INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 3 - 2011

INCLUSIEF DOSSIER: 'IB IN HET ONDERWIJS'

SAMENWERKING HOGER ONDERWIJS WERPT VRUCHTEN AF

SURFibo ONTWIKKELT STARTERKIT

INFORMATION SECURITY MANAGEMENT OP HBO

SECURITY AWARENESS IN MBO

VOORWOORD

Ik besef me dat wat ik nu schrijf pas over een maand wordt gelezen. Alles kan tegen die tijd anders zijn. Dat is een risico dat ik bewust neem, omdat ik vind dat ik niet aan de aardbevingsramp bij Japan kan voorbijgaan. Nu hebben we nog weinig informatie over wat er is gebeurd en de ontwikkelingen die nog gaande zijn. Tegen de tijd dat dit blad wordt gepubliceerd, is het herstel in Japan allang ingetreden, hoop ik. Ik leef mee met diegenen die hier direct of indirect mee te maken hebben. Ik hoop dat herstel spoedig kan beginnen en dat er geen grote incidenten meer volgen. Dit is mijn reactie als mens. Als beveiliger kijk je hier ook analytisch naar.

Het doet me terugdenken aan Katrina, ruim vijf jaar geleden. Door toeval was ik in Houston de dag voor Katrina toesloeg. Toen leek het allemaal mee te vallen. De orkaan nam op het laatste moment aan kracht toe en meer dan 50 dijken braken door. Ondanks evacuatieorders waren veel mensen thuis gebleven. Hoe anders was dat tijdens Rita, een kleine maand later. Dubbel toeval: ik was weer in Houston, net voor de orkaan. Nu was het heel spannend, ik zat in het laatste vliegtuig dat vertrok. Opvallend was dat mensen zich heel anders gedroegen. Evacuatie werd serieus genomen, alle snelwegen waren helemaal gevuld met uitgaand verkeer, op de luchthaven werd alles vastgesjord. Men had duidelijk geleerd.

Een vergelijking tussen de twee rampen: Katrina overviel New Orleans, Japan lijkt juist heel goed voorbereid op zo'n ramp. Niet alleen op het vlak van techniek, ook de 'gewone' mensen zijn getraind in hun gedrag tijdens zware aardbevingen. Hoe immens groot de schade van deze aardbeving ook is, als je beschouwt dat deze aardbeving in de top 10 van de geschiedenis staat, dan zie je wat goede voorbereiding voor een verschil kan maken.

In deze tijd wordt alles heel nauwgezet vastgelegd, zo ook het verloop van deze aardbeving en de vervolgrampen (tsunami, kerncentrales). We zien een ramp van nabij, ook al zitten we aan de andere kant van de aardbol. Nu is Japan nog in chaos. De chaoskenmerken uit het boek 'Business Continuity Management' zijn nog allemaal van toepassing: weinig informatie, grote schade, weinig reactietijd, beperkte opties tot handelen. Ook zie je dat de crisis goed wordt opgepakt. Alle succesfactoren om de crisis te bedwingen worden toegepast.

Als we straks terugkijken naar deze ramp, dan hebben wij, de beveiligers, een rijke bron aan informatie erbij, waar we met zijn allen flink van kunnen en vooral moeten leren. In de tussentijd moeten we de ruimte geven aan de menselijke, emotionele aspecten en beslissen hoe we dat willen steunen. De beveiliger in ons zal moeten afwachten.

Lex Borger,
hoofdredacteur

Foto omslag: Steve Jurvetson

INHOUDSOPGAVE

INFORMATIEBEVEILIGING: PEOPLEWARE (2)

Sanne Schaler is sociaal psychologe. Zij is te bereiken via Schaler@gmx.net

Hans Labruyere is directeur en mede-eigenaar van LBVD informatiebeveiligers. Hij is te bereiken via hans.labruyere@lbvd.nl

In een serie van drie artikelen over informatiebeveiliging en het bewustzijn en onbewustheid van de mens in deze, zet de schrijver een keten methoden uiteen die elkaar in de praktijk kunnen versterken. De keten bestaat globaal gezien uit analyseren, informeren, kanaliseren en toetsen. In dit tweede deel gaat Sanne Schaler in op het helende effect van groepen.

In het algemeen kun je stellen dat mensen met hetzelfde leed, met dezelfde zorgen, elkaar opzoeken. Ze vinden gehoor, begrip en steun bij elkaar. Medewerkers die getroffen zijn door een incident kunnen in een groep worden samen gebracht waarbinnen zij over hun ervaring kunnen praten. Dat incident kan heel goed een vooropgezet incident zijn, zoals het bezoek van een mystery guest of het doorbreken van een penetratietest.

Doordat de groepsleden hetzelfde hebben meegemaakt, veelal in hetzelfde bedrijfsproces werken én collega's zijn, ontstaat een samenhang: de groepscohesie. Groepsleden identificeren zich met hun groep en voelen dat ze tot de groep behoren. Naarmate deze samenhang sterker is hebben groepsleden meer invloed op elkaar. Er zal meer feedback worden gegeven en geaccepteerd.

Groepen worden hechter naarmate groepsleden meer persoonlijke, intieme informatie onthullen. Door het delen van persoonlijke informatie met de groep laten groepsleden zien dat ze elkaar vertrouwen. Zelfonthulling en groepscohesie zijn dus wederkerig gerelateerd. Elke zelfonthulling maakt de groepsintimiteit sterker en deze verbondenheid stimuleert dat groepsleden meer persoonlijke informatie met de groep delen. Daarnaast kan het uiten van zorgen en stressvolle gedachten de spanning bij groepsleden zelf wegnemen.

> Groepen worden hechter naarmate groepsleden meer persoonlijke, intieme informatie onthullen

Doordat groepsleden hetzelfde hebben meegemaakt -het eerder besproken (vooropgezette) incident - realiseren zij zich dat hun probleem niet uniek is maar dat het hier algemene incidenten betreft die andere medewerkers ook hebben ervaren. Door dit besef kan de individuele medewerker vaststellen dat een incident niet geheel aan hemzelf te wijten is, maar dat er ook algemene factoren een rol spelen.

Groepsgedrag

Zodra mensen met anderen worden samengebracht die gelijke problemen hebben, voelen ze zich beter, gaat hun eigenwaarde omhoog, en er heerst een prettige stemming van saamhorigheid. Groepsleden ondersteunen elkaar en geven elkaar hoop. Het helpen van anderen geeft een goed gevoel, het gevoel dat men nodig is, belangrijk is. Het eigen belang wordt op deze manier op sommige momenten ondergeschikt gemaakt aan het belang van een ander of de groep. Dit effect roept wederkerigheid op. Doordat je iets geeft, kan je iets terugverwachten. Als je anderen helpt, zullen ze jou ook helpen. Veel charitatieve instellingen baseren hun communicatiestrategie op dit fenomeen.

> Een groep laat je persoonlijke aspecten zien, waarvan je zelf niet eens wist dat je die had

Daarnaast geven groepen objectieve informatie over jezelf, zoals je persoonlijkheid, je sterke en zwakke punten en geven ze inzicht in je kwaliteiten. Ze houden je als het ware een spiegel voor. Groepsleden kunnen op deze wijze nieuwe dingen leren over zichzelf, over persoonlijke problemen en sociale relaties. In het geval van het (vooropgezette) incident kunnen medewerkers inzien waarom ze zich op dát moment, op díe wijze hebben gedragen tegenover díe persoon of situatie. Groepsleden kunnen elkaar verbeteren en een goed alternatief geven. Door de interactie van groepsleden kunnen medewerkers leren inzien wat het effect is van hun gedrag op anderen, ze worden zich bewust van hun gedrag. Groepsleden leren naar zichzelf te kijken, naar hun eigen gedrag en de situatie waarin

Schutters in een bommenwerper in de tweede wereldoorlog.

dat gedrag voorkomt, en kunnen hier lering uit trekken. Medewerkers krijgen een beter inzicht in de mogelijke oorzaken van hun inadequate gedrag.

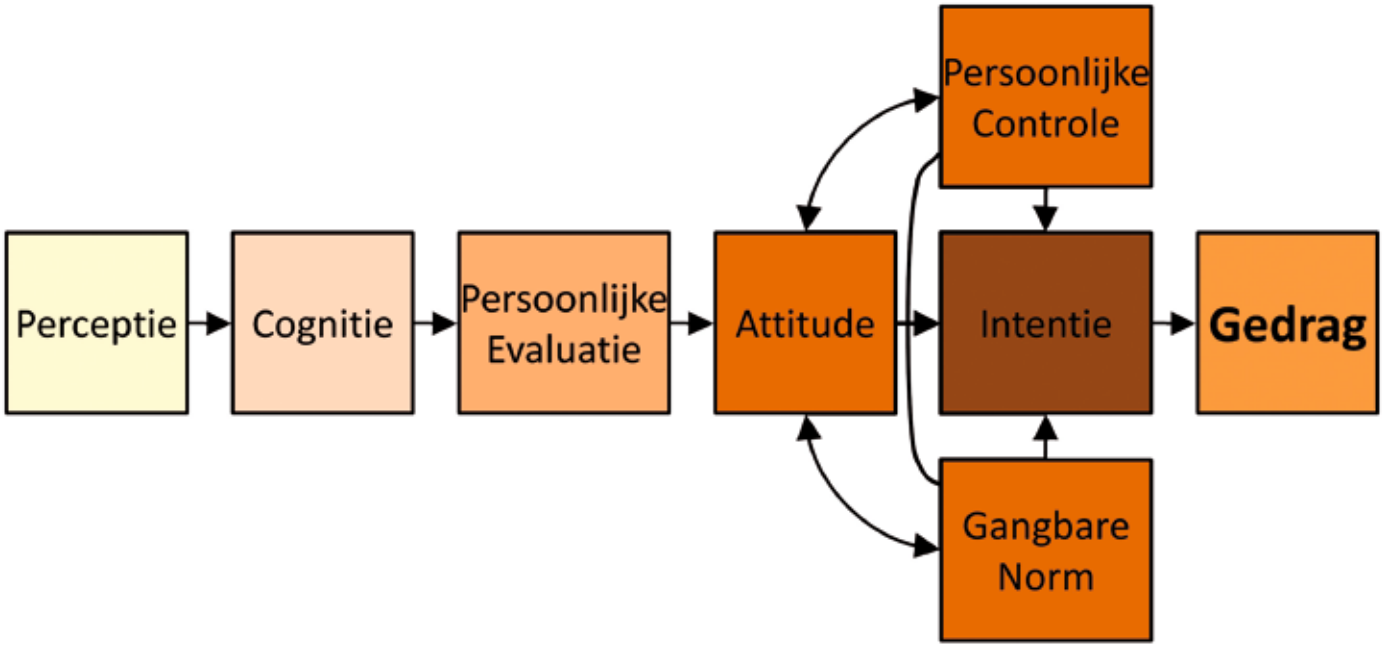
Groepsleden helpen elkaar

In een groep verkrijgen mensen derhalve zelfinzicht. Ook kunnen groepsleden door de interactie met elkaar persoonlijke aspecten laten zien, waarvan ze vaak zelf niet eens wisten dat ze die hadden. Groepsleden geven elkaar feedback over hun individueel en groepsgedrag in een bepaalde situatie. Omdat groepsleden gelijk zijn aan elkaar, zal feedback die van meerdere groepsleden komt en in een vertrouwelijke setting gegeven wordt serieus genomen worden en worden aangenomen. Groepsleden helpen elkaar hun normen en waarden, kwaliteiten en identiteit te definiëren.

Neem nu de mannen op bijgaande foto. Zij verdedigen niet zichzelf. Dat kón ook niet. Een aanvallende gevechtsjager was zo snel, en had een zó klein profiel dat hij nauwelijks te raken was. De bommenwerper waar deze mannen in zitten is echter zo groot, en zo langzaam, dat hij nauwelijks te missen is. Daarom vlogen dit soort grote vliegtuigen zwaarbewapend dicht bij elkaar. Er was altijd wel iemand in een andere bommenwerper die op de invliegende vijand kon schieten. Deze mannen verdedigen niet zichzelf, ze wagen hun leven om een ander uit de groep te verdedigen. Net zo goed als dat die ander zijn leven waagt om deze twee te verdedigen.

Op dezelfde manier hebben alle medewerkers van eenzelfde bedrijfsproces dezelfde uitdagingen, dezelfde risico's, dezelfde oplossingen. Alleen moeten ze dat onderling overleggen om dat te beseffen. En dat is mede de helende kracht van groepen: van perceptie via cognitie en persoonlijke evaluatie naar een te wijzigen attitude... groepsgewijs.

Het helpen van anderen geeft het gevoel dat men nodig is



Model: beïnvloeding van gedrag volgens de sociaal psychologie.

COLUMN

"MEISJE, IK ZIE JE BORSTEN!"

OF HOE ANDEREN JOUW REPUTATIE KUNNEN VERPESTEN

Vaak, nadat ik een lezing gegeven heb, komt er minstens één persoon op me afgelopen met een persoonlijk verhaal over waar het online is misgegaan met privacy en identiteit. Soms is dat een grappig verhaal, meestal valt het uiteindelijk nog allemaal wel mee, maar een enkele keer kom ik een verhaal tegen waar ik even van moet slikken. Zo ontmoette ik onlangs een verontruste vader. Hij vertelde me dat zijn dochter naar een schoolbal was geweest en dat er daarna een hele nare film van haar op YouTube was opgedoken. En dat deze film verder verspreid raakte over de hele school. Haar klasgenootjes hadden er plezier aan beleefd haar jurk naar beneden te trekken en haar met ontblote borsten te filmen.

Ik moest aan deze vader en dochter denken toen ik onlangs in de Huffington Post las dat uit onderzoek gebleken zou zijn dat maar liefst 80% van de zogeheten Amerikaanse 'deans of admission' sociale netwerksites bezoekt van de kandidaten voor wie zij een college-aanvraag ontvangen. Nu bleek Huffington Post niet helemaal netjes met de feiten om te springen. In het eigenlijke onderzoek staat dat 80% van de 'deans' sociale media gebruikt om studenten te *werven*. Dat is wel even iets anders. Verder lezend blijkt dat 9% van de scholen een beleid heeft over het inzien van de profielen van toekomstige studenten, een schrikbarend laag aantal. Die 9% met social media-policy is het wel in meer dan de helft van de gevallen toegestaan de profielen in te zien. Helaas is niet gevraagd aan de scholen die geen beleid hebben of zij al dan niet profielen inzien. Hoeveel aanstormende studenten bekeken worden door de 'deans' is dus nog steeds niet duidelijk. Dat er gekeken wordt mag echter wel worden aangenomen.

Maar waarom sloeg ik hier nu op aan? Wat vaak wordt vergeten in verhalen en onderzoek over identiteit en privacy is het feit dat niet alleen ikzelf, maar ook anderen bijdragen aan mijn identiteit. Wat ikzelf over mijzelf naar buiten breng en hoe ik mezelf presenteer, heb ik tot op bepaalde hoogte in de hand. Wat anderen over mij zeggen en het beeld dat zij daarmee van en over mij achterlaten in de online wereld, daarover heb ik praktisch geen controle. En toch weegt ook dat mee in de vorming van jouw persoonlijke identiteit en de daarmee verbonden reputatie. Vaak wordt, indien gesproken wordt over wat privacy in de online wereld betekent, geroepen dat het gaat om controle. Ik ben degene die bepaalt welke informatie op welk moment gedeeld wordt met welke personen. Hoewel volgens mij een juiste opvatting, biedt het helaas geen soelaas in die gevallen dat een ander ervoor zorgt dat informatie over mij online verschijnt.

