december 2009 nummer 8

INFORMATIEBEVEILIGING

De aanpak van cybercriminaliteit: verdeel en heers

Integriteit bekeken vanuit het oogpunt van informatiebeveiling

Process control security en SCADA security: een realitycheck

De NORA als architectuur-aanpak voor IB-patronen

PvIB
Platform voor InformatieBeveiliging

ib

Voorwoord/colofon

Beste lezer,

Zoals jullie weten, ben ik een enthousiast web 2.0 gebruiker. Wikipedia (en natuurlijk ibpedia.nl), Facebook (al een hele groep PvIB-leden is daarop te vinden: hallo allemaal, gaat ie goed op de boerderij?), rss feeds en natuurlijk Twitter. En naarmate je wat langer rondhangt op al die sites en de linkjes weet te vinden, ontdek je vanzelf waar leuke informatie te vinden is. Een paar vondsten van vandaag wil ik jullie niet onthouden.

De leukste vondst van vandaag: het interview van @boris (voor de niet-Tweeps onder ons: met @naam wordt een account op Twitter bedoeld) met de Armeense hacker, die de wordpress blog van Boris verminkte. Leuk om te lezen over hoe en waarom hij dat deed.
Ook aardig om te lezen hoe Boris de hacker adviseert om zijn tijd te steken in pr voor zijn heilige zaak, in plaats van het blind platgooien van 50.000 sites per dag. De snelle link: *http://tnw.to/5Lai*.

Journalist Brenno de Winter meldde vandaag dat de waterschapsverkiezingen niet helemaal zo schoon als water zijn verlopen. Het is inmiddels volop in het nieuws geweest, maar hij meldde de scoop al op Twitter: volg @brenno.

Privacy is niet alleen vanwege de stemcomputers een hot topic. Misschien ben ik bevooroordeeld, omdat ik een paar privacygerichte Twitteraars volg, maar het onderwerp kent wel veel ongeruste burgers. Ik vond deze quote van Bob Blakley (van Burton): 'Privacy is the problem you have after you share sensitive information'. *(http://bit.ly/6W6LQk)*. Nou, dat klopt. Vandaag ontdekte ik de zaak van een anonieme blogger die te trots was om haar succes voor zich te houden: *http://bit.ly/8K5Hyk*. Jammer, want dan is zo'n blog ook helemaal niet zo spannend meer.

Reputatie is net als privacy ook erg interessant. Misschien nog ongrijpbaarder dan privacy. Er bestaat geen wet bescherming reputatie, er is vrijwel niets wettelijk over geregeld, behalve misschien dat we smaad kunnen aanpakken. Maar een slechte reputatie kan minstens zulke ingrijpende gevolgen hebben, als de inbreuk op persoonsgegevens. Mijn reputatie: die kun je gewoon via Google, Facebook en Twitter zelf vaststellen. Maar het blijkt betrekkelijk eenvoudig een reputatie te verminken. Een leerzame case over het gebruik van de Twitter List functie om iemand (blij dat ik niet Matt Cutts heet) in een kwaad daglicht te stellen, is te vinden op *http://bit.ly/5ubnME*.

Heel iets anders: Graham Cluley (van Sophos) is een leuke Twitteraar. Elke dag heeft hij wel iets aardigs te melden. Hij verwijst in zijn tweets naar zijn blog. Vandaag meldt hij dat de virtuele runescape dief bij de kladden is gepakt: *http://bit.ly/50wsZ4*

Dit is maar een kleine bloemlezing uit de vangst van vandaag, 30 november. Er gebeurt zo veel, daar hoef je de deur niet voor uit. En dan zijn dit waarschijnlijk alleen nog maar de interessante en, voor de meeste lezers, niet eens relevante zaken. Nóg niet relevante zaken, lijkt me, want volgens mij kun je uit elke case wel een lesje leren.

André Koot
Hoofdredacteur

PS: We willen Marnix Dekker van harte feliciteren met zijn promotie aan de Universiteit van Twente over access control!

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
Peter Westerling/Monique van Diessen (eindredactie, TOPpers Media bv, Berlicum)

Redactieraad
Tom Bakker (Delta Lloyd)
Mario de Boer (Logica)
Lex Borger (Domus technica)
Lex Dunn (Capgemini)
Rob Greuter (Secode Nederland)
Aart Jochem (GOVCERT.NL)
Renato Kuiper (HP)
Henk Meeuwisse (Sogeti)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving
Van Velzen Grafisch Ontwerp, 's-Hertogenbosch

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.

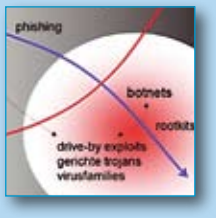
PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

creative commons

PvIB
Platform voor InformatieBeveiliging

Inhoud



(e) ID(eeën) in Europa

Auteur: Elisabeth de Leeuw > Elisabeth de Leeuw is Management Consultant bij TopForce en is bereikbaar via elisabeth.de.leeuw@topforce.com.

Op woensdag 16 september vond aan de Katholieke Universiteit Leuven de workshop e-IDea 2009 plaats, ter afsluiting van een tweejarig researchproject aan diezelfde universiteit naar e-applicaties, die de veiligheid en de privacy van de gebruiker kunnen waarborgen. Onder het publiek bevonden zich ontwikkelaars, gebruikers en onderzoekers afkomstig uit verschillende sectoren en disciplines; uit de wetenschappelijke wereld, bedrijfsleven en overheid. Op het programma stonden onder meer presentaties rondom het thema eID en andere elektronische identificatiemiddelen in het publieke domein in respectievelijk België, Duitsland en Nederland[1]. De workshop werd afgesloten met een paneldiscussie.

eID

Met behulp van elektronische identificatiemidden kunnen gebruikers zich elektronisch identificeren en documenten van een elektronische handtekening voorzien.
De beoogde toepassing van elektronische identificatie ligt binnen het domein van e-government en (op termijn) ook op het gebied van e-business. De ontwikkeling van eID loopt in de verschillende landen, zowel inhoudelijk als qua tijdpad, niet parallel.

Ontwikkelingen op het gebied van elektronische identificatie in België, Duitsland en Nederland

België introduceerde als één van de eerste landen binnen Europa al in 2002 een elektronische identiteitskaart voor haar burgers. Verschillende applicaties die hierop aansluiten, op het gebied van gezondheidszorg, overheidsdiensten en zakelijke dienstverlening, worden momenteel ontwikkeld. De Belgische eID is er voor alle leeftijden: kinderen jonger dan zes jaar krijgen een gestripte versie, voorzien van ingetrokken certificaten. De geldigheid zal op korte termijn verlengd worden van vijf naar tien jaar. In verband daarmee wordt de lengte van de RSA-sleutels aangepast van 1024 naar 2048, om zo de robuustheid van de cryptografie ook op de langere termijn te waarborgen. Deze en andere aspecten van de beveiligingsarchitectuur worden daarnaast periodiek aangepast aan courante eisen van betrouwbaarheid. Verschillende 'generaties' beveiliging van elektronische identiteitskaarten zullen daardoor gelijktijdig circuleren. Aspecten van privacy en pseudonimiteit vallen buiten de scope van het Belgische eID-programma. Parallel daaraan wordt daarom software ontwikkeld om in deze aspecten te voorzien. Ondanks alle inspanningen ligt de Belgische eID veelal bij de burger op de plank, om er jaarlijks vanaf gehaald te worden, wanneer het tijd is voor de belastingaangifte.

Nederland heeft de plannen voor een eID voorlopig afgeblazen. Op 9 december 2008 gaf staatssecretaris Bijleveld van Binnenlandse Zaken aan dat er op korte termijn geen behoefte is aan een Nederlandse eID. In het kader van ontwikkelingen rondom het Elektronisch Patiënten Dossier is weliswaar behoefte aan elektronische authenticatie, echter zij acht deze businesscase op zichzelf te zwak. De eID zal, als deze er ooit komt, gebaseerd worden op de Nederlandse Identiteits Kaart (eNIK), die naast het paspoort één van de rechtsgeldige Nederlandse Reisdocumenten is. De bedoeling is om met de eNIK te voorzien in het hoogste betrouwbaarheidsniveau (3) van het DigiD stelsel.

Naast de uitgestelde plannen voor een Nederlandse eID lopen er enkele andere initiatieven. OpenID+[2], eerder onder de vlag ConsumentenID, is een samenwerkingsverband van private partijen (onder auspiciën van ECP-EPN) om te komen tot eID in het domein van B2C[3], gebaseerd op OpenID. Het programma eHerkenning[3], is een publiek-privaat samenwerkingsverband op initiatief van het Ministerie van Economische Zaken met als doel om te komen tot een afsprakenstelsel rondom elektronische authenticatie en autorisatie van personen en organisaties. Vooralsnog in het domein van G2B[4], maar met als uitgesproken optie om het model op termijn uit te bouwen in de richting van B2C en C2C[5].

Duitsland is vergevorderd met de voorbereidingen voor eID, de uitrol wordt binnen een jaar verwacht. De *gründliche* plannen, waar menigeen iets van leren kan, wijken drastisch af van de lichter uitgevoerde Belgische specificaties. Opvallend is de aandacht voor built-in privacy architectuur, een thema dat België in het kader van eID niet heeft opgepakt. Zo zijn de data op de Duitse kaart voorzien van een elektronische handtekening en kunnen ze niet - voorzien van deze handtekening - geforward worden. Een challenge response mechanisme is ingericht om gegevens op te vragen. Zo kan bijvoorbeeld gevraagd worden of iemand ouder is dan een bepaalde leeftijd, maar niet om de exacte geboortedatum. Door de toepassing van random documentnummers is de kans dat de toegepaste cryptografie kan worden gebroken, tot een minimum teruggebracht. De public key is voor alle

DigiD *laagste niveau*	Gebaseerd op een gebruikersnaam / wachtwoord algoritme.
De volgende varianten van DigiD zijn beschikbaar of in ontwikkeling:	
DigiD *level 2 / SMS*	Laagste niveau van DigiD, uitgebreid met mobiele certificaten
DigiD *level 2 / SMS+*	Gelijk aan DigiD *level 2 / SMS*, uitgebreid met face to face verificatie van mobile device
DigiD *level 2+ / RTDA*	Gelijk aan DigiD *level 2 / SMS*, uitgebreid met authenticatie van reisdocumenten (**RTDA** staat voor **R**emote **T**ravel **D**ocument **A**uthentication)

documenten gelijk. Met behulp van multilevel PKI kan gebruikgemaakt worden van verschillende pseudoniemen, welke niet te herleiden zijn tot de identiteit van de houder van de kaart en die elk afzonderlijk kunnen worden gecreëerd en herroepen.

Discussie

Kinderen

De presentaties werden gevolgd door een levendige discussie. Eén van de eerste vragen was, wat een Belgisch kind, jonger dan 5 jaar, met een eID moet[6]. Die vraag bleef onbeantwoord.

Europa

Verder vroeg men zich af of - en zo ja, wanneer - er ooit een eenvormige Europese eID zal komen. Snel zal dat niet zijn, zo is de algemene verwachting. Maar met een bankkaart kunnen we ook de grens over, wereldwijd zelfs, dus zou dat met een eID niet ook moeten kunnen? Echter; grensoverschrijdende financiële transacties zijn sinds jaar en dag gebruikelijk, terwijl transacties tussen burger en overheid zich van oudsher voornamelijk binnen de landsgrenzen afspelen. Oftewel, eID is bedoeld voor G2C. En G2C is naar binnen gericht.

Weerstand

Wat weerhoudt mensen er nu van een eID te gebruiken? Een mogelijke verklaring is watervrees voor de elektronische handtekening. Want met een klassieke handtekening is het stuk papier dat je ondertekent tastbaar, maar hoe weet je nu zeker dat wat je op het scherm ziet, ook datgene is dat je tekent? Bij banktransacties is dat in principe ook zo. Vergelijkbare waarborgen kunnen rondom de elektronische handtekening worden ingebouwd. De elektronische handtekening is voor burgers echter nieuw. De financiële sector heeft in de loop van de jaren vertrouwen opgebouwd. De transitie van papier naar elektronisch is ook hier niet in één klap gekomen, maar is geleidelijk gegaan. En het liability model speelt

'E-sign', Erhin Sahin, www.sxc.hu

mee: in geval van security incidenten - die over het algemeen niet naar buiten komen - wordt de financiële schade niet op de klant afgewenteld. Alhoewel het liability model van creditcardmaatschappijen enigszins lijkt te kantelen sinds de invoering van pincodes op creditcards. Kortom; vertrouwen komt te voet.

Business case

En dan, is er een business case voor een (nationale) eID? Biedt eID inderdaad uitzicht op een e-gebouw, waarin met één sleutel alle deuren opengaan? En zo ja, is dat wat we willen? Of is de business case van de overheden te smal? Het beperkte gebruik van de Belgische eID lijkt in die richting te wijzen. Staat de business case van de overheid op gespannen voet met de commerciële (neven)doelstellingen? Wordt eID wel goed in de markt gezet? En, *wiens* business case is het nu eigenlijk? Ofwel - naar analogie van discussies rondom het Burger Service Nummer - is het nou service *voor* de burger of service *door* de burger? Al met al zijn er veel vragen en daarmee is de business case (nog) niet evident.

Identity brokers

Willen we de business case van eID boven het domein van G2C uittillen, en gegeven de diversiteit aan Europese oplossingen, dan lijkt een EU-brede identity broker onmisbaar. Zo'n broker kan bemiddelen tussen eID's uit de verschillende Europese landen en andere elektronische identificatiemiddelen, die op de markt worden aangeboden. Het gebruik van eID wordt zo bevorderd, met behoud van diversiteit.

Privacy

Zo'n identity broker komt dan wel 'alles' van de Europese burger te weten. Weg privacy. De uitdaging is om daar met zero knowledge cryptografie en challenge response architectuur een mouw aan te passen. Dus, linksom of rechtsom, er is nog veel werk aan de e-winkel!

---

1. Presentaties zijn te vinden op http://www.msec.be/eidea/ws2009/index.php?page=presentations

2. Het gaat om een jong initiatief, in het voorjaar werd een globale presentatie gegeven van de plannen, zie http://www.slideshare.net/evidos/consumentenid

3. B2C ofwel Business-to-Customer: het domein van communicatie tussen Bedrijven en Klanten

4. G2B ofwel Government-to-Business: het domein van communicatie tussen Overheden en Bedrijven

5. C2C ofwel Citizen-to-Citizen: het domein van communicatie tussen Burgers onderling

6. Katholieke Universiteit Leuven, Department of Computer Science, Heverlee http://www.msec.be/eidea/ws2009/index.php

Aanpak cybercriminaliteit: verdeel en heers

Auteur: Henk-Jan van der Molen > Henk-Jan van der Molen is senior projectleider/ICT-adviseur bij de Inspectie Verkeer en Waterstaat en is bereikbaar via henk-jan.vander.molen@ivw.nl.

Momenteel zijn misbruik van bankrekeningen en het verlies van (bedrijfs) informatie door malware-incidenten aan de orde van de dag. Oorzaak is de groeiende, criminele bedrijfstak rondom malware, waar miljoenen in omgaat. Toch zie je dat veel organisaties dezelfde standaardproducten blijven gebruiken, terwijl dit de *return on investment* van malware maximaliseert. Dit artikel schetst de effecten van het veranderen van standaardsoftware en hoe deze maatregel kan worden toegepast.

Malware wordt hier gedefinieerd als programmatuur met kwaadaardige functionaliteit, zoals virussen, bots, wormen, Trojaanse paarden en spyware. Een cybercrimineel kan een systeem vanaf het internet met malware infecteren door kwetsbaarheden in software te misbruiken. Ook kan een gebruiker onbewust malware activeren door een besmette website of een besmet programma te openen. Zelfs een bestand met macro's, beeld, geluid of video kan malware bevatten. Tegenwoordig valt malware steeds vaker de webbrowser aan, het aantal *drive-by-infection* sites groeit explosief. Het bezoek aan één geïnfecteerde website kan al voldoende zijn om een systeem te compromitteren.

Volgens het SANS Internet Storm Center kunnen cybercriminelen steeds sneller malware ontwikkelen doordat ze over meer kennis beschikken en onderling samenwerken. Voor het schrijven van de succesvolle *Sobig* worm werd bijvoorbeeld universitaire kennis ingezet. De broncode van verschillende virussen werd hergebruikt en er zijn testversies uitgebracht *(zie literatuurverwijzing 1)*.

Bijna alle software bevat fouten of kwetsbaarheden die een kraak mogelijk maken. Om fouten in uitgebrachte software te verhelpen, verspreiden leveranciers zogenaamde patches via het internet. Het aan zekerheid grenzende vermoeden bestaat dat cybercriminelen stelselmatig patches analyseren om daaruit nieuwe malware te ontwikkelen. Hierdoor loopt niet alleen iedereen die te langzaam patched het risico dat hun kwetsbare systemen worden gekraakt, de snelle patchers lopen hetzelfde risico. Op de zwarte markt wordt malware per exploit verkocht, ook voor de nieuwste systemen. Botnets van pc's, die via malware zijn overgenomen, worden per uur verhuurd, bijvoorbeeld om een webwinkel plat te leggen en zo geld af te persen. De omvang van het *Storm worm* botnet wordt geschat op anderhalf miljoen 'zombie' computers. Dit botnet zou momenteel twintig procent van alle spam wereldwijd versturen. Het recent ontdekte Conficker virus kan de miljoenen besmette pc's flexibel inzetten door de eigen broncode te vernieuwen. Cybercriminelen kunnen gekraakte systemen tevens misbruiken voor bedrijfsspionage of fraude met opgeslagen creditcardgegevens. Daarnaast veroorzaakt malware voor organisaties indirecte schade door programmatuur of data te verminken en de continuïteit van bedrijfsprocessen te verstoren.

