijt van de Security Development Lifecycle. Toch is de buffer overflow, het meest basale programmeerprobleem, nog niet de wereld uit. Dit soort basisfouten zou niet meer voor mogen KUNNEN voorkomen. Er moet iets fundamenteel anders.

Maarten Hartsuijker: Op het moment dat je niet van een kwetsbaarheid op de hoogte bent, is het lastig om jezelf ertegen te beschermen. Om deze reden ben ik er een groot voorstander van dat beveiligingsspecialisten op internet de details van ontdekte kwetsbaarheden publiceren. Helaas informeer je op het moment dat je de details van fouten publiek maakt ook gelijk alle mogelijke kwaadwillenden. Prioriteit voor zorgvuldig contact met de leverancier is daarom op zijn plaats.
Deze zomer publiceerde een onderzoeker reeds vijf dagen na het contact met Microsoft de details van een fout in Windows. Zijn belangrijkste argument hiervoor was dat de fout zo eenvoudig gevonden kon worden dat kwaadwillende hackers deze ongetwijfeld ook al hadden aangetroffen. Hij achtte het onacceptabel om de fout nog maanden onbekend te laten. Door de fout publiek te maken, zou deze niet meer inzetbaar zijn voor serieuze aanvallen. Begrijpelijk, zeker met wat extra achtergrond, maar hij zadelde de rest van de ICT-industrie wel op met een risicoverhoging zonder goede compenserende maatregelen. Hoewel zijn actie op de lange termijn hopelijk helpt om leveranciers bewust te maken van het feit dat ze sneller kwetsbaarheden moeten verhelpen, was iets meer publicatiegeduld hier wel op zijn plaats geweest.

André Koot: We worden vrijwel dagelijks geconfronteerd met zero-day vulnerabilities en exploits. En meestal betekent dat ook dat we meestal en hopelijk niet te lang daarna, een update van de software kunnen verwachten. Zero-day, dat betekent dat een kwetsbaarheid bekend wordt gemaakt en er (dus) nog geen lapmiddel is. Op zich geen knelpunt, totdat de kwetsbaarheid misbruikt wordt.
Waar ik me eigenlijk meer zorgen om maak is de minus-x day kwetsbaarheden, ofwel de lekken die wel bekend zijn bij de ontdekker, maar niet bij de maker van de software. Als die ontdekker de kwetsbaarheid niet meldt, maar wel benut, dan zijn de rapen gaar.
Microsoft maakt al geruime tijd globaal de inhoud van de patches bekend, met name welke component geraakt wordt door ene patch. Daarmee zijn beheerorganisaties beter voorbereidend op de wijzigingen. Dit is geen full disclosure. De aard en inhoud van de patch en de daaraan ten grondslag liggende kwetsbaarheden worden niet bekendgemaakt. Het uitbrengen van een patch is niet altijd de oplossing voor het probleem dat een lek wordt misbruikt. Beheer is meestal het knelpunt. Dit is geen pleidooi voor het niet meer patchen, laat dat duidelijk zijn, maar enige relativering is op zijn plek. Er moet een tussenweg zijn tussen minus-x day exploits, zero-day exploits en het blijven bestaan van nooit gepatchte, al dan niet verborgen lekken.
Commerciële belangen en technische problemen zorgen ervoor dat niet elk lek in een keer wordt gedicht. Maar het zou al winst zijn als de commerciële drijfveer wordt gestimuleerd. Kan er niet een onafhankelijke instantie komen die minus-x day en zero-day exploits registreert en aankaart bij de leveranciers? En die pressie kan uitoefenen om de gaten te dichten? En die door producenten en leveranciers wordt vertrouwd? En die white hats kan belonen voor vondsten van gaten? Alles in ieder geval beter dan de melders van gaten als criminelen te beschouwen.

ACTA en netneutraliteit

Auteur: J.M.T. Wijnberg > J.M.T. Wijnberg is voorzitter van de vereniging Vrijbit; zij is bereikbaar via bestuur@vrijbit.nl

Anders dan de naam doet vermoeden is de Anti-Counterfeiting Trade Agreement (ACTA) niet beperkt tot de bestrijding van namaakgoederen.
In de verdragstekst is een uitgebreid hoofdstuk over de handhaving van intellectuele eigendomsrechten in de digitale omgeving opgenomen. ACTA heeft daarmee gevolgen voor het grondrecht op communicatievrijheid. En dus voor de democratische rechtsstaat, onze kenniseconomie en de persoonlijke vrijheid van internetgebruikers.

