iB

INFORMATIEBEVEILIGING

jaargang 15 - 2015

#5

CSIRT Maturity Kit

Cybersecurity in de boardroom

Interview Digidentity

Innovatieve vingerafdruktechnologie pakt fraude aan

Verslag IDnext-event

Security Analyst - SOC Specialist

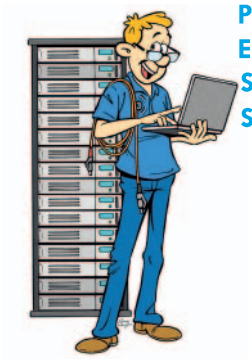
Secure Labs
Security Analyses & Audits

Malware &
Root Cause Analyses
Big Data
Highly skilled
Teamwork

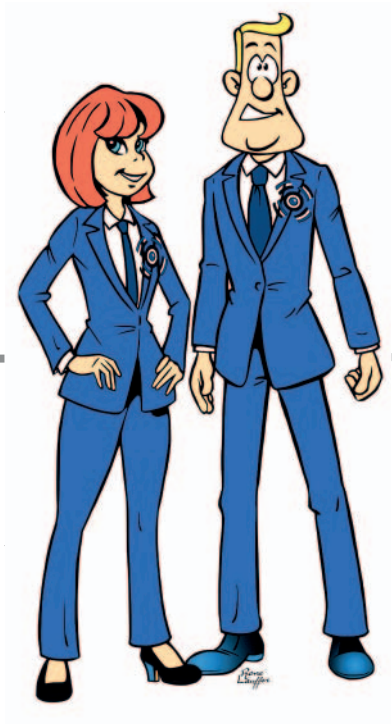
Locatie

4 vestigingen in Nederland en België.

Vulnerability management



Penetratietesten
Ethical hacking
Security audits
Systeem audits



"Naar hartenlust experimenteren in een lab met state-of-the-art apparatuur"

"Handelen met de snelheid van het licht"

Secure Link
Infrastructure Security Solutions

GREAT PLACE TO WORK Best Workplaces 2014
Securelink Nederland B.V.

Opgericht in **2003**
200 enthousiaste SecureLinkers!

Positieve gedreven, **no-nonsense** organisatie

Detail • Klantgerichtheid
Respect • Commitment
Bezieling • Creativiteit
Enthousiasme

Secure UNIVERSITY

"Maak het onzichtbare zichtbaar"

Interesse? Neem contact op via T +31 88 1234 200
of mail naar jobs@securelink.nl.

DE CRYPTO VAN LASTPASS

LastPass is gehacked. Gebruikers zijn boos en teleurgesteld. Maar iedereen kan toch gehacked worden? Als je publicaties op het Cybersecurity Beeld Nederland leest, dan kun je er maar beter van uitgaan dat je al gehacked bent. Het gaat dus meer over hoe je er mee omgaat, dan of je gehacked wordt.

Als jouw dienst is een online wachtwoordenkluis te beheren voor je gebruikers, dat kun je maar beter je cryptografie goed implementeren en beheren. Ze lijken goed omgegaan te zijn met de hack: Maak het bekend, ga uit van het ergste, maar blijf realistisch [1].

Veel bedrijven doen hun cryptogebruik af met "uw informatie is versleuteld met de beste cryptografie", of iets genuanceerder: "uw informatie wordt versleuteld met AES-256". LastPass doet het anders. Ze leggen exact uit wat ze doen en waarom: eerst duizenden rondes PBKDF2-SHA-256 op de cliënt uitvoeren om een niet-terugrekenbaar wachtwoord-hash aan te maken die de kluis ontsluit. Vervolgens cryptografisch zout toevoegen en 100 duizend keer hashen om het resultaat op te slaan in hun gebruikersdatabase. Dit is praktisch niet te kraken. Daarom geven ze ook aan dat "... if you used your master password for any other website, we do advise changing it – on LastPass as well as on the other websites." Ze hebben in hun infrastructuur de risico's zodanig teruggebracht dat de grootste risico nu bij de gebruiker liggen: wachtwoord hergebruik of een te eenvoudig wachtwoord gebruiken.

Toch is dit ook niet perfect, want niet iedereen begrijpt het. Vorige week kreeg ik weer een opmerking over de "schandalige hack van LastPass". En dan merk je dat begrip van de basisbewerkingen van cryptografie en hun toepassing toch niet breed genoeg begrepen worden. Dat is een uitdaging die breder is dan wat LastPass kan aanpakken. Voor de leken zeggen ze nog wel "Cracking our algorithms is extremely difficult, even for the strongest of computers", maar dan moet je wel daarop vertrouwen.

Het is duidelijk dat LastPass zijn basis goed heeft neergezet: een goede business impact analyse, goed gebruik van cryptografie, goede communicatie naar de gebruikers. Dan mag je gehacked worden, denk ik dan maar.

Lex Borger, hoofdredacteur

Links

[1] https://blog.lastpass.com/nl/2015/06/lastpass-security-notice.html/

In dit nummer

CSIRT MATURITY KIT

Best practices om cyber-security-incident-response te verbeteren.

Het NCSC neemt als gevestigd "Cyber Security Incident Response Team" (CSIRT) graag de verantwoordelijkheid om CSIRT-maturity wereldwijd te verbeteren. Hiermee helpt NCSC-NL landen en organisaties om weerbaarder te worden tegen digitale dreigingen. Dit is ook onderdeel van het grotere capacity-building-initiatief dat binnen de CSIRT-gemeenschap wordt omarmd om individuele organisaties en landen beter in staat te stellen om adequaat te reageren op cyberdreigingen, en daarmee dus te werken aan de slagkracht van de CSIRT- en securitygemeenschap in Nederland en wereldwijd.

Op 16 en 17 april 2015 was Nederland gastheer van de vierde Global Conference on Cyber Space (GCCS2015). Onderdeel en deliverable van deze GCCS was het Global Forum of Cyber Expertise (GFCE) [1]. Het GFCE is opgezet als de verzamelplek waar landen initiatieven kunnen delen en ideeën kunnen opdoen om hun capaciteit op het gebied van cyberspace te versterken. Het doel van het GFCE is om expertise op een zo breed mogelijk scala aan onderwerpen binnen cyberspace te kunnen bundelen en zo mondiaal samenwerking op het onderwerp te kunnen stimuleren. Voorafgaand aan de GCCS, tijdens de NCSC-ONE-conferentie op 13 en 14 april [2], zijn drie Nederlandse initiatieven gepresenteerd en behandeld met als doel deze te lanceren binnen het GFCE. Één van deze initiatieven is de CSIRT Maturity Kit (CMK). Dit artikel beschrijft de reden waarom het NCSC is gestart met dit CMK-initiatief en waarom het als solide basis gebruikt kan worden door startende CSIRTS, maar ook als baken voor gevorderde teams om hun maturity te vergroten. Om beter te kunnen bepalen hoe bruikbaar de CMK is in je eigen situatie, sluiten we af met een korte beschrijving van de inhoud per hoofdstuk.

CSIRT

Elke organisatie is een complex geheel dat zorgvuldig moet worden bestuurd en beveiligd. Voor dat laatste kennen we direct onder het bestuursniveau de C(I)SO, de onafhankelijk opererende "linking pin" qua informatiebeveiliging tussen het bestuur en de rest van de organisatie. Om te kunnen zien wat er allemaal gebeurt op het netwerk, hebben veel organisaties een Network Operations Center (NOC) opgericht. Hier wordt gekeken hoe het netwerk draait en of de continuïteit gewaarborgd kan blijven. Veel organisaties hebben als aanvulling op het NOC een Security Operations Center (SOC), waar met behulp van verschillende technische detectie- en monitoringmiddelen netwerkverkeer wordt gecontroleerd op mogelijke dreigingen voor de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en systemen binnen het netwerk.

Steeds vaker richten organisaties ook een "Cyber Security Incident Response Team" of CSIRT op – we hebben in die term "computer" bewust vervangen door "cyber" – om de security-incidenten die worden aangemeld van binnen of buiten de eigen organisatie, te onderzoeken en te verhelpen. Het gaat bij de CSIRT om cyberincidentmanagement in de breedste zin des woords – het voorkomen én genezen van IB-incidenten. En het gaat niet alleen om de bescherming van de bekende drie "BIV"-aspecten, maar om de bescherming van de organisatie in alle facetten, inclusief reputatie en vertrouwen. Daarnaast is bij ernstige incidenten een direct contact met de bestuurslaag noodzakelijk, zonder tussenkomst van hiërarchie. De CSIRT stijgt daarmee uit boven een reguliere ICT-functie, en we zien dan ook steeds vaker dat de CSIRT als staffunctie wordt ingericht, bijvoorbeeld in het "C(I)SO office".

CSIRT's bestaan, zoals we later in dit artikel zullen zien, op verschillende niveaus bij verschillende typen organisaties. Naast overheid teams zoals onze nationale NCSC-NL, en teams van andere landen, zoals NCSC-FI, CERT-UK, US-CERT en CERT.BR, hebben ook grote en minder grote bedrijven een eigen CSIRT. Denk hierbij aan telecomaanbieders, banken en organisaties in andere vitale sectoren binnen Nederland, universiteiten, research/educatie netwerken zoals SURFnet en IT/software "vendors".

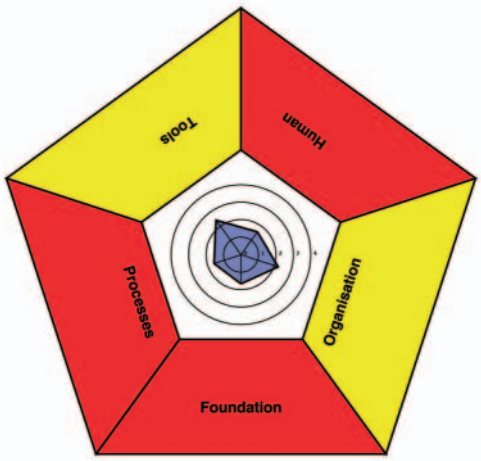
Het opzetten van een CSIRT is geen triviale taak. Het is een proces waarbij rekening moet worden gehouden met veel variabelen. Hiernaast is er online een grote hoeveelheid documentatie beschikbaar, waaruit maar moeilijk een consistente boodschap kan worden gedestilleerd. Tot slot is een CSIRT pas toekomstvast wanneer hij zowel binnen de eigen organisatie is geborgd op bestuursniveau, als daarbuiten de goede contacten heeft gelegd om vroegtijdig informatie te krijgen – maar ook te brengen, want "wederkerigheid met gesloten beurzen" is een cruciaal principe binnen de CSIRT-gemeenschap.

Één van de initiatieven die Nederland - met behulp van het NCSC - heeft ingebracht bij het GFCE is de CSIRT Maturity Kit [3]. De CMK is geen kookboek en geen kant-en-klare handleiding hoe een organisatie een CSIRT opzet. Het is een logisch gerangschikte verzameling zorgvuldig gekozen best practices, waarmee een organisatie wel meteen aan de slag kan bij de inrichting of verbetering van hun CSIRT-functie.