Hoe hiermee om te gaan, blijft ook voor mij een lastig vraagstuk. Afgezien van de praktische component (spreek de plaatser van de informatie aan en verzoek tot verwijdering, neem bijvoorbeeld contact op met de ouders van de jongere, wend je tot de aanbieder van de dienst waar de informatie staat, enz.) is er ook nog zoiets als het weer 'goed' managen van de persoonlijke reputatie. Hetgeen in het geheel niet makkelijk is en vaak gecompliceerd door het feit dat saillante informatie 'viral' gaat en zich met een razend tempo online verspreidt. Amerikanen hebben dit als een 'gat in de markt' gezien en al enkele jaren bestaan daar gespecialiseerde bedrijven die je kunnen helpen om jouw aangetaste reputatie weer wat omhoog te krikken. En dat omhoog krikken bedoel ik dan vrij letterlijk. Wat zij doen is onder meer zogenaamde negatieve resultaten in Google naar beneden duwen door ervoor te zorgen dat de meer positieve berichten in de search in Google als eerste te zien zijn. Wat onverlet laat dat die negatieve informatie wel met een paar klikken door de pagina's heen, nog steeds te zien en te raadplegen is. Het lijkt een beetje een lapmiddel, maar het is in ieder geval iets. Ik heb hier geen pasklare oplossing voor (en ik denk dat die er ook niet echt is) vooral omdat het om een gecompliceerde issue gaat. Met alleen de wet kom je er niet en daarbij is dat vaak een (te) lange en kostbare weg. Voorlichting kan helpen, maar is ook niet zaligmakend. Praktische oplossingen schieten vooralsnog wat tekort (want, wat te doen met een onwillende of anonieme tegenpartij?). De handen ineenslaan en samenwerken aan een convergentie van oplossingsrichtingen? Graag. Ik moet er namelijk niet aan denken dat mijn dochter over tien jaar zelf met haar blote borsten op internet staat…

mr Rachel Marbus
@RachelMarbus op Twitter

DOSSIER

INFORMATIE BEVEILIGING IN HET ONDERWIJS

Het vakgebied Informatiebeveiliging krijgt in heel veel sectoren aandacht. Door internationalisering en toenemende regelgeving is het niveau van beveiliging in de afgelopen jaren sterk toegenomen. Wij als professionals weten maar al te goed dat er ook nog wel heel veel te winnen is in onze individuele werkomgevingen. Maar we hebben ook weinig zicht op andere dan onze eigen omgeving. Zo weten de meesten van ons niet wat er in bijzondere sectoren plaatsvindt. Dit jaar schenken we in het blad aandacht aan de onderwijs- en onderzoekssector. In dit nummer doen we dat met een dossier waarin heel veel ontwikkelingen binnen de sector staan. We willen Alf Moens (die het introductieartikel op bladzijde 8 schreef) en SURF hartelijk bedanken voor hun hulp.

Namens de redactiecommissie,
André Koot

BREDE SAMENWERKING WERPT VRUCHTEN AF

Alf Moens is projectmanager BIS (Informatiebeveiliging en Identity Management) bij SURFfoundation en Security Manager bij TU Delft. Alf is bereikbaar via moens@surf.nl.

In het hoger onderwijs wordt op verschillende niveaus intensief samengewerkt om verschillende bedrijfsvoeringthema's efficiënt aan te pakken. De resultaten hiervan zijn zichtbaar in een brede deelname, sterke ondersteuning en in een brede waardering door de deelnemende instellingen. De motivatie om aandacht te besteden aan informatiebeveiliging is hoofdzakelijk intern met als voornaamste redenen het borgen van continuïteit en het voorkomen van imago schade.

Naast de Wet Bescherming Persoonsgegevens legt de Wet Hoger Onderwijs enige eisen op, met name ten aanzien van een deugdelijke administratie. Er zijn momenteel geen toezichthouders die aandacht vragen voor beveiliging. In kamervragen[1],naar aanleiding van een informatielek bij een van de hogescholen, gaf de toenmalige minister van Onderwijs Ronald Plasterk aan dat wat hem betreft de eisen die volgen uit de WBP afdoende zijn voor de onderwijssector. In het hoger onderwijs is een start gemaakt met zelfregulering. Binnen de sector wordt een normerings- en controlemechanisme opgezet.

Hoe staan de onderwijsinstellingen er nu voor?

In 2008 is bij een groot aantal instellingen gemeten hoe informatiebeveiliging ervoor staat (zie Informatiebeveiliging, jaargang 2008 - 8). De conclusie was dat informatiebeveiliging in het hoger onderwijs nog onvolwassen was. De instellingen voor hoger onderwijs zijn al vele jaren bezig door door middel van intensieve samenwerking het niveau van beveiliging te verhogen. Een jaar of vijf geleden was er zeker sprake van een achterstandsituatie. Er zijn inmiddels flinke stappen gemaakt maar men is er nog niet. Beveiliging en privacy nemen een prominente rol in in het meerjarenplan van SURF, het bestuurlijke draagvlak is er. Op instellingsniveau moet er nog veel gebeuren. Soms zijn ict-afdelingen volledig klaar, maar staat het beveiligingsbewustzijn bij ict-gebruik in de vakgroepen nog in de kinderschoenen. Er zijn veel verschillen, zowel binnen als tussen de instellingen. De cultuur bij de informatiebeveiligers van het hoger onderwijs is er een van (onderlinge) openheid en delen. Dat uit zich in een intensieve samenwerking en in een gezamenlijk verantwoordelijkheidsgevoel om te leren en te verbeteren. In deze onderwijsspecial wordt een aantal resultaten en producten van die samenwerking toegelicht, gezamenlijke resultaten van een goed op elkaar ingespeelde community waarin security officers, wetenschappers en brancheorganisaties participeren.

> Er zijn momenteel geen toezichthouders die aandacht vragen voor beveiliging

Organisatie

SURF staat oorspronkelijk voor Samenwerkende Universitaire RekenFaciliteiten en bestaat uit drie 'werkmaatschappijen' die ieder een specifiek deel van de samenwerking voor hun rekening nemen. In SURF werken universiteiten, hogescholen en onderzoeksinstellingen samen aan grensverleggende ict-innovaties. Hierdoor kan het hoger onderwijs en onderzoek optimaal gebruikmaken van de mogelijkheden van ict om zo de kwaliteit van onderwijs en onderzoek te verbeteren.

- SURFfoundation initieert, regisseert en stimuleert ict-vernieuwingen, door kennisdeling en partnerschappen.
- SURFnet zorgt dat onderzoekers, docenten en studenten eenvoudig en krachtig samen kunnen werken met behulp van ict. SURFnet richt zich daartoe op het stimuleren, ontwikkelen en exploiteren van een hybride netwerk, een vertrouwde identiteit en een geïntegreerde samenwerkingsomgeving.
- SURFdiensten is de licentieorganisatie voor het hoger onderwijs en onderzoekt en faciliteert het gebruik van ict. Zij bemiddelt bij de inkoop van software, hardware en diensten op het gebied van ict en sluit raamovereenkomsten af met leveranciers.

Samen met de communities (zie kader) ondersteunt de SURFfamilie de onderwijsinstellingen op zeven beveiligingsgebieden.

Juridische aspecten: onder meer een

1 https://zoek.officielebekendmakingen.nl/ah-tk-20092010-356.html

De Informatiebeveiligingscommunities van het Hoger Onderwijs

- SURFibo: een 'Community-of-Practice' waarin de security officers van de hoger onderwijsinstellingen kennis en ervaring uitwisselen en bundelen in best practices, starterkits en leidraden.
- SCIRT: een community gericht op de operationele aspecten van security en het afhandelen van incidenten.
- CIO beraad: een formeel adviesorgaan van de informatiemanagers van het hoger onderwijs. Een van de werkgroepen van het CIO-beraad houdt zich specifiek bezig met informatiebeveiliging en zorgt voor de link tussen de informatiebeveiligers en de bestuurders.
- SURFcert: het Computer Emergency Respons Team van SURFnet, met een sterke adviserende en signalerende rol in het schoon en netjes houden van het netwerk en de hier op aangesloten instellingen..

juridische kennisbank met de belangrijkste vragen op het gebied van 'rechtmatig operationeel handelen', en alle aspecten van auteursrecht.

Organisatie van informatiebeveiliging: best practices en collegiale ondersteuning bij het inrichten van informatiebeveiliging.

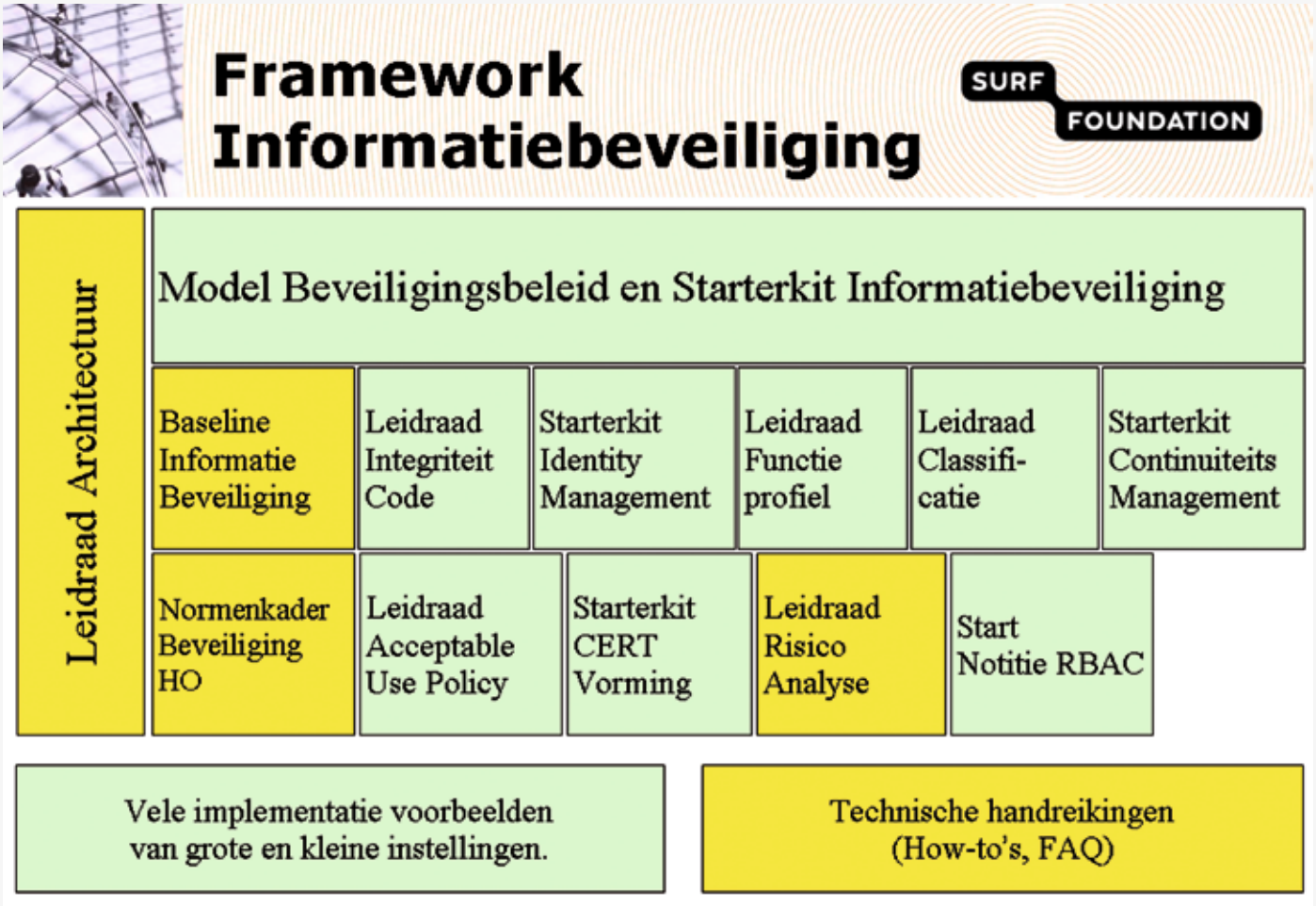
Beleidsontwikkeling: vormgegeven in de ontwikkeling van het Framework Informatiebeveiliging.

Tooling: SURFnet zorgt voor een aantal tools op het gebied van netwerkmanagement, SURFdiensten zorgt voor gunstige inkoopvoorwaarden voor het beschermen van servers en clients.

Identity management: zowel een bundeling van best practices voor het inrichten en ontwikkelen van identity management bij de instellingen als het ontwikkelen en faciliteren van het federatief identity management SURFfederatie.

Incident afhandeling: instellingen worden gestimuleerd en ondersteund om zelf incident respons teams in te richten. De ondersteuning bestaat uit een starterkit en trainingen voor incident respons teams, variërend van algemene incidentafhandeling tot specialistische forensische trainingen.

Voorlichting en bewustwording: gezamenlijk is een grote verzameling van voorlichtingsmateriaal opgebouwd, direct inzetbaar bij awareness-



Framework Informatiebeveiliging. Groene blokken: gerealiseerd, gele blokken: wordt aan gewerkt.

SURFnet/Kennisnet Innovatieprogramma
SURFnet en Kennisnet werken in een innovatieprogramma samen aan innovatieve, educatieve ict-toepassingen, toepassingen waarover het hele onderwijs in Nederland kan beschikken en op grote schaal kan gebruiken. Momenteel lopen onder meer onderzoekprogramma's op het gebied van cloudcomputing, het leren van de toekomst, augmented reality en de natuurlijke leeromgeving. Meer informatie over de projecten in dit innovatieprogramma is te vinden op www.surfnetkennisnetproject.nl/.

campagnes. Daarnaast zijn ondersteunende websites opgezet zoals cybersaveyourself.nl.

Brede Samenwerking
De activiteiten van SURFfoundation en SURFibo zijn primair gericht op de universiteiten en hogescholen, zo'n 55 instellingen van groot (38.000 studenten) tot klein (300 studenten). Daarnaast behoren ook de wetenschappelijke instituten en de Universitair Medisch Centra tot de doelgroep. Binnen dit netwerk wordt intensief kennis en ervaring uitgewisseld. Dat gebeurt in

Nieuwe security-collega's worden door de 'oude rotten' wegwijs gemaakt

openheid en op basis van onderling vertrouwen. Nieuwe security-collega's worden door de 'oude rotten' van andere instellingen wegwijs gemaakt en snel in de community opgenomen. De kennis en ervaring die zij meenemen van buiten het onderwijs zorgt ook weer voor nieuw bloed in het netwerk. Voor kleine instellingen, die het veelal zonder aparte beveiligingsfunctionaris moeten stellen, is het verbeteren van de veiligheid laagdrempeliger door het gebruik van best practices en starterkits.
Door het bundelen van de krachten van de instellingen en de innovatieve kracht van SURF is het hoger onderwijs in staat de snelle ontwikkelingen op het beveiligingsgebied bij te benen. Hierbij wordt steeds vaker gebruikgemaakt van expertise van de wetenschappers van de onderwijsinstellingen. De juridische experts van de Universiteit van Tilburg(TILT) en Universiteit Utrecht worden geregeld betrokken bij onderzoeken en presentaties.
De security onderzoekers van Universiteiten van Nijmegen en Amsterdam zijn geregeld en intensief berokken bij actuele vraagstukken. Op het gebied van informatiebeveiliging weten de uitvoerders en de wetenschappers elkaar goed te vinden.

Framework Informatiebeveiliging Hoger Onderwijs
In het najaar van 2010 is een model beveiligingsbeleid opgesteld voor onderwijsinstellingen. Tezamen met een stappenplan voor de implementatie (zie artikel starterkit informatiebeveiliging) is dit aangeboden aan de besturen van alle hoger onderwijsinstellingen. Het model en de starterkit maken deel uit van het *framework informatiebeveiliging Hoger Onderwijs*, een samenhangend stelsel van modellen en leidraden. Momenteel wordt gewerkt aan de laatste componenten van het framework, zoals een baseline informatiebeveiliging.

Baseline en Normenkader
In vervolg op het model beveiligingsbeleid wordt in 2011 gewerkt aan een baseline. Hierin worden sets van aanbevolen maatregelen beschreven, voor verschillende niveaus van beveiliging. De kern van de baseline bestaat uit een matrix van ten hoogste twee pagina's. Hiermee kunnen snel en overzichtelijk keuzes worden gemaakt voor maatregelen. De baseline wordt gekoppeld aan een normenkader. Dit normenkader wordt opgesteld als onderdeel van SURFaudit en zal dienen als referentie bij volwassenheidsmetingen.

Samen werken, samen delen
De publicaties van SURF en van de SURF beveiligingscommunities worden onder een creative commons licentie voor niet-commercieel gebruik beschikbaar gesteld. Gebruik en hergebruik wordt van harte toegejuicht.

Literatuur

Informatiebeveiliging 2008-8,

Volwassenheid Informatiebeveiliging Het 4 Aspecten Model

Informatiebeveiliging 2008-8, Informatiebeveiliging in HO onvolwassen

SURFnet/Kennisnet innovatieprogramma, www.surfnetkennisnetproject.nl/.