Uit de ICT barometer 2009 van Ernst & Young blijkt dat bedrijven veel last hebben van cybercrime. Ter illustratie een overzicht van het type incidenten in 2008:

- 16% malware op werkstation
- 8% computerinbraak (hack aanval)
- 8% phishing
- 5% denial of service (platleggen systeem)
- 4% diefstal bedrijfsinformatie

Malware lijkt grotendeels op privé pc-gebruikers gericht, je hoort er zelden iets over bij bedrijven. Dat beeld is niet altijd terecht. Veel organisaties doen geen aangifte van een malwarebesmetting, om negatieve publiciteit te vermijden. Soms merkt een organisatie ook niets van een malwarebesmetting, bijvoorbeeld als malware wordt ingezet voor bedrijfsspionage. Wel zijn zakelijke systemen vaak beter beveiligd, bijvoorbeeld doordat medewerkers zelf geen software kunnen installeren. Ook overheden zijn betrokken bij cybercriminaliteit, zoals de Russische cyberoorlog tegen Estland in 2007. Onlangs meldde de AIVD dat China en Rusland op grote schaal digitaal spioneren.

Maatregelen bieden geen garanties

Zelfs een ICT-infrastructuur met de meest veilige instellingen is niet immuun voor alle malware-aanvallen. De maatregelen die organisaties nemen tegen malware blijken namelijk steeds minder effectief om incidenten te voorkomen *(zie literatuurverwijzingen 2 en 3)*. Een gangbare maatregel om de beschikbaarheid van systemen te verbeteren, is het inrichten van back-up voorzieningen. Reservesystemen met dezelfde software zijn echter vatbaar voor dezelfde exploits als het operationele systeem. Back-up voorzieningen zijn dus ineffectief bij een malware-aanval, omdat zogenaamde

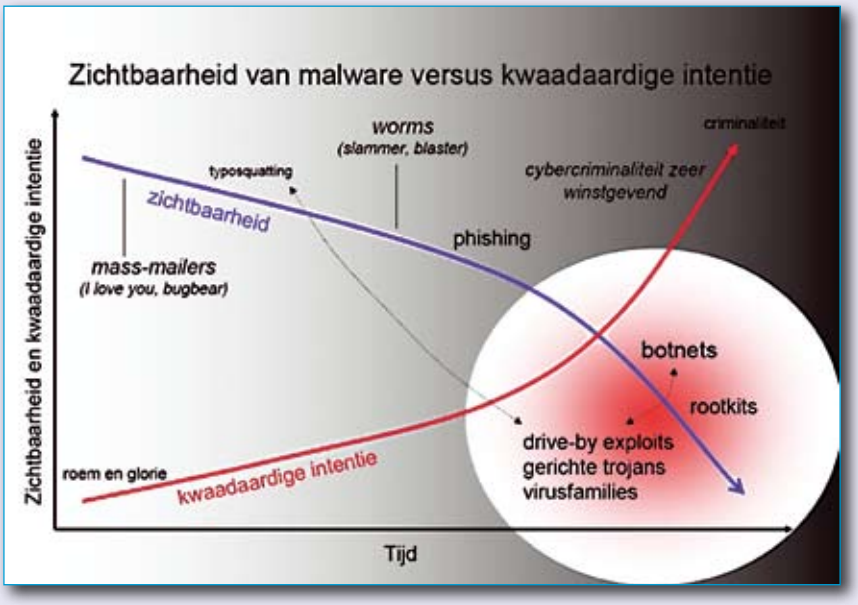
Jaarlijks overlijdt slechts 0,01 procent van de Nederlandse bevolking aan de gevolgen van griep. Daarentegen heeft de mens geen specifieke resistentie tegen een H5Nx virus, zoals de vogelgriep. Het immuunsysteem herkent zo'n virus niet direct, waardoor het virus zich gemakkelijker kan vermenigvuldigen. Het lichaam keert zich pas specifiek tegen de besmetting als de besmette persoon, vaak letterlijk, doodziek is. (Wikipedia et al).

Zero Day exploits (hiertegen bestaat nog geen beveiliging, althans niet van de betrokken hard- of software vendor) regelmatig voorkomen. Ook de veiligheid van extra maatregelen zoals two factor authenticatie (het gebruik van een token plus een pincode bij internetbankieren of telewerken) staat onder druk met de nieuwste browser plugin malware.

Bij veel organisaties kan een malwarebesmetting bedrijfsprocessen verstoren, omdat systemen vaker gekoppeld worden via het internet (Web 2.0), zoals bij banken, verkoopsites en nutsbedrijven, met sensoren en actuatoren. Ook de overheid loopt meer risico: in 2007 zou al minstens 65 procent van de dienstverlening via het internet moeten lopen. Het aantal gekoppelde systemen zal verder toenemen met de invoering van basisregistraties, zoals het GBA. Door toenemende centralisatie en uniformering zullen ICT-infrastructuren steeds meer op elkaar gaan lijken en de afhankelijkheid van ICT toenemen.

Malware goes where the money is

Cyberbendes willen zoveel mogelijk geld 'verdienen'. Daarvoor moet de verspreiding van malware 24x7 kunnen doorgaan en moet een malwarebesmetting zo lang mogelijk verborgen blijven. Daarvoor gebruiken zij bijvoorbeeld encryptie, *stealth rootkits* en verspreiden ze malware op roulerende webservers, zodat het uitschakelen van enkele servers geen effect heeft. Door voor elke besmetting unieke malware te genereren en die selectief te richten op enkele bedrijven, verschijnt deze malware niet meer op de radar van de leveranciers van bijvoorbeeld virusscanners. Volgens www.security.nl laten virusscanners zestig procent van alle nieuwe malware door. Er circuleert bovendien malware die niet gedetecteerd kan worden, omdat die sneller updates ophaalt van het internet dan dat virusscanners worden bijgewerkt. Antivirus softwareleverancier Kaspersky meldde hierover al in 2007: "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" *(zie literatuurverwijzing 4)*.



Bedrijven die aangifte doen van computercriminaliteit ervaren vaak dat de verantwoordelijke criminelen niet kunnen worden veroordeeld, omdat cyberbendes meestal vanuit het buitenland opereren en er alles aan doen de dans te ontspringen. Door de lage pakkans en de hoge inkomsten neemt cybercriminaliteit een enorme vlucht. Het bedrijf F-Secure gaf onlangs aan dat waar de malwaregroei in 2007 is verdubbeld, deze in 2008 is verdrievoudigd.

Cybercriminelen moeten blijven investeren in de ontwikkeling van malware, omdat ze continue strijden tegen patches en antimalware software. Omdat cybercriminelen die kosten willen terugverdienen, is hun inkomstenmodel samen te vatten met de volgende stelling:

Stelling 1: professionele cybercriminelen maximaliseren de return on investment van hun malware (= P x Q) door te focussen op (P).

Hierbij staat P voor het aantal computers dat per malware-aanval wordt besmet en Q als de gemiddelde opbrengst per computer. Het focussen op Q vergt specifieke voorkennis en biedt minder zekerheid. Het kraken van één vitaal systeem kan veel geld opleveren, maar dergelijke systemen zijn vaak goed beveiligd.
Het focussen op P biedt meer zekerheid qua inkomsten omdat veel computers onvoldoende zijn beveiligd. Bovendien is het eenvoudiger, omdat alleen informatie nodig is over de verhoudingen in de softwaremarkt. Bijkomend voordeel is dat als duizenden gedupeerden aangifte doen van een kleine diefstal, vervolging voor justitie moeilijker is dan wanneer één partij aangifte doet van een groot misdrijf.

Veel cyberbendes maximaliseren daarom hun *return on investment* door hun exploits te richten op software die op dat moment marktleider is. Ze kunnen deze producten gewoon kopen, om daarna uitgebreid te onderzoeken welke kwetsbaarheden misbruikt kunnen worden. Malware voor deze software levert het meeste op, omdat in de beschikbare tijd (van uitgebrachte exploit tot geïnstalleerde patch) de meeste systemen worden besmet. Deze strategie maximaliseert ook de kans dat een gericht exploit kan worden hergebruikt. Het marktaandeel van softwareproducten bepaalt dus welke producten cyberbendes onderzoeken op kwetsbaarheden. Op pagina 8 bovenaan staat per categorie het dominante softwareproduct.

Categorie	Softwareproduct	Markt % (schatting)	Populariteit bij criminelen
Office suite	MS Office	95%	+ +
Besturingssysteem	MS Windows	90%	+ +
Webclient	MS IE	79%	+ +
Mailserver	MS Exchange	78%	+
Mailclient	MS Outlook *(Express)*	62%	+
Webserver	Apache	53%	+
Database server	Oracle	44%	+

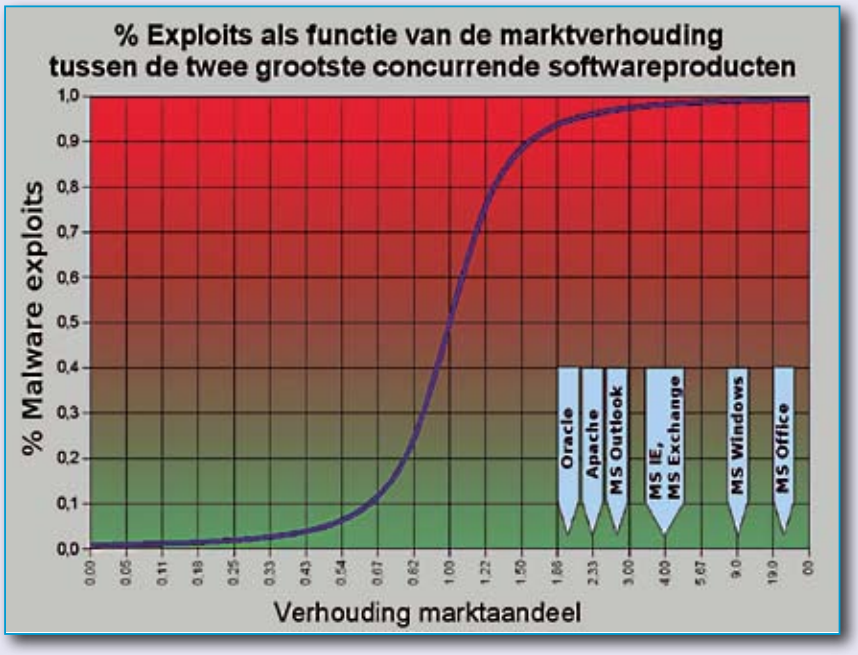
Het najagen van marktleiders lijkt op de varkenscyclus, het economische verschijnsel dat aanbieders massaal reageren op de hoogte van de vraagprijzen. Tegen de tijd dat deze reactie doorwerkt op het aanbod, is de prijs alweer omgeslagen. Het resultaat is dat vraag en aanbod golfbewegingen zijn, waarbij het aanbod na-ijlt op de vraag.

Marktaandeel exploits

De softwaremarkt kent echter weinig golfbewegingen. Omdat enkele producten de markt domineren, vormt het pc-landschap een monocultuur. Als systemen met dezelfde software werken, zijn ze gevoelig voor dezelfde malware. De meest succesvolle softwareproducten trekken daarbij onevenredig veel exploits aan. Een geschikt model om vanuit het marktaandeel van software het aandeel van de exploits te schatten dat voldoet aan dit economische principe, is de S-kromme. De figuur hierna geeft deze functie vereenvoudigd weer.

De landbouw kweekt tegenwoordig vanuit efficiencyoverwegingen relatief weinig gewassoorten in grote monoculturen. Moderne gewassen met steeds meer uniforme karakteristieken vervangen traditionele gewassen in de hele wereld en vormen daarmee een dreiging, omdat de genetische basis smaller wordt. De gekweekte gewassen worden steeds kwetsbaarder voor ziekten en plagen. (World Resources Institute, 2001).

Het vraag-en-aanbod mechanisme is ook toepasbaar op de malware situatie. De 'vraag' bestaat uit het marktaandeel van de software waarop de malware zich kan richten. De exploits voor die software vormen dan het aanbod.



Uit diverse lijsten met beveiligingsadviezen blijkt dat het marktaandeel van een softwareproduct niet correleert met het aantal gesignaleerde kwetsbaarheden. Wel lijkt er een sterke relatie te bestaan tussen het marktaandeel en het aantal verspreide exploits *(zie literatuurverwijzing 5)*. Dit klopt met het veel gehoorde argument dat het grote aantal exploits, van bijvoorbeeld MS Windows, aan het marktaandeel van negentig procent ligt en niet zozeer aan de kwaliteit van de software.

De kwaliteit van software wordt vaak aangeduid met het aantal fouten per duizend regels broncode. De complexiteit en de omvang van een computerprogramma bepalen het aantal fouten en daarmee de kansen voor malware. Een objectieve kwaliteitsvergelijking tussen de open en de gesloten broncode van besturingssystemen is lastig. Je moet dan aannemen dat het aantal kwetsbaarheden per kilobyte broncode ongeveer gelijk is. Open source is qua veiligheid geen *silver bullet*, ook hiervoor blijven patches nodig om fouten te verhelpen. Het is dus niet onmogelijk om malware te ontwikkelen voor Linux of MacOS, maar met een marktaandeel dat twintig keer lager ligt, zullen de inkomsten per exploit evenredig minder zijn.
Je kunt dan redeneren dat als MacOS of Linux marktaandeel wint, meer exploits zullen volgen. Migreren van een marktleidend softwareproduct naar een alternatief product verhoogt dus niet de veiligheid volgens dit argument.

Deze redenering verklaart weliswaar de onbeweeglijkheid van de huidige monocultuur, maar toch is dit geen goed argument tegen softwarediversiteit. Het is bijvoorbeeld onwaarschijnlijk dat marktaandelen in de softwaremarkt zullen omslaan, laat staan snel zullen wijzigen. Het aantal gebruikte applicaties op een platform, de lopende investeringen, de gesloten standaarden, de onbekendheid van alternatieven, de benodigde nieuwe softwarekennis, de behoudende gebruikers, de gekleurde informatie en de angst voor verandering remmen vaak een migratie. Het veiligheidsvoordeel van zo'n productverandering blijft dus sowieso langer bestaan dan algemeen wordt aangenomen.

De druifluis is zeer schadelijk voor druivenplanten. In de negentiende eeuw vernietigde deze bladluizensoort veel Europese wijngaarden; in Frankrijk zo'n zeventig procent van alle planten. Het bestrijden van de druifluis was vrijwel onmogelijk. Men ontdekte dat de wijnrankfamilies in Noord-Amerika wel resistent waren tegen de druifluis. De oplossing was deze wortelstokken te importeren en Europese varianten hierop te entten. (Wikipedia).

Effecten van diversificatie

Om de effecten van diversificatie ruwweg te schatten, stellen we vooraf dat het onwaarschijnlijk is dat productmigraties het aantal uitgebrachte exploits zal vergroten. Het lijkt namelijk onlogisch dat cyberbendes meer activiteiten gaan ondernemen, zonder dat daar een goed rendement tegenover staat. Er zal eerder sprake zijn van een varkenscyclusachtige verschuiving van focus.

aanschafprijs van hard- en software. Omdat de ondersteuning en de downtime eindgebruikers en het beheer van de infrastructuur de resterende tachtig procent vormt, zal een lagere impact van exploits dus sterk doorwerken in de ICT-beheerkosten. Daar staat tegenover dat een organisatie die migreert naar andere software eenmalig extra kosten heeft voor opleidingen en conversie. Maar dat geldt meestal ook voor een productupgrade. Hiermee is diversificatie een beveiligingsmaatregel als elke andere: een investering. Het Amerikaanse *Department of Defense* heeft dit goed begrepen en zij diversifiëren door deels over te stappen op Apple computers *(zie literatuurverwijzing 6)*.

Als de markt bijvoorbeeld 50/50 tussen twee producten verdeeld is, neemt de *return on investment* per exploit met vijftig procent af, omdat een exploit maar maximaal de helft van de systemen kan besmetten. Ook hergebruik van gerichte exploits wordt moeilijker als de softwaremarkt meer verdeeld is. Het dwingt cybercriminelen meer nieuwe malware exploits te ontwikkelen, die per stuk ook nog eens minder opleveren.

Voor softwareleveranciers zal meer diversiteit in de markt naar verwachting resulteren in minder openstaande *Zero Day* exploits per product en daarmee tot minder achterstand bij het ontwikkelen van patches. Dit versterkt het veiligheidseffect verder, omdat de periode waarin kwetsbaarheden kunnen worden misbruikt korter wordt.

Stelling 2: als organisaties standaardiseren op software voor kantoorautomatisering, introduceren ze een single point of failure dat misbruikt kan worden door malware. De hoogte van het risico hangt af van het marktaandeel van de gebruikte softeware.

Een organisatie die overstapt van het marktleidende product A naar een alternatief product B, zal minder geraakt worden door exploits - zoals het lagere marktaandeel van B dicteert. Stel dat, extreem gesteld, alle migraties van A naar B ervoor zorgen dat de markt uiteindelijk 50/50 verdeeld wordt tussen beide producten. De S-kromme geeft dan aan dat vijftig procent van de exploits zich zal richten op product A en vijftig procent op product B. Zelfs in deze situatie vermindert op die manier het aantal exploits per organisatie dus met de helft. Vanuit deze optiek kunnen organisaties dus beter niet-marktleidende software als standaardproduct kiezen. Deze notie is weergegeven in stelling 2.