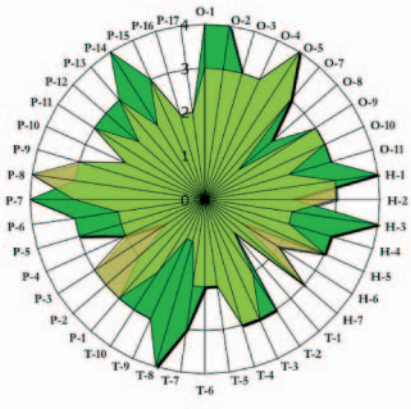
Martijn de Hamer is in 2000 gaan werken voor een commerciële ICT-dienstverlener, waarvoor hij bij verschillende klanten een groot aantal opdrachten gedaan als security-consultant. In 2006 is hij overgestapt naar GOVCERT.NL/NCSC en heeft daar verschillende werkzaamheden gedaan in de rol van senior security specialist. Momenteel is Martijn coördinator van een van de operationele clusters binnen het NCSC en is hij actief in verschillende capacity-building-initiatieven en draagt bij aan de verdere ontwikkeling en professionalisering van CSIRT's wereldwijd. Hij is bereikbaar via Martijn.deHamer@ncsc.nl

CSIRT Maturity Kit

De CMK is gebaseerd op twee waardevolle pijlers. Allereerst zijn daar de best practices, een staalkaart aan resultaten uit de internationale CSIRT-gemeenschap. Dit alles gebaseerd op publiek beschikbare en door CSIRT-experts ontwikkelde teksten. Gezamenlijk vertegenwoordigen deze teksten 25 jaar ervaring in het opzetten en opereren van CSIRT's voor wisselende doelgroepen in een veranderende tijd, overal ter wereld. Er is immers veel gebeurd sinds het uitbreken van de Morris-worm en de hierop volgende oprichting van CERT/CC in 1988. De CMK wijst naar praktische handvatten om organisaties met de juiste argumenten, de juiste keuzes te laten maken.
Een tweede pijler is de onderliggende structuur. Deze is gebaseerd op het SIM3 (Security Incident Management Maturity Model) [4] , zoals gebruikt binnen de TF-CSIRT Trusted Introducer, het Europese verband van CSIRT's [5]. SIM3 biedt een model waarmee een CSIRT op een consistente en beproefde manier haar eigen volwassenheid kan toetsen. Een organisatie kan zich tevens laten certificeren op basis van dit model – binnen Europa zijn thans 14 teams gecertificeerd , waaronder NCSC-NL [6]. Doordat de CMK geënt is op de SIM3-structuur, kan het werk dat wordt uitgevoerd bij het doorlopen ervan eenvoudig worden getoetst binnen een SIM3-self-assessment. Hiermee kan de organisatie alvast voorsorteren op een eventuele SIM3-certificering.
Naast de CMK is er de "Quick Scan" [7]. Dit is een online vragenlijst, waarmee een CSIRT organisatie de mogelijkheid krijgt om in korte tijd een idee te krijgen van haar huidige volwassenheid. Het gaat hier om een snelle meting, waarvan de resultaten bedoeld zijn als managementtool – het is geen vervanging van een SIM3-self-assessment. De resultaten van zowel de Quick Scan als van een SIM3-assessment zijn grafisch weer te geven, zie figuren 1 en 2.



Figuur 1 - Voorbeeld resultaat Quick Scan



Figuur 2 - Voorbeeld resultaat SIM3-assessment

Ontstaan

De CSIRT Maturity Kit is tot stand gekomen door nauw samen te werken met verschillende organisaties, die wereldwijd hun sporen op het gebied van CSIRT-werk ruimschoots hebben verdiend. Er is gebruik gemaakt van de documentatie die deze organisaties op diverse terreinen hebben uitgebracht. Verder zijn er uitvoerige gesprekken geweest met zowel gevestigde als nieuwe en opkomende CSIRT's. Een uitgebreide review-groep heeft bijgedragen aan inhoud en kwaliteit. Een aantal van deze reviewers zijn ook tijdens de GCCS2015 in een panel het gesprek met de security-gemeenschap aangegaan om de rationale achter de boodschap te bespreken.
De CMK is een levend document. Dit betekent dat het niet klaar is met het uitbrengen van een gedrukt exemplaar. De organisaties die betrokken zijn geweest bij het maken ervan hebben hun commitment afgegeven om het document aan te passen en te verbeteren wanneer hiervoor een aanleiding is.

Don Stikvoort was in zijn SURFnet jaren één van Europa's Internet pioniers sinds 1989 en werd toen ook al snel actief in beveiliging. Hij begon zijn eigen bedrijf in 1998. Don is grondlegger van de Europese samenwerking van CSIRT's en "founding father" van NCSC-NL en diverse andere teams. Thans is hij partner in m7 en internationaal actief in IB, als consultant, trainer en keynote-spreker. Daarnaast is Don actief als management- en "life"-coach en is trainer in NLP, coaching, communicatie en effectieve psychotherapie. Hij is bereikbaar via don@m-7.nl

Hiernaast wordt de CMK ook op verschillende podia op verschillende manieren onder de aandacht gebracht, in binnen- en buitenland. Denk hierbij aan artikelen zoals dit, workshops, panels en presentaties.

Structuur

De CSIRT Maturity Kit geeft een organisatie concrete handvatten om een CSIRT op te zetten. Hierbij wordt de basisstructuur van SIM3 gevolgd, waar "Foundation" als inleidend thema aan is toegevoegd, gevolgd door "Organisation", "Human Aspects", "Tools" en "Processes". Hieronder beschrijven we kort per thema wat de achterliggende gedachte per punt is.

1) Foundation

Bij het opzetten van een CSIRT moet een plan worden gemaakt en een aantal fundamentele keuzes worden ingevuld. Het businessplan moet aansluiten bij de strategie van de organisatie – op land-niveau is dat de nationale cyber-security-strategie. In het plan moeten de belangrijkste "stakeholders" benoemd worden en een strategie en tactiek naar voren komen hoe deze partijen te overtuigen c.q. met hen samen te werken. Ook is het belangrijk om het plan tegen de eigen juridische kaders te toetsen. In dit hoofdstuk zijn verschillende praktijkvoorbeelden opgenomen, die een mogelijke aanpak laten zien.
Een onderschat onderdeel van het thema Foundation, is dat de ophanging binnen de eigen organisatie bepalend is voor het succes van de CSIRT. De CSIRT als ICT-functie zien is te beperkt en stelt de CSIRT niet in staat haar waarde te tonen – zelfs als de CSIRT binnen ICT is opgehangen, dienen zaken als governance, mandatering en escalaties een directe wisselwerking met het bestuursniveau te kennen, bijvoorbeeld langs de weg van de C(I)SO.

2) Organisation

De basis van de CSIRT wordt het beste gelegd in een charter of "organisational framework" die verankerd wordt op bestuursniveau. Dit document wordt samen met vertegenwoordigers van de relevante afdelingen binnen de organisatie opgesteld en bevat informatie over governance, mandaat, doelgroep, escalatielijnen, rapportage en auditing. Ook worden in dit document de diensten beschreven die de CSIRT aan haar doelgroepen levert.
De diensten die de CSIRT kan bieden worden geselecteerd uit een lijst die is opgesteld door CERT/CC. Deze lijst is in de beginjaren van de CSIRT-gemeenschap opgesteld en voldoet niet meer volledig in onze veranderende wereld. Om die reden wordt deze lijst momenteel herzien door vertegenwoordigers uit de internationale CSIRT-gemeenschap onder leiding van het Forum of Incident Response and Security Teams (FIRST) [8].
Één van de meest belangrijke activiteiten waarin een CSIRT moet investeren, is bekend raken in de CSIRT-gemeenschap. De belangrijkste stap in het proces van het opzetten van een CSIRT, is het besef dat de organisatie een onderdeel is van een groter geheel, de CSIRT-gemeenschap. De enige manier om incidenten te voorkomen en verhelpen is door te participeren in deze gemeenschap. Hoewel het bij het opzetten van de CSIRT nuttig is om te leren van soortgelijke organisaties – van hun fouten en van hun succes - is het in de dagelijkse operatie van essentieel belang om de contacten te onderhouden.
Er is een aantal belangrijke nationale en internationale netwerken waar een zichzelf vestigende CSIRT bij kan aansluiten. De snelheid waarmee de organisatie wordt opgenomen in een netwerk wordt bepaald door de mate van participatie en de mate van ernst waarmee informatie en andere resources worden opgenomen - én gedeeld! Delen met elkaar is cruciaal binnen de CSIRT-gemeenschap, en vertrouwen is de Haarlemmer Olie voor dat delen.

3) Human Aspects

De mens is het grootste kapitaal van de CSIRT. De medewerkers van een CSIRT hebben specifieke en specialistische kennis nodig in verschillende gebieden. Deze kennis is slechts voor een beperkt deel technisch. Organisatorische, sociale, persoonlijke en met name communicatie vaardigheden zijn onmisbaar om de CSIRT zowel intern als naar buiten toe tot een succes te maken. Een adequate beschrijving van vaardigheden en kennis zou als leidraad moeten dienen voor het werven én opleiden van nieuwe medewerkers. Hoewel opleiding en training niet goedkoop is, is het CSIRT-werk dusdanig veelzijdig en tegelijk specialistisch, dat investering op dit gebied noodzakelijk is: met name de technische en communicatieve vaardigheden vereisen veelal scholing en oefening. De medewerker moet ook zelf, vooral relationeel, investeren om het netwerk en de nodige kennis op te bouwen via cursussen, trainingen, oefeningen en conferentiebezoek.
Naast kennis en vaardigheden zijn ook eigenschappen als betrouwbaarheid en consistentie in het werk belangrijk om het vertrouwen van de doelgroep organisaties op te bouwen en te behouden. Wanneer het vertrouwen door doelgroepen en partners op enigerlei wijze ernstig wordt geschaad, zullen geen incidenten meer worden gemeld en droogt de informatiestroom op en wordt het bestaansrecht van de CSIRT bedreigd. Om vertrouwen op te bouwen en te onderhouden, is regelmatige en kwalitatief goede interactie tussen de medewerkers van de verschillende organisaties nodig.

4) Tools

Wanneer bekend is wat voor diensten de CSIRT gaat leveren en welke activiteiten de medewerkers hiervoor zullen moeten uitvoeren, kan ook bepaald worden welke tools hiervoor nodig zijn. Binnen de security-gemeenschap is een groot aantal tools

De CSIRT Maturity Kit biedt een logisch raamwerk om de kennis uit de bestaande documenten te kunnen plaatsen en zo effectief mogelijk in te kunnen zetten.

beschikbaar om een grote hoeveelheid specifieke taken uit te voeren. Veel van de tools die nodig zijn binnen een CSIRT worden ontwikkeld, gebruikt en gedeeld met partnerorganisaties. Hierbij kan worden gedacht aan technische systemen – een geïntegreerd en beveiligd e-mail- en incidentenregistratiesysteem zijn bijvoorbeeld essentieel, evenals allerlei scantools – maar zeker ook tools die de steeds toenemende hoeveelheid aan binnenkomende dreigings- en incidentinformatie gedeeltelijk automatisch verwerken. Daarnaast kan worden gedacht aan organisatorische gereedschappen, zoals een lijst met de resources zoals die in gebruik zijn binnen de doelgroep (asset-management).

5) Processes

Om consistente, transparante en herleidbare diensten te kunnen leveren is het belangrijk om telkens terugkerende processen effectief te beschrijven: niet te kort-door-de-bocht maar zeker ook niet te fijnmazig. Te fijnmazig werkt namelijk niet omdat de uitdagingen die een CSIRT heeft voortdurend evolueren. Omdat een proces ook niet in een keer perfect bedacht kan worden, is het zaak om ook hier te leren van gevestigde CSIRT's. Bij het ontwikkelen van de processen moet ook worden gezocht naar technische en organisatorische middelen om deze snel, foutloos en herhaalbaar uit te voeren. Mogelijke hulpmiddelen hiervoor zijn procedures en werkinstructies, gevat in cheatsheets en checklists. Hiernaast zijn processen zoals het "incident resolution"- en het "information handling"-proces te faciliteren met speciaal binnen de CSIRT gemeenschap ontwikkelde tools. Een voorbeeld van een dergelijk tool is Taranis. Deze tool is ontwikkeld omdat er grote behoefte was aan een geautomatiseerde manier om grote hoeveelheden nieuwsberichten te kunnen verwerken.
Een soms onderschat, maar essentieel proces binnen een CSIRT is het "Media Relations"-proces. CSIRT werk is slechts gedeeltelijk technisch werk. De afhandeling van incidenten kent veelal een significante media-component, waarbij het belangrijk is om een juiste en gebalanceerde boodschap naar buiten te brengen. Dit is gespecialiseerd werk en kan alleen worden gedaan met medewerkers die hiervoor geschikt en getraind zijn. Het is een best practice om alle verzoeken van de media en contact hiermee te laten afhandelen door aangewezen medewerkers, bijvoorbeeld in een communicatiegroep.