Model beveiligingsbeleid HO: www.surffoundation.nl/nl/themas/organiserenmetICT/informatiebeveiliging/Pages/Leidradeninformatiebeveiliging.aspx

Juridische kennisbank: www.surfdirect.nl

STARTERKIT IB

René Ritzen is security officer van Universiteit Utrecht en zit in de stuurgroep van SURFibo. René heeft als trekker van een werkgroep van SURfibo gezorgd voor de totstandkoming van deze starterkit en is per e-mail bereikbaar via r.ritzen@uu.nl

SURFibo heeft voor haar doelgroep een starterkit ontwikkeld voor het inrichten van informatiebeveiliging. De aanpak is opgedeeld in vijf fasen, die in volgorde doorlopen kunnen worden of kunnen dienen als checklist.

Informatiebeveiliging, waar begin je? Vooral kleinere hoger onderwijsinstellingen hebben veelal moeite met de inrichting van informatiebeveiliging. De verantwoordelijkheid voor informatiebeveiliging is bij deze instellingen vaak bij een ict-afdeling belegd, of een ict-afdeling voelt zich hiervoor verantwoordelijk zonder expliciet de bijbehorende bevoegdheden te hebben gekregen. De verantwoordelijke persoon weet niet goed waar hij of zij moet beginnen en wat er allemaal moet worden gedaan om tot een verantwoord niveau van informatiebeveiliging te komen. Over het algemeen is de Code voor Informatiebeveiliging een goede leidraad om het totale spectrum van informatiebeveiliging mee in te richten, maar deze is op een vrij hoog abstractieniveau geschreven waardoor het lastig is de vertaling te maken naar de praktijk van een hoger onderwijsinstelling.
Om de startende informatiebeveiliger in het hoger onderwijs op weg te helpen is de starterkit informatiebeveiliging geschreven. In deze starterkit is de Code voor Informatiebeveiliging weliswaar leidend, maar wordt zoveel mogelijk getracht om per onderdeel laagdrempelig te starten met als doel in relatief korte tijd zoveel mogelijk resultaat te boeken.

Omdat niet alles tegelijk kan worden gerealiseerd is een fasering aangebracht waarvan hieronder een samenvatting. Informatiebeveiliging staat niet bij alle bestuurders scherp op het netvlies. Een letterlijke uitspraak van een lid van een College van Bestuur: "Het moet gewoon geregeld zijn en ik ga ervan uit dat IT dat heeft gedaan." Impliciet is er vanaf het begin management commitment. Om dit expliciet te maken is het vaak eerst nodig inzichtelijk te maken waar het eigenlijk om gaat en binnen de ict-afdeling te beginnen met implementeren van een gestructureerde aanpak. Vandaar dat in de starterkit niet wordt begonnen op bestuurlijk niveau, maar dat dit pas in de derde fase wordt geadresseerd.

Informatiebeveiliging staat niet bij alle bestuurders scherp op het netvlies

Fase 1: inventarisatie huidige situatie
Het is belangrijk dat een informatiebeveiliger weet hoe de organisatie in elkaar zit, wat de primaire en ondersteunende bedrijfsprocessen zijn, welke informatiesystemen worden gebruikt om die bedrijfsprocessen te ondersteunen, wie verantwoordelijk is voor het beheer daarvan, enz. Fase 1 bestaat dan ook uit het voeren van (kennismakings)gesprekken met eigenaren en beheerders van bedrijfsprocessen, informatiesystemen, applicaties, en dergelijke.

Als dat inzicht is verkregen (en gedocumenteerd), wordt in overleg met die eigenaren bekeken hoe kwetsbaar de bedrijfsprocessen zijn voor verstoringen in de ict-voorziening.

Voor de belangrijkste applicaties wordt voor beschikbaarheid, integriteit en vertrouwelijkheid gescoord op een schaal van 1 (nog niets aan beveiliging gedaan) tot 3 (voldoende gedaan waarbij in dit stadium samen met de proceseigenaar wordt bepaald wat voldoende is).

Daarnaast wordt geïdentificeerd voor welke onderdelen van informatiebeveiliging beleid en procedures bestaan. Denk hierbij onder meer aan de aanwezigheid van een goedgekeurd beleidsdocument, het hebben van een beveiligingsorganisatie waarin iedereen zijn of haar verantwoordelijkheden kent, een gebruiksreglement, een incident registratiesysteem, viruscontrole, enz. Meestal zijn er al technische voorzieningen op beveiligingsgebied getroffen zoals bijvoorbeeld het gebruik van viruscheckers, maar is de organisatie nog niet gerealiseerd en het beleid niet vastgesteld.

Fase 2: kortetermijnverbeteringen en opstellen plan van aanpak
Om aan het bestuur aan te kunnen tonen dat het loont om structureel aandacht aan informatiebeveiliging te geven, worden de meest lonende maatregelen doorgevoerd (laaghangend fruit). Deze zijn afgeleid uit de inventarisatie van kwetsbaarheden en de stand van zaken met betrekking tot te nemen maatregelen.

Een starterkit voor iedereen?
De starterkit is geschreven om instellingen waar nog weinig tot niets aan informatiebeveiliging wordt gedaan snel en met niet al te grote inspanning op weg te helpen naar een volwaardige inrichting van het security managementproces. Met stap 4 en 5 wordt feitelijk al procesmatig (volgens PDCA) gewerkt. Hiermee wijkt de onderwijssector niet af van andere sectoren. Deze starterkit zou met minimale wijzigingen (vervang 'bestuur' door 'directie') ook door kleinere bedrijven kunnen worden gebruikt. Daar kampt men vaak met hetzelfde probleem: geen specifieke capaciteit en kennis voor informatiebeveiliging, en angst voor het onbekende.
De starterkit wordt in de praktijk gebruikt als stappenplan maar ook als checklist. Deze kit is geen 'rocket science'. De toegevoegde waarde ligt in het feit dat hij door 'peers' is opgesteld, door 'peers' wordt aanbevolen, en pragmatisch is en de juiste termen gebruikt voor het onderwijsveld.

In deze fase wordt ook een plan van aanpak voor de lange termijn opgesteld waarin alle aspecten van informatiebeveiliging aan de orde komen. In dat plan komen projectvoorstellen te staan die de komende jaren moeten worden uitgevoerd. Denk hierbij aan het opstellen van een baseline informatiebeveiliging, het inrichten van de informatiebeveiligingsorganisatie en maatregelen op het gebied van bedrijfscontinuïteit.

Fase 3: de dialoog met bestuurders
In deze fase is het belangrijk om commitment van het bestuur te krijgen. Kan de informatiebeveiliger het bestuur overtuigen van het belang van structurele aandacht voor informatiebeveiliging?

Toolkit van Neil T.

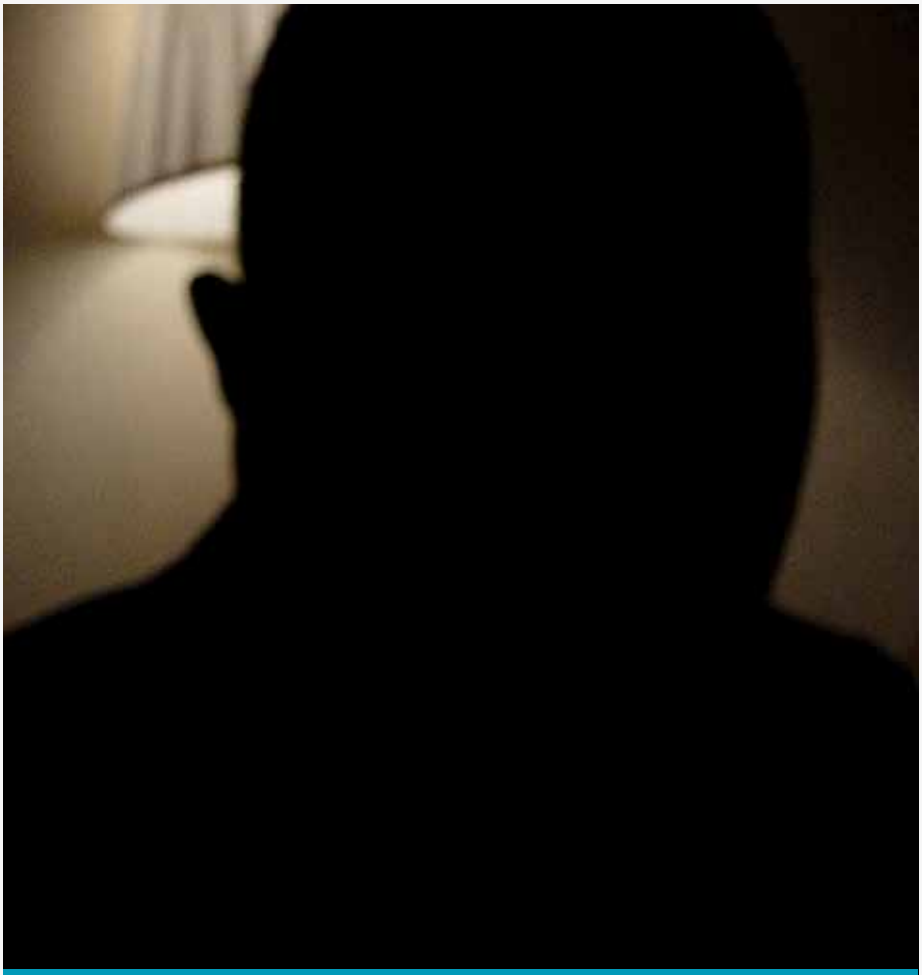
In principe zou dit moeten lukken op basis van de al eerder genomen maatregelen (laaghangend fruit) en de risicoverlaging die daarmee is gerealiseerd.

Het kan best zijn dat er meerdere gesprekken en presentaties nodig zijn om duidelijk te maken dat informatiebeveiliging helpt om de overalldoelstellingen van de onderwijsinstelling te realiseren. Aandacht voor de Wet Bescherming Persoonsgegevens, aansprakelijkheidsclaims van opdrachtgevers (bijvoorbeeld bij contractonderzoek), reputatieschade, het niet 'in control' zijn, zijn doorgaans zaken die tot inzicht kunnen leiden. Uiteindelijk zal er commitment ontstaan en zullen middelen (menskracht en financiering) ter beschikking worden gesteld voor de uitvoering van het gepresenteerde plan van aanpak.

Fase 4: projectmatige uitvoering plan van aanpak
Informatiebeveiliging is geen eenmalige actie, maar heeft geregeld aandacht nodig, de omgeving verandert immers ook. Onderdeel van het plan van aanpak is dat er een beheerorganisatie voor informatiebeveiliging wordt ingericht en aansluiting wordt gezocht bij de interne budgetteringscyclus. Naast het opstellen van beleid en het inrichten van een beveiligingsorganisatie zal er ook moeten worden gewerkt aan het inrichten van de Plan-Do-Check-Act-cyclus voor informatiebeveiliging. Dat geeft ook mogelijkheden om delen van het plan van aanpak in de jaarbegroting mee te nemen.

Verder moet een afweging worden gemaakt voor de inrichting van een risicomethodiek, het incident managementproces, het inrichten van een communicatie- en rapportagestructuur en de uitvoering van diverse deelprojecten uit het plan van aanpak.

Fase 5: beheer
Het is belangrijk periodiek de status van informatiebeveiliging in de instelling te monitoren en, bij geconstateerde tekortkomingen, maatregelen te treffen. Dit kan door het uitvoeren van nieuwe risicoanalyses, door het (laten) uitvoeren van audits, door het inhuren van een 'mysteryman' die de vinger op de zere plekken legt, enz.
Onderdeel van beheer is ook de bevordering van bewustwording. Dat kan met trainingen via een intranetsite, posters en/of e-learning. Waar het om gaat is dat het beleid bekend wordt gemaakt en wordt gehandhaafd. Dit vergt de nodige aandacht. Mensen kennen de risico's onvoldoende en doen, soms



Mystery Man van Clyde Robinson.

uit behulpzaamheid, dingen die beter achterwege gelaten kunnen worden (social engineering) en daar moet op worden getraind.
Controle, naleving en sancties vormen het onvermijdelijke sluitstuk van een serieus informatiebeveiligingstraject. Interne en externe accountants kunnen daarbij behulpzaam zijn.

Tot slot

Vaak wordt gezegd dat de ict-afdeling ervoor dient te zorgen dat er veilig kan worden gewerkt. Informatiebeveiliging is echter een onderwerp dat de gehele organisatie aangaat. Ondanks dat het dan misschien een onmogelijke opgave lijkt, helpt de starterkit om de inrichting van de informatiebeveiliging op een hoger plan te krijgen. De fasen 1 en 2 kunnen ook zonder bestuurlijk commitment en zonder al teveel budget worden uitgevoerd.

Fase 3 is cruciaal. De uitkomst daarvan is bepalend voor de verdere uitvoering van de fasen 4 en 5. Voor fase 4 zullen personen uit de hele organisatie een bijdrage moeten gaan leveren en zullen ook budgetten beschikbaar moeten worden gesteld.

Naarmate men verder in het proces zit, is het niet alleen voldoende materiekennis te bezitten, maar worden de sociale skills van de informatiebeveiliger ook steeds belangrijker.
Om die reden geeft de starterkit voor elke fase aan hoe de opstelling en instelling van de informatiebeveiliger het beste kan zijn en welke 'soft skills' hij of zij nodig heeft. In de praktijk blijkt dat het eigenlijk niet uit maakt of je start vanuit een functie bij de afdeling Informatiemanagement of dat je op de ict-afdeling werkt. Betrokkenheid bij het onderwerp is in eerste instantie het belangrijkste.

> Een 'mysteryman' die de vinger op de zere plekken legt

Met het doorlopen van de vijf fasen uit de starterkit is een stevig fundament voor de informatiebeveiliging gelegd die vervolgens verder op een procesmatige manier kan worden beheerd en kan worden aangepast aan de over het algemeen voortdurend veranderende risico's en bedreigingen.

De Startkit blijkt in de praktijk aan een behoefte te voldoen en wordt zowel bij 'green-field'-situaties gebruikt als bij lopende inrichtingsprojecten als checklist.

De Starterkit Informatiebeveiliging is beschikbaar op de website van SURFfoundation.

Derde geldstroom onderzoek

Hoger onderwijsinstellingen zijn voor hun bedrijfsvoering deels afhankelijk van de zogenaamde derde geldstroom. Dit is vaak contractonderzoek voor bedrijfsleven maar ook voor onderzoek, veelal sterk innovatief of fundamenteel wetenschappelijk. Daarmee is dit concurrentiegevoelig en, bij overheidsopdrachten, maatschappelijk of politiek gevoelig. Van sommige onderzoeken is het niet gewenst dat er überhaupt bekend wordt dat een dergelijk onderzoek wordt uitgevoerd. Een aantal jaar geleden was zelfs onderzoek naar de consequenties van de afschaffing of beperking van hypotheekrenteaftrek zo gevoelig dat dit niet bekend mocht worden. De derde geldstroom stelt de universiteiten en hogescholen in staat om meer wetenschappelijk onderzoek te doen waardoor meer topwetenschappers kunnen worden gebonden aan de instellingen. Een goede relatie met opdrachtgevers is daarbij essentieel en daarbij hoort zorgvuldig omgaan met onderzoekopdrachten en onderzoeksresultaten.

INTERVIEW

'HOGER ONDERWIJS HEEFT NOG ONVOLDOENDE GRIP OP BEVEILIGING EN PRIVACY'

Interview met Wim Liebrand, directeur ICT-samenwerkingsorganisatie SURF.

Sandra Kagie met medewerking van Alf Moens

'Samen excelleren' is de titel van het Meerjarenplan van SURF 2011-2014. In het plan geeft de ICT-samenwerkingsorganisatie voor het hoger onderwijs en onderzoek aan welke thema's op ICT-gebied voor de sector in de komende jaren van belang zijn. De onderwerpen beveiliging en privacy nemen in het meerjarenplan een belangrijke plaats in. Reden voor de redactie van Informatiebeveiliging om SURF-directeur Wim Liebrand uit te nodigen voor een interview.