Het is bekend dat circa twintig procent van de *Total Cost of Ownership* bestaat uit de

Wel standaardiseren, niet allemaal dezelfde standaard

Diversificatie van standaardsoftware voor kantoorautomatisering functioneert macroscopisch als compartimentering tegen exploits. Wanneer de softwaremarkt beter verdeeld is tussen verschillende producten, spreidt dat het risico van malware. Men kan verwachten dat de BV Nederland veiliger wordt als organisaties niet allemaal dezelfde standaardsoftware kiezen. Deze vermindering van de impact van malware is het grootst als de markt gelijk verdeeld is.

Diversificatie van standaarden raakt de internetmaffia waar het zeer doet: de reductie van malware-inkomsten. Vanuit het oogpunt van veiligheid is diversificatie dus een maatregel die voordeel oplevert, die op een andere manier moeilijk te behalen is. In stelling 3 is samengevat met welke software het risico van malware vermindert.

Aanbevelingen voor diversificatie

Om een goede variatie in softwareproducten te bereiken, is het noodzakelijk dat wereldwijd de marktaandelen van softwareproducten en het aantal uitgebrachte exploits per softwareproduct objectief worden bewaakt en gepubliceerd. Momenteel is dat namelijk lastig te bepalen. Bij gelijke ge-

Stelling 3: de impact van malware vermindert door software te kiezen:
- met een klein marktaandeel
- waarvoor snel patches beschikbaar komen
- waarvan de broncode klein en kwalitatief hoogwaardig is

schiktheid is het wenselijk een standaardproduct te kiezen dat werkt met open standaarden, zodat gegevensuitwisseling met andere software gegarandeerd is en *vendor lock-in* wordt voorkomen. Hierdoor is migratie naar andere producten in de toekomst ook beter mogelijk. Het actieplan *Nederland Open in Verbinding* - in de volksmond *Plan Heemskerk* - is een positieve eerste stap om daarvoor de juiste voorwaarden te scheppen *(zie literatuurverwijzing 7)*.

Softwarediversiteit binnen één organisatie conform de Amerikaanse DoD visie vermindert de kwetsbaarheid van een organisatie wel, maar verhoogt de beheerskosten. Als de hele organisatie op alternatieve standaardsoftware overstapt, heeft dat in eerste instantie een grote impact, maar op de lange termijn is dat minder kostenintensief.

Overstappen op een alternatief besturingssysteem is erg ingrijpend en alleen te overwegen bij vitale systemen. Een organisatie kan makkelijker overstappen op alternatieve software voor websurfen, kantoortoepassingen en e-mail. Dergelijke migraties zijn relatief laagdrempelig: de meeste softwareproducten bieden dezelfde functionaliteit, alleen de bediening ervan kan verschillen.

Migratie naar een ander standaardproduct wekt vaak weerstand op, bijvoorbeeld omdat gebruikers en beheerders nieuwe kennis moeten opbouwen. Dat betekent dat migreren naar andere standaardsoftware het beste kan worden doorgevoerd bij het uitfaseren van oude softwareproducten. De gemiddelde pc-gebruiker heeft thuis vaak dezelfde software als op kantoor. Een organisatie die het thuisgebruik van nieuwe standaardproducten faciliteert, verhoogt daarmee de acceptatie van de productverandering. Bovendien elimineert dit het risico dat thuiswerkers softwarepakketten gebruiken uit het illegale circuit, die vaak geïnfecteerd zijn met malware. Het is dan financieel aantrekkelijk om te standaardiseren op *open source software*. In de onderstaande resultatenketen zijn de relaties tussen acties en effecten weergegeven.

De marktverhoudingen zijn echter al jaren min of meer constant, dus weinig bedrijven veranderen van standaardsoftware. In tegenstelling tot de *Convention on Biological Diversity* is het nog ongewoon ICT-diversiteit als beleid tegen digitale verlamming te ontwikkelen. Vasthouden aan standaardproducten, die zich in het vizier van de meeste cybercriminelen bevinden, betekent echter impliciet instemmen met een hoger veiligheidsrisico. Tegelijkertijd wordt het onacceptabel geacht als een cyberaanval vitale overheidssystemen, het betalingsverkeer, telecommunicatiesystemen of de energievoorziening grootschalig lam legt. De NERC in Amerika heeft gemeld dat na de massale uitval van elektriciteitscentrales in 2003, maatregelen tegen cybercrime nog op de agenda staan. Zolang computersystemen kwetsbaar blijven voor malware, kan een betere spreiding van standaardsoftware een domino D-day van vitale voorzieningen voorkomen en cybercriminaliteit verminderen.

Met dank aan Douwe Leguit en Erik de Jong, respectievelijk teammanager en adviseur bij GOVCERT.NL, het *Computer Emergency Response Team* van de Nederlandse Overheid.

Literatuurverwijzingen

1 *http://spamkings.oreilly.com/WhoWroteSobig.pdf*
2 Govcert Trendrapport 2007
3 Incident Management broodnodig, Computable 26 mei 2006
4 The Zero-Day Dilemma, *www.eweek.com/article2/0,1759,2087034,00.asp*
5 Malicious Web Servers, The Honeynet Project, 7 augustus 2007
6 Apples for the Army, *www.forbes.com/home/technology/2007/12/20/apple-army-hackers-tech-security-cx_ag_1221army.html*
7 Nederland Open in Verbinding, ministerie van Economische Zaken, *www.minez.nl/content.jsp?objectid=153180*

Integriteit betreft ons allemaal

Auteur: Pieter IJfs > Pieter IJfs is directeur van IJfs Business Consultancy en is bereikbaar via info@ijfsbusinessconsultancy.nl.

Vrijwel iedereen weet tegenwoordig de aspecten van informatiebeveiliging te noemen: B(etrouwbaarheid), V(ertrouwelijkheid) en I(ntegriteit). Over dat laatste aspect gaat dit artikel dat geschreven is vanuit de praktijk van alle dag. De invalshoek waarmee integriteit bekeken wordt, is mogelijk een iets andere dan u gewoon bent, maar daarom niet minder interessant. Pieter IJfs geeft een inzicht in de praktijk van alledag.

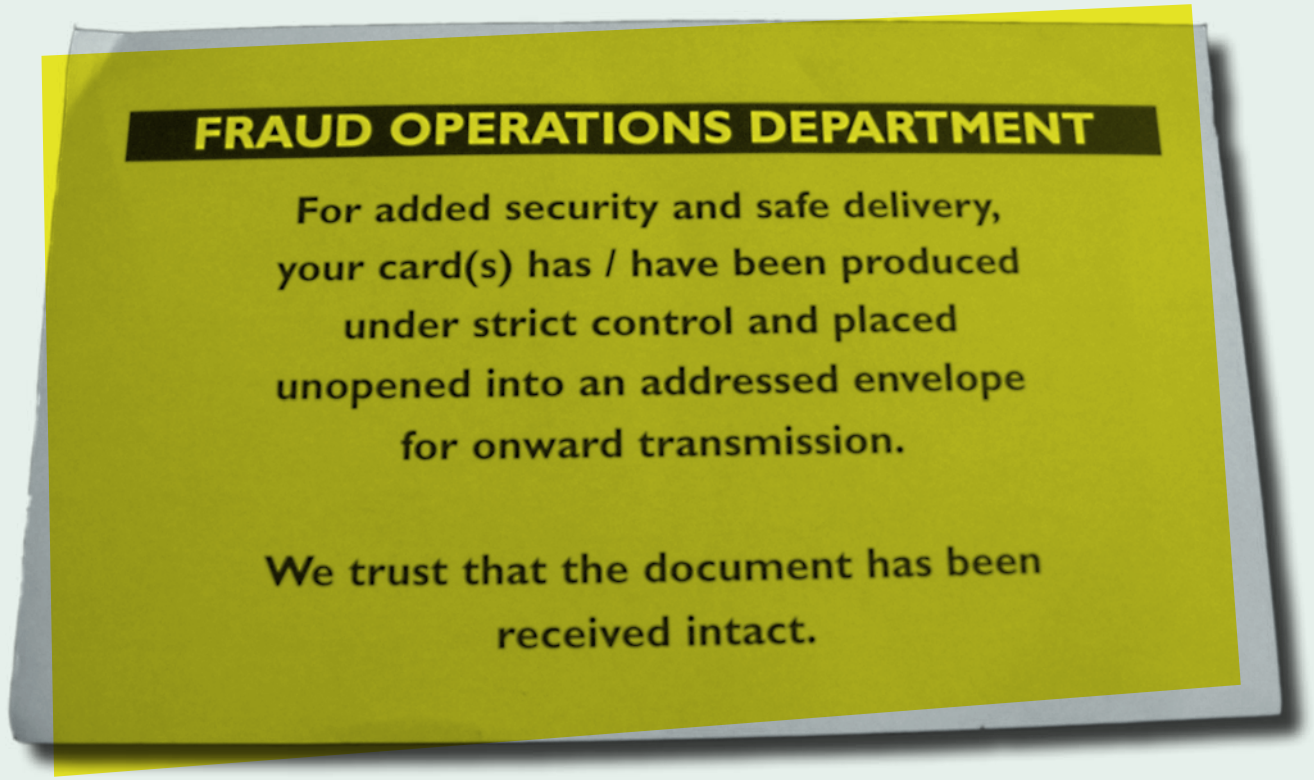
Ondernemers weten best dat ze het risico lopen bestolen te worden en ze willen daar ook wel wat tegen doen. Maar ja: de kosten! Om maar met de deur in huis te vallen, het bedrijfsleven raakt in Nederland per jaar ongeveer zeven procent van haar winst kwijt aan fraude (bron: ACFE-survey 2008). Dat komt neer op 5,7 miljard euro per jaar. En dat is dan ook nog eens door fraude van binnenuit, door de eigen medewerkers. Daar moet de werkgever dus wel degelijk mee aan de gang. Is het niet om zichzelf te beschermen, dan is het wel omdat hij ook de plicht heeft zijn medewerkers tegen de verleidingen te beschermen. De schade is overigens helaas niet specifiek onder te verdelen in branches.

Intern vs. extern

Interne diefstal (de officiële term in dienstbetrekking is verduistering) is een veelvoorkomend verschijnsel, terwijl de meeste beveiligingsmaatregelen die men neemt, hoe noodzakelijk en nuttig ook, er op zijn gericht de gevaren van buitenaf tegen te gaan. Artikelen zijn vaak voorzien van beveiligingslabels en er staan poortjes bij de winkeluitgang, maar die poortjes staan niet bij de personeelsuitgang (het personeel kan die labels bovendien makkelijk verwijderen). Er zijn zichtbare camera's geplaatst die de winkel bestrijken, maar er is vaak niet goed geregeld om, als het nodig is, onzichtbare camera's te gebruiken. Want het gebruik van onzichtbare camera's is sinds 2004 verboden, tenzij...

Er valt veel te bereiken door vooral naar de interne organisatie te kijken. Een fraudeur zal namelijk bij voorkeur gebruikmaken van een gat in de organisatie. Daardoor zal hij in staat zijn zodanig te frauderen dat het niet snel opvalt en hij de fraude langere tijd kan volhouden. Dat bleek in de praktijk een keer wel heel schrijnend. Het was uitgekomen dat een medewerker 4.000 euro naar zijn eigen bankrekening had weten over te maken. De organisatie die daar het slachtoffer van was, zat niet eens in over de hoogte van dat bedrag, maar men wilde wel graag uitgezocht hebben hoe die medewerker dat voor elkaar had weten te krijgen. Uit het onderzoek, en vooral uit het interview met de medewerker bleek het echter om het topje van de bekende ijsberg te gaan. Hij gaf toe dat hij dat gemiddeld tien keer per jaar deed en dat al tien jaar lang! Totale schade: 400.000 euro. Tien jaar geleden had hij een gat gevonden in het systeem, daar was hij gebruik van gaan maken en hij had 'kinderlijk eenvoudig tien jaar lang als God in Frankrijk kunnen leven' (zijn woorden).

Het loont dus met zekerheid om dergelijke gaten te ontdekken en deze met behulp van vaak organisatorische ingrepen te dichten. Daarbij moet u denken aan het vaststellen van wie bij welke bedrijfsinformatie kan komen, het waar mogelijk invoeren van functiescheiding (de boekhouder beheert niet de kleine kas, maar controleert de beheerder van die kas), het instellen van controlemogelijkheden en die ook daadwerkelijk en vastgelegd steekproefsgewijs uitvoeren, het beperken van tekenbe-



voegdheden, en dergelijke. Per bedrijf kan het pakket van maatregelen nogal afwijken, waardoor het lastig is om in algemeen opzicht diep in te gaan op de diverse beveiligingsmogelijkheden. Van belang is wel dat het pakket samenhang heeft en dat de maatregelen met behulp van de kennis onder de medewerkers wordt gemaakt. Niet alleen hebben de medewerkers over het algemeen goed inzicht in de zwakke plekken van de organisatie, zij moeten straks werken met de nieuwe maatregelen (en met de mogelijke inperking van hun 'vrijheid'). Bovendien is de draagkracht bij het personeel voor de invoering essentieel.

Aanpakken aan de bron

Waar beginnen dergelijke integriteitsproblemen nu eigenlijk? Als de werkgever zelf niet duidelijk is naar het personeel wat wel en wat niet mag, hoe moeten zij het dan weten? Dat betekent dat het al veel kan schelen als de werkgever goed vastlegt wat de interne regels zijn, zoals over het gebruik van het kopieerapparaat, e-mail, internet, hoe te handelen bij personeelsaankopen, bij het tijdelijk gebruiken van bedrijfseigendommen (even de bedrijfsbus lenen voor een verhuizinkje). Zo zijn er legio mogelijkheden waar grenzen aan gesteld kunnen worden. Vaak blijkt het technisch heel goed mogelijk om bepaalde zaken te monitoren. Bij veel kopieermachines kan ingesteld worden dat de kopieerder een persoonlijke code hanteert alvorens te kunnen printen en kunnen de printopdrachten gekoppeld worden aan een dossier. Zo wordt het maken van veel privékopietjes al een stuk lastiger te doen zonder dat het opvalt.

En als het dan toch fout gaat, is het zaak een fraudegeval goed aan te (laten) pakken. Het bij elkaar krijgen van voldoende hard bewijs voor een ontslag op staande voet is namelijk aan allerlei regels gebonden. Als werkgever wil je natuurlijk niet dat een rechter het bewijs van tafel veegt als onrechtmatig verkregen, of dat de rechter vindt dat het niet voldoende bewijs is. Want dan sta je als werkgever met lege handen, er is inmiddels wel sprake van een verstoorde arbeidsrelatie en er moet er een schadevergoeding worden betaald. Terwijl die werkgever belazerd is. Maar ja: de kosten! Het is daarom goed te weten dat er uitspraken zijn van rechters die hebben bepaald dat de kosten voor het professioneel laten uitvoeren van een fraudeonderzoek op de daders mogen worden verhaald (bron: Rechtbank Arnhem, 25 juli 2007, LJN: BB2317). En dat mag ook met de toegebrachte schade door het frauderen. Dus dan zou het met die kosten nog weleens kunnen meevallen.

Naast het wegnemen van geld of goederen is de zogenoemde tijdfraude een groeiende schadepost. Daar is sprake van als een medewerker onder werktijd heel andere dingen doet dan waarvoor hij of zij is aangenomen. Denk aan het bezoeken van allerlei sites op internet, die geen zakelijk karakter hebben. Dan kan om porno gaan, maar ook om tijd die besteed wordt aan bijvoorbeeld Hyves, Facebook, Marktplaats, Funda, et cetera. En wat doet die buitendienstmedewerker nu eigenlijk werkelijk? Is die ziekgemelde medewerker eigenlijk echt wel zo ziek dat hij of zij niet kan werken, ook geen aangepast werk? Vertrouwen is goed, maar controle is beter.

En tijd is dan vaak niet alleen de factor die telt. Feitelijk wordt er vaak ook misbruik gemaakt van de bedrijfsmiddelen. De centrale server kan behoorlijk overbelast raken als medewerkers via internet live de Tour de France gaan volgen. En als er muziek wordt gedownload (of films) via de bedrijfsserver kan er naast de overbelasting ook zomaar een heel vervelend virus worden binnengehaald, dat zich in het systeem nestelt en

vervolgens de nodige schade aanricht. De hele bedrijfsvoering kan dan in gevaar komen. Zo bleek bij routineonderhoud aan een laptop van een medewerker dat deze, ondanks een uitdrukkelijk verbod om op internet te gaan, een enorme hoeveelheid sites bezocht, tot en met pornosites toe.

Digitaal forensisch onderzoek

Het komt regelmatig voor dat in dergelijke situaties een digitaal forensisch onderzoek op computers moet worden uitgevoerd, om te achterhalen wie waar verantwoordelijk is geweest. En dat is bepaald geen sinecure. Allereerst is het van belang ervoor te zorgen dat het onderzoeksmateriaal aantoonbaar een werkelijke weergave is van het oorspronkelijke materiaal. Kan dat namelijk niet worden aangetoond, dan kan de mogelijke dader terecht en met een gerede kans op succes manipulatie van de onderzoekgegevens aanvoeren. Niet hij heeft bepaalde informatie laten lekken, bepaalde sites bezocht of films gedownload, maar die gegevens zijn er achteraf aangebracht om hem een loer te draaien. Om dat verwijt te voorkomen, zal er met speciaal daarvoor ontwikkelde software een zogenaamd image van databestanden moeten worden gemaakt. Met die software wordt dan een specifiek gegeven van die data vastgelegd, wat men de hash-waarde noemt, een soort vingerafdruk van de data. Vervolgens kan dan worden aangetoond dat die waarde gedurende het onderzoek niet is veranderd en daarmee ligt dan gelijk vast dat er met de data tijdens het onderzoek niet is gemanipuleerd.