Conclusie

Een CSIRT is conceptueel gesproken geen ICT-functie. Het heeft een ankering op bestuursniveau nodig, en moet geborgd zijn via een van bovenaf vastgestelde verantwoordelijkheid en mandaat, doelgroep en kerndiensten – tevens moeten governance, rapportage en auditing geregeld zijn. Om een goede CSIRT te kunnen opzetten moet een aantal zaken goed worden georganiseerd. Er is geen "one size fits all". Wèl is er binnen de CSIRT-gemeenschap een grote hoeveelheid ervaring vastgelegd in verschillende documenten. Dit zijn levende documenten die worden aangepast naargelang de dreigingen en incidenten in de wereld om ons heen veranderen, evenals de eisen die aan onze gemeenschap worden gesteld.
De CSIRT Maturity Kit biedt een logisch raamwerk om de kennis uit de bestaande documenten te kunnen plaatsen en zo effectief mogelijk in te kunnen zetten. Hiernaast is de CMK zo opgezet, dat na het doorlopen van de vijf thema's al op veel punten is stilgestaan bij de parameters van het SIM3-model. SIM3 stelt een CSIRT vervolgens in staat om haar prestaties op een consistente manier op verschillende momenten te meten. Hiermee kan de ontwikkeling inzichtelijk gemaakt worden.

Links

[1] https://www.gccs2015.com/nl/programma/global-forum-cyber-expertise-gfce
[2] https://www.ncsc.nl/conference
[3] https://check.ncsc.nl/ : selecteer "CSIRT MATURITY KIT"
[4] https://www.trusted-introducer.org/SIM3-Reference-Model.pdf
[5] https://www.trusted-introducer.org/index.html
[6] https://www.trusted-introducer.org/directory/alpha_certification_Z.html
[7] https://check.ncsc.nl/questionnaire/
[8] https://www.first.org/

DE BLUNDERENDE GEMEENTE

Vaak hoor ik mensen fulmineren tegen bedrijven als ware het allemaal grote privacyschenders. Nu gaat er zeker eens wat mis, echter het loont om eens kritischer te kijken naar de achtertuin. Gemeenten blunderen keer op keer als het om de privacy van burgers gaat. Daar waar een bedrijf je doorgaans een product wil aansmeren dat je eigenlijk niet wilde hebben en waar je dan teveel voor betaalt, staat er bij gemeentelijke privacy meer op het spel. Gemeenten weten veel meer over jou dan bedrijven; doe maar eens een inzageverzoek in de Basisregistratie. De privacyimpact bij geblunder is vaak vele malen groter.

Het meest recente geblunder heeft te maken met Suwinet. Suwinet biedt overheidsorganisaties de mogelijkheid om persoonsgegevens van burgers te raadplegen. Suwinet is lek. Gemeenten houden zich niet aan de verplichte gebruiksmaatregelen. Een aantal feiten op een rijtje:

- Suwinet wordt door ambtenaren gebruikt om oneigenlijk gegevens op te zoeken (in welk blijf-van-mijn-lijf-huis woont mijn ex?).
- Suwinet wordt gebruikt door organisaties die daar helemaal geen toegang toe horen te hebben (deurwaarders).
- Eind 2013 bleek uit onderzoek van SZW dat slechts vier procent van de gemeenten voldeed aan de normen voor het gebruik van Suwinet. Dat is nu opgelopen tot 17 procent. 83 procent van de gemeenten heeft de zaken dus niet op orde!
- Het CBP deed in 2014 onderzoek naar Suwinet en de gemeente Den Bosch. Er bleek geen beveiligingsplan en incidenten werden niet afgehandeld, nergens werd bijgehouden wie toegang tot Suwinet had en tot overmaat van ramp bleek het Ierse ministerie van Sociale Zaken toegang te hebben.

VVD en D66 opperen nu dat gemeenten aan de schandpaal moeten als zij voor 1 oktober de zaken niet op orde hebben. En als ze op 1 januari nog steeds niet voldoen, moeten zij afgesloten worden van Suwinet. Een dergelijke suggestie werd ook geopperd in 2014 toen bleek dat de beveiliging van Digid bij veel gemeenten niet op orde was. De aanleiding voor deze suggestie was het feit dat bij 24 gemeenten gewoon het standaardwachtwoord gebruikt werd zonder dit ooit te wijzigen. Bij 12 van de onderzochte gemeenten bleek ook nog eens een onveilige koppeling met Digid gebruikt te worden.

De zorg voor dit geblunder is alleen maar groter geworden nu gemeenten in de toekomst nog meer zeer gevoelige persoonsgegevens gaan verwerken (jeugdzorg, werk, inkomen, zorg langdurig zieken en ouderen). Het CBP schreef daarover al een brandbrief, onder meer over het feit dat één en ander geheimhoudingsplichten zou doorbreken en verwerkingen in vele gevallen onrechtmatig zouden zijn omdat daartoe een wettelijke grondslag ontbreekt.

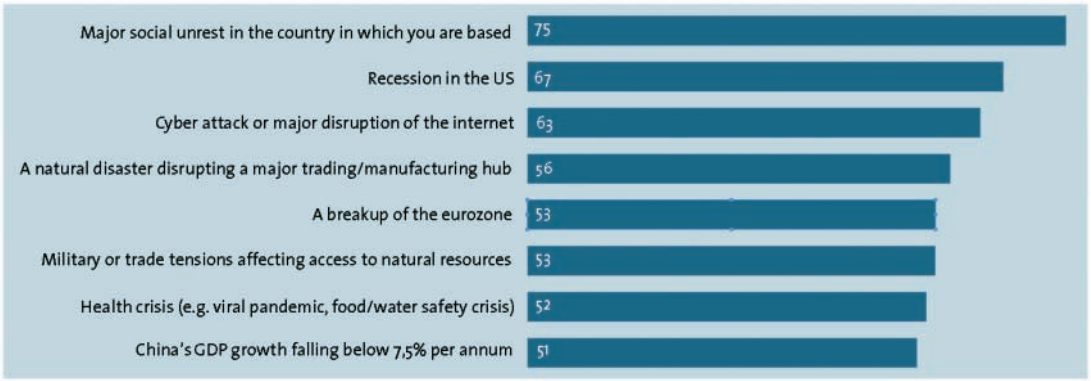
Ik weet niet hoe het met u zit, maar ik ben het helemaal beu. Het wordt tijd om gemeenten onder privacycuratele te zetten, onafhankelijke privacy-officers met mandaat bij elke gemeente te plaatsen, meer handhavend op te treden en dikke boetes uit te delen. Vol aan de schandpaal! Het is genoeg geweest; wij burgers hoeven dit niet langer te pikken.

Mr. Rachel Marbus
@rachelmarbus op Twitter

CYBERSECURITY IN DE BOARDROOM

Wat beweegt bestuur en commissarissen?

Bedrijven worden steeds meer informatie- en ICT-gedreven. Dit betekent dat raden van bestuur en raden van commissarissen zich moeten (gaan) bezighouden met deze kritische assets. De zekerheid en adviezen die wij als IT-auditors hierover verschaffen, zouden daarom ook in deze gremia moeten landen. Dat zal beter lukken naarmate wij als beroepsgroep meer in staat zijn om het gesprek aan te gaan met bestuurders en commissarissen over zaken die zij als belangrijk zien en naarmate het ons beter lukt om in dat licht bezien relevante activiteiten te ontplooien. Dit artikel, oorspronkelijk geschreven voor Chief Information Security Officers kan hierbij helpen doordat het duidelijk maakt wat de zaken zijn waar bestuurders en commissarissen zich vooral druk over maken. Dit artikel is gebaseerd op een hoofdstuk in een andere publicatie van dezelfde auteur. Zie het tekstkader 'publicaties van de auteur' aan het eind van dit artikel.



Figuur 1: Onderwerpen waar de CEO wakker van ligt (bron: PWC)

Met de intrede van cybersecurity in de boardroom wordt de vraag actueel hoe dit onderwerp te duiden. Hoe specificeren we het? Wie is verantwoordelijk en aansprakelijk? Dit is noodzakelijk om greep op de materie te krijgen. Het duiden is vooral lastig omdat de kritische assets (in dit geval data) doorgaans niet als zodanig op de balans staan en dus ook niet in het jaarverslag terugkomen. Zelden wordt de goodwill van de data op de balans tot uitdrukking gebracht. Daarom staat dit onderwerp in de meeste gevallen ook niet op het netvlies van de bestuurder (Raad van Bestuur) of de toezichthouder (Raad van Commissarissen). Incidenten waarbij de bestuurdersaansprakelijkheid nadrukkelijk aan de orde is, doen hun intrede in de media en creëren daarmee de urgentie meer grip te krijgen op dit fenomeen.
Een treurig dieptepunt vormde een incident bij de Nederlandse Zorgautoriteit (NZa). Hier ging het op werkelijk alle fronten mis. Er was sprake van falende systemen (vrije toegang tot data op de fileshares), falende processen (geen beleid en borging daarvan) en falend toezicht. Sterker nog, het besturende orgaan maakte zich schuldig aan mismanagement en malversaties. Klokkenluider Gotlieb sloeg met de volgende woorden alarm: 'Helaas zie ik geen andere route dan het u te melden langs deze onsympathieke weg. De geest moet uit de fles en het deksel van de pot. Opdat het management tijdig kan bijsturen. Dit schreeuwt namelijk om interventie.' Twee weken nadat hij dit dossier bij zijn werkgever had ingeleverd, pleegde Arthur Gotlieb zelfmoord [1]. De toenemende politieke druk naar aanleiding van deze zaak leidde tot het aftreden van beide bestuurders van de NZa.

Met integrated reporting kan de organisatie zich profileren

De NZa-case gaat verder dan het niet goed omgaan met informatiebeveiligingsrisico's. Er is tevens sprake van een falende organisatiecultuur. Meerdere duidelijke signalen werden structureel genegeerd. Het is daarom onder andere deze NZa-case die het belang onderstreept van de verantwoordelijkheden en aansprakelijkheden van governance (RvC) en executive management (in niet-Angelsaksische landen is dit de RvB). In Angelsaksische landen en bij sommige Nederlandse organisaties kennen we zowel een one-tier board, waarin toezicht en uitvoer zijn verenigd, als een two-tier board, waarbij toezicht en uitvoering strikt gescheiden zijn. Zodra we per niveau duidelijk hebben wat er wordt verwacht, kan er invulling worden gegeven aan de information-security- of cybersecurity-functie binnen de besturing van de organisatie.