Binnen SURF werken universiteiten, hogescholen en onderzoeksinstellingen samen aan grensverleggende ICT-innovaties. Maar hoe bepaalt SURF haar visie en programma's op het gebied van security eigenlijk?
Wim Liebrand: "Eind 2008 vond de aftrap plaats voor het Meerjarenplan 2011-2014 in Den Haag. In de Eerste Kamer debatteerden bestuurders van diverse onderwijsinstellingen over de thema's die in de komende jaren de ICT-strategie binnen het hoger onderwijs en onderzoek gaan bepalen. Op basis van deze discussie hebben wij na uitgebreid overleg met de betrokken deskundigen in het hoger onderwijs en onderzoek het meerjarenplan 2011-2014 'Samen Excelleren' opgesteld.
De nadere invulling hiervan gebeurt vanuit de werkmaatschappijen van de SURF-organisatie en binnen het gezamenlijke innovatieprogramma SURFnet/Kennisnet.
In de verschillende projecten spelen onderwijs- en onderzoeksinstellingen zelf een belangrijke rol. Niet SURF bepaalt wat er gaat gebeuren, maar de instellingen zelf. Heb je het bijvoorbeeld over een onderwerp als 'open content' dan ligt de bijdrage van SURF in het realiseren van de infrastructuur voor het bewaren, vinden en ontsluiten van deze content. Het is echter aan de instellingen zelf om de content met behulp van deze infrastructuur te publiceren."

Wim Liebrand.

Wat ziet SURF als trends? Wat zijn met andere woorden de speerpunten in het Meerjarenplan 'Samen excelleren'?
Liebrand: "Ik vertel niets nieuws wanneer ik zeg 'internet verandert'. Van doorgeefluik van informatie naar een wereldwijd platform voor gezamenlijke activiteiten en bron van services. Niet gehinderd door landsgrenzen wordt internet een 'wolk' van resources."
Voor het onderwijs betekent dit volgens de SURF-directeur dat we toegaan naar een situatie van open educatie op alle fronten. Er ontstaan nieuwe vormen van (internationale) samenwerking. Zo is het volgens hem al mogelijk om dure specialistische apparatuur zoals telescopen en massaspectrometers op afstand te delen. Of om grootschalige, gedistribueerde computer- en datafaciliteiten en gegevensbronnen gezamenlijk te gebruiken. Rond kennisinstellingen ziet Liebrand ecosystemen ontstaan. Vormen van samenwerking tussen kennisontwikkelaars, -aanbieders en -gebruikers met overheden en intermediaire organisaties.
Vraag naar en aanbod van kennis worden zo in de ogen van Liebrand beter op elkaar afgestemd.

'Onvoldoende grip'

Genoemde ontwikkelingen brengen volgens Liebrand onvermijdelijk met zich mee dat zaken als betrouwbaarheid, standaardisatie, beveiliging en

privacy meer aandacht moeten krijgen. "In het Meerjarenplan van SURF nemen beveiliging en privacy daarom een prominente plaats in", geeft hij aan. "Onderwijsinstellingen zijn zich er op bestuurlijk niveau terdege van bewust dat vruchtbare samenwerking staat of valt met onderling vertrouwen. Bestuurders omarmen dan ook het idee om voor de gehele sector te streven naar een hoog en meetbaar niveau van informatiebeveiliging en privacybescherming. Het is hierbij essentieel om een balans te vinden tussen veiligheid en gebruiksvriendelijkheid waarbij rekening moet worden gehouden met onderwerpen als identitymanagement, informatiebeveiliging en privacy."
Met name op die twee laatste aspecten hebben we volgens de SURF-directeur 'nog onvoldoende grip'. Het is volgens hem daarom de bedoeling dat voor 2015 alle bij SURF aangesloten instellingen een computer emergency response team hebben, dat zowel reactief als proactief op beveiligingsinbreuken inspeelt. Deze teams worden gecoördineerd door SURF. Daarnaast zal een expertisenetwerk worden opgebouwd en ook wordt de bestaande dienstverlening op het gebied van authenticatie en autorisatie verder uitgebreid.
Liebrand: "Zo moet uiteindelijk iedereen die in Nederland binnen het hoger onderwijs en onderzoek werkzaam is, op basis van een geauthenticeerde rol toegang hebben tot diensten en content van publieke en private leveranciers op het internet."

SURFnet7

Terugkomend op de speerpunten voor de komende jaren wil Liebrand ook zeker de aandacht vestigen op het behoud van de wereldwijde koppositie op het terrein van netwerkinfrastructuur. Dit door de realisatie van de volgende generatie SURFnet – SURFnet7, een schaalbaar hybride netwerk. "Het is onze ambitie dat studenten, docenten en onderzoekers in 2015 de eerste gebruikers zijn van een landelijk dekkend fixed-wireless seamless netwerk", vertelt hij. Om deze ambitie waar te maken, zoekt SURF samenwerking met operators en leveranciers van mobiele netwerkdiensten. Dit om afspraken te maken over een identieke dienstverlening en eenduidige standaarden. Dat de toevoeging van draadloze communicatie aan het glasvezelnetwerk consequenties heeft voor opnieuw security en privacy, realiseert Liebrand zich terdege. "Deze aspecten moeten daarom door ons worden uitgezocht en geregeld".

Over de vraag wat het gewicht is dat SURF binnen de onderwijssector in de schaal legt, is hij vervolgens glashelder. "SURF is ván de onderwijssector. Er zal op landelijk niveau geen substantiële ICT-innovatie(dienst) voor het hoger onderwijs worden gestart zonder dat de instellingen in SURF-verband hiermee instemmen. We zijn met andere woorden duidelijk de facilitator van het gesprek.
Daarnaast treden we als SURF op een aantal vlakken op als leverancier. Van SURFnet bijvoorbeeld, maar ook op het gebied van gemeenschappelijke inkoop door middel van SURFdiensten. Ook deze diensten komen echter voort uit de gebundelde vraag van de hoger onderwijssector".
De vraag of SURF ook voor de overheid een gesprekspartner is, wordt door de directeur met een volmondig 'ja' beantwoord. "Voor de overheid zijn wij hét loket om in een klap met de gehele sector in gesprek te komen. Dit over issues op het gebied van ICT-ondersteuning voor hoger onderwijs en onderzoek, maar ook ten aanzien van bedrijfsprocessen."

Wie zijn er aangesloten?

In totaal zijn er veertien universiteiten en zo'n veertig instellingen voor hoger beroepsonderwijs aangesloten bij de stichting SURF. Dat zijn alle instellingen voor hoger onderwijs die door Den Haag bekostigde opleidingen verzorgen. De verschillen tussen hbo-instellingen en universiteiten worden volgens Liebrand overigens steeds kleiner. "De opleidingsstructuur met een bachelor- en masterfase is vergelijkbaar en ook op hogescholen wordt in toenemende mate aan onderzoek gedaan."

Ook op het gebied van informatiebeveiliging draaien beide soorten instellingen volgens hem goed mee. "Onze ervaring is dat met name grotere organisaties prima zelf hun keuzes kunnen bepalen. Binnen het hbo zijn er qua grootte echter veel verschillen. De kleinste organisatie telt zo'n vierhonderd studenten terwijl de grootste hbo-instelling er zo'n veertigduizend heeft. Verschillen die je tussen universiteiten veel minder ziet. Deze zijn qua structuur dan ook redelijk vergelijkbaar. Om de beperkte mankracht van de kleine instellingen te compenseren zet SURF daarom voor die organisaties op het gebied van bijvoorbeeld informatiebeveiliging extra ondersteuning in. Op deze manier bieden we dus alle bij ons aangesloten instellingen de mogelijkheid gelijk op te trekken."
Dit laatste is volgens Liebrand essentieel voor de gehele sector. "Want uiteindelijk weten we allemaal dat verregaande samenwerking staat of valt met het elkaar onderling kunnen vertrouwen", besluit hij. "Een collectief hoog en meetbaar niveau van informatiebeveiliging en privacybescherming is hiertoe een voorwaarde. Je bent immers als collectief zo sterk als de zwakste schakel."

Meer informatie: www.surf.nl

INFORMATION SECURITY MANAGEMENT OP HBO-NIVEAU

Ellen Wesselingh, docent aan de opleiding

In september 2008 is aan De Haagse Hogeschool, vestiging Zoetermeer, de opleiding Information Security Management van start gegaan. In deze opleiding krijgen de studenten te maken met alle invalshoeken van waaruit betrouwbaarheid van informatie in organisaties kan worden bekeken. Naast algemene vaardigheden als adviseren en samenwerken, concentreert het onderwijs zich op de volgende aspecten: de mens (psychologie), de organisatie (organisatiekunde), de techniek en de wet- en regelgeving waaraan organisaties moeten voldoen.

In de opleiding Information Security Management staat de juiste omgang met informatie centraal. Onderwerpen die raken aan integrale veiligheid (zoals bedrijfshulpverlening en hulpdiensten) komen zijdelings aan bod in het onderwijs over business continuity management. In dit deel van het onderwijs kan het zijn dat informatie minder centraal staat, hoewel bijna ieder bedrijf in Nederland tegenwoordig een informatieverwerker is. Ook productiebedrijfjes waarvan men vroeger vond dat de informatiestromen minder van belang waren.

Het onderwijs is ingedeeld in vier onderwijsperioden per jaar, van tien weken. Zo'n onderwijsperiode noemen we een blok. In de eerste zeven weken voeren de studenten een praktijkopdracht uit in een projectgroep en krijgen ze de bijbehorende theorie in colleges en workshops aangeboden. De groepsgrootte is meestal rond de vier studenten, maar kan variëren afhankelijk van het aantal deelnemers. Na afronding van het project wordt de theoriekennis getoetst en de praktijkopdracht verdedigd in een assessment.

Het programma van de opleiding is enigszins gewijzigd ten opzichte van de eerste opzet (waarover eerder in dit blad is gepubliceerd), maar ziet er ruwweg als volgt uit:

Eerste jaar
Het propedeusejaar van de opleiding is oriënterend en selecterend. In de eerste onderwijsperiode maken de studenten kennis met de belangrijke standaarden van het vakgebied (ISO 27001 en 27002) en hoe de informatie in die standaarden in een organisatie kan worden gecommuniceerd. Daarna leren de studenten wat de belangrijkste begrippen zijn die moeten worden geborgd in het kader van betrouwbaarheid van informatie en informatievoorziening.
Aan de hand van interviews met proceseigenaren in een fictieve organisatie maken de studenten een analyse van de business impact en van de risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid. In de laatste periode leren de studenten over de menselijke factor, hoe mensen te manipuleren zijn en hoe je dit kunt gebruiken om een omgeving te creëren waarin op de juiste wijze wordt omgegaan met informatie. De praktijkopdracht wordt uitgevoerd bij een extern bedrijf.

Tweede jaar
In het tweede studiejaar komen de onderwerpen cybercrime, business continuity management en compliance/auditing aan bod. In het blok cybercrime voeren de studenten een forensisch onderzoek uit en rapporteren ze de bevindingen die als bewijs worden opgevoerd in een rechtzaak, waarna ze door middel van het hardenen van systemen en penetratietesten een veiliger systeem opleveren. Voor business continuity analyseren de studenten een extern bedrijf en maken afhankelijk van de behoefte van de opdrachtgever een continuïteitsplan of een crisisplan. Compliance en auditing vindt plaats in een fictieve organisatie, waarbij wederom door middel van interviews moet worden onderzocht wat de situatie is, waarna bijvoorbeeld een verbeterd protocol wordt opgeleverd.

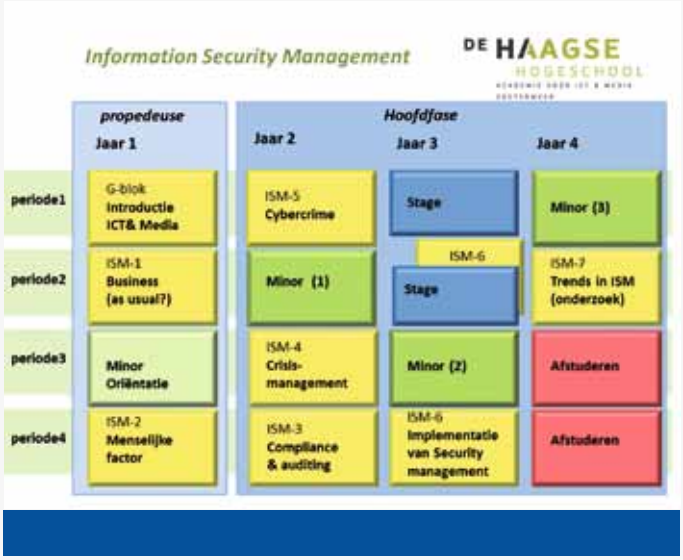
> Voor business continuity analyseren de studenten een extern bedrijf

Derde jaar
Het derde studiejaar staat grotendeels in het kader van de stage. Daarnaast leren de studenten het belang van een solide architectuur op verschillende niveaus in de organisatie. Voor de bijbehorende praktijkopdracht moeten de studenten als consultant zelf een opdracht verwerven en uitvoeren. De studenten leveren een product op dat kan gaan over een architectuurbouwsteen, een policy of 'controls'.

Vierde jaar
In het laatste jaar voeren de studenten een onderzoek uit naar trends in de informatiebeveiliging. De student kiest

zelf een onderzoeksonderwerp, stelt onderzoeksvragen op en voert een passend onderzoek uit, bijvoorbeeld met een enquête of interviews.
Naast het verplichte programma volgen de studenten één blok per jaar waarin ze zelf het onderwijs kiezen, dat is het zogenaamde minorprogramma. In totaal kiest de student dus 25% van het onderwijs zelf. Sommige studenten gebruiken de keuzeruimte om zich te verbreden in allerlei aanpalende vakgebieden (bijvoorbeeld bedrijfsinformatie en techniek), andere studenten kiezen er voor om zich te verdiepen op een onderwerp door opeenvolgende keuzeblokken die een samenhangende minor vormen.

Beroepspraktijk
De focus van de opleiding ligt bij het opleiden van studenten voor de beroepspraktijk. Dit is op verschillende manieren in het curriculum uitgewerkt. Zo voeren de studenten al in het eerste jaar een opdracht uit voor een 'echte' opdrachtgever. Ze spelen mystery guest voor een bedrijf en rapporteren de bevindingen ook terug aan de opdrachtgever. Deze opdrachtgevers willen bijvoorbeeld weten of hun call centers of afdeling klantcontact zich houden aan de protocollen die moeten voorkomen dat gevoelige informatie wordt meegedeeld aan derden.



Studenten spelen 'mystery guest' voor een bedrijf

In het tweede jaar lichten de studenten een extern bedrijf door op het volwassenheidsniveau voor wat betreft de bedrijfscontinuïteit. Er wordt onderzocht wat het bewustzijnsniveau is en welke preventieve, repressieve, correctieve maatregelen het bedrijf heeft genomen om de continuïteit te waarborgen bij een crisis. Aan de hand van de resultaten van de analyse wordt vervolgens met de opdrachtgever afgesproken welke vervolgstappen in het project worden gedaan. Deze verschillen per opdrachtgever omdat de werkelijke situatie ook sterk uiteen loopt.

Gastcollege
In de onderwijsblokken waar door middel van simulatie aan de praktijkopdracht wordt gewerkt, worden waar mogelijk mensen die in de praktijk werkzaam zijn gevraagd om hun praktijkervaring te delen in gastcolleges (datzelfde gebeurt overigens in de andere onderwijsblokken ook). Kortom, de opleiding Information Security Management doet er veel aan om de praktijk de opleiding binnen te halen en om de studenten vanaf het eerste jaar de praktijk in te sturen.

Ook in het derde en vierde jaar gaan de studenten veelvuldig de praktijk in. De eerste lichting studenten is nu bezig met stage of heeft deze onlangs afgerond. Daarvan hebben twee studenten stage gelopen in China, in het project Check-IT. Dit project is een samenwerkingsverband van een aantal Nederlandse universiteiten en hogescholen, en de universiteit van Xiamen, dat buitenlandstages moet bevorderen.

Toekomst
De Haagse Hogeschool heeft met de opleiding op bachelorniveau een unieke opleiding in het vakgebied informatiebeveiliging. De opleiding laat de student kennismaken met alle aspecten die van belang zijn voor organisaties waarvoor de betrouwbaarheid van de informatie voor de business van belang is.
De studenten leren nadenken over oplossingen op meer dan alleen het technische vlak, ook oplossingen op organisatorisch en menselijk gebied spelen een belangrijke rol gedurende de gehele opleiding. Omdat de eerste student(e) in april begint met afstuderen kunnen we op dit moment nog geen indicatie geven waar de studenten in de beroepspraktijk terecht gaan komen.
Op basis van de stages die tot nu toe zijn gedaan is de verwachting dat ze aan de slag zullen gaan bij uiteenlopende bedrijven, van midden- en kleinbedrijf tot grote bedrijven en de overheid op allerlei niveaus.