Pas dan kan het feitelijke onderzoek worden uitgevoerd met gebruik van speciale onderzoekssoftware. Met gebruik van bepaalde zoekwoorden kan in de data bijvoorbeeld worden gezocht naar specifieke bronbestanden, naar e-mailberichten, naar cookie-informatie en dergelijke. Weer andere software kan worden gebruikt om met wachtwoord beveiligde bestanden leesbaar te maken, om gewiste data te herstellen (zelfs als een harde schijf is gedefragmenteerd, is er vaak nog data terug te halen). En is er dan materiaal aangetroffen dat het vermoeden van misbruik bevestigt, is het nog niet vanzelfsprekend dat de gebruiker van de computer verantwoordelijk was voor het misbruik. Want wie laat zijn computer nu niet zo af en toe even onbeheerd op zijn werkplek achter? Wie is soms niet wat slordig met de inlogcode, waardoor een ander ook in staat kan zijn geweest die computer te misbruiken. Een dader met een beetje verstand zal dat zeker proberen aan te voeren.

Dan kan het zeer nuttig zijn ook de data te onderzoeken die kort voor en/of kort na het misbruik is bewerkt of aangemaakt. Want als die data, waar dus helemaal niets mis mee hoeft te zijn, wel aan de gebruiker kan worden gekoppeld, kan daarmee worden aangetoond dat die vlieger niet opgaat. Helemaal als ook nog eens kan worden aangetoond dat op de computers van de buurcollega's gewoon is doorgewerkt.

Het is niet voor niets dat digitaal onderzoeken een vak apart is, dat zijn waarde ruimschoots heeft aangetoond. Een welwillende amateuronderzoeker zal in ieder geval vaak meer kapot maken, dan wettig en overtuigend bewijs leveren. Afblijven is het parool!

Bespreekbaar maken schept draagvlak

Het lijkt of er geen einde aan komt, aan de ellende die een ondernemer kan overkomen. Maar we kunnen er niet omheen: aantasting van de integriteit raakt ons allemaal. En je kunt je kop in het zand steken, maar daar gaat het niet door weg. Het grappige is dat het personeel eigenlijk graag wil dat er duidelijkheid is en dat er gecontroleerd wordt. En helemaal willen ze dat er wordt ingegrepen wanneer een collega zich op een oneerlijke manier verrijkt. Want zij hebben het vaak veel eerder in de gaten, dan de werkgever zelf. Maar er bestaat nu eenmaal niet vanzelfsprekend een sfeer dat van die kennis melding wordt gedaan. Die sfeer zou wel kunnen worden bereikt als integriteit één van de agendapunten wordt tijdens het werkoverleg. En dan natuurlijk niet als loos woord, maar als een serieus onderwerp. Daarbij zouden ook beperkingen ter sprake kunnen worden gebracht.

Stel dat de werkgever een beperking wil stellen aan de tijd die werknemers aan privéactiviteiten besteden, zoals naar huis bellen, even wat opzoeken op internet, et cetera. In plaats van zo'n beperking van bovenaf op te leggen, kan het zeer nuttig zijn dat eerst met de werknemers te overleggen. Laat de werknemers zelf eens met een voorstel komen van wat zij als acceptabel ervaren. U moet niet raar opkijken dat er dan een grotere beperking wordt aangedragen dan wat u zelf in gedachten had. En er is gelijk draagkracht. Daag medewerkers uit om ook zelf onderwerpen aan te dragen over het onderwerp integriteit. De werkgever zou nog weleens verbaasd kunnen staan bij wat er dan op tafel wordt gebracht.

Van groot belang is ook het geven van het goede voorbeeld. Zeker door de directie, maar absoluut ook door de direct leidinggevenden. Stel dat er een visitatieregeling is afgesproken; laat dan ook openlijk de tassen van de directie controleren. Als de werkgever actief aan de gang gaat met fraudebestrijding en dat zelf bespreekbaar maakt, kan hij het personeel mee krijgen en zou hij zijn winst zomaar kunnen zien stijgen. Dan kost het opeens niet, maar dan levert het op.

Over de auteur

Pieter IJfs is directeur van IJfs Business Consultancy en hij heeft een lange staat van dienst in de opsporing en preventie van (bedrijfs)fraude. Hij is onder andere bestuurslid van de VPB (Vereniging van Particuliere Beveiligingsorganisaties en Recherchebureaus) en treedt op binnen de toonaangevende Europese belangenorganisatie voor recherchebureaus. Hij heeft zitting in de examencommissie, die is belast met de ontwikkeling van de examens voor de opleiding Particulier Onderzoeker.

Process control security en SCADA security: een realitycheck

Auteur: Maarten Oosterink > Maarten Oosterink is werkzaam als managing consultant bij Capgemini en richt zich hierbij op IT-security, specifiek op het gebied van infrastructuur en process control (SCADA). Daarnaast neem hij deel aan de plant security workgroup van het WIB. Hij is te bereiken via maarten.oosterink@capgemini.com

Proces control security of SCADA security staat de laatste tijd volop in de belangstelling in de wereld van de informatiebeveiliging. De problematiek is vast bekend, dit is in ieder geval het beeld: de systemen zijn uit de vorige eeuw, de software en de besturingssysteem worden nooit gepatched en iedereen gebruikt al jaren 'operator' als wachtwoord. Verder zijn de systemen allemaal aan het internet geknoopt of bereikbaar via een ouderwets modem.

Bron: My first working VAX-11/780 setup van vaxomatic via Flickr

Het is dus tijd voor een reality check. Natuurlijk zijn er veel dingen die beter kunnen in de wereld van process control security. Als je vanuit de relatief comfortabele positie van IT-security kijkt, kun je wel concluderen dat deze tak van sport een paar jaar achterloopt. Dat klinkt als een nadeel, maar vergeet niet dat het ook betekent dat je weet welke kant dingen op zullen gaan.

Windows

Omwille van kostenbesparing zijn leveranciers van process control systemen jaren geleden overgestapt van propietary systemen (UNIX, Vax VMS, Sun Solaris, PDP11) naar Windows. De reden was eenvoudig: kostenbesparing. Niet alleen zijn de systemen goedkoper, ook de ontwikkeling van applicaties is goedkoper en eenvoudiger, bijvoorbeeld omdat er meer libraries, tools en ontwikkelaars voorhanden zijn.

Waar we in de traditionele IT al een tijdje achter zijn, is dat de komst van Windows echter niet alleen maar prijsvoordeel en de voordelen van een wijdverspreid platform met zich meebrengt. Mede dankzij die wijdverspreidheid kan zo'n beetje iedereen met een bovengemiddelde interesse voor beveiliging zich uitleven op de (on)veiligheid van Windows. Bovendien heeft de tijd ons inmiddels geleerd dat Windows niet ontwikkeld is met security en stabiliteit als uitgangspunten. We vergeten wel eens dat Windows lang geleden begonnen is als een gelikte schil om PC-DOS van IBM. Niemand had op dat moment kunnen vermoeden dat de wereld een kleine vijfentwintig jaar later afhankelijk zou zijn van het correct functioneren ervan. Kortom; hotfixes, security updates, virussen en moeilijk verklaarbare crashes kreeg de process control industrie er ook gratis bij, net als iedereen.

Patchen

De afgelopen jaren was het motto rond process control systemen dan ook: 'If it ain't broken, don't fix it'. In de IT hebben we al ontdekt dat dit een weinig houdbaar motto is. Elke IT-organisatie vreest inmiddels de tweede dinsdag van de maand, in de wetenschap dat de lading patches snel gevolgd (of ingehaald) wordt door kwaadaardige codes (malware), die deze kwetsbaarheden uitbuit.

Dat besef is er in de process control industrie inmiddels ook, in ieder geval bij de organisaties die hun handelswijze niet hebben laten inspireren door een Australische loopvogel. Elke zichzelf respecterende organisatie in de industrie weet, dat met het bewust laten passeren van de tijd tussen het beschikbaar komen van patches en de installatie ervan, het risico op incidenten toeneemt. Niet alleen door de dreiging van malware of hackers, maar ook doordat het valideren van de correcte werking van je systemen lastiger wordt naarmate er meerdere patches tegelijkertijd geïnstalleerd worden.

Bron: Ostrich, door lorentey via Flickr.com

Kortom; organisaties maken inmiddels volwassen overwegingen tussen een bewuste downtime van productiesystemen tijdens een regelmatige patchcyclus, versus een onvoorspelbare downtime als gevolg van incidenten. Bovendien is de voorspelbare downtime (deels) af te vangen door de introductie van redundatie in de systemen. Voor de doorgewinterde IT-er inmiddels ook een 'done deal'. Een volgende oplossing die uit de hoek van de IT komt kijken, is die van virtual patching, kortweg het afstoppen van (bekende) kwetsbaarheden, voor ze het feitelijk kwetsbare systeem bereiken. Dit kan bijvoorbeeld door een intelligente firewall of intrusion prevention systeem (IPS).

Internet

De ongebreidelde verspreiding van netwerken, waaronder het internet, heeft uiteraard ook de wereld van process control bereikt. Waar thuisgebruikers of kleine- en middelgrote bedrijven 'the hard way' hebben ontdekt dat je met de komst van internet ook minder goede dingen in huis haalt, kunnen de meeste organisatie die process control systemen gebruiken deze wijsheid overnemen van eerdergenoemde early adopters. En ook hier bieden beproefde oplossingen goede diensten. Denk hierbij aan het complete arsenaal aan netwerkbeveiligingen: van segmentatie en VLANs tot 'deep packet inspecting' firewalls of application firewalls. De industrie kan en heeft (ten dele) op haar gemak en door de schade en schande van anderen de juiste ingrediënten kunnen kiezen om tot een (voor hun) acceptabel niveau van beveiliging te komen.

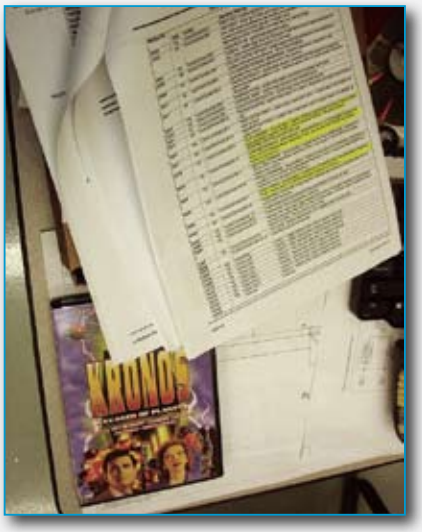
Rozengeur en maneschijn?

Is het dan allemaal rozengeur en maneschijn? Uiteraard niet. Zoals overal heb je mensen en organisaties die vooroplopen, een (grote) middengroep en de achterblijvers. Zo langzamerhand is de middengroep gewaarschuwd. Al was het maar doordat de IT-beveiligingsindustrie haar pijlen momenteel op process control lijkt te richten, nu bestaande markten ingezakt zijn. De middenmoot is zich bewust van de kwetsbaarheden en dreigingen en is in ieder geval bezig met oplossingen. Dat we daarmee verlost zullen zijn van incidenten rond process control of SCADA-systemen in, al dan niet kritische, infrastructuren is natuurlijk een utopie. Vergeet niet dat de levenscyclus van een process control systeem eerder vijfentwintig dan vijf jaar is. Wel kan worden geconcludeerd dat de industrie zich gelukkig mag prijzen dat ze in de luwte van de IT-wereld heeft geleefd, waardoor er inmiddels ruim voldoende oplossingen voorhanden zijn.

Aandacht

Zoals ook Adobe, de Mozilla Foundation en Apple hebben mogen ontdekken, komen er met de toegenomen aandacht voor security in de process control industrie ook een hoop geïnteresseerden op je af, die je liever kwijt dan rijk bent. Daar waar het voor amateurs (jeugdige hackers, hobbyisten) steeds lastiger wordt om kwetsbaarheden te vinden in Windows of veelgebruikte

Bron: MVN_0353London Ave. Canal gates opening 9-14-09 van Team New Orleans, US Army Corps of Engineers via Flickr



Bron: List of Modbus variable addresses, Van Фигушки via Flickr

applicaties, is de vijver van de process control wereld nog vol met vette vis. De overgang van proprietary systemen naar Windows (of Linux) in de industrie betekent niet automatisch dat er ook een overstap naar veiliger protocollen en navenante applicaties is gemaakt. De meeste protocollen versturen informatie nog plaintext over het netwerk, ze bieden nauwelijks tot geen controle op integriteit of authenticiteit en ze zijn gevoelig voor onverwachte inhoud. Koren op de molen van leergierige hackers dus, die op internet steeds meer informatie kunnen vinden. Zoek maar eens op Google, Wikipedia of Scadapedia naar informatie over protocollen als Modbus, DNP3 of OPC. Voor applicaties geldt helaas ook vaak dat lang geleden ontwikkelde applicaties met kunst en vliegwerk van hun originele platformen 'getransplanteerd' worden naar recentere versies van het onderhavige besturingsysteem. Zeker voor de grote spelers in de markt lijkt het vasthouden aan het bestaande systeem een aantrekkelijker keus te zijn, dan herschrijven volgens (recente) Microsoft richtlijnen en standaarden. Dus waar de bewustwording bij de gebruikers een goede vorm aanneemt, lijken de leveranciers nog een zetje nodig te hebben.

Links

- Scadapedia: http://www.digitalbond.com/wiki/
- WIB Plant security workgroup: http://www.wib.nl/files/miniseminar2009_item_9.pdf

Verslag Information Security and Risk Management Conference

Auteur: Tom Bakker > Tom Bakker is lid van de redactieraad van Informatiebeveiliging en te bereiken via tom_bakker@deltalloyd.nl.

Van 9 tot en met 11 november werd de jaarlijkse ISACA Information Security and Risk management Conference Europe, net als vorig jaar, gehouden in het fraaie NH Grand Hotel Krasnapolsky in Amsterdam. Voorheen was deze conferentie beter bekend onder de naam Network Security Conference en Information Security Management Conference, wat in feite twee aparte conferenties waren. Deze nieuwe opzet sluit beter aan bij de huidige opvattingen over risico management. Er waren 260 deelnemers uit 45 landen, Nederland was vertegenwoordigd met 56 deelnemers. Op de zaterdag en zondag voorafgaand aan de conferentie kon men eventueel deelnemen aan een aantal workshops.

Voor de conferentie waren drie streams opgezet:

1. Security Technology
2. Information Security Governance, Standards and Practices
3. Information Risk Management

De conferentie had maar één key note spreker, Charlie McMurdie, die de conferentie opende. Verder waren er break-out presentaties verspreid over bovenstaande streams. Een impressie van een aantal presentaties:

Key note speaker Charlie McMurdie, Detective Superintendent, Metropolitan Police, e-Crime Project

Charlie McMurdie vertelde over het e-Crime project in Groot-Brittannië. Dat project behelst de oprichting van een nationale e-Crime Unit in de UK. Zij ging vooral in op de aanpak en de problemen van het project. Daar de Britse politie niet de benodigde kennis in huis heeft, zoekt zij contact met experts, het (IT) bedrijfsleven en internationale organisaties, zoals Interpol en Europol. Mijn indruk was dat we in Nederland al een stuk verder zijn met onze Govcert en de KLPD (Computercriminaliteit).

Information Security Governance: From the Boardroom to the Keyboard door Todd Fitzgerald (National Government Services, USA)

Todd Fitzgerald ging in op Security Governance. Wat is het en hoe krijg je aandacht? Welke competenties heb je daar voor nodig? Informatiebeveiliging wordt nog steeds vanuit IT aangestuurd, in plaats vanuit de business. Onderzoek van CSO Online wijst uit dat het overgrote deel nog rapporteert aan een CIO/CTO. Communicatie is juist essentieel met de board. Daarom zijn 'soft skills' van een CISO juist zo belangrijk.

Todd heeft altijd een aparte manier om onderwerpen voor het voetlicht te krijgen, zoals verkleedpartijen en vooral interactief bezig zijn. Zo was de zaal verdeeld in CEO's, CIO's en CISO's. Zelfs in een rollenspel kwam naar voren dat communicatie tussen bijvoorbeeld een CEO en een CISO uiterst moeizaam verloopt. Vraag aan de CISO: 'Wat zeg je tegen de CEO als je hem of haar in de lift tegenkomt?' Doodse stilte.

Transforming Information Security to Information Risk management door John Pironti (Archer Technologies LLC Charlestown, MA, USA)

John Pironti ging in op de huidige stand van zaken rond informatiebeveiliging en waarom het nu niet effectief genoeg is. Informatiebeveiliging is te technisch en vooral ook te Compliance-gericht. Informatiebeveiliging moet evolueren in Information Risk Management. Taak voor de organisatie is om voortdurend waarde te creëren, business aansluiting te krijgen en te houden en de beslissers in de organisatie van die informatie te voorzien, die nodig is om betere beslissingen te kunnen nemen. Daarbij is een gestructureerde Governance-benadering essentieel voor succes in de toekomst.

Virtualisation: Securing and Auditing Virtual Environments door Carlos Escapa (Qumotech Sant Cugat, Spain)

Carlos Escapa hield een betoog over de voordelen van virtualisatie en over de introductie van nieuwe risico's (getypeerd als 'the good, the bad and the ugly'). Naast de bekende voordelen (the good) kwamen de nadelen (bad en ugly) aan bod; de extra bescherming die nodig is voor de toegevoegde laag boven de OS van de losse servers (de Hypervisor) en de virtuele (geneste) datacenters (waar is/staat mijn data?). De huidige toolsets zijn ontworpen voor de fysieke omgeving. Zijn die ook toegerust voor een virtuele omgeving? Licenties zijn vaak niet berekend op virtuele omgevingen. Nieuwe aanvalsmechanismen steken de kop op.