Onder governance verstaan we het creëren van een setting waarin effectief management mogelijk wordt. De taken hierbij zijn: het evalueren van de context en de invloeden daarvan op de organisatie; richting geven ('direct' in het Engels); en monitoren van bestuur. Binnen COBIT noemen we dit het EDM-proces: Evaluate, Direct en Monitor. [ISAC12]

Lec. Yuri Bobbert Msc is PhD onderzoeker en lector op het terrein van bedrijfskritische informatiebeveiliging (Business Information Security). Bobbert combineert zijn lectoraat bij Hogeschool NOVI met zijn rol als CISO bij UWV en Non-executive director bij DPA|B-Able. Hij is bereikbaar via yuri.bobbert@b-able.nl

Misstanden
Voorbeelden van transparante media die publiceren over misstanden (zoals data incidenten):
https://rejo.zenger.nl/
http://allestoringen.nl/
http://datalossdb.org/
http://www.spaink.net/dutch-data-breaches/
https://www.bof.nl/category/zwartboek-datalekken/
http://www.hallofshame.com/
http://www.pcworld.com/article/2453400/the-biggest-data-breaches-of-2014-so-far.html

Executive management op zijn beurt heeft als primaire taak het nemen van besluiten. De activiteiten die daar bij horen zijn het maken van plannen, het bouwen van de organisatie (structuren en processen), het runnen van deze organisatie en het monitoren op het gewenste resultaat. Het onderliggende operationele niveau effectueert de operationele beslissingen die het executive management neemt. De vragen die ik zelf frequent stel aan RvB- of RvC-leden zijn: Waar is binnen uw organisatie de cybersecurity belegd op governance- en managementniveau (RvC respectievelijk RvB)? Waar zou het volgens u belegd moeten zijn (reporting lines)? Welke meetmethoden en indicatoren (metrieken, ratio's, KPI's) hanteert u naar de RvB? Welke metrieken, ratio's, KPI's hanteert u als RvC? Hoe verkrijgt u deze data? In hoeverre neemt u dit mee in uw verslaglegging?
Het is anno 2015 nog steeds zo dat veel van deze vragen onbeantwoord blijven. De belangrijkste oorzaak hiervan is dat de bestuurder veelal onvoldoende wordt gevoed met input om een gefundeerde discussie te kunnen voeren. De CISO kan hierin een belangrijke rol vervullen, zowel als adviseur als in de rol van sparringpartner van het bestuur. Het kan hierbij geen kwaad om te weten van welke zaken de bestuursvoorzitter vooral wakker ligt (zie figuur 1).

Wat drijft de RvB?

Om als CISO het bestuur goed bij te kunnen staan met advies is het van belang om te begrijpen wat bestuurders drijft. Onderzoek van Berenschot, PwC [PWC13] en Forbes [FORB12] definieert de volgende drivers:

- Differentiatie. Overleven door zich te onderscheiden ten opzichte van concurrentie.
- Risicomanagement. Risico's tijdig kwalificeren en de impact indiceren. Veelal financiële risico's die zijn ingegeven door de striktere regels voor verslaglegging (IFRS, SOx, Basel II). Voornamelijk voor beursgenoteerde bedrijven en/of bedrijven die moeten voldoende aan de wet op de jaarrekening (IT-audits). Sinds kort zijn er ook een (rechtstreeks werkende) verordeningen, zie bijvoorbeeld [2] en [3].
- HR-management (talent-management). Het boeien en binden van de meest kritische asset anno 2014. Veel bedrijven zijn sterk afhankelijk van kenniswerkers, die zich op een andere manier laten managen dan via de traditionele technocratische managementstijlen.
- Toegang tot kapitaal. Dit gaat vooral om het verkrijgen van geld op de kapitaalmarkt. Daar waar kasposities voor bedrijven belangrijk zijn, wordt de toegang tot extra kapitaal schaarser en duurder. Bedrijven worden dus kritischer op kosten.
- Kostenreductie. Dit is in lijn met het bovenstaande. Bedrijven kijken kritischer naar hun operationele kosten en personeelskosten. Beide kostensoorten zouden meer moeten meedeinen met de bedrijfsvoering. Dit geldt zeker ook voor IT-kosten.

Wat drijft de RvC?

Om als CISO de toezichthouder (RvC) goed te kunnen bijstaan met advies is het van belang om te begrijpen wat de commissaris drijft. Onderzoek van Grant Thornton definieert de volgende drivers die allemaal net een iets andere insteek hebben dan die van de RvB. [KLAA13]

1. Differentiatie in verslaglegging
De nieuwe regels voor verslaglegging (integrated reporting) gaan uit van het adequaat rapporteren over non-financial-risks. [IIRC13] Bijvoorbeeld information-security-risico's. Onderzoeken in de VS [WEST07] en Japan [ISHI11] hebben al aangetoond dat het verslagleggen over goed securitymanagement een positief effect kan hebben op de gepercipieerde waarde van de onderneming. [CAMP03] Volgens Nancy Kamp van EY [KAMP13] zal geïntegreerde verslaglegging overigens 'niet zozeer leiden tot meer, maar vooral tot anders rapporteren.' En zij voegt hier ter verduidelijking aan toe: 'Overigens is de EU-richtlijn meer dan een administratieve oekaze. In feite is het een spiegel van wat er in de maatschappij leeft. Het samenvoegen van verschillende rapportages tot een holistisch verslag is meer dan het slaan van een nietje tussen twee afzonderlijke verslagen; het is een uiting van een andere manier van kijken, denken en handelen. Een manier die getuigt van besef van onze impact op de wereld en van de bereidheid om verantwoordelijkheid te nemen voor de omgeving waarin we opereren, de mensen die erbij betrokken zijn en onze

ecologische voetafdruk. We zitten in een paradigmaverschuiving – van de korte naar de lange termijn, van kwantiteit naar kwaliteit en van welvaart naar welzijn. De EU-richtlijn is een eerste stap in de goede richting.'
Het rapport van Grant Thornton legt ook de verschillen bloot tussen de standaard reportingsnormen en die voor integrated reporting. Zo bleken de in dat rapport bevraagde commissarissen grote waarde te hechten aan het rapporteren van risico's op het vlak van veiligheid, reputatie, maatschappelijk rendement, vertrouwen van publiek, continuïteit van de onderneming, marketing en customer-relations en human resources. Terreinen waarmee de CISO steeds vaker verbinding moet kunnen maken om de dialoog te voeren en daarmee de rapportages te kunnen voeden.

2. Actuele informatie over risico's en daardoor adequaat risicomanagement
De commissaris wil vanuit zijn toezichthoudende rol kunnen beschikken over adequate, betrouwbare data over de feitelijke situatie. Dus exacte gegevens over systeemintegriteit, beschikbaarheid en vertrouwelijkheid. Precies zoals het geval is bij financiële data over liquiditeitspositie, vermogenspositie en overige financiële ratio's gaat het de commissaris hier om actuele kerngegevens over de stand van zaken van de informatiehuishouding van de organisatie. Deze data mag niet verouderd zijn, want op een cyberincident (bijvoorbeeld een datalek) dient direct te worden gereageerd. De commissaris wil in geen geval via de media vernemen dat bij een bedrijf waarop hij of zij toezicht houdt data zijn gelekt. De CISO vervult hier een belangrijke rol door de essentiële data up-to-date te houden en daarover frequent te rapporteren. Essentiële gegevens dienen bij voorkeur met één druk op de knop beschikbaar te zijn. Een belangrijk aspect hierbij is dat de RvC deze informatie rechtsreeks van de CISO moet ontvangen en nimmer indirect via de RvB. Laten we leren van de NZa-case. De RvC heeft behoefte aan ongefilterde kerngegevens. Daarom is het belangrijk dat de CISO een situationeel onafhankelijke positie kan innemen ten opzichte van de RvB.

3. Talent-management met het oog op het verwerven van de juiste kennis en competenties
Het rapport onderstreept het belang van de aanwezigheid van de juiste competenties bij de RvC en de RvB. Zeer belangrijk voor de RvC zijn helikopterview, kritisch doorvragen, rechte rug en beoordelingsvermogen. Voor de RvB zijn dat commitment, resultaatgerichtheid, ondernemingszin en strategisch inzicht. De RvC dient up-to-date te blijven met actuele kennis over diverse ondernemingsvraagstukken. Het aantrekken van een commissaris met kennis van informatiesystemen en technologie is anno 2014 geen sinecure. Laat staan iemand met kennis van security, risk en compliance. En deze drie elementen dan nog zowel opzichzelfstaand als in relatie tot elkaar. Het is prachtig als een commissaris deze kennis heeft, maar strikt noodzakelijk is het niet. Het allerbelangrijkste is het vermogen om doortastend de juiste kritische vragen te stellen op de juiste momenten.
Het is verder wenselijk dat de voorzitter van de RvC zorg draagt voor een regelmatige vernieuwing van de samenstelling van de Raad en voor een evenwichtige mix van talenten binnen de Raad. Alleen zo kan de RvC aan de talrijke uitdagingen op dit vlak het hoofd bieden. De CISO kan de RvC assisteren in het formuleren van onderwerpen waarop de bestuurder bevraagd kan worden.

4. Frequente communicatie met alle relevante stakeholders
Het is voor de RvC van belang om daadwerkelijk alle stakeholders te kennen. De traditionele stakeholders zoals banken en toezichthouders zal de Raad ongetwijfeld kennen. Met nieuwe, meer dynamische krachten, zoals hacktivisten, cybercriminelen die uit zijn op intellectueel eigendom, en ongecensureerde media zal hij mogelijk minder bekend zijn. Het Grant Thornton-rapport pleit voor een minder afhankelijke positie ten opzichte van de RvB als het gaat om de relatie met stakeholders. Dat geeft de commissaris de vrijheid in contact te treden, vragen te stellen en verslag te doen. Het rapport pleit verder voor meer controle van buiten de RvB en voor het afleggen van verantwoording naar stakeholders zonder inmenging van de RvB. De NZA-case is ook hierin een leerzame ervaring. Had de RvC hier doortastender opgetreden, met toezicht op informatierisico's zoals datalekken en met een sluitende controle, onder meer door te valideren of de benodigde controls aanwezig zijn, dan was tijdig aan het licht gekomen dat er interne en externe richtlijnen werden overtreden. Volgens Gotlieb hield de RvB deze informatie echter in de doofpot. Daarom is een CISO die direct rapporteert aan zowel RvB als RvC over vooraf opgestelde criteria een vereiste. De CISO kan dit doen door het (laten) uitvoeren van een stakeholderanalyse waarin technische en juridische afhankelijkheden worden beschreven en deze in te brengen in de vergaderingen van de RvC en de RvB.

Alle bevraagde commissarissen in het Grant Thornton-rapport geven aan dat de kwaliteit van de risicorapportages aan de RvC verbetering behoeft. Dat is ook in lijn met andere meningen van de commissarissen in het onderzoek over risicomanagement. De RvC zal meer gevoed moeten worden met feitelijke data uit de bedrijfsvoering over continuïteit van de onderneming, het vertrouwen dat het publiek heeft en de reputatie die hiermee gepaard gaat. Net als bij boekhouden

Publicaties van de auteur

Yuri Bobbert schreef in 2010 het boek Maturing Business Information Security, a framework to establish the desired state of security maturity, dat wordt gebruikt op verschillende universiteiten en hogescholen. Vanuit dit boek zijn de MBIS-methode en het MBIS-platform ontstaan (mbis.eu). In 2014 verscheen zijn tweede boek: Hoe Veilig is mijn 'aandeel'?, Het borgen van Reputatie, Vertrouwen en Continuïteit met de MBIS methode'. Dit artikel is een bewerkte versie van het hoofdstuk 'Governance en integrated reporting' dat is opgenomen in dat boek. Dit boek is het resultaat van praktisch en wetenschappelijk onderzoek bij ruim 100 organisaties naar de beveiliging van kritische assets en de wijze waarop bestuurders en managers hun reputatie, vertrouwen en continuïteit kunnen borgen.

zal ook de administratie van informatierisico's actueel moeten zijn. Intelligente systemen kunnen hierin een bijdrage leveren. Bijvoorbeeld Security Information Event Management systemen (SIEM). Deze systemen hebben echter maar een beperkt effect als de organisatie niet is toegerust om de hoeveelheid data die een SIEM-systeem genereert te kunnen ontvangen, interpreteren en begrijpen en indien nodig actie te ondernemen. De CISO zal eerst van bovenaf moeten vaststellen wat de risico's zijn, wat de houding is van de organisatie tegenover deze risico's (risicobereidheid) om vervolgens te kunnen bepalen welke informatie de RvB en RvC nodig hebben om de risico's adequaat te managen. Deze benodigde informatie kan dan uit een SIEM-systeem onttrokken worden. Dit zal mogelijk maar een fractie zijn van wat een dergelijk systeem kan verzamelen en rapporteren. Vooraf focus aanbrengen vanuit een bedrijfsmatige doelstelling is hier dus van belang. Naast systeeminformatie zal de organisatie ook behoefte hebben aan meer kwalitatieve data, zoals de mate van vertrouwen of de reputatie die een organisatie heeft. Verschillende instrumenten kunnen de CISO helpen in het meten van de reputatie van de organisatie op het internet.