CERT: VEILIGHEIDSINCIDENTEN VOORKOMEN EN GENEZEN

Don Stikvoort MSc CTNLP, adviseur & coach, don@s-cure.nl

Veiligheidsincidenten kennen we allemaal. Computerinbraken, wormen, virussen, phishing, website 'defacement', haat-mail, 'denial-of-service'-aanvallen, identiteitsdiefstal, auteursrechtschendingen, noem maar op. Deze incidenten negeren is meestal niet mogelijk, en is ook niet wenselijk. Als een organisatie onder cybervuur ligt, dan is optreden de enige optie. Als er vanuit de eigen organisatie wordt gehackt, is ook actie nodig. Beter is het natuurlijk om incidenten te voorkomen. Het voorkomen en genezen van veiligheidsincidenten is dus een belangrijke taak. Deze taak heeft een naam: CERT, dat staat voor 'Computer Emergency Response Team'.

Wie anders dan de leiding van een organisatie kan de verantwoordelijkheid nemen voor de organisatie rondom veiligheidsincidenten? Incidenten bedreigen immers zelfs het primaire proces en daarmee de reputatie. Dus het mandaat voor de CERT-taak komt van de top. En escalaties naar het bestuur moeten te allen tijde mogelijk zijn. Als dit geformaliseerd is, kan de CERT-taak op verschillende manieren worden belegd. Meestal zal dit in de ICT-organisatie zijn, omdat daar de experts zitten. Als er een CISO is kan deze heel goed de brug zijn tussen het bestuur en de CERT. Maar moet die CERT nu echt, of kan het ook anders? Het antwoord is dat security incidentmanagement inderdaad op verschillende manieren kan worden ingericht. Maar dat we voor allemaal de term CERT gebruiken. CERT is een taak, een functie, een proces. En niet per se een paar mensen in een kamertje! Het begrip CERT is ook duidelijk voor de 'buitenwereld'. En incidenten beperken zich nu eenmaal niet tot de grenzen van een lokaal netwerk. Zelfs als het incident managementproces is uitgesmeerd over een groot aantal ICT-functionarissen onder het motto 'die pet past iedereen', dan nog zal er een kleiner aantal tweedelijns experts zijn die de 'moeilijkere' incidenten zullen afhandelen. Dat is dan de CERT-kern.
Kortom, CERT moet. De essentiële taken worden nu al uitgevoerd. En het 'CERT-label' helpt om deze taken beter te mandateren, te organiseren en uit te voeren.

> De CERT-taak gaat voor reguliere taken

CERT Starterkit
Ik ben al twintig jaar actief op CERT-gebied en was mentor bij de oprichting van zeven teams, waaronder GOVCERT.NL. Voor SURFnet heb ik een 'CERT Starterkit' ontwikkeld. Deze kit maakt het eenvoudig om het incident managementproces, dat in beginsel al bestaat, om te vormen tot een CERT. Dat kost alleen een beperkte eenmalige inzet in de vorm van menskracht om de CERT vorm te geven. Daarna betaalt een CERT zichzelf terug! Immers, elke organisatie moest altijd al reageren op incidenten. Door dit als een CERT beter te organiseren zal een organisatie in de toekomst slagvaardiger zijn, beter toegerust en georganiseerd, en in de rug gedekt.

De starterkit biedt handreikingen op alle niveaus. De belangrijkste onderdelen zijn:

1. qua governance zijn er kant-en-klare argumenten voor het bestuur om een CERT in te richten. Hier horen ook de trendrapportages van GOVCERT.NL bij, die zonneklaar aantonen dat we alle reden hebben om ons zorgen te maken over veiligheidsincidenten;

2. er is er een stappenplan voor het implementeren van de CERT-taak;

3. de starterkit bevat twee concrete voorbeelden van een 'organisationalframework' voor de CERT. Deze voorbeelden kunnen zelf eenvoudig worden aangepast aan de eigen situatie en vervolgens vastgesteld door het bestuur;

4. ten slotte is er een voor-ingevulde versie van RFC-2350. Deze RFC is het internationaal geaccepteerde invulformulier waarmee een CERT publiekelijk zijn operationele dienstverlening kan presenteren. 'Voor wie werkt de CERT?' 'Wat zijn de diensten?' 'Wanneer is de CERT open?' 'En wat zijn de contactgegevens?' Dat soort gegevens en meer.

Met de starterkit staat de CERT-taak in zeer korte tijd in de startblokken. Het is vooral belangrijk om het bestuur te wijzen op zijn verantwoordelijkheid voor dit proces en zo mandaat te krijgen. De

operationele uitdagingen zijn meestal klein. Als regel worden drie tot vijf mensen aangewezen die de CERT-taak in deeltijd uitvoeren, en meestal waren deze al bij dit werk betrokken. Bij instellingen voor onderwijs en onderzoek heeft degene die CERT-dienst heeft meestal niet meer dan 20% van zijn tijd nodig voor deze taak. Als er een ernstig incident is kan dat wel ineens meer dan 100% zijn gedurende een aantal dagen. Die flexibiliteit moet worden geborgd. De CERT-taak gaat voor reguliere taken!

The Bigger Picture

Als een instelling aangesloten is op SURFnet, kan SURFcert het lokale CERT van dienst zijn.
SURFcert is het CERT van SURFnet en is in Nederland en wereldwijd zeer goed ingevoerd en 'connected'. SURFcert zal incidenten die met een aangesloten organisatie te maken hebben bij het CERT van die organisatie melden. Andersom kan een CERT incidenten die hun oorsprong buiten de betreffende instelling hebben, rapporteren aan SURFcert. SURFcert zal dan in contact treden met andere CERTs in de wereld om het probleem zo mogelijk op te lossen. Dit is niet altijd eenvoudig maar wel de moeite waard en in feite een 'internet-burgerplicht'. Samen moeten we het internet zo veilig mogelijk houden.
SURFcert vraagt van het CERT om de eerder genoemde RFC-2350 in te vullen en online beschikbaar te stellen. Verder wordt van een aangesloten instelling verwacht dat die binnen een werkdag reageert op meldingen van SURFcert. Als aan deze zeer redelijke voorwaarden wordt voldaan, dan wordt het CERT van een aangesloten instelling door SURFnet geregistreerd.

'Samenwerking' is het adagium van CERTs wereldwijd. Daarvoor bestaan diverse samenwerkingsverbanden. Die van SURFcert en de CERTs van SURFnet-klanten is net al genoemd. Dan bestaat er binnen Nederland een CERT-vergadering die wordt gefaciliteerd door GOVCERT.NL. In Europees verband zijn 75 teams geaccrediteerd door de 'TrustedIntroducer' (www.trusted-introducer.org) waaronder SURFcert, GOVCERT.NL en KPN-CERT. Deze accreditatie stelt een aantal minimumeisen aan CERTs en is ook de basis voor het lidmaatschap van 'FIRST' (www.first.org), een mondiale ontmoetingsplaats voor de CERT-gemeenschap.

Maturity

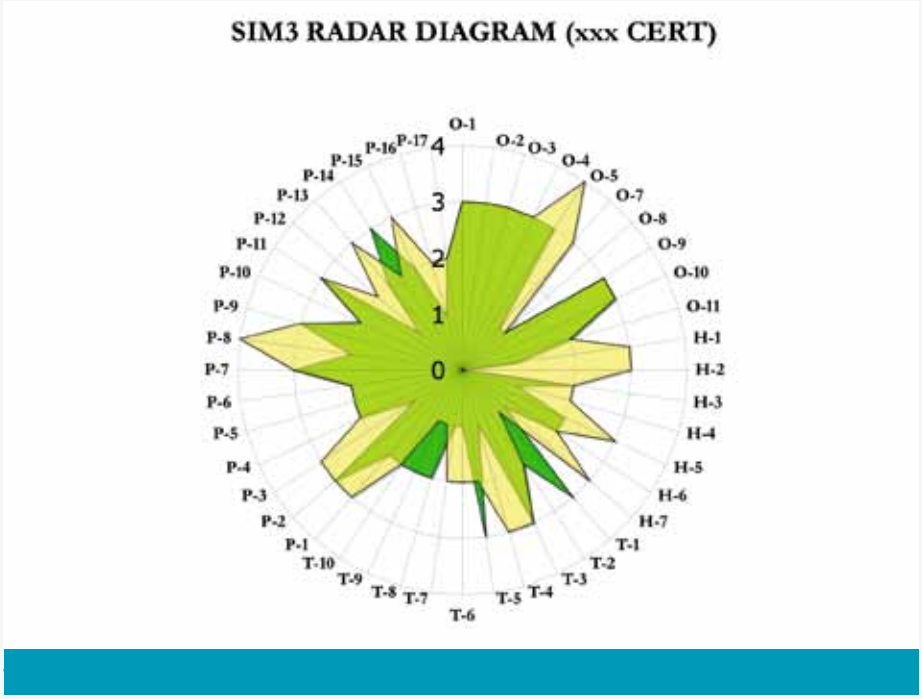
Het CERT-model van samenwerking is ontstaan in 1989 en is daarom bijna net zo jong als het internet. Hoewel er thans honderden CERTs bestaan mondiaal, bevindt de 'maturity' van de CERT-gemeenschap zich nog in de puberteit: de groeispurt naar volwassenheid. Omdat het internet kritieke infrastructuur is geworden worden er steeds hogere eisen gesteld, zo ook aan CERTs en hun samenwerking. Niet alleen eisen vanuit de bestuurslagen van organisaties, maar ook vanuit de overheid.

> Incidenten beperken zich niet tot de grenzen van een lokaal netwerk

Met het oog op deze ontwikkeling heb ik in de afgelopen jaren een CERT 'maturity' model ontwikkeld. Dit model heet SIM3 wat staat voor Security Incident Managament Maturity Model. SIM3 meet de status van vijftig parameters, verdeeld over de categorieën organisatie, personeel, processen en 'tools'. Die status kan per parameter variëren van 'niet bekend' tot 'volledig ingeregeld en als deel van een onafhankelijk audit gecontroleerd', met drie tussengradaties. Een SIM3-meting geeft een CERT een goed beeld van de eigen 'maturity' en kan als basis dienen voor een verbeteringstraject.

SIM3 is door de 'TrustedIntroducer' in Europa geadopteerd als basis voor een CERT-certificering. Dit is de eerste in zijn soort en bestaat sinds september 2010. GOVCERT.NL was wereldwijd het eerste team dat volgens deze standaard is gecertificeerd.

SURF heeft SIM3 ook geadopteerd, als onderdeel van 'SURFaudit'. SURFaudit is een auditproces dat SURF aan het opzetten is voor het hoger onderwijs en onderzoek in Nederland.
De audit meet de status van essentiële onderdelen van informatiebeveiliging. Nu zijn dat informatiebeveiliging algemeen, identity management en de CERT-functie.



ROLE BASED ACCESS CONTROL IN HET HOGER ONDERWIJS

Bart van den Heuvel is Information Security Manager bij de Universiteit Maastricht (UM) en voorzitter van SURFibo. Hij is bereikbaar via bart.vandenheuvel@maastrichtuniversity.nl

Voor wetenschappers, docenten en studenten werd de laatste decennia een informatienetwerk gerealiseerd vanuit de gedachte dat alle informatie snel en eenvoudig met iedereen gedeeld moest kunnen worden. Decentralisatie van taken, privacy aspecten, copyright en bescherming van intellectueel eigendom maken het echter noodzakelijk dat de toegang tot informatie strikter geregeld wordt en wordt toegesneden op de specifieke medewerker of student, gekoppeld aan zijn of haar rol binnen de in hun instelling vastgestelde processen voor onderwijs, onderzoek en bedrijfsvoering.

Toegangsbeheer 1.0

Vanuit de *bedrijfsvoering* (de administraties) werd in het Hoger Onderwijs altijd al het principe gehanteerd dat toegang tot systemen en informatie gekoppeld was aan de taken en bevoegdheden van de medewerkers. De traditionele processen rondom de financiële, personeels- en studentenadministratie werden uitgevoerd door een beperkte groep medewerkers en ondersteund door niet gekoppelde informatiesystemen. Bevoegdheden werden gedeeld onder groepjes nauw samenwerkende collega's en afscherming vond plaats op systeemniveau. Wetenschappers en studenten kregen toegang tot e-mail en deelden hun informatie op een elektronische leeromgeving.
So far, so good. Althans tot het eind van het vorige millennium.

Ontwikkelingen

De ontwikkelingen op het gebied van informatieverwerking bieden een scala aan voordelen, maar leiden helaas ook tot valkuilen en risico's.

Ontwikkelingen in informatievoorziening? Alles kan.
De enorme ontwikkelingen op het gebied van toegangsmogelijkheden, dataopslag en applicaties hebben geen toelichting nodig. De gebruiker wordt daarnaast geconfronteerd met een mengeling van gebruikersaccounts en, al dan niet federatieve, Single-Sign-On. Als we dat relateren aan de komst van Enterprise Databases, gekoppeld via Brokers en ontsloten via een Portal met Selfservice, dan is er voor de eindgebruiker een tijdperk aangebroken van bijna onuitputtelijke, maar ook nauwelijks nog controleerbare informatievoorziening.

Ontwikkelingen in taken en bevoegdheden? Zelfredzaamheid.
Informatie wordt niet meer verzameld en aan anderen aangeboden voor verwerking, maar rechtstreeks door de eindgebruikers digitaal gecreëerd en verwerkt in de informatiesystemen. Cijferlijsten, salarisgegevens, persoonsgegevens, projectdocumenten, onderzoeksresultaten, enz. worden direct door eindgebruikers ingezien en bewerkt.

Voordelen
De voordelen zijn evident. De verwerking is efficiënter en goedkoper en de informatie is completer, inzichtelijker en vooral ook sneller beschikbaar.

Valkuilen
De valkuilen zijn terug te brengen op de drie pijlers van informatiebeveiliging, Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).
Beschikbaarheid is de minste zorg. Over het algemeen is de informatie de laatste jaren juist alsmaar *sneller* beschikbaar. De gebruikers verwachten natuurlijk ook steeds meer op dit gebied, maar met goede afspraken en voldoende technische ondersteuning is dit goed in te regelen.
Op het gebied van *Integriteit* zijn de risico's al een stuk groter. Door de toenemende selfservice dreigt het aloude vier-ogenprincipe verloren te gaan. Informatie kan, al of niet bewust, door een persoon veranderd worden zonder dat een andere persoon daar noodzakelijk bij betrokken is of wordt. Dat maakt niet alleen het risico op fouten groter, maar ook de kans op ontdekking kleiner. Deels kan dit in de systemen worden opgelost door inputverificatie, transactielogging en dergelijke. Deels kan dit organisatorisch worden opgelost, bijvoorbeeld door rapportages en audits.
Inbreuk op *vertrouwelijkheid* is het grootste risico. Als autorisaties niet goed zijn ingeregeld kan vertrouwelijke informatie in verkeerde handen terechtkomen. Dat is feitelijk niet meer ongedaan te maken. Als de vertrouwelijkheid niet goed geborgd is lopen de ook instellingen in onderzoek en onderwijs het risico op imagoschade en voldoen ze meestal ook niet aan de wettelijke richtlijnen in het kader van de Wet Bescherming Persoonsgegevens (WBP).