Key Considertions for Business Resiliency door John Pironti (Archer Technologies LLC Charlestown, MA, USA)

Business Resiliency gaat volgens de spreker over de consolidatie van verschillende bekende disciplines in één programma: Centraal belegd Command en Control (Crisis Management), Incident respons, Business continuity en Disaster Recovery. Resiliency voorziet de organisatie van de mogelijkheid

om op een gestructureerde en georganiseerde manier de impact van incidenten af te handelen. En dan vooral proactief in plaats van reactief. John's betoog ging verder met hoe je dat vorm zou kunnen geven.

New Generation Workforce: Legal, Technical and management Concerns door Peter Wood (First Base Technologies West Sussex, UK) and Jonathan Armstrong (Eversheds London, UK)
Peter Wood ging in op de, in de titel genoemde, aspecten rondom Web 2.0-achtige zaken. Security issues zijn nieuwe draagbare opslagmedia met grote capaciteit, toegenomen (IT) kennis van medewerkers, baanonzekerheid, de toegenomen gelegenheid om meer schade aan te kunnen richten (reputatie, snelle koersfluctuaties, razendsnelle verspreiding van informatie). Dus reputatieschade, het lekken van gevoelige informatie (financieel, intellectueel eigendom, persoonsgegevens). Peter gaf tenslotte nog wat praktische tips om hier mee om te gaan. Een voorbeeld was de roep door het management om toegang tot sociale netwerken te blokkeren op het werk. Dat is een slecht idee, omdat er dan toch gezocht worden naar wegen een blokkade te omzeilen en dan heb je er helemaal geen grip meer op. Peter ziet meer in het bevorderen van het bewustzijn van medewerkers over de te lopen risico's.

Malicious Insiders: The Growing Threat to Information Security door Chris Archinal (McAfee, Houston, USA)
Dit was bekende materie. Het bijzondere was wel de definitie van Insiders. Hiertoe behoren niet enkel de werknemers die op de payroll staan, maar ook voormalige werknemers, leveranciers, externe consultants, uitzendkrachten en business partners. Dus personen die een min of meer vertrouwde status hebben. Speerpunten zijn: specifieke Insider Threat & Risk Assessments, Security Awareness, Need-to-know/have permissies, functiescheidingen, password management, logging, monitoring, auditing en (insider) incident response plan. Vooral monitoring is belangrijk. Wat gebeurt er in het netwerk?
Ik miste in het betoog wel specifieke aandacht voor Privileged Users.

Forensics: When it went wrong, what really happened door Matthijs van der Wel (Verizon Business Amsterdam, The Netherlands)
Verizon publiceert jaarlijks een rapport met een overzicht van de data breaches die wereldwijd gespeeld hebben ('285 million records were compromised in 2008').
Naast een samenvatting van het rapport gaf Matthijs een nadere toelichting over de oorzaken van die incidenten. Het jaar 2008 gaf min of meer hetzelfde beeld als voorgaande jaren alleen werden nieuwe invalshoeken en trends waargenomen.

- Bronnen: qua distributie geen nieuwe wegen, maar vooral een toename van georganiseerde misdaad die achter de aanvallen zit.
- Aanvallen: criminelen exploiteren fouten (patches!), installeren malware, breken in in systemen. In 2008 waren er meer doelgerichte aanvallen, speciaal tegen organisaties die grote volumes aan gewilde data verwerken of opslaan. Echt moeilijke aanvallen zijn zeldzaam maar die zijn wel zeer schadelijk. Grote toename van speciaal aangepaste, intelligente malware.
- Assets en data: focus ligt op online inbare (cashable) data. Bijna alle inbraken komen van servers en applicaties. Nieuwe datatypen (bijvoorbeeld pingegevens) zijn zeer gewild. Nieuwe doelen en technieken zijn nodig.
- Ontdekking: vaak ontdekt men een inbraak pas maanden later en dan vaak nog door derde partijen (69 procent!).
- Preventie: basismaatregelen, indien consistent toegepast, zijn in de meeste gevallen effectief (55 procent ten opzichte van het aantal incidenten).
  Eén van de fundamentele self assessments van een organisatie is te onderzoeken of men een Target of Choice of een Target of Opportunity is. Bij de eerste kan men doelgerichte, geavanceerde aanvallen verwachten. Daar moet men zich specifiek op voorbereiden.
  Bij de laatste moet men de inbraakgelegenheid minimaliseren door basic controls in te richten zodat men niet de aandacht trekt. In ieder geval minder aandacht dan de 'buurman'.

Het volledige rapport van Verizon is te downloaden via *http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf*. Lees ook het uitgebreide artikel van Matthijs in nummer 6 van dit blad uit dit jaar.

Het was een leerzame en goed verzorgde conferentie. Niet alle onderwerpen waren even vernieuwend, maar hier en daar waren toch wel weer punten te horen, vooral in de discussies, die tot nadenken stemmen. Jammer dat de conferentie niet afgesloten werd met nog een key note spreker, zoals bij ISF gebruikelijk is. Na de laatste presentaties in de streams, die niet alle tegelijk eindigden, ging iedereen snel huiswaarts of nog even Amsterdam in. Beetje een anticlimax, toch.

Een serious game voor informatiebeveiliging

Auteur: Marcel Spruit > dr. Marcel Spruit is lector informatiebeveiliging aan de Haagse Hogeschool en adviseur aan Het Expertise Centrum. Hij is te bereiken via m.e.m.spruit@hhs.nl.

Elke organisatie heeft cruciale informatie, waarvan de organisatie in hoge mate afhankelijk is. Er kan veel misgaan met deze informatie en beveiliging ervan is onmisbaar. In de praktijk blijkt goede informatiebeveiliging echter lastig te realiseren. Dit komt enerzijds doordat het complexe materie is, anderzijds doordat de gangbare opleiding en training op het gebied van informatiebeveiliging wel wat te wensen overlaat. Het is vooral lastig om het menselijke aspect goed voor het voetlicht te brengen. Een realistische simulatie, een serious game, kan helpen het broodnodige inzicht in informatiebeveiliging te verbeteren.

Informatie speelt een cruciale rol in onze maatschappij. Ook in organisaties, die in hoge mate afhankelijk zijn van allerlei informatie. Het kan dan gaan om personeelsinformatie, marktinformatie, opdrachtinformatie, financiële informatie, et cetera. Elke organisatie vereist dat belangrijke informatie correct en op de juiste tijd beschikbaar is en dat vertrouwelijke informatie niet op straat belandt. Gezien het aantal beveiligingsincidenten dat optreedt, is dat niet zo eenvoudig. Waar ligt dat dan aan? Als we naar de oorzaken van beveiligingsincidenten kijken, zien we dat de meeste incidenten terug zijn te voeren op menselijk falen. Blijkbaar zijn mensen de zwakke schakel in de informatieverwerking. Anderzijds zijn het ook de mensen die informatiebeveiliging moeten invullen en tot een succes moeten maken.

In het algemeen kunnen we zeggen dat informatiebeveiliging een sterke menselijke-organisatorische component heeft. De theorie ervan wordt door verscheidene instellingen in het middelbaar en hoger onderwijs aangeboden. Voor de 'klas' blijkt echter dat kennis over de menselijke-organisatorische component moeilijk omgezet kan worden naar inzicht. Met aanschouwelijke middelen is het mogelijk om de studenten meer inzicht in de menselijke-organisatorische component van informatiebeveiliging te laten krijgen. Dat was de reden om de hier besproken information security game te ontwikkelen.

Er bestaan al games op het gebied van informatiebeveiliging, maar deze richten zich vooral op het aspect vertrouwelijkheid. In de meeste gevallen gaat het om scenario's waarin iemand vertrouwelijke gegevens verliest of een spion op tijd moet ontmaskeren. In de praktijk komen dergelijke scenario's weliswaar voor, maar ze zijn niet representatief voor de problematiek van informatiebeveiliging.

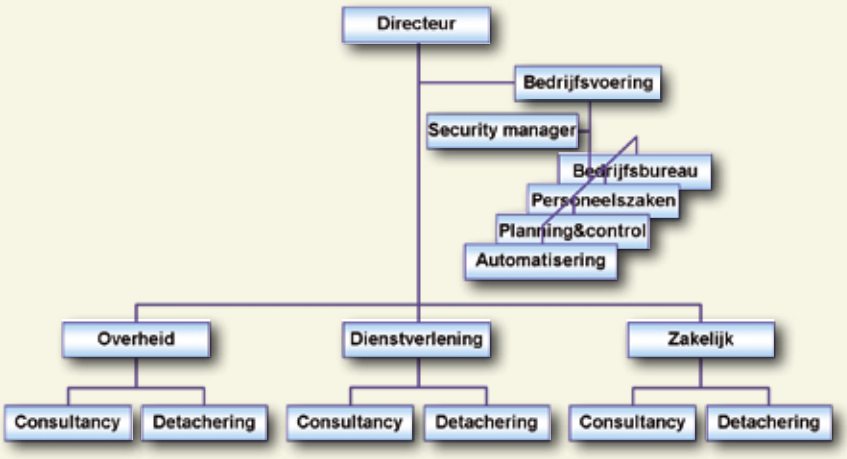
Waar gaat het dan wel om? In de praktijk blijkt het lastig om een ondersteunende discipline, zoals informatiebeveiliging, bij het management en de collega's op de agenda te krijgen. Bovendien is het lastig om de juiste balans te vinden tussen het eigen werk en informatiebeveiliging. Naast gebrek aan kennis en inzicht spelen ook eigenbelang en kortetermijndenken een rol.

Uitgangspunten

De information security game is een managementgame die specifiek ontwikkeld is om het inzicht in de menselijke-organisatorische component van informatiebeveiliging te vergroten. De game heeft tot doel de deelnemers inzicht te laten krijgen in de praktijk van informatiebeveiliging in een organisatie, aan de hand van realistische bedreigingen en dilemma's in een gesimuleerde bedrijfssituatie. Van de deelnemers wordt verwacht dat zij de basistheorie van informatiebeveiliging voldoende beheersen (Overbeek e.a., 2005). Verdere voorkennis is niet nodig.

De game speelt zich af in het hypothetische bedrijf Insecure, een middelgroot adviesbureau. De deelnemers aan de game krijgen verschillende functies in dit bedrijf toebedeeld. De game kan in drie uur uitgevoerd worden, inclusief een inleidende presentatie en een nabespreking. De game doorloopt een aantal ronden, waarbij iedere ronde een vaste periode van een jaar representeert. De game verloopt zonder hulp van een computer, hoewel een laptop gebruikt kan worden om een inleidende presentatie te ondersteunen en om de berekening van scores in de game te vergemakkelijken.

Figuur 1: Organogram van Insecure



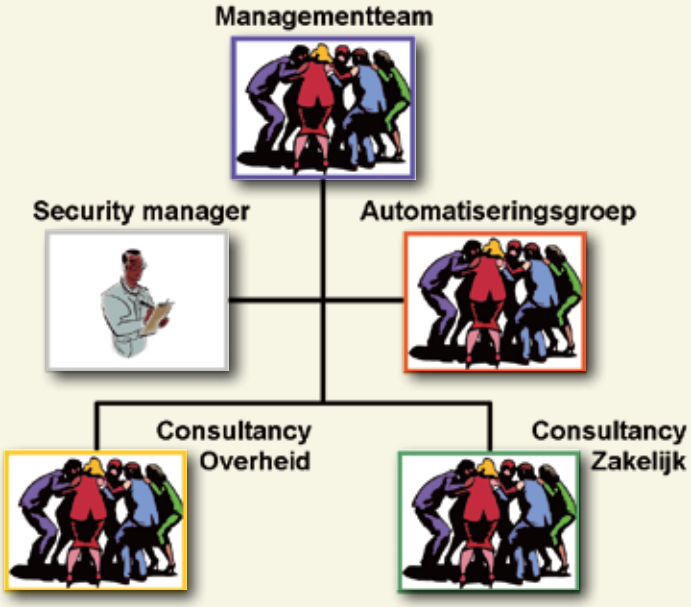
Situatieschets
Het bedrijf Insecure is een middelgrote onderneming, die zich richt op het leveren van managementadviezen en -ondersteuning aan merendeels grote bedrijven en instellingen. Insecure heeft ongeveer honderdvijftig medewerkers in dienst. Een aanzienlijk aantal van deze medewerkers werkt extern op een klantenlocatie. De organisatie van Insecure is op hoofdlijnen geschetst in onderstaand organogram.

Het primaire proces van de organisatie is belegd bij een drietal branchegeoriënteerde afdelingen: Overheid, Dienstverlening en Zakelijk. Deze afdelingen hebben ieder een consultancygroep en een detacheringsgroep. Daarnaast is er een ondersteunende afdeling, de afdeling Bedrijfsvoering.
De automatiseringsgroep en de security manager zijn in deze afdeling ondergebracht. De afdelingshoofden vormen samen met de directeur het managementteam.
De automatisering is niet uitbesteed, maar er is wel gekozen voor het consequent toepassen van standaard 'off the shelf' hardware en software.

Structuur van de game
De information security game speelt zich af met de volgende functionarissen van Insecure:
- Het managementteam (directeur en afdelingshoofden)
- De automatiseringsgroep (hoofd IT en IT-beheerders)
- De security manager
- Een of twee consultancygroepen (per groep een groepshoofd en consultants)

Alle functionarissen hebben hun eigen werk en ze hebben daar hun handen vol aan. Daarnaast moeten ze ook nog aandacht besteden aan informatiebeveiliging.
Alleen voor de security manager geldt dat het primaire werk en informatiebeveiliging samenvallen. Voor de andere functionarissen is het de kunst om naast het eigen primaire werk ook nog tijd te vinden voor beveiliging; niet te weinig, maar ook niet te veel.

Gedurende de gesimuleerde jaren gebeurt het een en ander. Ieder doet zijn primaire werk en doet daarnaast wat nodig is aan



Figuur 2: De groepen in de information security game

informatiebeveiliging. In de tussentijd manifesteren zich bedreigingen. Als de juiste maatregelen getroffen zijn, is dat geen probleem. Zo niet, dan leidt dat tot incidenten en daarmee tot kosten. Informatiebeveiliging kost dus altijd geld: voor maatregelen of anders door incidenten. Net als in het echt. De kunst is de kosten voor zowel maatregelen, als incidenten te minimaliseren. Maar er is, net als in de realiteit, weinig tijd om dat eens goed uit te gaan zoeken. Alle tijd die aan informatiebeveiliging wordt besteed, gaat af van de tijd voor het primaire werk, en het primaire werk levert juist geld op.

De reeks bedreigingen die zich gedurende de game manifesteert, ligt vast en is gebaseerd op praktijkervaring en -onderzoek (SpLo, 1996; BSI, 2007; CSI, 2008). Hetzelfde geldt voor de schade die optreedt bij incidenten en de kosten die gemoeid zijn met het nemen van beveiligingsmaatregelen. Op deze manier zijn de optredende bedreigingen en de kosten voor maatregelen en incidenten tamelijk realistisch.

Welke bedreigingen zich manifesteren, wordt de deelnemers uiteraard niet van tevoren verteld. Ze weten dat de situatie realistisch is, maar ze hebben over het algemeen geen goed beeld van de bedreigingen die in de praktijk optreden en de schade die dat kan veroorzaken. Zij kunnen, en moeten, hierover wel een inschatting maken. Maar in feite weten ze even weinig als functionarissen 'in het echt'.
De kosten voor het treffen van maatregelen zijn daarentegen wel bekend. Uiteindelijk moeten de deelnemers zelf maatregelen treffen en daarvoor betalen.

Karakteristieke elementen
In de game spelen de deelnemers de rol van verschillende functionarissen. De game zou te gecompliceerd worden als het werk van alle verschillende functionarissen nagebootst zou moeten worden. Gelukkig is dat ook niet nodig. Het gaat per slot van rekening niet om de inhoud van het werk, maar om het vinden van de balans tussen het werk en informatiebeveiliging. Voor de game volstaat het als iedere deelnemer aantrekkelijk werk heeft en daarmee een nuttige bijdrage aan de eigen groep kan leveren.

In de game wordt het primaire werk van iedere functionaris gesymboliseerd door het oplossen van puzzels. Iedere deelnemer die een puzzel oplost, creëert een financiële bijdrage aan het groepsbudget. De meeste mensen vinden puzzels maken aantrekkelijk werk en de financiële beloning maakt het werk nuttig voor de groep. Daarmee voldoet het oplossen van puzzels als primair werk voor de deelnemers.

Een cruciaal aspect van de security game is dat de deelnemers de juiste balans tussen werk en informatiebeveiliging niet al te gemakkelijk bereiken. Elke deelnemer kan

goede redenen vinden om te weinig of juist te veel aan informatiebeveiliging te doen. Te weinig aandacht voor informatiebeveiliging kan veroorzaakt worden doordat de deelnemer zich mee laat sleuren door het primaire werk, de puzzels oplossen, dat rechtstreeks tot beloning leidt. Te veel aandacht voor informatiebeveiliging kan veroorzaakt worden door het besef dat de game over informatiebeveiliging gaat. De deelnemer gaat zich dan op het gebied van informatiebeveiliging voorbeeldig gedragen en treft alle mogelijke maatregelen, maar creëert te weinig inkomsten voor de eigen groep.