Uit de onderhandelingsteksten volgt dat de partijen online-tussenpersonen willen inzetten bij handhaving van intellectuele eigendomsrechten. Ook staan de onderhandelingspartners in ACTA vergaande schadevergoeding en strikte handhaving van het auteursrecht jegens individuele gebruikers voor. En aan de hand van een recent uitgelekte tekst kan worden opgemaakt dat zelfs het linken naar inbreukmakend materiaal als auteursrechtinbreuk zou kunnen worden aangemerkt.

ACTA zou zo het grondrecht op communicatievrijheid en de persoonlijke vrijheid van internetgebruikers kunnen beperken.
De rol van online-tussenpersonen als neutraal doorgeefluik zal verder onder druk komen te staan.
Dat kan leiden tot zelfcensuur van onze informatie-infrastructuur en repressieve handhaving van het auteursrecht jegens individuele internetgebruikers.

Bedreiging van vrij internet via ACTA:
Via de anti-namaak overeenkomst (ACTA) zou men voortaan alleen gebruik mogen maken van internet als de gebruiker betaalt voor wat binnen ACTA als verplichte betaling voor goederen en intellectueel eigendom wordt afgesproken. Als sanctie kunnen mensen worden afgesloten van vrije toegang tot internet.
De Nederlandse ministers betrokken bij deze onderhandelingen, schreven op 15 maart 2010 aan de Tweede Kamer dat het 'niet zo'n vaart zou lopen' met het afsluiten van internetsites van gebruikers die bijvoorbeeld na drie waarschuwingen nog geen auteursrechten betaald hebben over muziek of films die zij van internet downloadden. Maar op 22 maart bleek in Brussel dat internetproviders wel degelijk via aansprakelijkheidsstelling gedwongen zouden kunnen worden om gebruikers af te sluiten.

Belang van commercie
In de praktijk zal het afsluiten van internetverbindingen, uitsluitend via de ACTA-handhaving, inderdaad zo'n vaart niet lopen. Het zou onvermijdelijk grote commotie teweegbrengen als mensen die een filmpje, foto, tekst of wat dan ook gratis zouden downloaden de toegang tot internet wordt ontzegd. Dat zou immers tot gevolg hebben dat door het afsluiten van internetverbindingen onevenredig grote belangen van gebruikers zouden worden geschaad. Het niet betalen voor commercieel beschermde goederen zou er dan toe leiden dat bijvoorbeeld gezinsleden, die van de internetverbinding van de 'wanbetaler' gebruikmaken, belemmerd worden bij het volgen van onderwijs. Of mensen hun inkomen kwijtraken doordat bedrijfsactiviteiten komen stil te liggen.
ACTA is bedoeld om commerciële belangen veilig te stellen. De afspraken die men nu wil vastleggen kunnen ook afgedwongen worden door de toegang tot internet af te knijpen. Dit verdrag geeft de aanzet om een nieuwe internetstructuur te ontwerpen waarbij gebruikers niet alleen voor de toegang tot internet te laten betalen, maar ook voor het gebruik.
Het afsluiten van gebruikers van internet levert geen profijt op. Men kan derhalve verwachten dat het afsluiten van internetverbindingen niet de weg is die bewandeld zal worden om commerciële uitbating te reguleren. Dat zal veeleer gebeuren door het ontwerpen van betaalsystemen waarbij vooraf via abonnementen betaald zal moeten worden voor het gebruik van internet.

Belang van de overheid
Waar het betalen voor producten en diensten op internet commercieel wordt geregeld ontstaat voor nationale en internationale mogendheden en veiligheids- en opsporingsdiensten de kans om meer greep te krijgen op het vrij gebruik van wat dit nieuwe medium de bevolking biedt.
Overheden, ook in het zogenaamde 'vrije westen' blijken bang te zijn voor wat met de term 'netneutraliteit' wordt aangeduid. Voor de schier onbeperkte mogelijkheden dus die internet momenteel biedt aan individuen om kennis te verwerven en snel en wereldwijd te kunnen communiceren. Bovengenoemde instanties komt het buitengewoon goed van pas als ze over de mogelijkheid beschikken om gebruikers, waarvan men het onwenselijk vindt dat ze gebruikmaken van internet, te kunnen laten afsluiten.
Het afsluiten druist echter in tegen de fundamentele grondrechten op vrije meningsuiting, vrijheid van communicatie en kennisvergaring. Mensen en groeperingen deze grondrechten ontnemen via democratische besluitvorming zou in het parlement

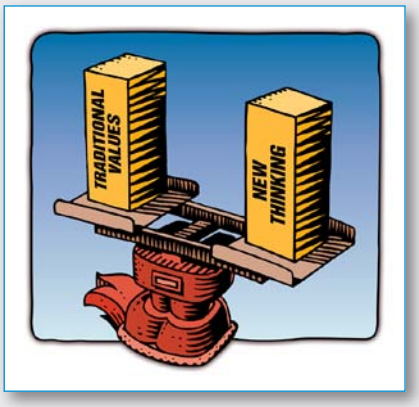
op grote bezwaren stuiten. De rechtmatigheid van dergelijke wetgeving zou tevens in rechte met succes aangevochten kunnen worden.