Toegangsbeheer 2.0

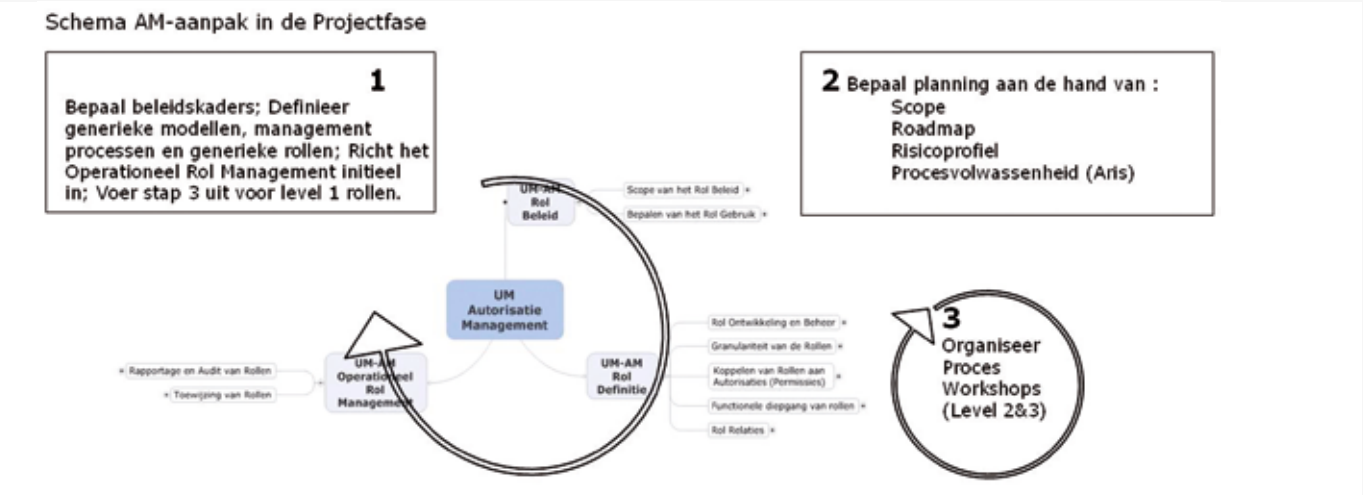
Uiteraard moeten de eindgebruikers om de ontwikkelingen te kunnen volgen wel toegang krijgen tot de diverse systemen. In de praktijk is de hierboven geschetste ontwikkeling een proces wat jaren geleden is gestart en wat nog steeds in volle gang is. In de loop der jaren is dan ook meestal een scala aan technieken, afspraken en koppelingen geïmplementeerd om de telkens uitgebreidere mogelijkheden en toegangen voor de gebruiker te regelen. Dat levert bij veel instellingen de volgende keten van ongewenste situaties:

- Toegang wordt vaak 'ad-hoc' geregeld en niet vanuit een goed beschreven proces. Als gevolg daarvan is er vaak geen goed overzicht over de feitelijk noodzakelijke accounts en autorisaties. Deze worden dan ook niet opgeruimd en er blijven zowel zogenaamde spookaccounts als spookautorisaties in de diverse systemen aanwezig.
- NB: een typerend voorbeeld van ad-hoc-procedures is de toekenning van autorisaties door het kopiëren van accounts van vergelijkbare medewerkers. Daarmee worden te vaak extra autorisaties van zo'n medewerker ten onrechte meegekopieerd naar een nieuwe medewerker.
- Een gebruiker wordt traditioneel geïdentificeerd via zijn of haar account. Dat account had in het verleden voor die gebruiker slechts een beperkte persoonlijke waarde. E-mailboxen werden dan ook regelmatig gedeeld met stagiaires of huisgenoten en wachtwoorden werden gedeeld om tijdens vakanties en dergelijke elkaars werk te kunnen overnemen.
- Door steeds meer functionaliteit te koppelen aan een account wordt niet alleen het persoonlijke belang van een account steeds groter, maar ook het belang voor de instelling en voor de regelgeving waar de instelling aan moet voldoen: de WBP, licentieovereenkomsten (denk aan de bibliotheek en educatieve software), ongeoorloofde toegang tot het instellingsnetwerk en daarmee tot SURFnet, enz.

Kortom, er is sprake van een sterk verhoogd risico dat een instelling niet meer de gewenste controle heeft over het aantal en de kwaliteit van de geregistreerde identiteiten en de daaraan gekoppelde autorisaties.

RBAC in het hoger onderwijs is *anders* dan in het reguliere bedrijfsleven omdat de *Business* en het *werknemersschap* anders zijn, of op zijn minst anders worden ervaren. Het hoger onderwijs ontwikkelt zich wel steeds meer in de richting van het bedrijfsleven omdat de financiering meer en meer op basis van output wordt ingericht. De overheidsbijdrage hangt inmiddels af van het aantal toegekende diploma's en het bedrijfsleven draagt bij aan onderzoeksprojecten (de zogenaamde derde geldstroom) op basis van zakelijke afspraken en zo groot mogelijke garanties op het verkrijgen van intellectueel eigendom.
De docent/onderzoekers hebben echter een van het bedrijfsleven afwijkende mix van taken, bevoegdheden en verantwoordelijkheden. Enerzijds moet men zich conformeren aan strikte afspraken om vertrouwelijkheid en integriteit in onderzoeksprojecten (bijvoorbeeld bij patenten) en in de bedrijfsvoeringprocessen (bijvoorbeeld bij cijferlijsten) te garanderen en anderzijds wil men in een open omgeving en vaak met afwijkende systemen informatie kunnen uitwisselen met collega's en studenten binnen en buiten de eigen organisatie-eenheid. Nieuw zijn daarbij het toenemende spionagerisico en het feit dat het hoger onderwijs ook wordt gezien als kennisbron voor terroristische activiteiten.
Ook de aanstelling van docent/onderzoekers is bij het hoger onderwijs anders dan bij het reguliere bedrijfsleven. Medewerkers starten vaak hun werkzaamheden voordat het dienstverband formeel is ingegaan, terwijl men vaak nog onbezoldigde werkzaamheden blijft verrichten nadat men formeel uit dienst is. Masterstudenten en promovendi hebben doorgaans naast een rol als student ook een rol als medewerker. Voor al deze, soms dubbele, identiteiten dienen dus autorisaties *toegekend*, maar vooral ook weer *ingetrokken* te worden in een proces wat niet synchroon loopt met de formele dienst- of studieverbanden

RBAC inrichten in een organisatie waarin men elkaars wachtwoorden deelt heeft geen zin



Een pas op de plaats

Zoals hierboven al te lezen is, is de lijst van valkuilen en risico's aanzienlijk langer dan de opgesomde voordelen. Dat neemt niet weg dat die voordelen wel degelijk de moeite waard zijn. Het is dus zaak om maatregelen te treffen die de voordelen in hun waarde laten, maar toch de risico's voor de instelling tot een aanvaardbaar niveau kunnen terugdringen. Het uiteindelijke doel is een efficiënt proces waarmee een instelling grip krijgt op de autorisaties die toegekend zijn aan haar medewerkers en studenten.

De notitie RBAC van SURFnet [SURFnet, 2010, p.18 ev.] geeft een goed overzicht van de randvoorwaarden waaraan een instelling zou moeten voldoen *voordat* een goed autorisatieproces kan worden ingericht. Ik zou daar alleen nog aan willen toevoegen dat het ook belangrijk is om een goede beschrijving van de *voornaamste bedrijfsprocessen* vastgelegd te hebben. Die beschrijving is nodig om vanuit de business aan te kunnen geven welke autorisaties door IT moeten worden gefaciliteerd. Autorisaties zijn immers een *business-verantwoordelijkheid* en geen IT-feestje.

Toegangsbeheer 3.0

In ons vakgebied is men het er wel over eens dat het autorisatieproces de autorisaties zou moeten toekennen (en weer intrekken) op basis van de rol van een individu in de organisatie: Role Based Access Control, ofwel RBAC.

De inrichting van RBAC vraagt, naast de al genoemde randvoorwaarden, een goed voorbereid proces en een aantal keuzes van de instelling. Voor het totale RBAC-proces verwijs ik naar de RBAC-documenten van SURFnet en de UM (zie kader). Een aantal van de keuzes die wellicht voor het hoger onderwijs wat specifieker liggen wil ik hieronder graag toelichten.

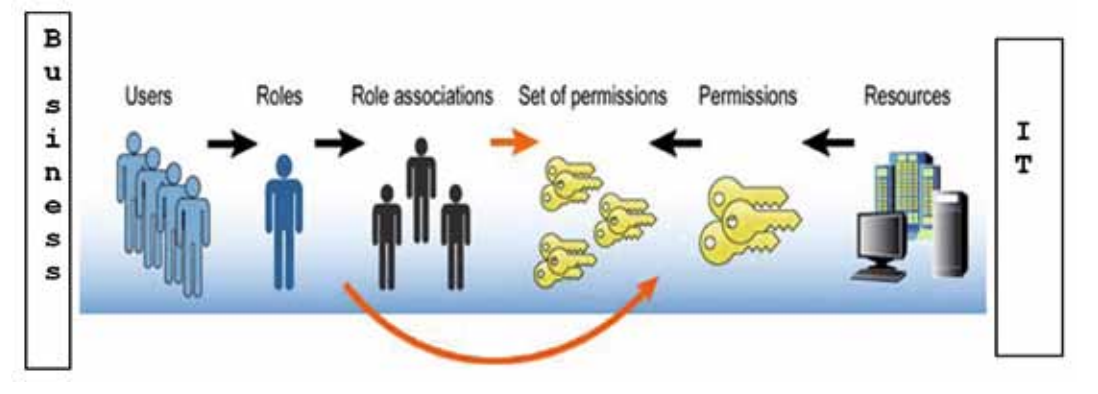
Het gebruik van een functiemodel voor basisrollen

Een functiemodel is in theorie een goede basis voor RBAC. Op basis van iemands functie kan immers worden bepaald welke resources voor deze persoon beschikbaar moeten zijn en welke rechten hij of zij daarbij nodig heeft. Bij de universiteiten wordt gebruikgemaakt van het functiemodel UFO (Universitair Functie Ordenen). In de praktijk (in ieder geval bij de UM) is het zo dat een persoon het profiel krijgt wat bij zijn of haar hoofdfunctie hoort. Maar vele medewerkers hebben meerdere deelfuncties of deeltaken en veel functies in het model zijn voor specifieke functies te generiek. Bij de UM is UFO bijvoorbeeld voornamelijk ingericht als salarismodel en daarmee is het niet geschikt als bron voor een RBAC-proces.

Advies: richt de rollen in op basis van iemands plaats in de organisatie en iemands rol(len) in de bedrijfsprocessen. Het personeel-/studentensysteem

> We zijn allemaal erg snel in het toekennen van rechten, maar voor het weer intrekken ontbreken meestal de procedures en soms zelfs het beleid

Instellingen in het hoger onderwijs hoeven gelukkig het wiel niet allemaal opnieuw uit te vinden. SURFibo werkt vanuit SURFfoundation samen met dienstenleverancier SURFnet aan een bundeling van starterkits, beleidsdocumenten en best practices ter ondersteuning van haar doelgroep. Het afgelopen jaar heeft dat ondermeer geresulteerd in de Starterkit Identitymanagement [SURFnet, okt. 2010] en de notitie Role Based Access Control [SURFnet, sept. 2010]. Het rapport UM-Autorisatiemanagement [Nobbe et al, apr. 2010], overigens opgesteld met steun van SURFnet, beschrijft het keuzeproces met betrekking tot RBAC en de specifieke keuzes daarin voor de UM



en de procesbeschrijvingen vormen dan de belangrijkste bronnen voor het RBAC-systeem.

De rollen van de Business en van IT

In het hoger onderwijs is men nog niet zo gewend om te werken met businessmodellen en de benadering dat de business (de verantwoordelijken voor het primaire proces van onderwijs en onderzoek) eindverantwoordelijk is voor de autorisaties en de afweging en eventuele acceptatie van de risico's als het gaat om de kwaliteit van het RBAC-proces (Top-Down).
De IT'ers kunnen doorgaans prima de techniek inregelen (bottom-up), maar hebben tot op heden weinig sturing gehad vanuit die business.

Advies: ontwikkel de rollen in een combinatie van top-down en bottom-up. Op die manier kunnen Business en IT van elkaar leren en elkaars referentiekader overnemen. Voor complexe processen kan dan wellicht in eerste instantie gekozen worden voor grofmazige rollen, gekoppeld aan individueel maatwerk aan de IT-zijde, waarbij pas later een verdere afbakening wordt aangebracht.

> RBAC kan er in belangrijke mate toe bijdragen dat een instelling 'In Control' is

Plan van Aanpak

Een RBAC-proces kan in theorie natuurlijk in één traject worden ontworpen in samenspraak tussen Businessmanagement en IT. Voor de meeste instellingen zal echter gelden dat er aanvankelijk niet voldoende expertise aanwezig is. Inhuren van kennis is natuurlijk een optie, maar uiteindelijk zal de werkwijze rondom RBAC moeten worden verankerd in de hele organisatie. De kennis moet dus opgebouwd worden in de eigen organisatie.

> Autorisaties zijn een businessverantwoordelijkheid en geen IT-feestje

Advies: ontwikkel het RBAC-proces in fases en organiseer per fase een aantal workshops met Informatiemanagers, Procesmanagers, Functioneel Beheerders, Key-user en IT. Richt de inspanning in eerste instantie op de beleidskaders, de generieke modellen en RBAC-deelprocessen (zoals provisioning, changemanagement en rapportage) en de hoofdrollen. Bepaal vervolgens in welke volgorde de workshops voor de vaststelling van de rollen in de verschillende bedrijfsprocessen worden gehouden. Doe dat aan de hand van de vooraf vastgestelde scope en ambitie, het risicoprofiel en de volwassenheid van de bedrijfsprocessen en de roadmap van de overige (IT-)projecten binnen de instelling.

Ter afsluiting

Het zal blijken dat RBAC inrichten voor een onderwijsinstelling een proces is van een lange adem en zorgvuldige voorbereiding. De workshops zullen in eerste instantie wellicht wat ongestructureerd verlopen omdat de deelnemers in eerste instantie niet allemaal op dezelfde golflengte zullen zitten. De workshops zullen in het begin dan ook een hoog awarenessgehalte krijgen, maar dat is ook goed. Zodra de neuzen dezelfde kant op staan wordt het makkelijker. Ook al duurt het dan nog geruime tijd (zeker meer dan een jaar) voordat de eerste processen naar behoren en zo veel mogelijk geautomatiseerd verlopen, toch kan er van het begin af aan al winst behaald worden.

Vanaf het moment dat in gezamenlijkheid is vastgesteld hoe de instelling RBAC wil gaan inrichten kan in alle processen en projecten deze manier van denken en werken al worden opgepakt. Ook al is een (legacy) systeem niet koppelbaar aan het beoogde RBAC systeem. Het RBAC-proces kan ook met traditionele middelen zoals e-mail, werkorders, handmatige instellingen en rapportages zodanig op dergelijke systemen worden toegepast dat de beoogde kwaliteitsslag wordt gehaald dat de instelling uiteindelijk 'In Control' is.

Literatuur

Nobbe, R.E., L.C. van den Heuvel, UM Autorisatiemanagement, UM, Maastricht, april 2010, beschikbaar via SURFibo www.surfibo.nl .

Role Based Access Control, SURFnet, oktober 2010, www.surfnet.nl/Documents/indi-2010-010-017%20(White%20paper%20RBAC).pdf , ingezien 5 maart 2011.

Starterkit Identity Management, SURFnet, Utrecht, september 2010.

SECURITY AWARENESS IN HET MBO

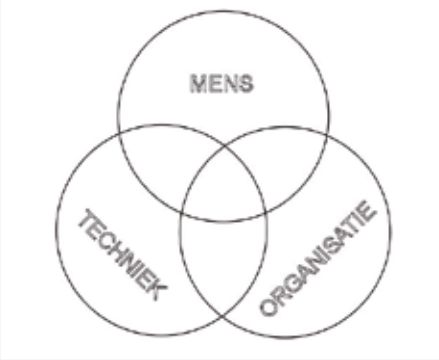
Noud Heuvelmans is coördinator Informatiebeveiliging vanuit de afdeling Informatiemanagement, onderdeel van de dienst Informatisering en Automatisering van ROC Eindhoven. Hij is onder meer verantwoordelijk voor het aandragen en opstellen van informatiebeveiligingsbeleid, maatregelen en procedures, en het houden van toezicht op handhaving.

Rein de Vries is directeur en mede-eigenaar van LBVD Informatiebeveiligers en adviseert opdrachtgevers met betrekking tot het onderwerp informatiebeveiliging. Zijn focus ligt daarbij met name op statusonderzoek en het komen tot een praktische maar toch doeltreffende invulling van informatiebeveiliging.

Vanuit informatiebeveiligingsperspectief wordt vaak het menselijk gedrag als zwakke schakel beschouwd. In sectoren met een intrinsiek 'open karakter', zoals de gezondheidszorg en het onderwijs, kunnen we wellicht zelfs spreken over de zwakste schakel. Recentelijk is voor ROC Eindhoven een bewustwordingscampagne geïnitieerd. Omdat anderen wellicht hun voordeel kunnen doen met de leerpunten, onderstaand een verslag van het doorlopen traject.