In de hitte van het spel is het voor de meeste deelnemers niet duidelijk of zij wellicht te weinig of te veel aandacht aan informatiebeveiliging besteden. Gedurende het spel wordt het de deelnemers steeds duidelijker, want zowel een tekort, als een overmaat aan aandacht voor informatiebeveiliging wordt in de game zichtbaar.

De game wordt gespeeld met meerdere groepen functionarissen. In de realiteit beïnvloedt het functioneren van één groep direct het functioneren van de andere groepen. Als bijvoorbeeld het managementteam niet goed functioneert, dan kunnen de andere groepen ook niet goed functioneren. In de game is dat een nadeel. Wanneer je als groep niet goed kan scoren, doordat één van de andere groepen er niets van bakt, dan is dat nogal onbevredigend. Als elke groep daarentegen volledig onafhankelijk opereert, dan is dat weinig realistisch en daardoor ook onbevredigend.

Binnen de game is gekozen voor een opzet met een zeer beperkte onderlinge invloed tussen de groepen: de groepen zijn in principe onafhankelijk, maar waar het de game niet teveel stoort zijn onderlinge invloeden ingebracht. In die situaties is het mogelijk dat één groep de andere groepen stoort. Deze stoorsituaties zijn gebaseerd op illustratieve voorbeelden van ongelukkig uitpakkende maatregelen. De effecten hiervan zijn voor de andere groepen weliswaar duidelijk merkbaar, maar de doorwerking ervan is beperkt. Voor de andere groepen betekent dit dat ze er iets aan kunnen doen, maar dat ze ook zonder er iets aan te doen goed kunnen functioneren.

Ervaringen

De information security game is inmiddels enige tientallen keren gespeeld, onder meer aan de Haagse Hogeschool, de Noordelijke Hogeschool Leeuwarden, de Open Universiteit, de Universiteit van Amsterdam en de Erasmus Universiteit. De reacties en evaluaties waren steeds zeer positief. Bovendien wijzen de reacties erop dat de game inderdaad het inzicht in de menselijke-organisatorische component van informatiebeveiliging verbetert.

Het is opvallend dat de deelnemers in de game veelal fouten maken die ook in soortgelijke functies in de praktijk gemaakt worden. Zo bekommeren de managers zich bijvoorbeeld te weinig om de werknemers, houden de automatiseerders te weinig rekening met het management en schuiven de consultants de informatiebeveiliging ongevraagd af op de automatiseerders. Over de hele linie blijkt dat de deelnemers moeite hebben met belangrijke aspecten voor informatiebeveiliging, zoals het zorgen voor draagvlak en het communiceren over informatiebeveiliging.

In de nabespreking herkennen de meeste deelnemers meestal hun belangrijkste fouten. Vaak echter pas nadat ze erop gewezen worden. Vanwege het groepsgewijze werken, zijn de deelnemers niet individueel verantwoordelijk voor deze fouten. Toch is de herkenning ervan relatief groot.

De game is in de huidige vorm zeer goed speelbaar. De ervaringen die hiermee opgedaan zijn, hebben geleid tot verfijningen in het draaiboek van de game. Verdere verfijningen die toegevoegd kunnen worden, zijn bijvoorbeeld het toevoegen van meer interacties tussen de groepen. Daarnaast is het mogelijk om computerondersteuning te realiseren, zodat bedreigingen zich geautomatiseerd bij de groepen manifesteren en ook de gevolgen hiervan geautomatiseerd bijgehouden kunnen worden.

Conclusie

De information security game is ontwikkeld om de menselijke-organisatorische component van informatiebeveiliging inzichtelijker te maken. De ervaring leert dat de game daar inderdaad in slaagt. Verdere verfijningen kunnen de game nog realistischer en dynamischer maken. Daarom wordt verder gewerkt aan het doorontwikkelen van de game.

Literatuur

- BSI, The IT security situation in Germany in 2007, Federal Office for Information Security, 2007.
- CSI, 2008 Computer crime and security survey. Computer Security Institute, 2008.
- P. Overbeek, E. Roos Lindgreen & M. Spruit, Informatiebeveiliging onder controle. Pearson Education, Amsterdam, 2005.
- M.E.M. Spruit & M. Looijen, IT security in Dutch practice. Computers & Security, nr. 2, 1996, pag. 157-170.

Een architectuuraanpak voor IB-patronen

Auteur: Jaap van der Veen > Jaap van der Veen is strategisch architect Informatiebeveiliging bij de Belastingdienst. Als auteur en lid van de expertgroep werkt Jaap mee aan het nieuwe NORA katern Informatiebeveiliging en hij is tevens trekker van de PvIB-community voor IB-patronen. Jaap is bereikbaar via jaap.vanderveen@gmail.com.

Na een eerste artikel over dit onderwerp, Securitycafé geslaagd!, in de Informatiebeveiliging van april 2009, neem ik u graag mee in een serie van twee artikelen over de uitgangspunten en de uitwerking van informatiebeveiliging-patronen, die we hierna IB-patronen noemen. In dit artikel behandel ik een *architectuuraanpak* als basis voor zowel IB-patronen als IB-architecturen. Verder gaan we in op een beschouwingsmodel, dat de PvIB-Patronencommunity als standaard context gebruikt voor IB-patronen. Over deze community leest u meer aan het eind van dit artikel.

Een artikel in de eerstvolgende Informatiebeveiliging motiveert de toepassing van IB-patronen en legt uit hoe ze zijn opgebouwd aan de hand van een voorbeelduitwerking. Als u geïnteresseerd bent in de achtergronden, dan kunt u nu alvast een kijkje nemen op www.ibpedia.nl, waar het werkdocument van de patronencommunity is gepubliceerd, inclusief uitleg en een drietal patronen.

Inleiding architectuuraanpak

Een architectuuraanpak helpt de gebruiker bij het analyseren, het adviseren en het toetsen van informatiebeveiligingsaspecten in architectuurmodellen. In een dergelijke aanpak wordt een verbinding gelegd tussen architectuurmodellen en een standaard model voor IB-functies met het daarbij behorende normenkader. De hier beschreven aanpak is gebaseerd op de NORA, de Nederlandse Overheid Referentie Architectuur. In de NORA zijn de architectuurprincipes voor informatiebeveiliging in een apart katern uitgewerkt *(literatuurverwijzing 1)*. Voor meer informatie over de NORA in het algemeen verwijs ik u naar literatuurverwijzing 2. Architectuurmodellen voor informatiebeveiliging richten zich meestal op de ICT-oplossingen, die in een organisatie worden gekozen voor beveiligingsfuncties. In het NORA katern informatiebeveiliging wordt uitgegaan van informatiebeveiliging als *kwaliteitsaspect*.

Het normenkader voor IB-functies wordt als document onderhouden vanuit de NORA en is daar bekend onder de titel Best Practice: *Normen Informatiebeveiliging ICT-voorzieningen (literatuurverwijzing 3)*. In dat document is een kruisverwijzing opgenomen met de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2007 nl, hierna de Code genoemd), voor zover die van toepassing is. Dit NORA-normenkader kent drie abstractieniveaus: doelstelling, maatregel en implementatierichtlijn, conform de Code.

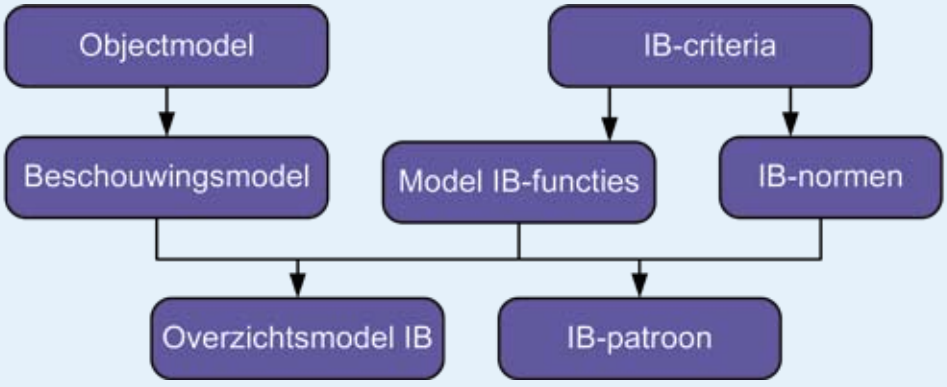
Deze architectuuraanpak wordt verder uitgebouwd en geconcretiseerd met IB-patronen, die als architectuurmodules kunnen worden gezien. In het volgende artikel gaan we daar verder op in. De patronen volgen in principe de abstractieniveaus van de normenset.

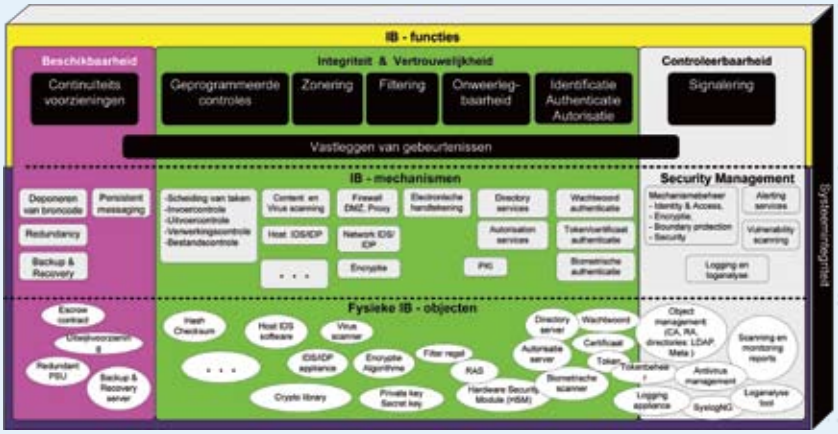
Modellering

Omdat beveiliging een aspect is van de bedrijfsvoering, hebben we een objectmodel nodig om te laten zien waar de IB-functies werkzaam moeten zijn. Architectuurplaten zoals objectmodellen zijn echter niet zonder uitleg geschikt om IB-functies op te projecteren. De reden daarvan is dat beveiliging als aspect integraal deel uitmaakt van het ICT-ontwerp, 'het zit overal in'. Beveiliging komt in het ICT-ontwerp voor als afzonderlijke objecten (zowel hardware als software), maar ook als configuratie-item van een ander object. Om die verwevenheid met ICT zinvol af te kunnen beelden, maken we vanuit de bedrijfsobjecten een *beschouwingsmodel*, waarin een belangrijke ordening voor ICT-beveiliging is verwerkt: de netwerkzonering (als IB-functie). Tussen dit beschouwingsmodel en de IB-functies worden vervolgens relaties gelegd, waaruit een architectuur voor Informatiebeveiliging kan ontstaan. Voor een globaal overzicht worden IB-functies op de gehele architectuur geprojecteerd. Voor meer details worden IB-patronen gebruikt.

Een IB-patroon is een abstractie van een probleem en een oplossing binnen een bepaalde context, waardoor de oplossing

Figuur 1: NORA aanpak architectuur IB





Figuur 2: IB-functies

algemener inzetbaar wordt. Patronen zijn te beschouwen als *bouwstenen* op architectuurniveau. De hier geschetste architectuuraanpak wordt momenteel verder uitgebouwd door het modelleren van veel voorkomende beveiligingssituaties in IB-patronen. De focus van de IB-patronen is gericht op ICT. De doelgroep van patronen is de architect, ontwerper, specialist en IT-auditor, die deze beknopte beschrijvingen gebruiken als gereedschap voor het maken, het ontwerpen of het toetsen van ICT.

Een IB-architectuur is een ontwerp, dat voor het aspect Informatiebeveiliging de *samenhang* duidelijk maakt tussen producten, processen, organisatie, informatievoorziening en infrastructuur. De focus van de hier beschreven aanpak ligt op ICT voorzieningen. Met de verschillende views van die samenhang heeft de IB-architectuur een belangrijke communicatierol richting andere architecturen van organisaties. De IB-functies en de IB-normen spelen daarbij een centrale rol.

Model IB-functies

Het referentiekader voor de modelleringaanpak wordt gevormd door het model IB-functies (zie figuur 2), dat is bedoeld als voertuig om te ordenen en te verbinden. Het model is een eigen doorontwikkeling van ISO-NEN 7498-2 Information processing systems - Open Systems Interconnection Basic Reference Model – Part 2: Security Architecture uit 1991.
Een IB-functie is een logische groepering van geautomatiseerde activiteiten, die op een bepaald beveiligingsdoel is gericht. In samenhang worden de acht afgebeelde beveiligingsfuncties dekkend geacht voor de informatiebeveiliging van ICT-voorzieningen (zwarte functieblokken in figuur 2). In het architectuurmodel zijn deze IB-functies geprojecteerd op de *IB-criteria* voor informatiebeveiliging: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid. In *samenhang* vormen ze de WAT-laag van het model.

De IB-functies met bijbehorende mechanismen en fysieke objecten zijn voor de eenvoud van de afbeelding op de criteria geprojecteerd, die ze *primair* ondersteunen, maar de functies voor integriteit en vertrouwelijkheid dragen bijvoorbeeld ook bij aan beschikbaarheid. Per IB-functie bestaat een principe, een definitie, een toelichting en een motivering. Voor de NORA zijn deze geformuleerd in best practice *(literatuurverwijzing 3)*.

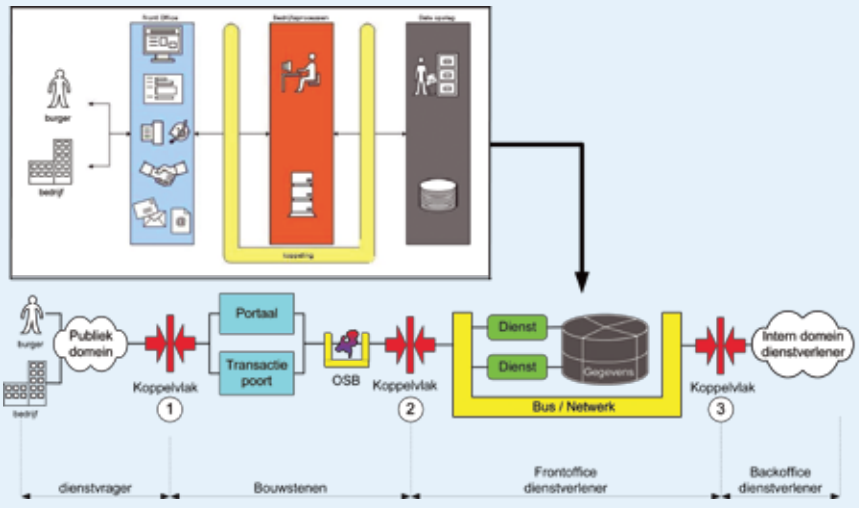
De IB-mechanismen vormen de HOE-laag en zijn *technische* concepten (technieken) die het WAT van de IB-functies invullen. Omdat techniek zich steeds verder ontwikkelt, illustreert de figuur slechts een aantal bekende voorbeelden. De IB-mechanismen zijn de *maatregelen* waarmee IB-functies worden ingevuld. In het NORA-katern *(literatuurverwijzing 1)* worden maatregelen *implicaties* genoemd. Elke maatregel kent één of meerdere implementatierichtlijnen *(literatuurverwijzing 3)*.

De fysieke IB-objecten vormen de WAARMEE-laag. Dit zijn ICT-onderdelen die de IB-mechanismen daadwerkelijk uitvoeren. Ze kunnen onderdeel zijn van een besturingsprogramma of een applicatie, maar ze worden ook als afzonderlijke fysieke modules uitgevoerd. Ook hier zijn slechts enkele bekende voorbeelden getekend. Hoewel referentiearchitecturen de HOE- en WAARMEE-laag meestal niet beschrijven, is dat hier wel gedaan, om duidelijk te maken hoe en waarmee beveiligingsfuncties uiteindelijk werkzaam zijn in de ICT.

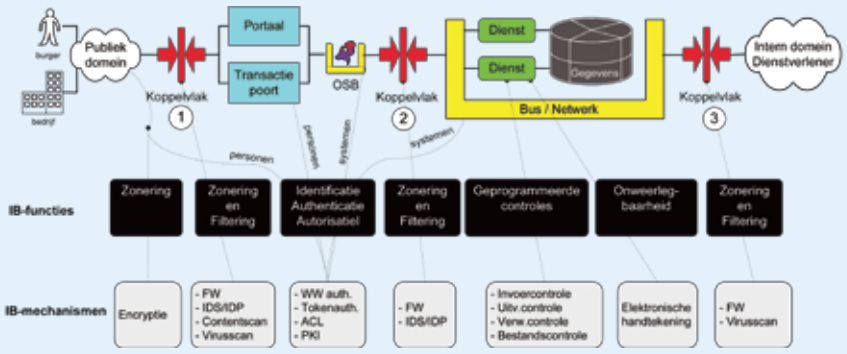
In de beschrijving die nu volgt, geef ik aan welke modellen we gebruiken om informatiebeveiliging van infrastructuren inzichtelijk te maken, zodat we daarmee IB-patronen kunnen samenstellen.