De mogelijkheid om via een handelsverdrag dergelijke afspraken te maken, betekent dat er geen parlement aan te pas hoeft te komen. De beslissingen kunnen zo buiten de democratische besluitvorming in het parlement om genomen worden. En de rechtspositie van een individuele gedupeerde legt het bij voorbaat af tegen internationaal vastgelegde handelsverdragen. Omdat die per definitie als groot economisch algemeen belang zullen worden aangemerkt.
In het verleden was het kabinet nog erg gecharmeerd van de mogelijkheden die internet bood. Men sprak over mediawijsheid als ontwikkeling tot nieuw burgerschap. Maar inmiddels lijkt het erop dat vrij gebruik van internet in Nederland snel tot het verleden gaat behoren. Dit wordt bewerkstelligd door de combinatie van verschillende wetten en nieuwe wetsvoorstellen.

De wetgeving 'Bewaarplicht telecommunicatiegegevens', ook wel dataretentie genoemd, zorgde ervoor alle gebruik van internet voor de overheid in principe toegankelijk te maken. Met wie, hoe vaak en hoe lang men telefoneert en e-mailt en welke websites men bezoekt worden geregistreerd. De gegevens worden bewaard, zijn toegankelijk voor gebruik door justitie en inlichtingen- en veiligheidsdiensten. En de gegevens worden niet als op zichzelf staande gegevens bewaard maar tevens gebruikt voor het samenstellen van gedragsprofielen.

Deze wetgeving lijkt niet het doel het bestrijden van de georganiseerde misdaad (waaronder terroristen) te kunnen realiseren, omdat uitgerekend de georganiseerde misdaad de mogelijkheden en middelen heeft om deze controlemogelijkheden te omzeilen. Het lijkt een middel om de gewone burger in de gaten te houden en het gevoel te geven dat men in de gaten gehouden wordt. Dat ook deze wetgeving indruist tegen fundamentele grondrechten werd omzeild door het in het parlement als verplichte implementatie van Europese Richtlijnen te presenteren.

Recent is aan de wetsvoorstellen die de persoonlijke vrijheid inperken, het wetsvoorstel 'versterking bestrijding computercriminaliteit' toegevoegd. Dit voorstel regelt dat de vrijheid van de burgers om informatie of meningen te publiceren op internet door de overheid kan worden gereguleerd. Het Openbaar Ministerie (OM) zou de bevoegdheid krijgen om zelf te bepalen of men iets strafbaar vindt. En het OM zou tevens bevoegd worden om websites, waarvan men meent dat daar iets



strafbaars op staat, ontoegankelijk te maken. De minister van Justitie, stelt feitelijk voor om de taak van de rechter af te schaffen door het OM direct websites op zwart te kunnen laten zetten. Momenteel heeft alleen de rechter de macht om het blokkeren van websites te bevelen.

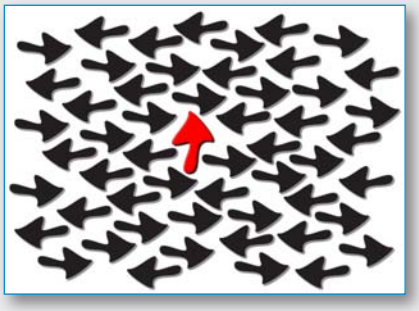
Samenhang wetgeving beperking internetgebruik

Wat dit voor de vrijheid van de burger betekent en waar dit toe leidt, wordt alleen duidelijk als men de maatregelen beziet in samenhang met alle andere wet-en regelgeving. Hoe strafbaarstelling van de ene wet en sanctiemogelijkheden via andere wetgeving elkaar afdekken of versterken. Via Acta wordt geregeld wat strafbaar is. Via de bewaarplicht is controle op internetverkeer geregeld. En via het OM wordt publicatie via internet gemonitord en beperkt.
Een factor van belang hierbij is tevens dat het rechtssysteem deels wordt veranderd. Waar men vroeger pas schuldig werd bevonden als daar wettig en overtuigend bewijs voor was geleverd, is dat allang niet meer het geval. Alleen al de verdenking van strafbare feiten is tegenwoordig voldoende om mensen te bestraffen. Verdenking op grond van technische verwerking van losse persoonsgegevens tot gedragspatronen voldoet soms al om mensen op grond van hun zo verkregen profiel als verdachte of schuldige te bestempelen.