Conclusie

De CISO zal te allen tijde zijn RvB en RvC moeten voeden met feitelijke data over hoe het er aan toegaat binnen de organisatie en de keten(s) waar zij deel van uitmaakt. Om zich een volledig beeld te kunnen vormen is het dan ook essentieel dat hij zijn eigen logging en monitoring en zijn eigen reporting lines up-to-date houdt. Dit proces kan manueel verlopen, maar deels ook automatisch via dashboard tooling. Alleen op die manier kan hij zijn RvB en RvC voorzien van de meest actuele informatie over risico's die worden gelopen ten aanzien van de stakeholder(s) en kunnen de RvB en RvC hierover proactief communiceren, onder meer in de verslaglegging (integrated reporting).

Met integrated reporting kan de organisatie zich profileren. Integrated reporting maakt aan alle betrokkenen duidelijk dat zowel de financiële risico's als arbo-, milieu- en informatierisico's in kaart zijn gebracht en dat de organisatie er alles aan gedaan heeft om deze het hoofd te bieden. Kortom: het is veilig zaken doen met deze organisatie. Ze zijn daar 'in control'.

Links

[1] NRC-verslag van de NZa-case: http://www.nrc.nl/nieuws/2014/04/10/het-nza-dossier-interne-wanorde-bij-de-toezichthouder/

[2] Verplichte toepassing van IFRS in 2005; EU Verordening 1606/2002 van 19 juni 2002: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:243:0001:0004:nl:PDF

[3] Internationale standaarden voor jaarrekeningen; EU Verordening 1725/2003 van 29 september 2003: http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32005R2106

Literatuur

[CAMP03] K. Campbell, The economic cost of publicly announced information security breaches: Empirical evidence from the stock market, Journal of Computer Security, 11:431-448, 2003.

[FORB12] Forbes, For Top CEOs, Culture Drives Value Creation, http://www.forbes.com/sites/robertreiss/2012/10/10/for-top-ceos-culture-drives-value-creation/, 2012 geraadpleegd op 23 januari 2015.

[IIRC13] IIRC, The international Integrated Reporting Framework, International Integrated Reporting Council (IIRC), 2013, http://theiirc.org/wp-content/uploads/2013/12/13-12-08-THE–INTERNATIONAL-IR-FRAMEWORK-2-1.pdf, geraadpleegd op 27 januari 2015. [ISAC12] ISACA, Cobit 5 for Information Security, ISACA, 2012.

[ISHI11] M. Ishiguro, T. Hideyuki, K. Matsuura and I. Murase, The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market, The Graduate School of Interdisciplinary Information Studies, The University of Tokyo, p. 15, 2011.

[KAMP13] N. Kamp-Roelofs, Integrated reporting; Clear vision of true company value in the perception of the 'share & stakeholder', 2013.

[KLAA13] A. Klaassen en H. Rijken, RvC moet meer proactief 'mee ademen' met bedrijf; Commissarissenonderzoek 2013/2014' GrantThornton, 2013.

[PWC13] PwC, 16th Annual Global CEO Survey; Dealing with disruption, 2013.

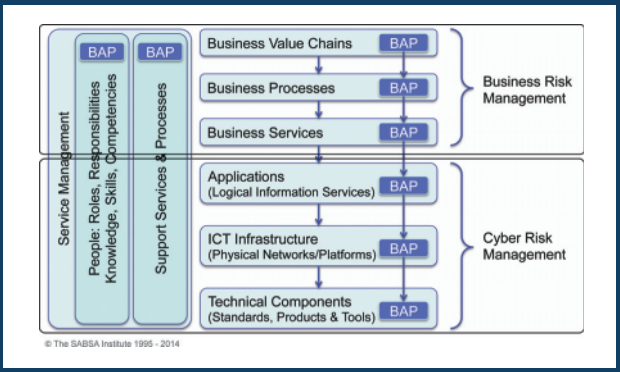
[WEST07] G. Westerman and R. Hunter, IT Risk, Turning Business Threats into Competitive Advantage, Boston MA: Hardvard Business School Press, 2007

BUSINESS CONTEXT ALIGNED

The British Computer Society June newsletter featured an article by Neil Cordell. The article opens with the following statement: "When it comes to dealing with cyber security, technologists must focus more on threats and controls and less on risk". Mr. Cordell is concerned that implementing security controls is entirely in the hands of technologists, who have no real idea of what impact these controls might have on business productivity or the protection of real business assets. So far, so good, but what's this about 'less risk'?

Although proposing business alignment of cyber security, Mr. Cordell has a classical technologist's view that 'risk' is the result of poor IT implementations, not the result of 'doing business'. He believes that risk is a problem that technology alone can solve. He does not see risk as being an essential element of doing business, grasping opportunities to enhance business value, and facing threats that would imperil those opportunities. This succinctly captures the problem of IT thinkers – they do not grasp the concept of business risk appetite. They believe that a 'risk-free' world is possible, if only we could spend enough time and money on looking at cyber-threats and implementing controls.

When the author refers to threats, he means cyber threats, such as hacking, denial of service, data theft, natural disasters, etc., unrelated to the business level. SABSA takes us into a new direction of thinking, in which we concentrate on understanding the business first and foremost, without reference to the technology that underpins its operations. We look at the business opportunities and threats, assessing those most relevant to business success. We see the world in terms of a 'business stack', as shown in the figure, which has technology layers towards the lower end, but which is populated in its higher layers with business focused thinking. Note that the concept of 'risk' is present at all layers.



In SABSA we develop Business Attribute Profiles (BAPs) to be used as proxy-assets for risk assessment. These BAPs form a multi-tiered balanced scorecard, in which performance targets are set for each individual attribute. Starting at the top of the stack we first develop a BAP for the business value chain. We then work down the stack deriving attributes for each layer, driven from the layer above. The attributes become more technical as we go down, and ultimately we derive some attributes that are specific to cyber security, but these can only be useful if we begin by considering the business value chain as the top-level driver for all things.

The concept of Balanced Score Card (BSC) was first published by Kaplan and Norton in the early 1990's. The overall summary of this approach is shown in the figure.

BSC takes four different views of enterprise strategy and encourages exploration of all four views. If you want to explore your value chain, this is a great place to begin. The method fits perfectly with the SABSA way of thinking. You should be able to identify your value-chain attributes by using the BSC framework as a guide. SABSA doesn't reinvent wheels that are already there, but it's a good framework for integrating methods that contribute to the holistic process of enterprise risk management.

The Attributer

INTERVIEW

Identiteitsprovider Digidentity:

‘JE MOET IN JE PRODUCT BLIJVEN GELOVEN’

In een artikelreeks kijkt Informatiebeveiliging Magazine mee bij innovatieve bedrijven in de branche. De aftrap was malware-opspoorder RedSocks. In deze editie: identiteitsprovider Digidentity. Het Nederlandse bedrijf wil ‘identiteit weer teruggeven aan de burger’. Het kleine bedrijf versloeg grote ICT’ers en bouwde onder andere het Nederlandse en later het Engelse DigiD. Een interview met oprichter en CTO Marcel Wendt.

Wendt: 'In 2008 zagen Carel Mackenbach en ik [samen de oprichters van Digidentity] dat er behoefte zou komen aan goede identiteiten op internet. Naast DigiD, dat alleen de publieke sector mag gebruiken, was er niets voor private partijen. En hoe kunnen die dan zeker weten dat iemand is wie die zegt dat 'ie is?' Ze begonnen met het ontwikkelen van het product. Na het startidee hebben ze er drie jaar achter de schermen aan gewerkt. 'We wilden het allerhoogste zekerheidsniveau garanderen, gemeten in STORK-levels (Secure idenTity acrOss boRders linKed).' Het laagste security-niveau is dat iemand zijn e-mailadres geeft, het hoogste is dat iemand langs komt bij je op kantoor om zijn gezicht te laten zien. 'Wij wilden dat onze klanten konden kiezen wat het beste bij hen past, dus we creëerden een product dat je desgewenst kan opschalen, zodat het met je meegroeit.'

Digitale kluis

Om nu het hoogste niveau te bereiken, heb je een smartcard en reader nodig met een kabeltje. 'Dat is nog steeds onveilig,' zegt Marcel. Hij demonstreert simpel hoe makkelijk je het kabeltje uit elkaar kunt halen - en dus kunt hacken. In plaats van de smartcard maakte Digidentity een persoonlijke digitale kluis. En in plaats van de reader een hardware-security-module (HSM), een apparaat dat via cryptologie jouw digitale kluis uitleest. Op dat gecertificeerde apparaat loopt een patentaanvraag ('patent pending'). Met je smartphone kom je via een secure app die een VPN-achtige verbinding legt bij je kluis. TNO heeft een onafhankelijke beoordeling gedaan en de producten en werkwijze van Digidentity 'worden steeds geaudit' om aan de benodigde certificeringen te blijven voldoen. Het gebruik van de digitale, op zichzelf staande, kluisjes betekent dat Digidentity het enige bedrijf ter wereld is dat identitymanagement doet zonder fysieke kaart. Een extra security check voor klanten is dat het bedrijf op hun servers ziet dat er een hack is. Met een pasje merk je niets... En mocht dat toch gebeuren, dan wordt er één kluisje getroffen, niet een hele database, omdat ze die niet gebruiken. Een nadeel voor klanten is dat als jij je inlogcode van je kluisje vergeten bent, de Digidentity-helpdesk je daar ook niet aan kan helpen, simpelweg omdat zij dat niet weten. Dan moet je een nieuw account aanvragen.

Hoewel in den beginne de klanten uitbleven, bleef Digidentity's werk niet onopgemerkt. De EU zag dat wat het bedrijf deed uniek was en paste daarop de wetgeving voor server-based signing [1] aan. 'Fijn voor ons, want dat maakte voor ons het werk ook makkelijker.'

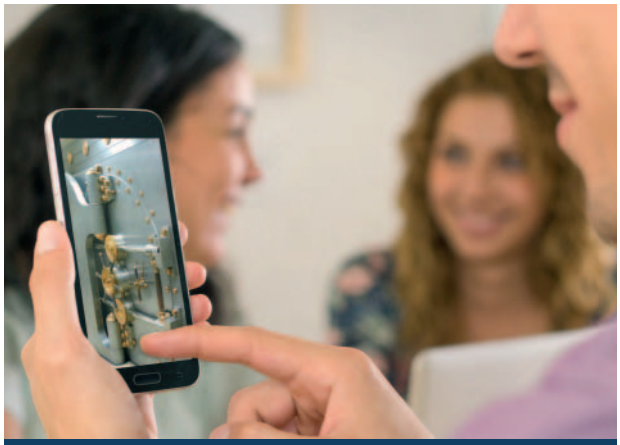
Na drie jaar was het zover. Het product was klaar. 'En toen begreep niemand er wat van.' En daarbij kwam eHerkenning in de lucht, een 'DigiD voor bedrijven' dat EZ had opgestart, voor een betere publiek-private samenwerking. 'Ze vroegen ons en concurrenten in eHerkenning te investeren. In ruil daarvoor zouden wij eerste aanbieders worden.' De Belastingdienst deed initieel ook mee. 'Voor ons zeer interessant, gezien het grote aantal MKB'ers waar zij een link mee hadden. Helaas trokken zij zich na twee jaar terug.' Desondanks werd eHerkenning toch een succes: het wordt nog steeds dagelijks gebruikt.