ROC Eindhoven bestaat uit 18 scholen voor middelbaar onderwijs, een school voor volwasseneneducatie en een school voor voortgezet onderwijs. Deze scholen verzorgen in totaal bijna 300 beroepsgerichte opleidingen voor circa 22.500 studenten. De scholen worden ondersteund door diensten op het gebied van onderwijsbeleid, huisvesting, financiën, personeelszaken, communicatie, ICT en projecten. Dit wordt gerealiseerd door circa 1500 personeelsleden en met een jaaromzet van circa 110 miljoen euro.
Informatie wordt gezien als een van de belangrijkste productiefactoren bij ROC Eindhoven. Het zorgvuldig omgaan met informatie(systemen) dient dan ook integraal onderdeel te zijn van de dagelijkse praktijk van alle medewerkers. Zowel in de primaire onderwijsprocessen als in de secundaire ondersteunende processen zijn er talloze voorbeelden te duiden die bijdragen aan de betrouwbaarheid van informatie.
De afgelopen jaren zijn er aanvullend op deze reguliere aandacht een aantal specifieke maatregelen geïnitieerd en/of uitgevoerd, zoals aanscherping van het wachtwoordbeleid, sterkere (2-factor) authenticatie ten behoeve van externe (VPN-)toegang voor medewerkers, herziening van het privacyreglement verwerking studentgegevens en de gedragscode gebruik ICT-middelen. In 2010 is met het vaststellen van het informatiebeveiligingsbeleid het kader bepaald voor toekomstige maatregelen en investeringen in informatiebeveiliging en de verantwoordelijkheden in de organisatie.
Het bovenstaande stelsel aan maatregelen raakt echter alleen nog maar de techniek en de organisatie. Dit is echter ontoereikend om informatiebeveiliging daadwerkelijk op het gewenste niveau te brengen en te houden. De factor 'mens' verdient evenveel aandacht als techniek en organisatie.

De factor 'mens' verdient evenveel aandacht als techniek en organisatie



Om inzicht te krijgen in het beveiligingsbewustzijn van de medewerkers is er met behulp van een enquete een nulmeting uitgevoerd.

Enquête
Maar liefst 44% van de per e-mail benaderde medewerkers heeft de enquête volledig ingevuld (42% van de medewerkers is werkzaam bij een school en 54% van de medewerkers is werkzaam bij een dienst).

In het algemeen geldt dat men 'enigszins tot redelijk bewust' (score 2 en 3 op een schaal met als maximum 4) is van het belang en de inhoud van informatiebeveiliging.

Bij de uitvoering van maatregelen en bewustwordingscampagnes ten behoeve van informatiebeveiliging verdienen met name de volgende items nog de aandacht:

- geheimhouding, identificatieplicht en anti-virussoftware worden in het algemeen herkend als onderdeel van informatiebeveiliging. Minder bekend zijn de fysieke beveiligingsmaatregelen;

- een meerderheid is zich (in meer of mindere mate) bewust van de vertrouwelijkheid van bedrijfsinformatie van ROC Eindhoven;
- nog niet iedereen vergrendelt zelf het systeem en/of sluit de deur bij het achterlaten van een lege kamer (afhankelijk van een risico-afweging);
- het is nog niet voor iedereen duidelijk waar informatiebeveiligingsincidenten gemeld dienen te worden;
- over informatiebeveiliging en de daarbij binnen ROC Eindhoven van toepassing zijnde afspraken is nog onvoldoende gecommuniceerd.

Naar aanleiding van deze bevindingen is besloten tot een bewustwordingscampagne informatiebeveiliging. Om deze maximaal effect te laten hebben helpt het als er wordt gerefereerd aan significante beveiligingsincidenten in de eigen praktijk. Omdat deze zich, voor zover bekend, gelukkig niet recentelijk hebben voorgedaan, zijn deze gecontroleerd geïnitieerd door middel van MysteryGuest-acties.

MysteryGuest

Een MysteryGuest-actie is een onderzoek waarbij een of meer specialisten (in dit geval afkomstig van LBVD) de opdracht krijgen om zichzelf als niet

bevoegd persoon toegang te verschaffen tot een doelobject van de opdrachtgever om vervolgens een specifieke missie uit te voeren. De wijze waarop dit moest plaatsvinden, het doen en laten van de MysteryGuest(s), was van tevoren nauwgezet afgestemd. MysteryGuest-acties testen in feite hoe weerbaar de organisatie is tegen eventuele onbevoegden die op welke manier dan ook trachten toegang te krijgen tot informatie. Niet alleen in digitale en papieren vorm, maar ook zoals deze vastligt in de medewerkers van de organisatie.

Velen reageren niet of amper op vreemde gedragingen van Mystery Guests

Veel is gelegen aan 'De Factor Mens'. Is men scherp, heeft men iets door? Komen medewerkers in actie of zien ze passief toe? Is men (te) loslippig? Handelt men doortastend? Ontmaskeren medewerkers de MysteryGuest nog voordat hij/zij heeft kunnen toeslaan? De uitvoering is uitgevoerd door twee samenwerkende MysteryGuests en heeft plaatsgevonden gedurende twee testdagen op twee locaties van ROC Eindhoven.

De werkzaamheden van de eerste dag waren oriënterend, inventariserend en terughoudend van aard. Hierdoor werden er geen incidenten veroorzaakt of de ware identiteit prijs gegeven. Op de tweede dag werden de grenzen opgezocht en werd bij gelegenheid bewust provocerend opgetreden tot het moment dat er tegen de lamp werd aangelopen.

Bevindingen

- Veel medewerkers reageren niet of amper op vreemde gedragingen van de MysteryGuests. Medewerkers die wél reageren vragen niet of niet ver genoeg door. Slechts een beperkt aantal medewerkers reageert zeer adequaat door naar autorisatie en/of legitimatie van de MysteryGuests te vragen of te escaleren naar bijvoorbeeld beveiliging.

- Veel kantoren waren bij afwezigheid op slot, met name waar zich ook veel studenten ophielden.

- Niet alle medewerkers vergrendelden bij het verlaten van de werkplek hun desktopsysteem of laptop.

Deze bevindingen zijn geanonimiseerd teruggekoppeld aan de directeuren van de diensten en scholen van de be-

zochte locaties en de directe 'slachtoffers' van de MysteryGuests. Daarnaast zijn de resultaten achtereenvolgend gepresenteerd aan alle directeuren en de adjunctdirecteuren Bedrijfsvoering.

Vertaling naar de praktijk geeft beveiliging betekenis

Campagne

Direct aansluitend is over alle locaties van ROC Eindhoven een bewustwordingscampagne gestart, waarbij met behulp van prikkelende teksten op posters zowel medewerkers als studenten gewezen worden op hun eigen gedrag met betrekking tot zorgvuldig omgaan met informatie.

Op de posters wordt gewezen naar 'tips & tricks' op intranet en Fronter (elektronische leeromgeving). Daarnaast is in het personeelsblad een artikel gewijd aan de MysteryGuest-acties (zie kader). De aanpak is daarbij bewust zeer sterk op de dagelijkse gang van zaken gericht door middel van aansprekende praktijkvoorbeelden. Immers, pas als de vertaling naar de eigen praktijksituatie wordt gemaakt, krijgt informatiebeveiliging betekenis.

Na afloop van de bewustwordingscampagne zal er op basis van de eerder uitgevoerde enquête worden vastgesteld hoeveel effect de bewustwordingscampagne heeft gesorteerd. De uitkomst maakt het mogelijk om de aanpak van toekomstige campagnes waar nodig bij te stellen.

Conclusie

Een MysteryGuest-actie is een zeer krachtig begin van een bewustzijnscampagne informatiebeveiliging. Via zo'n vooropgezette actie krijgt de organisatie niet alleen inzicht in de actuele kwetsbaarheid die de factor mens met zich meebrengt, maar ook waardevol materiaal uit de praktijk om de bewustzijnscampagne te voeden. Het is niet ergens gebeurd. Nee, het is ***hier*** gebeurd. De anekdotes, belevenissen en het beeldmateriaal spreken aan en zorgen voor discussie omdat het de eigen omgeving betreft. De diverse voorvallen, mits breed uitgemeten, doen de ogen openen en beseffen dat je als medewerker (of student!) er zelf deel van uitmaakt en er wat aan kunt doen.

Leerpunten en adviezen voor andere instellingen

- Laat buitenstaanders de MysteryGuest-actie uitvoeren. Volslagen vreemden die succesvol zijn geweest geven een veel groter effect dan de beveiliging die een loopronde heeft gedaan en schendingen heeft geconstateerd.
- Werk met heldere doelstellingen en onderzoeksvragen. Deze geven richting aan de MysteryGuest-actie en zorgen voor een adequate en effectieve uitvoering.
- Leg de nadruk op zones met een verhoogd risico, zoals de computerruimte en andere ruimten waar je waardevolle bedrijfsmiddelen aantreft, maar zie overige ruimten niet over het hoofd.
- Ontzie de directie- of CvB-vloer niet. Ook de directie of het CvB kan een 'target' zijn.
- Laat de MysteryGuests veel interactie met medewerkers opzoeken ('social engineeren'). Hier komen sprekende belevenissen uit voort.
- Lok tegen het einde van de actie incidenten uit die een organisatie-brede uitwerking hebben, bijvoorbeeld met inschakeling van de leidinggevende, de directeur, ICT of de beveiliging. Laat de MysteryGuest een aantal keren bewust tegen de lamp lopen, althans, *als dat lukt*!

We hopen u met dit uitneembare dossier meer inzicht te hebben gegeven in de ontwikkelingen op ons vakgebied binnen de onderwijssector. Als u deze vorm prettig vindt, willen we in de toekomst vaker een dossier in deze vorm plaatsen. Aarzel dus niet om te reageren!

Namens de redactiecommissie
Lex Borger

BOEKBESPREKING

MATURING BUSINESS INFORMATION SECURITY

Ronald van Erven

a framework to establish the desired state of security maturity

Auteur Y. Bobbert, ISBN/EAN: 978-90-815925-1-2, 256 pagina's, in het Engels

Yuri Bobbert is Managing Director van B-Able (www.b-able.nl). Een 'Business Information Security' adviesorganisatie. Naast zijn functie als directeur is Bobbert als onderzoeker verbonden aan het Information Technology Alignment & Governance Research Institute (ITAG) van de Universiteit Antwerpen. Aan het boek hebben verschillende andere autoriteiten hun medewerking verleend, zoals prof.dr. Wim van Grembergen, prof.dr. Steven de Haes, prof.dr. Hans Mulder, prof. Gilbert Silvius en dr. Said el Aoufi.

Dit boek is het resultaat van vijf jaar wetenschappelijk onderzoek naar een raamwerk voor 'business and IT (security) alignment (BIA)' en dan met het doel om een raamwerk te krijgen dat goed toepasbaar en pragmatisch is. En niet alleen voor grote bedrijven maar ook voor het middenbedrijf.

De onderzoeksvraag voor dit onderzoek was: "welke set aan methoden en maatregelen, gebaseerd op best-practices, kunnen worden toegepast om het volwassenheidsniveau, qua business security, te verhogen bij middelgrote organisaties (100 tot 2500 geautomatiseerde werkplekken)?"
Deze set aan methoden en maatregelen worden in het boek interventies genoemd. Ze moeten naast effectief ook eenvoudig te implementeren zijn, om de toepasbaarheid en acceptatie te verhogen. Zeker omdat veel raamwerken en methoden worden ervaren als academisch en niet toepasbaar door de operationele afdelingen van bedrijven.

Uit de interventies die zijn onderzocht is een zorgvuldige selectie gemaakt aan de hand van gesprekken met IT- en beveiligingsexperts, het expertpanel. De geselecteerde interventies zijn voorgelegd aan IT-managers, security managers en directeuren van diverse bedrijven.
Als best-practice basis voor interventies gebruikt de schrijver bekende modellen en raamwerken als het Business and IT Alignment maturitymodel; de ISO/IEC 27000-serie, ITIL v3 en Cobit. Deze modellen worden afgebeeld op de organisatie, cultuur en bedrijfsvoering van middelgrote bedrijven. De interventies worden getoetst op mate van implementatie in de markt en eventuele barrières die organisaties ervaren bij het implementeren worden genoemd.

Daarnaast heeft de onderzoeker de organisaties zelf suggesties laten doen over welke maatregelen hun inziens het beste bijdragen aan het verhogen van hun eigen beveiligingsvolwassenheidsniveau. Interessante conclusie is dat veel van de interventies die ze aandragen tegenstrijdig zijn met hun aangedragen barrières. Een voorbeeld hiervan op pagina 145 is dat de belangrijkste barrière kennis is bij het doorvoeren van risico- en impactanalyses en dat ze deze analyses niet doen vanwege de complexiteit ervan, maar dat ze de interventie wel als een van de meest verhogende maatregelen noteren.

Het boek vermeldt ook dat de directies van benaderde bedrijven wel hun beveiliging willen verbeteren met als doel om het klant-, en medewerkersvertrouwen en de bedrijfsintegriteit (compliance) te verhogen. Maar aandacht voor bewustwording en financiering van beveiliging blijft onder druk staan van krappe budgetten. Het gevolg hiervan is verkeerde alignment van ICT, informatiebeveiliging en de business.

Het boek is taai door de vele verwijzingen en wetenschappelijke onderbouwingen. Het beschrijft een goed onderzoek, zeker voor mensen die allang methodisch bezig zijn om de volwassenheid van hun organisatie te bepalen. De bevindingen geven een goed inzicht in hoe middelgrote organisaties tegen informatiebeveiliging en ICT aankijken. Voor mijzelf is dit een enorm leuk boek omdat ik in 2000 ben afgestudeerd op het ontwerpen van een dashboard voor informatiebeveiliging. De bepaling van de volwassenheid van informatiebeveiliging in een organisatie was daar een essentieel onderdeel van. Het is interessant om te zien hoe meningen en technieken zijn veranderd en dat zaken als bewustzijn en financiering nog steeds het punt van aandacht zijn. Wellicht moet hier specifieker onderzoek naar worden gedaan. Ik ben hiervoor beschikbaar…

ACHTER HET NIEUWS

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

INGRIJPEN IN INTERNET

Als je vindt dat het moeilijk is om de netwerken van een middelgroot bedrijf te beveiligen tegen ongewenste activiteiten, bedenk dan eens hoe dat zou zijn voor een land of voor Europa. Er is geen houden aan en de roep om vergaande mogelijkheden voor nationale of Europese autoriteiten wordt de laatste tijd regelmatig gehoord. Europa had een *cyber authoriteit* nodig die ondermeer de macht heeft IP-adressen te blokkeren. Maar ook in de Verenigde Staten werd de zogenaamde *internet kill switch* openlijk besproken. Sinds het ingrijpen van Arabische dictators in het nationale internetverkeer brokkelt de steun voor de kill switch snel af. Is dat terecht? We vroegen vier redacteuren van Informatiebeveiliging hun mening hierover.

Maarten Hartsuijker:
In een wereld waarin de digitale en de tastbare realiteit in elkaar verweven zijn geraakt, is het niet vreemd dat er wordt nagedacht over manieren waarop de digitale wereld onder controle kan worden gebracht. We zijn immers steeds afhankelijker geworden van internet en kunnen binnen ons bestaande welvaartsniveau niet meer zonder.
Als we een parallel met onze tastbare wereld trekken, dan zien we dat grensposten, handelssancties of marineschepen, die een vaarroute blokkeren om een territorium te beschermen, een normaal onderdeel van onze realiteit zijn. In dat licht bekeken is de internet kill switch als beschermer van vitale infrastructuur een bijna vanzelfsprekende maatregel tegen ongewenste invloeden van buiten. Maar de vraag is natuurlijk of dat wel echt vanzelfsprekend zou moeten zijn. Je kunt internet in het gareel van de controlemaatschappij brengen, of dromen over de wijze waarop internet ons aan een vrijere wereld helpt.