Om te beseffen hoe een onschuldige burger in een machteloze positie kan manoeuvreren tekent het scenario zich uit. Volgens ACTA had de gebruiker auteursrecht moeten betalen voor een afbeelding, muziek of video en heeft u dat verzuimd. Al dan niet om principiële redenen. Uw verbinding kan dan als straf worden verbroken of afgeknepen. Maar u bent dan ook officieel een crimineel geworden. Als zodanig gaan oplettende justitie-, inlichtingen- en veiligheidsdiensten u nauwkeurig in de gaten houden. Die diensten mogen op grond van de Wet Vorderen Gegevens (2005) alle gegevens die er van u waar dan ook zijn opgeslagen opvragen en aan een onderzoek onderwerpen. Deze gegevens kunnen via zoekmachines worden doorzocht op trefwoorden op interesses, eetgewoonten, betalingsgedrag, reisgedrag en dergelijke. Uw internetgebruik, e-mail en telefoonverkeer kunnen dan onder de loep worden genomen. Met gebruikmaking uiteraard van software die andere gegevens over u met uw internetgedrag kan combineren. Het is gerechtvaardigd om te stellen dat men zo bij iedereen die gebruikmaakt van internet wel iets valt te ontdekken wat als verdacht kan worden aangemerkt.

Zorgen om inperking persoonlijke vrijheid

De impact van de ACTA-onderhandelingen moet men bezien in samenhang met andere wetsvoorstellen die het leven van burgers op andere terreinen van het maatschappelijk leven pogen te registreren, te controleren, en te reguleren. Kilometerheffing, OV-chipkaart, legalisering van preventieve huiszoeking bij niet van fraude verdachte gebruikers van alle sociale voorzieningen, het EKD en het EPD. Deze samenhang maakt duidelijk dat het niet overdreven is en dat we met recht kunnen stellen dat het lijkt alsof er een juridische infrastructuur gebouwd wordt, waarbij het evenwicht tussen de rechten van de overheid en de rechten van de bevolking uit balans lijkt te geraken.



Column

Wilde vakanties

Tegen de tijd dat dit artikel wordt gelezen zal iedereen wel weer vergeten zijn dat ze in de zomerperiode op vakantie zijn geweest. Ondergetekende is inmiddels wel alles weer vergeten behalve die dingen die mij overkwamen. Voor het eerst sinds jaren ben ik met het vliegtuig weggeweest en dat was een avontuurlijk iets. We vertrokken dit jaar van een regionaal vliegveld en de eerste ergernis was bij mij al geboren toen ik zag dat er geen vloeistoffen meegenomen mochten worden. Ik dacht dat de douane er wel overheen zou kijken maar nee hoor, mij werd onmiddellijk gevraagd of die mooie blauwe tas van mij was en dat kon ik alleen maar beamen. Ze vroeg of ze in de tas mocht kijken op een manier waaruit bleek dat het haar niet uitmaakte of ik ja of nee zou zeggen. Zonder mijn antwoord af te wachten trok ze een bus scheerschuim, shampoo en tandpasta uit mijn tas en liet het met een wijde boog in de achter haar opgestelde blauwe container verdwijnen. De douanier ritste mijn tas weer dicht en ik meende op haar gezicht zelfs een lachje te bespeuren maar ze keek mij wederom streng aan en vroeg mij of ik de regels niet kende? Onverstaanbaar verontschuldigde ik mij in de hoop dat het theater daarmee dicht zou gaan. Ze duwde mij de tas in handen en ging naar haar volgende klant. Dit bleek een man op leeftijd (ik denk een jaar of 80 mijn vrouw houdt het op dik zestig) die met de broek op de hakken aan het testen was of de broekriem daadwerkelijk de oorzaak van het gepiep van het controlepoortje was. De man had inmiddels net zo'n kleur als ik en de schop van mijn vrouw tegen mijn schenen was voor mij voldoende om mij er eens een keer niet mee te bemoeien.
De vlucht was goed ondanks het feit dat ik mij nog steeds ergerde aan het verlies van mijn spulletjes en de gedachte dat morgenochtend een douanier zich met mijn spullen aan het opfrissen was.
De terugreis zou hoop ik wat vriendelijker gaan omdat we gebruikmaakten van een groot internationaal vliegveld. Na een lange wachttijd kwam ik bij de douanier aan. Ik gaf mijn paspoort aan de boos kijkende man, die een aantal keren van het document naar mij keek en uiteindelijk mijn paspoort weer teruggaf. Hij knikte vervolgens naar mijn vrouw, die gaf haar paspoort en het ritueel herhaalde zich. Ik maakte nog een grapje, door aan te geven dat mijn vrouw inderdaad een lekker ding is maar ook hiervan werd hij niet vrolijker. Ook mijn vrouw kreeg haar paspoort terug en ze sloot zich bij mij aan. Vervolgens werden we naar een apparaat geleid dat een bodyscan maakte. Deze scanner is in staat ieder slachtoffer zonder kleding te kunnen afbeelden en het moet toch een vermakelijke baan zijn om iedere vakantieganger ineens zonder kleding te zien staan. Je ziet ze aankomen met een trainingspak aan en nog geen tel later staan ze ontkleed op je beeldscherm. Ik zag inmiddels de lol er wel van in en grapte tegen mijn vrouw dat het apparaat rechtsreeks verbonden was met het internet en dat je tegen betaling mee kon kijken naar de resultaten van de bodyscanner. Mijn vrouw vond het niet grappig en de douanier die wel zag dat ik lol had om zijn apparaat leek nu helemaal uit zijn sas maar liet ons lopen. "Waarom zei je dat nou?", zei mijn vrouw toen we uit het zicht en het gehoor van de douanier waren. Ik vertelde haar dat er na 11 september allerlei zware maatregelen op luchthavens geldig waren. En na de aanslagpoging op 25 december 2009 die door een landgenoot van ons is tegengehouden, is men helemaal doorgeschoten en wil men van iedereen een bodyscan. Welke zekerheden heb ik dat er geen harde schijf in de machine zit die ze allemaal opslaat? Of nog gemakkelijker; dat de machine aangesloten is op het netwerk van het vliegveld? "Dat zullen ze toch niet doen?", zei mijn vrouw. Ik leg haar uit dat als je een machine ontwikkelt die foto's kan maken dat het geen enkele moeite is om de foto's ook op te slaan. Natuurlijk worden er geen foto's opgeslagen of voor andere doeleinden gebruikt. Natuurlijk zijn deze machines zo goed afgeschermd dat het onmogelijk is om data van de machine af te halen. Natuurlijk.