DigiD

In 2011 schreef de overheid ook de DigiD-aanbesteding uit. Tot dan toe was DigiD nog een 'uit de hand gelopen' pilot. 'Het was te populair geworden voor de techniek erachter. Het moest van de grond af opnieuw worden gebouwd. Wij hebben toen samen met Siemens (wij development, zij de hosting) meegedaan en werden gekozen… Toen ik het telefoontje kreeg, reed ik net weg naar huis. Ik kon het niet geloven, het was zo'n prestigieuze opdracht.' Het project verliep goed. In 2012 werd het in gebruik genomen. 'Erg spannend, want we moesten in één nacht 11 miljoen identiteiten naar nieuwe systemen migreren. En de ochtend erna moesten gemeenten en andere overheidsinstanties ze weer gewoon kunnen gebruiken. Alles ging goed: een succesvol overheids-ICT-project waar je nooit meer iets over hoort...'

Digidentity's werk voor DigiD bleef niet onopgemerkt bij

Chantal Craandijk is eigenaar van Craandijk Communicatie. Chantal is onder andere werkzaam als interviewer en is bereikbaar via www.craandijk.com



Digitale kluis, hoe werkt het?

Digidentity's oplossing is gecertificeerd om een juridisch rechtsgeldige handtekening te zetten. Het is een laagdrempelig product, in tegenstelling tot fysieke smartcards. Je gebruikt je eigen smartphone -waar je vaak zuinig op bent - en hebt geen smartcard reader nodig. En bij verlies of diefstal ben je wel je telefoon kwijt maar niet de controle over de smartcard.
Digidentity ontwikkelde hiervoor een gepatenteerde digitale kluis waarin je persoonsgegevens veilig worden opgeslagen. Daarnaast introduceerde het bedrijf de virtuele smartcard, die ook in de kluis wordt bewaard; net zoals je een fysieke smartcard vaak bewaart in je portemonnee. Om een juridisch rechtsgeldige handtekening te zetten, log je in op de digitale kluis met je username en password. Je haalt daarmee de virtuele smartcard 'uit je portemonnee'. Daarna zet je de handtekening met je smartphone als afstandsbediening. De smartcard wordt centraal opgeslagen en beheerd. Het systeem is zo opgezet dat zelfs Digidentity-medewerkers niet bij de data in de digitale kluis kunnen: privacy-by-design.

Nederlandse bedrijven. 'We kregen meer opdrachten,' vooral vanuit de verzekeringsbranche, waar ben-je-wel-wie-je-zegt-dat-je-bent de basis is van alles. 'We hadden ook een nieuwe aandeelhouder, Solera, die uit die hoek kwam.' Ondanks de goede pers en verbeterde naamsbekendheid 'werden onze eigen producten nog steeds niet begrepen en konden we ze dus nog niet verkopen. Het duurt heel lang om een vertrouwensrelatie op te bouwen. En je bent die ook snel kwijt.' Gelukkig voor de cashflow van het bedrijf zorgde het succes van DigiD voor genoeg andere opdrachten, naast de werkzaamheden voor DigiD.
In 2012 schreef de Engelse overheid de aanbesteding uit voor een Engelse DigiD, waar Digidentity ook op inschreef. 'We stonden daar tussen de multinationals. Een groot ICT-bedrijf dat we bij de start van het werk voor de aanbesteding belden om te kijken of ze met ons wilden partneren, zei 'we bellen jullie wel als we gekozen zijn'. En toen wonnen wij de opdracht! Daarna vroegen zij ons om samen te werken. Ik heb zelden met zoveel genoegen nee verkocht,' zegt Wendt lachend.

'Near-perfect product'

Na twee jaar bouwen, is het systeem in november vorig jaar in gebruik genomen. 'Het bouwen gaat op eigen kosten, als bedrijf verdienen we er pas aan als er identiteiten verkocht worden. Je moet er dus wel een lange adem voor hebben.' De Engelse pers reageerde lovend en hebben het zelfs over een 'near-perfect product'. Met het Engelse DigiD kwam Wendts grote droom uit: 'Je kunt daar als klant kiezen welke identity provider je wilt gebruiken. Dus als er eentje gehackt wordt, zoals bijvoorbeeld bij de DDOS-aanval op DigiD, kun je kiezen uit een andere. In Nederland kan dat nog niet.' Een van de redenen waarom nu de hele wereld kijkt naar het Engelse model. Ondertussen legde het succes de naamsbekendheid van Digidentity geen windeieren: 'Nederland en Engeland staan op respectievelijk nummer twee en drie van de wereldwijde eOverheidslijst (op één staat Zuid-Korea), wat ook goed op ons afstraalt. Mensen zien nu dat we bestaan en nemen gezien onze trackrecord aan dat we wel goed moeten zijn.'
In 2013 won Digidentity de aanbesteding voor de Engelse postdienst, de Post Office. 'Dat was voor ons heel bijzonder: het was de eerste keer dat we ons eigen product verkochten, als 'white label', waar later de Post Office-branding aan zou worden toegevoegd.' Daarnaast verzorgt Digidentity ook de hosting en bemannen zij de servicedesk (vanuit Den Haag): de Post Office krijgt 'identity as a service'. In tegenstelling tot Nederland is de Engelse Post Office nog steeds een overheidsbedrijf. Er zijn nog steeds postkantoren en daarnaast is het bedrijf een mobiele provider en een bank. 'We praten wel met PostNL, maar de situatie hier is heel anders. Naast Nederland is er ook interesse uit Finland, Denemarkten, Australië… 'Laatst was hier een delegatie vanuit Indonesië over de vloer'. Daar heeft EZ ook een grote hand in: 'Zij verwijzen hen naar ons door.'

Op dit moment werkt Digidentity aan 'het perfectioneren van ons Engelse product. We moeten ons voorbereiden op de grote aantallen identiteiten die verwerkt moeten worden. Groot-Brittannië heeft 60 miljoen inwoners, waarvan 45 miljoen identiteiten. Gelukkig gaat het registreren daarvan in golfbewegingen. Dat is veel beter te hanteren dan het in één klap te doen via een soort Postbus 51-achtige campagne. De techniek houdt dat niet vol, kijk maar naar het Medicare-systeem in Amerika. Daar moesten ook alle burgers zich in één keer registreren, het systeem kon het niet aan, klapte eruit en het is eigenlijk nooit meer van de grond gekomen. Dat wilden we koste wat kost voorkomen.'

Idensys-netwerk

Verder werkt het bedrijf in Nederland mee aan de transformatie van eHerkenning naar Idensys, dat DigiD en eHerkenning moet combineren in één platform. 'Een heel groot voordeel: in dat platform kun je ook kiezen uit meerdere identity-providers.' Idensys moet in principe in 2017 in de lucht zijn. 'Het is wel een lastig traject, omdat er meerdere ministeries in samenwerken - BZK voor DigiD, EZ voor eHerkenning, Financiën voor een identiteitssysteem voor de banken - maar geen van die ministeries de baas is van het project. Gelukkig is sinds de commissie-Elias (die overheids-ICT-projecten onderzocht) 'Digicommissaris' Bas Eenhoorn aangesteld. 'Hij heeft die onafhankelijke rol gekregen. Ik hoop dat als het nodig is, hij met zijn vuist op tafel kan slaan.'

Selfies

In Groot-Brittannië is het samenstellen van je identiteit moeilijker voor een identiteitsprovider dan in Nederland. 'In Nederland hadden we Napoleon die voor ons de basis van het GBA legde. In Engeland is er echter 'vrijheid van identiteit'. Een grondrecht. Als je morgen Elton John wilt heten, dan heet je morgen Elton John. Voor ons als identityprovider betekent dat we een moeilijk proces moeten doorlopen om je identiteit echt te kunnen checken.' Om dan te voorkomen dat je steeds zelf ergens langs moet voor een fotocheck als je identiteit gecontroleerd moet worden, gebruikt Digidentity een fenomeen van deze tijd: selfies. 'We hebben onlangs een systeem van selfies gelanceerd, die mensen insturen om bijvoorbeeld een paspoortcheck mee te doen. Het systeem checkt of je selfie lijkt op je paspoortfoto, doet eigenlijk hetzelfde als er nu gebeurt bij de douane op het vliegveld. Het is een douanepoortje in een mobiele telefoon.'

Het bouwen ervan kostte aardig wat tijd: 'Het is niet moeilijk een appbouwer te vinden, maar wel eentje die daarnaast zo'n ingewikkeld securitysysteem kan bouwen.' Voordat het systeem de lucht in ging, zijn er heel veel gebruikerstests gedaan. Wat soms leidde tot pijnlijke resultaten: 'Op een gegeven moment testten we het in Engeland, bleek niemand er iets van te begrijpen. Dus zijn we opnieuw begonnen. En we doen nog steeds aanpassingen als het nodig is.'

Dood paard?

'We willen de Apple van de identity-providers zijn.' In Engeland vindt men dat nu al maar 'we moeten zorgen dat we steeds voorop lopen.' Dat lukt met name door klein te blijven en te blijven focussen op één ding: identity-management. Hoe komt het dat Wendt in die beginjaren nooit het gevoel heeft gehad aan een dood paard te trekken? 'Je moet flexibel blijven en echt de ballen hebben in je product te blijven geloven. Ook al doet nog niemand dat.' En dat werkt.

Links

[1] http://wetten.overheid.nl/BWBR0015046/geldigheidsdatum_02-07-2015

VERSLAG

BLACK HAT SESSIONS XIII: DONKERE TINTEN EN LICHTPUNTJES

Op 18 juni 2015 heb ik de 'BlackHat sessions XIII' van Madison Gurkha bezocht met een vrijkaartje van het PvIB. Ik was nog nooit geweest en mijn eerste indruk van de dag geeft een hint naar het waarom. Ik ken hier bijna niemand. Waar een bijeenkomst van het PvIB steevast een warm bad van herkenning is, voelde ik me in de Reehorst in Ede een buiten-staander. Een blanke kip tussen bruine Barnevelders, een gans in eendenland. Hier slaan techniek en hacken de maat; de harde kant van beveiliging. En ik? Ik ben een softie... De eenzaamheid duurde niet lang want ook Tom Bakker dook op en natuurlijk was ons aller Debbie, beschermmoeder van alle PvIB-ers, aanwezig met een 3-in-1 stand voor NOREA, NLUUG en PvIB. Een kop koffie onder haar vleugels gaf me weer snel de moed om de omgeving te verkennen.

In de grote foyer trof ik aanbieders van crypto- en communicatiediensten, hardware (firewalls), een verzekeraar en diverse adviseurs. Alleen sommige standbemanningen droegen een pak (fout), verder zag ik vooral t-shirts in donkere tinten met cryptische teksten (goed). De mannen van de gastheer (Madison Gurkha) vervulden hun gastheerrol met verve en waren passend gekleed.

Zoals altijd bij dit soort gelegenheden is het zaak te kiezen voor de juiste presentaties en sessie om het beste uit de dag te halen. Daar was voor velen de koek al verdeeld: de live-hacking-sessies en de PGP-keysigning-party waren volgeboekt. Die laatste duurde maar een uurtje in een afgesloten ruimte en toonde zich als een soort massahuwelijk. Zo'n 40 mensen met een papiertje, identiteitsbewijzen en een pen in de hand die een full mesh marriage aangingen, voor veilige communicatie tot digital death hen scheidt. Het gaf een mooi beeld.