Beschouwingsmodel NORA-keten

Het beschouwingsmodel is een basisplaat, waarmee in grote lijnen aangegeven wordt hoe IB- functies samenhangen met ICT-voorzieningen. Een beschouwingsmodel ontstaat vanuit een objectmodel van bedrijfsfuncties. Figuur 3 geeft aan hoe een beschouwingsmodel, van bijvoorbeeld een NORA-keten, ontstaat vanuit het objectmodel Basisarchitectuur overheidsorganisatie *(literatuurverwijzing 2)*. Op de objecten van deze basisarchitectuur worden de te beveiligen zones geprojecteerd met koppelvlak-



Figuur 3: Beschouwingsmodel van een NORA-keten



Figuur 4: Overzichtsmodel voor Integriteit en Vertrouwelijkheid in een NORA-keten

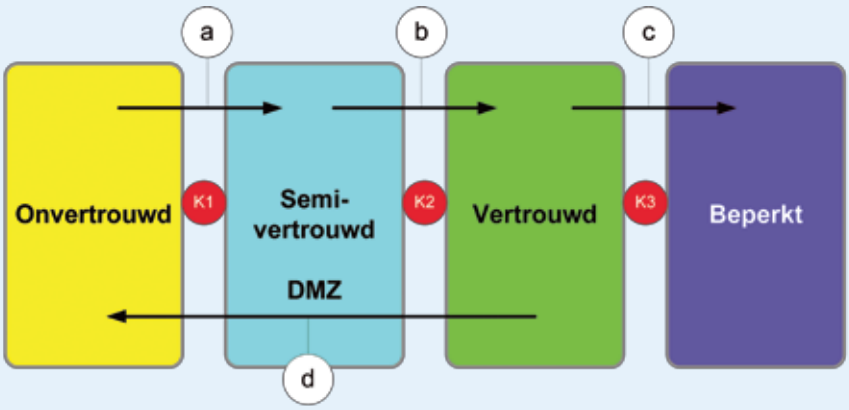
ken daartussen. De koppelvlakken zijn voor de herkenbaarheid genummerd. De bouwstenen van dit beschouwingsmodel zijn de centrale overheidsdiensten ten behoeve van overheidsdienstverleners. OSB staat voor Overheid Service Bus.

Samengevat zet een beschouwingsmodel de verschillende bedrijfsobjecten op een zodanige manier neer, dat het aangrijpingspunt van IB-functies in de view kunnen worden aangegeven. In het overzichtsmodel laten we vervolgens de IB-functies zien.

Overzichtsmodel IB

Het overzichtsmodel ontstaat door op het beschouwingsmodel de relevante IB-functies af te beelden met de bijbehorende IB-mechanismen. De daarmee verkregen schets van functies en uitvoerende mechanismen is overigens niet uitputtend, maar dient voor het verkrijgen van overzicht en inzicht in de plek waar IB werkzaam is in bedrijfsketens en infrastructuren. Voor de eenvoud beperken we de scope van het overzichtsmodel bijvoorbeeld tot het afbeelden van Integriteit en Vertrouwelijkheid voor een bepaalde infrastructuur, of alleen voor het criterium Controleerbaarheid. Op dit globale niveau worden de fysieke IB-objecten weggelaten. De IB-functie continuïteitsvoorzieningen blijkt in de praktijk maar ten dele te kunnen worden afgebeeld in overzichtsmodellen. Daarvoor is een gedetailleerder en meer fysiek georienteerd model nodig, zoals een configuratieschema.

Als voorbeeld van een overzichtsmodel geeft figuur 4 een view op de IB-functies voor de criteria Integriteit en Vertrouwelijkheid in een NORA-keten. Voor betrouwbare communicatie tussen burger en overheid is een vertrouwd toegangspad gewenst tot het portaal van de overheid. Daarvoor is encryptie gebruikt. Vanaf het portaal tot aan het interne domein van de ketenpartner is er sprake van een besloten netwerk. Ook dit kan als een vertrouwd toegangspad worden beschouwd, mede door de werking van de andere in dit pad gepositioneerde IB-functies. Merk op dat de functies Zonering en Filtering op verschillende plaatsen in de keten door IB-mechanismen op een andere manier wordt ingevuld. De positionering van geprogrammeerde controles kan in de keten maar beperkt zichtbaar worden gemaakt, als gevolg van de verwevenheid daarvan met applicaties (hier Dienst genoemd). Dit geldt in zekere zin ook voor alle andere mechanismen.



Figuur 5: Zonering volgens de Burton Group

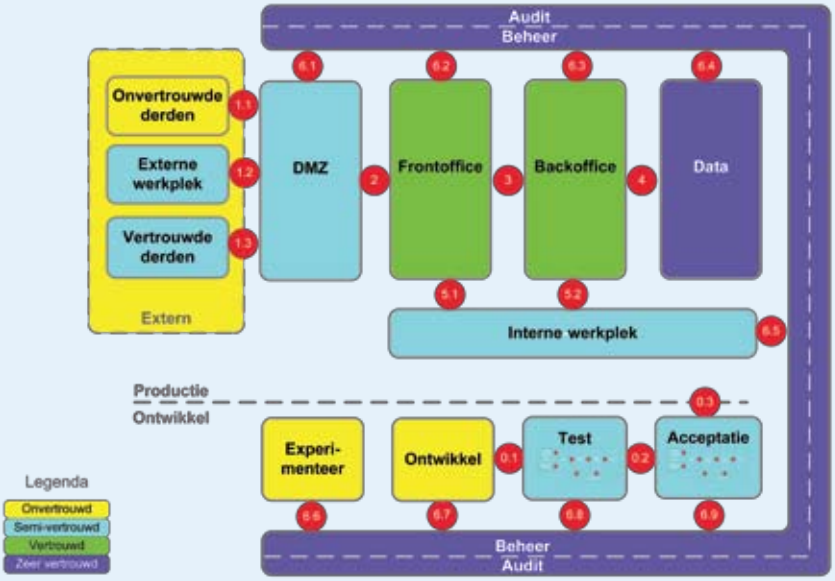
Samengevat zit kracht van deze architectuurmodellen niet in de volledigheid van de views, ze pretenderen juist een *globaal* inzicht te geven, maar wel met voldoende diepgang om de posities waar de beveiligingsfuncties werkzaam zijn duidelijk te maken. De volledigheid en de nodige details moeten worden aangebracht in de onderliggende ontwerpen van applicaties en infrastructuur.

Beschouwingsmodel Burton

Voor het uitwerken van veel IB-patronen gebruiken we een standaard beschouwingsmodel, dat is afgeleid van het Burton referentiemodel *(literatuurverwijzing 4)* van figuur 5. In deze figuur is zichtbaar dat de toegang vanuit de onvertrouwde omgeving (extern) naar de vertrouwde omgeving (intern) in *lagen* is opgebouwd. Een beveiligingslaag wordt gevormd door een set van maatregelen in de zone zelf én maatregelen in het verbindende koppelvlak K, weergegeven door K1, K2 en K3 van figuur 5.

Mocht één laag worden doorbroken, dan voorkomt de volgende beveiligingslaag in deze structuur dat bedrijfsprocessen en gegevens direct kunnen worden benaderd vanuit de onvertrouwde zone. De gelaagdheid is tevens gebaseerd op het stapsgewijs communiceren van onvertrouwd naar vertrouwd en omgekeerd, zie (a), (b), (c) en (d) in figuur 5.

- **Onvertrouwde zone:** deze zone, ook bekend als de *externe* zone, bevat systemen, die niet bekend zijn of beheer worden door de organisatie. Het internet is een goed voorbeeld van een onvertrouwde zone, waarin klanten of partners vanuit hun eigen omgeving communiceren met de organisatie.
- **Semi-vertrouwde zone:** DMZ (demilitarized zone), bevat systemen die door de organisatie beheerd en gecontroleerd worden. De DMZ fungeert voornamelijk als doorgeefluik, waar de communicatie wordt onderbroken en geïnspecteerd wordt op ongewenste communicatie, zowel naar binnen als naar buiten, virussen, malware et cetera. Semi-vertrouwd houdt in dat in dit type zone geen gevoelige bedrijfsinformatie mag worden opgeslagen.
- **Vertrouwde zone:** deze zone bevat alle informatieverwerkende systemen voor de



Figuur 6: Beschouwingsmodel voor zonering

primaire bedrijfsvoering en staat onder het beheer en controle van de organisatie. Bij grotere organisaties wordt deze zone soms onderverdeeld in de zones: frontoffice, midoffice en backoffice. Opslag van informatie in vertrouwde zone is beperkt tot office-data, mail en samengestelde informatie die aan klanten beschikbaar wordt gesteld.

- **Zeer vertrouwde zone:** in deze extra beveiligde zone wordt *bedrijfskritische* informatie opgeslagen. Communicatie met deze zone is mogelijk voor een beperkt aantal systemen vanuit de vertrouwde zone, waarbij de gegevensuitwisseling zorgvuldig wordt gecontroleerd. Soms wordt daarbij gebruikgemaakt van een proxy. Backup- en recoverysystemen zorgen voor replicatie van bedrijfskritische informatie.

In de koppelvlakken K1, K2 en K3 zijn allerlei filterfuncties opgenomen, die ervoor zorgen dat die communicatie wordt getoetst aan het voor de organisatie geldende IB-beleid. Bepalend daarbij zijn de communicatieprotocollen en de communicatierichting. De koppelvlakken bevatten naast filterfuncties ook sensoren die het afwijkend gedrag opmerken, daarover informatie vastleggen en potentiële doorbraken signaleren aan een intern security response team.
In deze gelaagde opstelling kan inkomend verkeer vanuit de onvertrouwde zone (a) alleen communiceren met systemen in de semi-vertrouwde demilitarized zone (DMZ). Vanuit de DMZ kan de communicatie worden doorgezet naar de zone Vertrouwd (b). Afhankelijk van het vertrouwelijkheidsniveau van de gegevens kan in deze structuur ervoor gekozen worden om uitgaand verkeer (d) alleen vanuit de vertrouwde zone naar buiten te laten plaatsvinden via koppelvlakken K2 en K1. Door beveiliging gelaagd in te richten, kunnen risico's van misbruik van bedrijfsgevoelige informatie beter worden beperkt dan met de traditionele zonering volgens het Kasteelmuurprincipe: je bent buiten (extern) óf je bent binnen (intern).

Zonering of deperimeterisatie?
Informatiebeveiliging zonder grenzen, oftewel *IB zonder zones*, is de toekomstvisie van het Jericho Forum[1] *(literatuurverwijzingen 5 en 6)*. Dit forum heeft elf aanbevelingen opgesteld, die in samenhang moeten leiden tot de doelen, die beogen dat:

- data in staat is zichzelf te beschermen tijdens het transport over onvertrouwde netwerken.
- data op het juiste niveau is beveiligd tijdens opslag, transport, gebruik en mutatie.

Deze doelen worden realiseerbaar wanneer de industrie daarvoor voldoende nieuwe mechanismen en producten ontwikkelt en last but not least: ze aanpassingen ontwikkelt voor de bestaande ICT (legacy).

Wat zijn dan de belangrijkste eisen waarvoor nieuwe mechanismen moeten worden ontwikkeld?

1 Dataframes moeten zodanig kunnen worden 'geoormerkt' en beschermd, dat de inhoud op weg van zender naar ontvanger niet kan worden gemuteerd of kan worden ingezien door onbevoegden.
2 De routering van dataframes moet plaatsvinden op basis van standaarden voor dataclassificatie en vertrouwensniveaus, voor zowel zender als ontvanger.
3 Elke implementatie van regels moet compleet zijn voor elke willekeurige context, oftewel de oplossing voor de eisen 1. en 2. moet zich zelfstandig kunnen handhaven op internet en daarmee de beschikbaarheid van data kunnen garanderen.

Hoewel de aanbevelingen van het Jericho Forum veelbelovend zijn voor de ultieme IB, is de situatie van nu nog ver verwijderd van de mogelijkheden om zelfs delen daarvan in te vullen. Het is tevens de vraag of het zover komt. Het verleden heeft ons geleerd dat de beste concepten of technische oplossingen niet altijd worden toegepast of zelfs 'overleven' in de markt.

We concluderen hieruit dat we het voorlopig nog moeten doen met zoneringfuncties zoals hiervoor beschreven, maar ondertussen zullen we ICT-trendsetters en leveranciers moeten aansporen om te bewegen richting Jericho.

Beschouwingsmodel Zonering
Op basis van het gelaagde model van de Burton Group is in figuur 6 een zoneringsmodel uitgewerkt dat toepasbaar is als beschouwingsmodel voor een willekeurig grote organisatie. Met de kleuren van het Burtonmodel is hieronder de gelaagdheid van het gewenste vertrouwensniveau aangegeven. Wat opvalt, is dat maar een deel van de ICT-omgeving als 'vertrouwd' is aan te merken.

Toegevoegd aan het Burtonmodel zijn de zones voor interne en externe werkplekken en zones voor derden, die informatie uitwisselen met de organisatie. De systeemontwikkelomgeving van de organisatie is

1. *Het Jericho Forum is een internationale denktank op het gebied van informatiebeveiliging, die zich buigt over nieuwe beveiligingsconcepten uitmondend in een Collaboration Oriënted Architecture.*

aangegeven als een apart cluster van zones, met koppelingen naar elkaar en naar de productieomgeving. Tenslotte is een beheer- en auditzone toegevoegd waaraan alle zones gekoppeld zijn.

Betekenis van de zones

- **Extern**
  Deze zone omvat alles dat buiten de directe bescherming en het beheer van een organisatie valt en moet daarom als *onvertrouwd* worden aangemerkt. De domeinen Externe werkplek en Vertrouwde derden nemen in het externe domein een bijzondere plaats in. De externe werkplek bevindt zich buiten de fysieke bescherming van een organisatie, maar kent verschillende beheervarianten. Het domein Vertrouwde derden valt, dankzij contracten over wederzijdse maatregelen en handhaving van het beveiligingsniveau, onder de invloedssfeer van de organisatie en kan daarom als semi-vertrouwd worden aangemerkt. Het koppelvlak tussen elkaar vertrouwende partijen (1.3) kan daarom eenvoudiger worden uitgevoerd dan het koppelvlak met onvertrouwde derden (1.1). Gelet op de benodigde autorisaties op de betreffende ICT-systemen van de organisatie wordt remote support uitsluitend door vertrouwde derden uitgevoerd.

- **DMZ**
  Dit domein is een neutraal gebied tussen de buitenwereld en de organisatie. De buitenkant van een DMZ wordt gevormd door solide filterfuncties. Binnen de DMZ bevinden zich mechanismen voor de filtering van protocollen en ongewenste communicatie, functies voor ontkoppeling (proxy), functies voor protocoltransformatie en misleiding van hackers en monitoring. De DMZ bevat in veel gevallen ook webservers, die publiek toegankelijke organisatiegegevens bevatten. Het beveiligingsniveau is semi-vertrouwd, omdat de aanwezige data en systemen in een DMZ in het uiterste geval als 'opgeefbaar' moet worden beschouwd. Als de scheiding van het eerste koppelvlak (1.1) namelijk wordt gebroken, dan kan een hacker toegang krijgen tot de data binnen de DMZ. De filterende mechanismen en koppelvlak (2) moeten voorkomen dat hackers vanuit de DMZ door kunnen gaan naar de vertrouwde domeinen.

- **Frontoffice**
  De frontoffice van een organisatie bevat met name de systemen die gericht zijn naar de klant en die communiceren met de buitenwereld, zoals webservers. In de frontoffice zijn zowel informatieverstrekkende webservers opgesteld, als webservers die transacties van gebruikers kunnen doorzetten naar de backoffice. Vanuit de klant bekeken, fungeert de frontoffice als poort, waar klantinformatie wordt verwerkt tot organisatie-informatie en omgekeerd. Het koppelvlak tussen front- en backoffice (3) fungeert als een netwerk of een 'servicebus', waarop de informatie vanuit de backoffice beschikbaar is. De frontoffice is een vertrouwd domein.

- **Backoffice**
  Dit domein bevat zowel ondersteunende systemen voor de frontoffice, als systemen voor het *vullen* van de bedrijfskritische systemen die in de Data zone staan opgesteld. De backoffice is een vertrouwd domein, waar applicaties draaien voor normale bedrijfsvoering van de organisatie zelf.

- **Data**
  Het datadomein bevat bedrijfskritische informatie, die van elementair belang is voor het voortbestaan van een organisatie. Communicatie met deze zone is mogelijk voor een *beperkt* aantal systemen vanuit de vertrouwde zone, waarbij de gegevensuitwisseling tevens zorgvuldig wordt gecontroleerd. Bedrijfskritische informatie wordt gerepliceerd door back-up- en recoverysystemen. Fysieke beveiligingsmaatregelen beschermen deze zone tegen gevaren als brand, water en inbraak.

- **Interne werkplek**
  In de kantooromgeving zijn de eindgebruikerwerkplekken, de LAN-netwerken en de netwerkprinters van een organisatie gesitueerd. Dit domein moet worden aangemerkt als semi-vertrouwd in verband met de grote aantallen aansluitingen en de relatief grote kwetsbaarheid voor inbraak. De controle op naleving van beveiligingsrichtlijnen in dit kantoordomein is doorgaans beperkt. Wanneer bedrijven besluiten om medewerkers in een kantooromgeving te laten werken met systemen in de ontwikkel-, test-, acceptatie- of beheerzone, dan dienen er aanvullende maatregelen genomen te worden om de voor de beveiligingsniveaus vereiste logische scheiding én scheiding van taken mogelijk te maken. Dit betreft zowel technische als organisatorische maatregelen.

- **Externe werkplek**
  In het externe domein kunnen werkplekken zijn gesitueerd voor externe toegang tot bedrijfsapplicaties, remotebeheer of telewerken. Deze werkplekken vallen logischerwijs onder het beheer van een organisatie, dat wil zeggen: de werkplek wordt eerst gescand op virussen en malware en getoetst op aanwezigheid van de juiste beveiligingsmaatregelen voordat bedrijfsapplicaties kunnen worden gekozen. Een beperkte uitvoering van een externe werkplek is een webmailvoorziening, waarmee medewerkers van een organisatie in het externe domein hun zakelijke e-mail kunnen lezen. Daarbij wordt bij voorkeur gebruikgemaakt van 2-factor authenticatie op basis van tokens.