Groetjes,
Berry

3 - 4 NOV 2010 JAARBEURS UTRECHT

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

IT SECURITY
INFOSECURITY.NL

Drie toonaangevende vakbeurzen onder één dak

STORAGE EXPO

infosecurity.nl NETHERLANDS

TOOLING EVENT

DÉ OPLOSSING VOOR ÁL UW SECURITY-VRAAGSTUKKEN.

WWW.INFOSECURITY.NL

INFOSECURITY.NL 2010: SECURITY OUT OF YOUR COMFORT ZONE

DE ROL VAN INFORMATIEBEVEILIGING IN NIEUWE ONTWIKKELINGEN

Bijblijven op uw vakgebied? Kom dan op 3 en/of 4 november naar dé vakbeurs over IT-security van Nederland. Ook dit jaar laten de toonaangevende bedrijven binnen de branche op Infosecurity.nl hun nieuwste producten, oplossingen, diensten en updates zien. Natuurlijk is er in 2010 ook weer een gratis uitgebreid seminarprogramma, dit jaar met onder meer de thema's Cloud, Social Media en Cybercrime. De keynote sessies worden o.a. verzorgd door Andrew Yeomans (Commerzbank AG), Koen Gijsbers (Ministerie van Defensie) en David Burg (PCW). Ook op de beursvloer zijn er diverse nieuwe initiatieven te vinden. Zo zijn consultants van o.a. Ernst & Young, Deloitte, Capgemini, KPMG en PricewaterhouseCoopers aanwezig voor 1 op 1 consults. Tenslotte kunt u onder de noemer NextGeneration IT demo's bekijken over virtualisatie & cloud computing en deze nieuwste snufjes zelf proberen.

Meld u nu aan via www.infosecurity.nl voor uw gratis toegangsbadge!

CONGRES & DEMO'S

2010 NEXTGENERATIONIT

VIRTUALISATIE › CLOUD COMPUTING

Reed Exhibitions

vnu exhibitions europe

Discover the next best thing since the introduction of FTP!

NOW
FREE EVALUATION!

BEFINE cryptshare®

- Easily send large files up to 2GB
- Confirmation of file download
- Simple and secure file transfer

BEFINE cryptshare®

CRYPSYS Data Security B.V. - Benelux Distributeur van Cryptshare
www.crypsys.nl - sales@crypsys.nl - (0183) 62 44 44

CRYPSYS data security