De PGP-signing-party

Eric Luijf - Keynote - Het blijft dweilen met de kraan open

Eric is al jaren een vaste waarde in ICT-beveiligingsland en dan vooral in het domein van de industriële automatisering (aka

SCADA / IA / PA / ICS / PCS afhankelijk van je afkomst). Hij citeerde vandaag beelden diep uit de vorige eeuw, toen data-gijzeling, wachtwoordloze ICT en programmeerfouten al net zo gewoon waren als nu.
En waarom is dat zo? Omdat niemand echt duidelijk vraagt om een veilig systeem. Daarom maken we het niet, waarna er weer kalveren verdrinken en we de security er aan gaan plakken. En zo wordt het er nooit ingebouwd, ook al weten we nog zo goed dat het zou moeten. Het grote verschil met het verleden is de breedte waarop we ICT inzetten en dat leidt tot heel nieuwe situaties. Zoals een schip dat stilvalt op de Noordzee omdat de besturings-PLCs besmet zijn via een mailtje naar een matroos, een Boeing 787 waarin je vanuit de toeristenklasse mag meesturen met de piloot, hartbewaking die tussen de slagen door een download afmaakt via Kazaa. En we gaan nog horen van Smart tv's die ons leven opnemen (en niet uitgezet of gepatcht kúnnen worden), gehackte (en verongelukte) auto's en nog heel veel meer. Tenminste als we onze houding tegenover nieuwe technologie niet aanpassen. En aanpassen, nou dat doen we nog niet echt.
Eric hoopt op een ontwikkeling die hij CyberSecurity 2.0 noemt, waarbij we serieus aan CyberScience, CyberEngineering en CyberEducatie gaan werken.
In de VS en UK wordt er al wel hard aan deze stappen gewerkt. Wat doen wij in onze kikkerlandje bomvol ICT en PLC? Draaien we de kraan ook wat meer dicht of blijven we gewoon verder dweilen?

Eric kleurt wel met heel donkere tinten, maar zijn schildering herken ik. De meeste mensen hebben een heel praktische manier van met risico's omgaan: als we het kunnen negeren genieten we ondertussen graag van de vele voordelen. De problemen zien we dán wel weer. En - het moet gezegd - die houding heeft ons mensen vooral veel goeds gebracht.

Teun van Dongen - Maakt data verzamelen over dreigingen ons veiliger?

Terroristische organisaties gebruiken digitale middelen en internet intensief en slim. Het idee dat meer informatie over deze wandelende dreigingen tot meer inzicht leidt over hun intenties en plannen is bewezen onjuist, want er zijn rondom aanslagen wel érg veel signalen gemist, vooral door gebrekkig delen en analyseren. De aanstelling van de coördinator terrorismebestrijding is hiervan een direct gevolg. Na eerdere beweringen van het tegendeel (zelfs door de NSA-baas zelf) is gebleken dat het succespercentage uiterst laag is en aanslagen veelal verijdeld worden door heel andere voorvallen, gedragingen van verdachten en andere waarnemingen. Daarnaast hebben datapatronen zeer beperkte voorspellende waarde, omdat terreur vaak niet op een voorspelbare manier tot stand komt.
Dus eerst beter gebruiken, dan pas meer informatie verzamelen. Meer informatie levert schijnveiligheid. Koppelen en delen van wat er al is levert veel meer op dan nog meer verzamelen.

K. Reid Wightman met zijn PGP-signature

K. Reid Wightman, Digital Bond labs - Vulnerability inheritance in PLC's

Digital Bond doet sinds 14 jaar in adviezen rondom ICS (Industrial Control Systems) en daarnaast veel vulnerability testing.
PLC-libraries worden door zeer weinig leveranciers gemaakt. Ze zijn een belangrijk element in ICS, want hierop draaien de feitelijke instructies aan machines die onze omgeving besturen, zoals bruggen, sluizen, pompen, klimaatinstallaties.. afin u weet het wel. De OSen eronder, WindowsCE of VXWorks, doen veel aan security en updates, maar doet de library-leverancier dat ook? Keith analyseerde een breed gebruikte library: CoDeSys van 3S Software = PLC 'ladderlogic runtime'-code die door 28 verschillende PLC-makers wordt gebruikt, waaronder ABB, Mitsibushi, Eaton etc..
De library is de applicatielaag die makkelijk benaderbaar is via een GUI en ook over API's en kan dus ook door gecompileerde binaries worden aangesproken. Het ecosysteem omvat ook een HMI/MMI, een engineering-station, een librarian en een gateway-server.. die onderling in cleartext over IP communiceren. Dan blijft voor access-control alleen nog authenticatie over, toch? Versies 2 én 3 van CoDeSys bevatten veel kwetsbaarheden, waarvan de belangrijkste wel ongeauthenticeerde upload van nieuwe ladderlogic (ook rootkits worden geaccepteerd en opgestart), commandline-access voor start en stop etc.
Onderwijl draait CoDeSys-runtime met admin-privileges op het gast-OS, vreet wat je hem voert en is zo een gewillig hulpmiddel voor de creatieve hacker.
Een zo onveilig ontworpen systeem 'patchen' is eigenlijk

onbegonnen werk en zolang de fabrikant liegt over kwetsbaarheden helemaal.
De systemen worden gebruikt in veel industrie robots maar ook in Airco-systemen en op tenminste één ferry in Nederland. Al deze systemen 'erven' dus ook de kwetsbaarheden van CoDeSys. Het vinden van kwestbare hosts is met Shodan simpel en goedkoop geworden.

Dit soort verborgen SPOVs (Shared Points Of Vulnerability) maken ICS veel kwetsbaarder dan je zou vermoeden, afgaand op de schijnbare diversiteit aan merken die allemaal steunen op hetzelfde onveilige fundament.
Grote waardering voor deze Mr. Wightman en zijn inspanningen en het bevestigt het beeld dat Eric neerzet: we vragen niet echt om veilige systemen, want zouden we dat doen, dan bestonden deze kwetsbaarheden allang niet meer. Het staat 2-0 voor Eric.

Erwin Kooi - Secure Smart grids

Erwin tikte in het begin van zijn presentatie Eric op de vingers, want de afschakelfunctie van Smart Meters, die in het boek BlackOut zo'n prachtige kans voor terroristen biedt is door de energieleveranciers terzijde geschoven en is dus in onze huizen straks niet te vinden. Eric verliest een puntje: 1-1.

Onze Erwin Kooi spreekt over .. SCADA!!!

De Smarts van de grids schuilt alleen in veel meer dan de meters thuis. De Bommelerwaard had gewoon door kunnen zoemen als het net slim genoeg was geweest om alle lokale energiebronnen te benutten en door te geven. Maar 3% van het verbruik kwam op het bewuste moment door de kapot gevlogen kabel. Een duidelijk potentieel voordeel van een SmartGrid dus (1-2 tegen, Eric, of toch niet?). Smart is handig maar computers zijn manipuleerbaar en dus heel risicovol om in te zetten, zoveel hebben we wel geleerd. Daarom is security een onvoorwaardelijk onderdeel van deze nieuwe ontwikkelingen. Dat hebben de netbeheerders zelf ook al wel gezien.
Er wordt actief onderzoek gedaan naar een goede beveiliging van 'the grid'. Daarbij wordt het model van anticiperen – detecteren – reageren – evalueren gebruikt met een duidelijke definitie van wat security is (en ook niet is). Niet alle hacks zijn te voorkomen, maar wel snel te detecteren, zodat er adequaat kan worden gereageerd. Verliest Eric nóg een puntje?

Hans de Vries, NCSC - Responsible Disclosure

Nederland wordt als 'Digital Gateway to Europe' beschouwd en dat is eigenlijk ook zo. AMS-IX is het grootste internetknooppunt ter wereld, NL is nummer 1 wat online bankieren betreft en 94% van de huishoudens heeft meer dan 1 'PC' in huis (is ook tablets, smartphones). Van de Nederlanders winkelt 62% via internet en daarmee zijn we de 4e in de EU.
Internet biedt naast veel mogelijkheden ook risico's, waarvan de grootste dreigingen op dit moment Cybercriminaliteit en Cyberspionage zijn. De schade is jaarlijks ca. 9 miljard dat komt neer op 530 euro per Nederlander. De pakkans is gering, eigenlijk veel te laag, vindt Hans. Is het nu allemaal slecht? Nee, zeker niet want NCSC heeft goede relaties en werkt goed samen met NCSC's van andere landen en de 12 ISAC's van de Nederlandse Vitale sectoren.
NCSC verzamelt data om inzicht te krijgen welke dreigingen op ons afkomen om zo de resilience (weerbaarheid / weerstand tegen aanvallen) van de Nederlandse vitale sectoren te verhogen (ik vraag me af: zou Hans de presentatie van Teun van Dongen ook gezien hebben?).
NCSC geeft daarnaast adviezen en helpt ook waar nodig bij crises, monitoren en response, rapportages (op de website), relationeel beheer. Relaties onderhouden zodat een goede samenwerking tot stand komt.
Waarom is juist samenwerken in cybersecurity zo belangrijk? 'Eigenlijk is samenwerking een maatschappelijke plicht', vindt Hans. De digitale dreigingen en de impact nemen toe. Cyber is overal en iedereen wordt er door geraakt.

Met Responsible Disclosure (RD) kunnen we veel betere beveiliging realiseren. Niemand heeft immers nog een kennismonopolie en met de ontwikkelingen die alleen maar sneller gaan, is de hulp van Helpende Hackers heel welkom (lees het boek over de Helpende Hackers van Chris van 't Hof - www.helpendehackers.nl).
Mét Eric is Hans van mening dat er ook veel meer aandacht voor security bij ontwikkelaars (codekrassers) nodig is voor veiliger software. Maar of dat kans maakt? Ik volg de gedachtegang van Eric en zet mijn kaarten op RD waarmee de stand 1-1 blijft en we allemaal toch weer gelijk hebben.

André Beerten CISSP CISM CISA. André is bereikbaar via andre@octopus-ib.nl

INTERVIEW

VINGERAFDRUKKEN TEGEN FRAUDE

Vingerafdrukken met een maatschappelijke functie: GenKey weet er alles van. Het bedrijf ontwikkelt technologie voor vingerafdrukherkenning en vermarkt die in onder meer Ghana. De inzet van deze technologie gaat identiteitsfraude tijdens verkiezingen en in de gezondheidszorg tegen en zorgt voor een betrouwbare administratie in Ghana. Inmiddels zijn ook andere Afrikaanse landen geïnteresseerd.

"Op de klassieke manier kun je middels een algoritme twee- tot vierduizend vergelijkingen per seconde maken, met onze FastAFIS-technologie zijn dit er honderd miljoen." Michiel van der Veen, CEO bij GenKey, heeft het over de unieke snelheid waarmee het bedrijf vingerafdrukken kan vergelijken. De eigenschappen van een vingerafdruk worden vertaald naar een binaire code, waardoor de computer in een database razendsnel kan zoeken naar een overeenkomst. "We hebben slechts één pc nodig om in één seconde een lijst van tien miljoen personen te doorzoeken."

Van afdeling naar zelfstandig bedrijf

De techniek voert terug naar 2001, toen bij Philips Semiconductors (het huidige NXP) werd gewerkt aan een softwarelaag in de chip van het paspoort. Na het verzelfstandigen van NXP bleef GenKey achter bij Philips, zonder afzetmarkt. Van der Veen: "Er zat zestig manjaren werk in de technologie, daar wilden we meer mee. Er werd gedacht aan een nieuwe toepassing in ontwikkelingslanden waar de basisadministratie van de bevolking vaak niet volledig op orde is." In 2008 werd GenKey een zelfstandig bedrijf en dat leidde

uiteindelijk naar Ghana. Daar was biometrie al in meer of mindere mate bekend, maar werd nog niet op grote schaal toegepast.