Persoonlijk hecht ik veel waarde aan vrijheid. Ik waardeer het internet om de rol die het speelt in het verspreiden en vergaren van kennis. Tegelijkertijd zie ik als informatiebeveiliger hoe kwetsbaar veel internetsystemen zijn en hoe deze kwetsbaarheden tot steeds meer risico's in onze samenleving leiden.
Tijdens een grootschalige cyberoorlog ben ik bang dat er op dat moment niet veel andere keuzes zijn dan het op grote schaal afkoppelen of reguleren van onderdelen van het internet. Om er vermoedelijk achter te komen dat het internet zoveel verbindingen kent dat de aanvallen zich vervolgens -via slimme routeringen, inbellijnen, of personen die zich op een vertrouwde locatie bevinden- vanuit onze eigen (gehackte) systemen voortzetten. Het is gelet op de huidige open inrichting van het internet een illusie om te denken dat we ons met kill switches kunnen beschermen. Om de impact van een kill switch op de reële economie acceptabel te laten zijn, zijn er te veel uitzonderingen nodig. Naar mijn mening doen overheden er daarom beter aan om de bescherming van de vitale infrastructuur te verbeteren zodat een paardenmiddel als een kill switch niet nodig is.

Rachel Marbus:
Kill de kill switch. Net als je denkt dat het echt niet erger kan worden met de staatsinmenging in het privéleven van burgers, roept 'men' dat er een kill switch zou moeten komen waardoor het mogelijk wordt om – in geval van een extreme crisissituatie – het internet even uit te zetten. Pardon? Dat lijkt me ten eerste een duidelijk geval van een draconische maatregel waarvan het effect nog maar eens moet blijken. Als Egypte ons een ding geleerd heeft, dan is het wel dat online communicatie niet tegen te houden is (en kwaadwillende boeven dus ook niet, in ieder geval niet op deze manier). Na de kill aldaar duurde het maar even voor de eerste ouderwetse inbellijnen beschikbaar werden gesteld en het nieuws vanuit Egypte weer naar buiten kon lekken.
Ten tweede maak ik me ernstige zorgen over deze inperking van de rechten en vrijheden van burgers. Wie garandeert mij dat de overheid niet willekeurig het internet gaat uitzetten als het even beter uitkomt zo? En wanneer is er dan eigenlijk sprake van een extreme crisissituatie en wie bepaalt dat? En, wie controleert de bepaler? Ik ben misschien niet zo goed van vertrouwen, maar daar geeft het nieuws me dan ook helaas wel aanleiding toe. De veiligheidsretoriek druipt van bijna alle politieke statements af. Ja, inderdaad, als veiligheid wordt afgezet tegenover privacy, delft de laatste vaak het onderspit. Ten dele wordt dat veroorzaakt door het feit dat het om ongelijke waarden gaat,

waarbij 'veiligheid' een meer primaire levensbehoefte is en daardoor bijna automatisch zal voorgaan. Dat is een vrij normale en ook menselijke reactie. Daarmee verband houdend, denken burgers dat zij ook echt veiliger zijn door alle voorgestelde maatregels. En dat blijkt in de praktijk nog best tegen te vallen. Een kill switch? Liever niet, lijkt me hartstikke gevaarlijk voor de privacy, vrijheid van meningsuiting en de democratie!

Ronald van Erven: De internet kill switch (IKS) is een goed idee maar bij de implementatie en activering plaats ik een paar kanttekeningen.
Ten eerste: wie bepaalt wanneer de IKS wordt geactiveerd? Gelet op de toenemende afhankelijkheid van internet kan het niet zo zijn dat een ministerie bepaalt de IKS te activeren. Wat ik mij voorstel is dat, net als bij de lancering van een atoomraket vanaf een onderzeeër, twee mensen tegelijkertijd hun sleutels om moeten draaien om de IKS te activeren. En dan nog enkel als er een streng protocol en risico-inschatting zijn doorlopen.
Een vaste partij heeft altijd een sleutel, bijvoorbeeld het nog op te zetten ministerie van Informatie en Informatiebeveiliging. Daarnaast twee partijen zoals het ministerie van Economische Zaken en het ministerie van Justitie. De vaste partij en een van de andere partijen moeten hun sleutel omdraaien om de IKS te activeren. Het ministerie van Economische Zaken bewaakt de bedrijfsbelangen en het ministerie van Justitie moet waken dat de privacy en vrijheid van meningsuiting niet in gevaar komt.
Ten tweede: hoe kan de schade worden verhaald? Er zullen afspraken moeten worden gemaakt voor personen en bedrijven om de schade te verhalen indien de IKS onterecht is geactiveerd. Wellicht moeten we een apart IKS-fonds oprichten waaruit de schade kan worden betaald.
Ten slotte: kan Nederland de IKS zelfstandig activeren? Natuurlijk kan Nederland het IKS zelfstandig activeren. Of dit verstandig is, is een ander verhaal. Niet alleen qua economische concurrentie ten opzichte van de omringende landen is dit een risico maar ook qua achterdeuren naar internet. Denk hierbij aan 3G-verbindingen in de grensstreek, satellietcommunicatie of radioamateurs. Mensen uit de grensstreken kunnen een soort 'ondergrondse' gateway gaan opzetten om de reguliere en gecontroleerde kanalen te omzeilen. De IKS moet dus met een totaal pakket aan stoorzenders en signaal blokkeerders worden uitgerust en Nederland zal in Europees verband afspraken moeten maken.
Kortom, IKS een goed idee maar met kanttekeningen die opgelost moeten worden maar wel oplosbaar zijn.

André Koot: Do Not press this button. Die internet kill switch lijkt me een grandioos ding. Ik kan me nog levendig een stripverhaal van Guust Flater herinneren, met Guust die in een gang een rode knop ziet met het opschrift **Niet Indrukken**. Je weet van tevoren wat dat betekent, ik hoef vast die laatste tekening niet te beschrijven. En zo´n soort ding moet dus ook die internet kill switch zijn. Indrukken maar en de hele wereld komt tot stilstand. Want zo mag je die toestand dan toch wel noemen.
Eigenlijk vind ik het wel prima, laat de Amerikaanse president op grond van de Protecting Cyberspace as a National Asset Act (PCNAA) het internet maar platgooien, maar dan natuurlijk alleen dat deel waar hij iets over te zeggen heeft, binnen het grondgebied van zijn grondwet. Plat is plat. Bespaart ons heel veel spam, malware, porno, hackers, advertenties en een heleboel hypocrisie. Maar helaas werkt het internet niet zo. De digitale snelweg lijkt in niets op een gewone snelweg die je even dicht kunt gooien. Want wij hebben er direct last van als er in Amerika iets gebeurt. Tenminste, als het aankomt op de hoofdstructuur van het internet. Een enkele ramp, ach daar kunnen we wel mee leven. Op 11 september bleef internet toch gewoon doordraaien?
Maar het idee dat de president op een hoger infrastructureel niveau wil ingrijpen, dat baart me zorgen. Door cyberspace als een 'National Asset' te beschouwen geeft Amerika blijk van zo´n grote naïviteit dat we dáár eigenlijk bang voor moeten zijn. Die knop is niet zo erg, maar het beeld dat de hele wereld om Amerika draait, dat is ernstig.
Dat PCNAA-gedoe zouden we volgens mij niet moeten tegengaan, maar juist aangrijpen om het beheer over het internet aan de orde te stellen. Cyberspace is niet van de Amerikanen, het is van zes miljard mensen (mits ze een netwerkaansluiting hebben natuurlijk).

Links:

Turn off the internet. http://www.turnofftheinternet.com. Accessed: 2011-03-08. (Archived at www.webcitation.org/5x2ZMkoAC)

S.3480 - Protecting Cyberspace as a National Asset Act of 2010. www.opencongress.org/bill/111-s3480/. Accessed: 2011-03-08. (Archived at www.webcitation.org/5x2Znq4ti)

ARTIKEL VAN HET JAAR 2010

Net voor de kopijafsluiting ontvingen wij het juryrapport over het artikel van het jaar 2010. Deze uitslag willen we de lezers niet onthouden. Zeker omdat deze uitgave net na de uitreiking bij iedereen in de bus zal liggen. Ik realiseer me dat bezoekers van de ledenvergadering en fervente twitteraars de uitslag dan al vernomen hebben. Het is opvallend dat sinds de bijeenkomst over sociale media het gebruik van de hashtag #pvib en het adres @pvib flink zijn toegenomen.

De uitslag
1e plaats: het artikel van Jan de Boer, De misleider te werk.
2e plaats: het artikel van Cor Rosielle, Trust audits.
3e plaats: het artikel van J.M.T. Wijnberg, Paspoortwet brengt burgers in gevaar.

De redactie feliciteert de drie prijswinnaars van harte.

Het juryrapport wordt in de volgende uitgave volledig geplaatst, samen met een verslag van de uitreiking van de prijzen op 19 april op de PvIB-bijeenkomst na de ledenvergadering en voor het avondprogramma.

'REKENEN AAN MALWARE' WINT OOK PRIJS

Nog voordat onze jury met een resultaat kwam, bereikte ons het bericht dat een artikel dat vorig jaar in Informatiebeveiliging stond een prijs gewonnen heeft. Het gaat hier om een artikel dat ook in het blad 'Intercom' van de Vereniging Officieren Verbindingsdienst is gepubliceerd. Het is deze versie die een prijs heeft verdient. Het artikel waar het om gaat is 'Rekenen aan Malware' van Henk-Jan van der Molen, wat ook in Informatiebeveiliging nummer 6 van vorig jaar is gepubliceerd. De jury van Intercom had de volgende motivering:

"In het artikel Rekenen aan malware slaagt de schrijver er in een actueel probleem dat ook defensie raakt, de bedreiging van netwerken door malware, te operationaliseren. Met behulp van een eenvoudig mathematisch model maakt hij de relatie tussen malware, besmettingen en te nemen veiligheidsmaatregelen inzichtelijk. Juist het evenwicht tussen theorie en praktijk maakt het artikel origineel. Daarnaast is het artikel goed gestructureerd, voorzien van een aantal functionele figuren respectievelijk, formules en helder geschreven."

Opmerkelijk is dat dit artikel niet eens is genomineerd voor artikel van het jaar in Informatiebeveiliging. In mijn ogen zegt dit iets over de hoge kwaliteit van de artikelen van vorig jaar. De redactie vond het ook niet makkelijk om tot een nominatie te komen.
De redactie feliciteert ook Henk-Jan van harte met dit resultaat! Wij hopen nog vaker een artikel van zijn hand te mogen publiceren.

COLOFON

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

Redactie
Lex Borger (hoofdredactie, werkzaam bij Domus Technica),
e-mail: lex.borger@domustechnica.com
Cynthia Kremer (eindredactie,
Motivation Office Support bv, Nijkerk)
e-mail: ibmagazine@pvib.nl

Redactieraad
Said El Aoufi (Metapoint)
Tom Bakker (Delta Lloyd)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Rob Greuter
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
André Koot (Univé-VGZ-IZA-Trias)
Rachel Marbus (KPMG, IT Advisory)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving en druk
Van de Ridder Druk & Print, Nijkerk
www.vanderidder.nl

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

Abonnementen
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

DE INTERNETREVOLUTIE

Een jaar of twintig geleden begonnen voor mij de eerste stappen op het world wide web en in die pioniersfase was het een hele kunst om met je 14K4 modempje connectie te maken met het web. Ik wil jullie graag besparen welke stappen er allemaal uitgevoerd moesten worden om uiteindelijk je eerste www-adres te kunnen invoeren, maar neem van mij aan dat je best wel trots was als je uiteindelijk de eerste websites kon bekijken. Het was een verademing nadat ik jaren op bulletin boards mijn software had gehaald voor mijn Commodore 64. De tijden zijn in die 20 jaar fors gewijzigd – behalve dan het bosje bloemen die ik altijd meenam voor mijn vrouw om haar af te koelen nadat ze de rekening van de KPN (toen nog PTT) had gezien. Vermogens heb ik in die jaren gestoken in dit bedrijf en ik kan mij ook wel voorstellen dat dit bedrijf in problemen kwam toen ik overging op ADSL. Dat het internet de wereld heeft veranderd is natuurlijk duidelijk. Ik wil toch een aantal voorbeelden noemen waaruit dat blijkt. De mogelijkheden om prijzen en kwaliteit van producten te vergelijken is enorm geworden, een televisie van merk X en type Y is overal hetzelfde, de prijs echter niet. Ik ben vast niet de enige die bij de Mediamarkt aangeeft dat ik de bewuste televisie wel mee wil nemen maar dat de prijs wel te hoog is en dat ik niet het op het kaartje geschreven bedrag wil betalen. Het (door mij) veel gehoorde antwoord van de leverancier op een vraag of klacht dat hij zegt dit nog nooit meegemaakt te hebben kan ik snel ontzenuwen want de diverse forums op het internet geven mij aan dat de klacht die ik over een bepaald product heb ook door anderen worden gevoeld.

Een enorme impact heeft het internet op de creatieve en artistieke medemens. Een popartiest moet het tegenwoordig niet meer hebben van de verkoop van zijn platen maar moet zijn inkomsten uit de concerten halen. Het verkoopsucces van Michael Jacksons 'Thriller' zal nooit meer worden geëvenaard. Hetzelfde geldt voor speelfilms en boeken. Het laatste boek van Kluun is op internet wel te krijgen, maar in de boekhandel is deze tijdelijk even uitverkocht.

Met deze voorbeelden geef ik aan dat de wereld sterk is gewijzigd en nog veel meer zal wijzigen. Ik juich dat toe, ik vind het fantastisch, maar er zijn natuurlijk ook voorbeelden te bedenken waar men niet zo blij is met deze openheid. In China bijvoorbeeld worden alle websites geblocked, ze zijn alleen te bekijken als een commissie van wijze mannen heeft bepaald dat de inhoud van de site niet schadelijk is voor de bewoners van China. Deze methodiek gaat natuurlijk tekort schieten, want Twitter en andere snelle communicatiemiddelen laten zich niet censureren.

Andere wereldleiders dachten dat het allemaal zo'n vaart niet zou lopen, hun dictatoriale opstelling ging vaak gepaard met een schrikbewind waarbij de wereldleiders zich schandalig verrijkten ten koste van de eigen bevolking. Deze wereldleiders zitten al jaren op de troon en laten zich opvolgen door hun zoon of een metgezel die uit het bevriende kamp komt. Oppositie tegen deze wereldleiders is lastig als je dit niet goed organiseert, maar het blijkt dat daar inmiddels sterk verandering in is gekomen. Vandaag kunnen we door het onvolprezen internet laten zien dat er tegenstand is tegen een regime. We twitteren dat rond, we sms'en, we plaatsen een filmpje op YouTube, we maken een forum en tegen de tijd dat de wereldleider door begint te krijgen dat hij meer en meer openlijke tegenstanders krijgt is hij vaak te laat.

Angstig om het pluche te moeten verlaten en de gouden badkranen over te dragen aan zijn opvolger doet hij een laatste wilde poging die bij voorbaat al tot mislukken is gedoemd. Hij sluit alle internetverbindingen in zijn land, de telefonie, de televisiestations en de radiostations maar daarmee krijgt hij zijn volk niet meer rustig. Nieuwszenders uit het buitenland worden nog ontvangen op de schotels, gruwelijkheden die op een telefoon zijn gefilmd zien we even later terug op tv die zijn signaal uit de lucht plukt, buitenlandse radiozenders zijn continu bezig berichten de ether in te sturen. Het ene regime is nog niet gevallen of de onrust gaat over de grens verder naar een ander land. Geen dictator voelt zich nog veilig. De eerste demonstraties worden uiteen geslagen, maar dan is het kwaad al geschied, de beelden staan op de telefoons en worden verspreid. Anderen zien die beelden en geven hun innerlijke woede de ruimte en doen mee.

Groeten,
Berry

[hiddn]™ ENCRYPTIE

* Volledige AES encryptie
* OS onafhankelijk
* 2 factor authenticatie
* Geen software/drivers nodig
* NATO restricted

[hiddn]™ Crypto Adapter

Maak iedere USB stick volledig hardwarematig versleuteld

[hiddn]™ LapTop

Slaapt u lekker als uw laptop is gestolen?

[hiddn]™ DeskTop

Partitioneerbare encryptie voor één of twee SATA Disks

[hiddn]™ SATA Adapter

Bescherming van printers, kopieer-machines en office werkstations

[hiddn]™ KMS

Management van encryptie sleutels en tokens

[hiddn]™ USB

De ideale oplossing voor secure back-up en forensics

Common Criteria EAL 4+

FIPS 140-2 Level 3

NATO Restricted

BEL NU VOOR EEN EVALUATIE!

CRYPSYS Data Security is de expert op het gebied van security oplossingen en distributeur van High Density Devices. Neem contact met ons op via sales@crypsys.nl of via 018 362 44 44 voor een evaluatie! Kijk voor meer informatie op www.crypsys.nl.

CRYPSYS data security