- **Beheer**
  Dit domein behoort, evenals het datadomein, tot zones met het niveau zeer vertrouwd, omdat beheerders met hogere bevoegdheden hun werk moeten kunnen uitvoeren. De toegang tot werkplekken van beheerders zijn afgeschermd van gewone kantoortaken, zoals die uitgevoerd kunnen worden vanaf de interne werkplek. Met behulp van functiescheiding en technische maatregelen worden beheertaken strikt gescheiden van auditwerkzaamheden. De beheerfuncties, die via remotebeheer werkplekken of interne werkplekken kunnen worden uitgevoerd, zijn wat betreft bevoegdheden beperkt ten opzichte van de bevoegdheden van beheerders binnen de beheerzone van een organisatie.

- **Audit**
  Dit domein wordt gebruikt voor het scheiden van monitoring en verificatiefuncties van de operationele beheerta-

ken. Vastleggen van audit-informatie is pas zinvol wanneer logfiles, die bestemd zijn voor auditing, niet - of niet ongemerkt - kunnen worden gewijzigd door beheerders of eindgebruikers. De voor audit-doeleinden verzamelde informatie wordt in de auditzone geaggregeerd en beveiligd opgeslagen en verlaat de deze zone via het netwerk niet meer in de oorspronkelijke vorm. Beheerders hebben geen toegang tot auditgegevens.

- **Experimenteeromgeving**
  Dit domein is een laboratoriumomgeving, die fysiek is gescheiden van de overige omgevingen. Dit is een onvertrouwd domein.

- **Ontwikkelomgeving**
  In dit domein worden nieuwe producten worden ontwikkeld en beproefd, of staan systemen in quarantaine in afwachting van de goedkeuring voor de productieomgeving van een organisatie. Het ontwikkeldomein is als onvertrouwd geclassificeerd, omdat er met utilities en tools gewerkt moet worden, die je in productieomgevingen niet, of zeer beperkt, ter beschikking wilt stellen.

- **Testomgeving**
  In dit domein worden systemen functioneel en technisch beproefd en getoetst of ze aan de eisen voldoen. Dit domein heeft een hoger vertrouwensniveau dan de ontwikkelomgeving, vanwege de voor testen noodzakelijke geïsoleerde opstelling. Het niveau is semi-vertrouwd, omdat het belang van productiebeveiliging minder is dan in de productieomgeving zelf.

- **Acceptatieomgeving**
  Dit domein is het voorportaal van de productieomgeving. Hier worden systemen gecertificeerd op productiewaardigheid. Het vertrouwensniveau is semi-vertrouwd, maar ligt qua maatregelen vrijwel op het niveau van de vertrouwde productieomgeving.

Voortgang van de patronencommunity

De community bestaat uit een vaste en enthousiaste groep schrijvende PvIB-leden en een aantal reviewers op de achtergrond. Het zijn consultants, architecten en specialisten vanuit het bedrijfsleven en de overheid. Deze community is ontstaan na het Securitycafé in maart 2009, met als doel een set van praktijkgerichte beveiligingspatronen te ontwikkelen, die gerelateerd zijn aan een geaccepteerde set van beveiligingsnormen. De resultaten zijn verzameld in een werkdocument dat gepubliceerd is op www.IBPedia.nl. De community stelt zich tot doel om IBPedia regelmatig aan te vullen met nieuwe patronen en de patronen te onderhouden. Hieronder staan de resultaten die de community inmiddels heeft bereikt en op welke vragen zij graag feedback krijgt van de lezer.

Resultaten

Het eerste resultaat van de community was de review en de acceptatie van de NORA-architectuuraanpak als basis voor de patronen. Vervolgens is het hiervoor besproken beschouwingsmodel Zonering gereviewd en goedgekeurd. Het derde resultaat is het opstellen en goedkeuren van een drietal patronen: PKI, Logging en Elektronische Handtekening. De onderstaande lijst bevat kandidaatpatronen, waaraan al gewerkt wordt óf het zijn patronen die als idee zijn voorgesteld door de communityleden. We realiseren ons dat de op IBPedia gepubliceerde patronen nog voor verbetering vatbaar zijn, maar als community willen we verbeteringen vooral voeden vanuit praktijkervaringen.

Vragen aan de leden

Hoewel de opzet van de IB-patronen pas in een volgend artikel wordt uitgelegd, is de community benieuwd naar uw visie op de praktische bruikbaarheid van de ontwikkelde concepten als de hiervoor beschreven architectuuraanpak en het zoneringsmodel.

Kandidaat IB-patronen

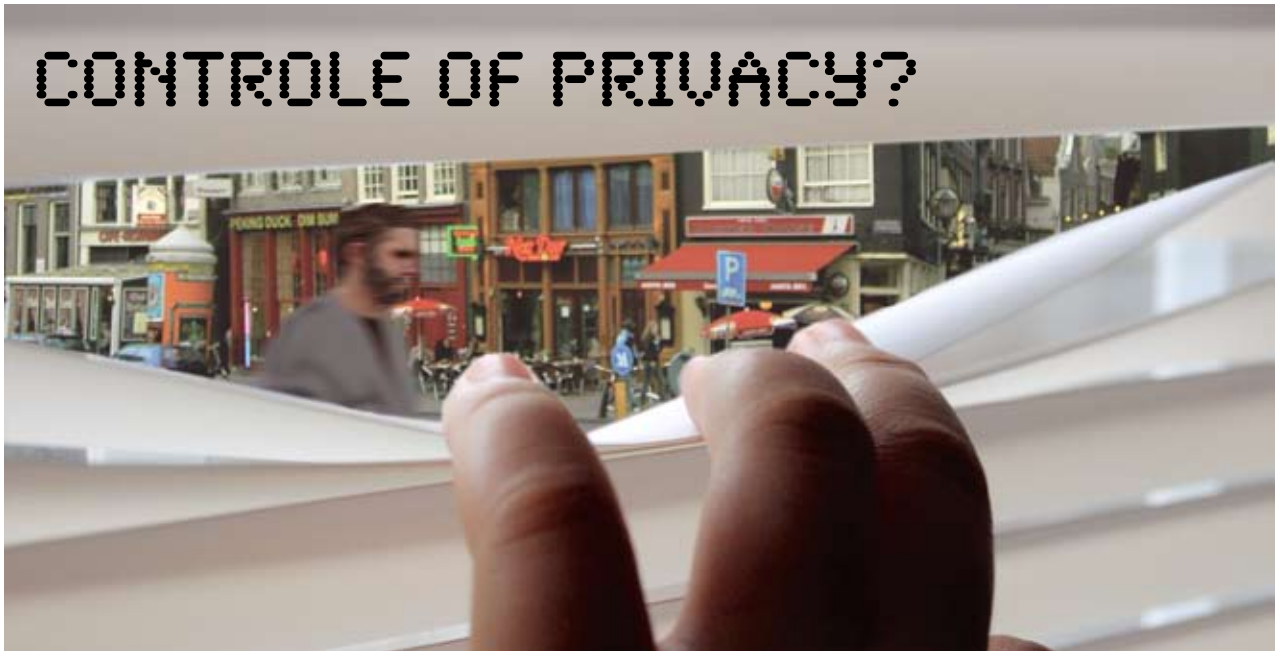
- Koppelvlak met onvertrouwde derden met DMZ
- Koppelvlak vertrouwde derden met DMZ
- Koppelvlak organisatie-organisatie via koppelnetwerk (basis)
- Koppelvlak organisatie-organisatie via koppelnetwerk met beveiligingsniveaus
- Koppelvlak tussen organisaties en koppelnetwerk
- Ketenbeveiliging
- Gegevensuitwisseling met vertrouwde derden
- Herleidbaarheid van handelen in SOA en EDA ketens
- Portaalbeveiliging
- Identity & Access Management
- Identity Management
- Federated Identity Management
- Monitoring
- Secure E-mail
- Autorisatie op afstand
- Archivering
- Wederzijdse authenticatie van applicaties
- Versleuteling (naast PKI) one-way, two-way, beheer, sleutelmanagement
- Symmetrische encryptie
- Beveiliging centrale gegevensverzameling
- Ontwikkel-, test- en productieomgevingen
- Cloud computing

Ook vraagt de community zich af aan welke patronen de meeste behoefte bestaat bij de PvIB-leden, zodat we die onderwerpen prioriteit kunnen geven. Tenslotte vragen we de leden of er in de praktijk al met IB-patronen gewerkt wordt en wat de ervaringen daarmee zijn. Uw reactie graag per e-mail naar: jaap.vanderveen@gmail.com.

Literatuurverwijzingen

1 NORA katern Informatiebeveiliging, *http://www.surfgroepen.nl/sites/…*
2 NORA katern Strategie, *http://www.surfgroepen.nl/sites/…*
3 NORA best practice Normen Informatiebeveiliging ICT-voorzieningen, *http://www.surfgroepen.nl/sites/…*
4 Burton Group Reference Architecture Technical Position paper: Zones; Auteurs: Dan Blum en Eric Maiwald *http://www.Burtongroup.com* en dblum@burtongroup.com
5 Managing Risk in Mashup Corporations, Aaldert Hofman, Ben Elsinga en John Sluiter; juli 2009 © Capgmini
6 The Book of Jericho 2.0; Auteurs: Marco Plas, Capgemini, Marco.Plas@capgemini.com. Meer informatie over dit onderwerp is te vinden op *www.Jerichoforum.org*

CONTROLE OF PRIVACY?



Het is begin november en ik zit met een paar vrienden lekker op een terrasje aan een rode wijn te nippen. De sfeer is geweldig en we genieten van het magere novemberzonnetje. Ondanks het feit dat het november is, blijken er meer mensen buiten te zitten dan in het café. Hetgeen overigens niet abnormaal is sinds de Klinkwet een rokertje verbiedt in de grotere cafés. We kijken uit op het plein en al snel wordt een camera opgemerkt. Blijkbaar vallen we uit de toon, want de camera richt zich op ons. Onder invloed van de bitterballen, de blokjes kaas en wellicht ook het rode wijntje, begint al snel een discussie over het wel en wee van dergelijke camera's.
De stemmen staken een beetje als we het hebben over goed of slecht, maar ik heb de indruk dat niemand van ons er heel erg mee zit.

Even later komt het gesprek op andere 'Big Brothertooling' en ondanks het feit dat het nog steeds gezellig is, komt het elektronische patiëntendossier voorbij. Iedereen is het er over eens dat het goed is dat medische gegevens op het juiste moment op de juiste plaats zijn, maar het woord misbruik valt. Men roept dat er toch niets te verbergen valt en dat er geen geheimen zijn voor anderen. Ik breng in dat het verhaal anders wordt als je vijf jaar geleden langdurig onder psychiatrische behandeling bent geweest en die gegevens misbruikt worden. Bij een sollicitatiegesprek zou een bevriende dokter van mijn toekomstige baas wellicht dingen uit het dossier kunnen plukken, die een aanname van mij in de weg staan.

Het wordt even stil om me heen, maar het volgende rondje wordt besteld en iedereen lijkt mijn opmerking te zijn vergeten.
Toch is mijn zorg over dit soort berichten de afgelopen jaren toegenomen en ik begin los te komen. Ik snijd een nieuw onderwerp aan en vraag of men weet hoeveel telefoontaps in Nederland plaatsvinden. En hoe zich dat verhoudt met het aantal telefoontaps in Amerika. Er begint iemand te gapen, maar ik zet door en ik geef aan dat er in Nederland tien keer zoveel taps worden uitgevoerd als in de Verenigde Staten. Let wel, dit zijn getallen in absolute zin.
Er wordt weer een rondje besteld en het onderwerp wordt gebracht op de slechte resultaten van het Nederlandse elftal.

Ik ben een meester in het ombuigen van gesprekken en kom via de clubcard, waarvan nog nooit iemand mij heeft kunnen uitleggen wat deze kaart toevoegt, al snel op de kilometerheffing. Ik weet niet of het door de rode wijn komt of door mijn enorme opwinding over dit onderwerp, maar ik raak helemaal op temperatuur. Wisten jullie al dat er een systeem wordt ingevoerd dat nergens op de wereld op deze schaal werkende is? Jullie wisten vast ook wel dat iedere gereden kilometer wordt geregistreerd en afgerekend? Jullie weten vast ook wel dat bevoegde autoriteiten inzage krijgen in de database waaruit mijn hele leven gaat blijken? Waar ik ben geweest is geen enkel geheim meer. Hoe snel ik van Amsterdam naar Utrecht ben gereden is straks zo uit te lezen (misschien wel een goed idee om ook het CJIB inzage te geven en de gegevens direct te verwerken naar een snelheidsbekeuring). Nee, dat zullen we echt niet gaan doen in Nederland. Nee, dat denk ik ook niet, we tappen ook alleen maar telefoons af die echt noodzakelijk zijn.

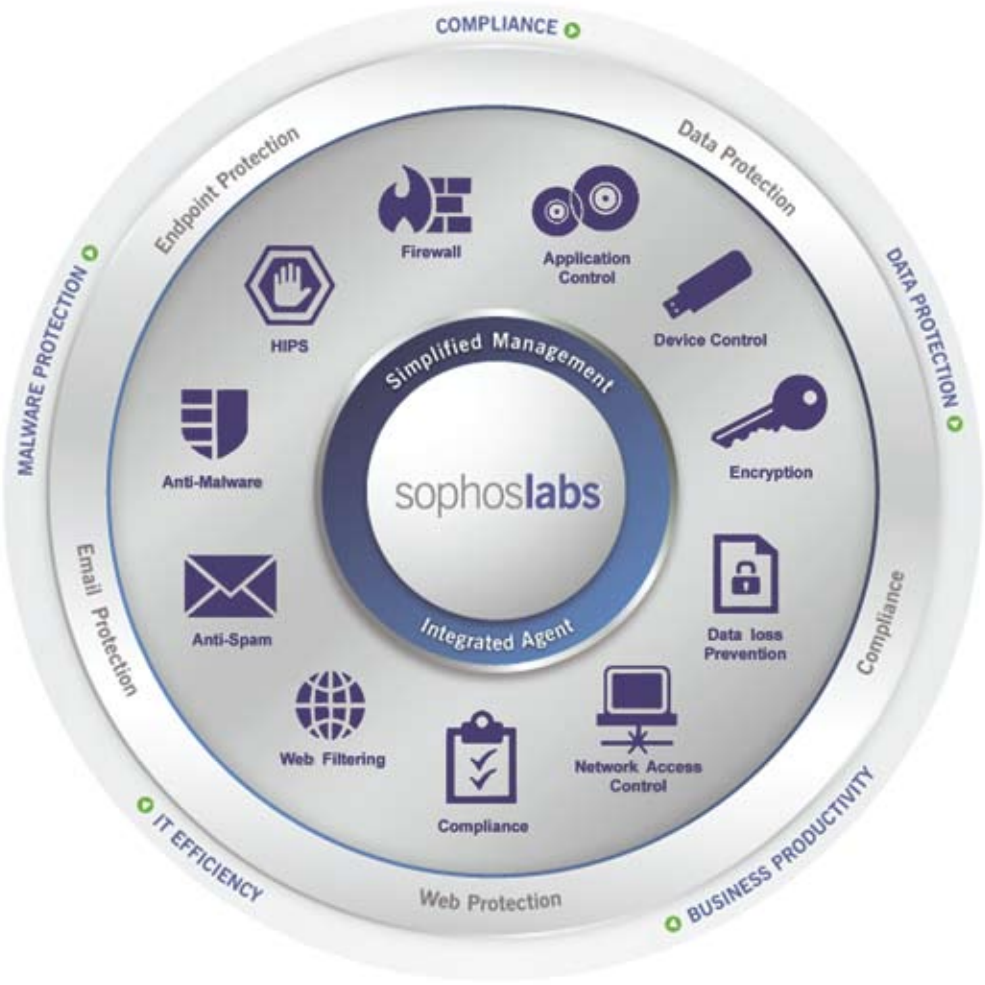
Ik denk dat ik mijn vrienden voldoende verveeld heb en ik probeer het luchtig te maken door nog even te noemen dat de kilometerheffing onder andere wordt ingevoerd om het milieu te sparen. Onze nationale boekhouder Bos wil echt wel de minimaal dezelfde inkomsten als nu en dus lijkt het milieu ineens weer niet zo belangrijk. Er is besloten om drie cent per kilometer te gaan berekenen en in spitstijden iets hogere tarieven te rekenen. De kou slaat toe, ik roep nog dat het misschien handig is om dertig cent opslag op de benzine te doen, maar ik erken dat dit een hele domme gedachte is, want dan moeten ook alle overheidsvoertuigen het hogere tarief betalen. De stemming is omgeslagen, het is kouder en we besluiten naar huis te gaan. Op de fiets draai ik me nog eens om, om te kijken of de camera's meedraaien, maar ik zie geen beweging. Ik kan rustig naar huis fietsen.

Groetjes,
Berry

SOPHOS

secured.

Complete to compete!



Protect your data simply anywhere!

Kijk voor meer informatie op www.crypsys.nl of bel (0183) 62 44 44.

CRYPSYS Data Security B.V. - Benelux Distributeur van Sophos
Edisonweg 4 - 4207 HG Gorinchem - Postbus 542 4200 AM Gorinchem
T (0183) 62 44 44 - F (0183) 62 28 48 - E sales@crypsys.nl

CRYPSYS data security