Ghanese verkiezingen

In 2012 stond het bedrijf voor de grootste uitdaging sinds de start. Van der Veen: "Voor de presidentsverkiezingen in Ghana hebben we in negen weken tijd de ruim 14 miljoen stemgerechtigde kiezers geregistreerd. We namen bij de Ghanese bevolking 10 vingerafdrukken per persoon af, zo'n 140 miljoen vingerafdrukken totaal. Dat is nauwkeuriger dan een afdruk van maar één vinger. Want hoewel een vingerafdruk uniek is, kunnen bewegingen of harder of zachter drukken tijdens de scan ervoor zorgen dat er toch overeenkomsten zijn op zo'n grote groep mensen. Met tien vingerafdrukken van één persoon is die kans vrijwel nihil."

Maatschappelijke bijdrage

De technologie draagt ook op het gebied van gezondheidszorg haar maatschappelijke steentje bij. Om je in Ghana te registreren voor het nationaal ziekenfonds, moet je betalen. Dat resulteerde in identiteitsfraude. "Familieleden gaven elkaar hun ziekenhuispasje door of ze gebruikten een valse naam", zegt Van der Veen. "Dat scheelde de Ghanese gezondheidszorg miljoenen aan inkomsten. Als mensen zich nu in het ziekenhuis melden, nemen ze hun pasje mee met daarop hun opgeslagen vingerafdruk. Ter plekke wordt de identiteit van de patiënt nogmaals geverifieerd door zijn vingerafdruk te scannen. Deze verificatie kan razendsnel door de geavanceerde techniek." De inzet van de vingerafdruktechnologie zorgt ook voor een kwaliteitsverhoging van de zorg. Van der Veen vervolgt: "Artsen weten zeker wie ze voor zich hebben en kunnen daardoor bijvoorbeeld makkelijker een bloedtransfusie toedienen. We dragen ook bij aan een update van het bevolkingsregister. De basisadministratie was niet op orde en met de gescande vingerafdrukken is die lijst nu ontdubbeld en opgeschoond."

Michiel van der Veen
CEO GenKey

Edwin Paardekooper
RVO.nl-adviseur

Financiële ondersteuning

Om de technologie geschikt te maken voor de Afrikaanse markt maakte GenKey gebruik van

Maaike Belder werkt bij Voxx Communicatieadviseurs. Zij schrijft in opdracht van RVO.nl over innovatief ondernemen en is bereikbaar via mbelder@voxx.nl.

financiële ondersteuning van het Rijk. Van der Veen: "Om de snelheid en nauwkeurigheid flink te verbeteren, waren nieuwe investeringen nodig. Daarvoor vroegen we het Innovatiekrediet en WBSO aan." Beide regelingen komen van het ministerie van Economische Zaken (EZ) en worden uitgevoerd door de Rijksdienst voor Ondernemend Nederland (RVO.nl). RVO.nl ondersteunt innovatieve ondernemers en wijst ze de weg naar financieringsmogelijkheden, zakenpartners, kennis en regelgeving, en fiscale voordelen. RVO.nl-adviseur Edwin Paardekooper: "Het Innovatiekrediet is een rentedragende geldlening van maximaal 10 miljoen euro, bestemd voor veelbelovende, innovatieve projecten die binnen enkele jaren leiden tot nieuwe producten, processen of diensten. Na afloop van het project betalen de bedrijven krediet en rente terug. De aflossingen komen terecht in het revolverende Innovatiefonds MKB+, voor de financiering van andere baanbrekende innovaties. De Wet Bevordering Speur- en Ontwikkelingswerk, WBSO, verlaagt de loonkosten van R&D-trajecten. Met deze fiscale regeling wil EZ ondernemingen stimuleren meer te investeren in onderzoek."

Vermarkten in Afrika

Na het succes in Ghana bevindt GenKey zich tegenwoordig ook in Mozambique, Kameroen, Kenia en Tanzania voor het registreren van de bevolking of kiesgerechtigden. Van der Veen weet inmiddels veel van vermarkten in Afrika. "Je moet het zelf doen, maar tegelijkertijd kun je het niet alleen. Direct aankloppen bij primaire klanten, zoals bijvoorbeeld het kiescomité in een land, werkt niet. Het is essentieel om samen te werken met een lokale partner. Een partij die het land kent en de bureaucratische weg weet. Ook nauwe contacten met ambassades zijn belangrijk. Het duurt gemiddeld één tot anderhalf jaar voor we tot actie kunnen overgaan. Die periode bestaat voornamelijk uit adviezen inwinnen en investeringen doen. Je hebt als nieuwkomer niet zomaar voet aan de grond." Naast de Afrikaanse landen is de UNHCR, de VN-organisatie die vluchtelingen ondersteunt, gebruiker van de technologie. Zij leggen de vingerafdrukken van deze groepen mensen vast, op dit moment in bijvoorbeeld Tsjaad.

Privacygevoeligheid

Dat GenKey zich voornamelijk buiten Europa beweegt, heeft volgens Van der Veen een reden. "In de westerse wereld is eerst een langdurige discussie nodig voordat een privacyrespecterende oplossing kan worden ingevoerd. In Afrika gaat men daar pragmatischer mee om als het helpt om fraude te voorkomen. Toch ben ik benieuwd of we in Nederland over tien jaar nog steeds met potlood en papier naar de stembus gaan. De nieuwe generatie heeft geen problemen met de vingerafdrukscanner op hedendaagse smartphones, dus wat mij betreft is het slechts een kwestie van tijd voor we vanaf de bank elektronisch stemmen." Tot het zover is, richt de onderneming zich op Afrika als leading market en Azië en Latijns-Amerika als potentiële afzetmarkten. Van der Veen: "Daar liggen genoeg mogelijkheden. We groeien nog steeds, dat is goed te zien aan ons personeelsbestand: in 2008 startten we met zes man, inmiddels zijn dat er vijftig." Bang voor concurrentie is Van der Veen niet. "De gevestigde orde is met grote systemen en agressieve prijzen een luis in de pels. Maar met onze unieke techniek, uitgebreide ervaring en rijke contacten tellen we meer dan mee."

VERSLAG

IDNEXT-EVENT

Op 15 en 16 april 2015 vond een nieuwe editie plaats van het IDnext-event. Alweer de vijfde editie, reden voor de programmacommissie om een excellent programma samen te stellen, met een keur aan onderwerpen uit de wereld van de digitale identiteit. Het evenement vond plaats in het NH Leeuwenhorst conferentiecentrum in Noordwijkerhout. Daar werd ook het congres van de NVVB (Nederlandse Vereniging voor Burgerzaken) georganiseerd, en op de tweede dag was er een gezamenlijk plenair programma.

Auteur: Robert Garskamp is oprichter van IDentity.Next.

Op de openingsdag van het IDnext-event verwelkomde Robert Garskamp, oprichter van het IDnext-platform, de aanwezigen van dit jaar. Met een overzicht van de sprekers en onderwerpen van de laatste vijf jaar ging het programma van start, met ook een aansprekende presentatie van Jerry Fishenden. Jerry (voorzitter van de Britse Government's Privacy and Consumer Advisory Group) gaf inzicht in de initiatieven van de Britse regering op het gebied van identiteit vanuit het perspectief in verleden, heden en toekomst. Jerry concludeerde dat de publieke sector de burger centraal en in controle van de eigen persoonsgegevens moet plaatsen.

Onze volgende spreker (en we zijn zeer blij dat ze erbij kon zijn) was Joni Brennan (executive director van Kantara Initiative). Ze begon haar presentatie over Identiteit als de 'I' in het IoT. Ze stelde dat identiteitsmanagement essentieel is voor het Internet of Things - omdat mensen geen dingen zijn, maar belangrijke

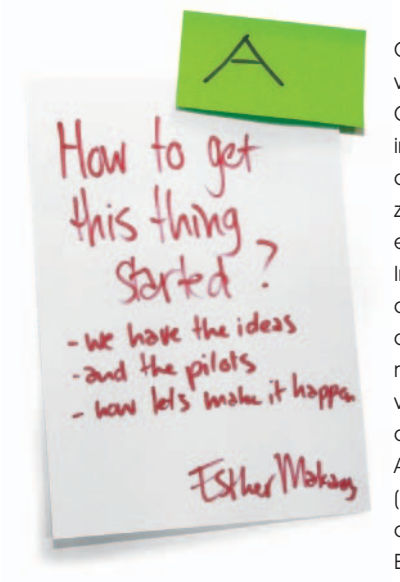
actoren blijven in ons dagelijks leven, nu en in de toekomst. Joni noemde ook het User Managed Access (UMA)-protocol, waarmee zowel het delen van toegangssleutels als meer beveiligingsopties voor de toegang tot onze gegevens mogelijk zijn, evenals een uitgebreide platformaanpak. De laatste spreker van de openingssessie was Ruben Hornbach. Voor wie het nog niet wist: Ruben is al geïntegreerd in het digitale leven, door het implanteren van een NFC-chip in zijn arm. Hiermee maakt hij verbinding met het Internet of Things. Het openen van zijn deur met deze chip is voor hem de gewoonste zaak van de wereld. Ruben sprak ook over nieuwe groeiende technologieën, en hoe deze ons dagelijks leven sterk beïnvloeden. Ruben gelooft in het verbinden van consumenten en bedrijven met de wereld van morgen, door het onder de aandacht brengen van de praktische toepassingen van futuristische apparatuur.

Na de netwerkpauze gingen de breakoutsessies van start, met de 'Identity of Things'-track. Allessandro Festa (Dell) sprak over BYOI (Bring Your Own Identity), van identiteitssilo's tot multi-identiteit-relaties. Immers, op het Internet weet niemand wie en wat je eigenlijk bent. Aansluitend daarop refereerde Jurgen van der Vlugt (Maverisk) aan Your Things' Es – Ich – Über-Ich. Jurgen noemde een beroemd citaat van Morpheus (in de Matrixfilm): "Je moet begrijpen dat de meeste van deze mensen niet klaar zijn om losgekoppeld te worden. En velen van hen zijn zo gewend, zo hopeloos afhankelijk van het systeem, dat ze zullen vechten om het te beschermen." De 'Identity of Things'-track werd afgerond door Bert van Beeck (Forgerock) voor wie identiteit het middelpunt is van alles. Bert noemde de Identity of Things voor Smart Cities als San Francisco, waar verkeersregelaars, luchtvervuiling- en overstromingssensoren de tentakels vormen van een hybride identiteits- en toegangsbeheersdienst.

Parallel daaraan liep de 'Innovation is Key'-tracks, met Dr. Niefeld die sprak over de Bio-pin. Bio-pin maakt het mogelijk een unieke e-ID te genereren via het unieke lichaamsmateriaal. Bij verlies is het mogelijk een nieuw uniek ID te genereren met dezelfde informatie. Irwin Oedayrajsingh Varma gaf inzicht in JanusID, een uitgebreide oplossing waarmee een goedgefundeerde en simpele benadering mogelijk wordt van identiteit, privacy en vertrouwen bij transacties via het Internet. Hierbij is de dienstverlening aan zowel consumenten als bedrijven het uitgangspunt. Lucas Rijen (RDC inMotiv) gaf als laatste spreker inzicht in Mobi-ID, dat gebruikt kan worden als een standaard voor identiteits- en toegangsbeheer in de automotive-wereld.

Na de lunch was het 'Unconference'-deel van IDnext geprogrammeerd. Dit Unconference-format creëert ruimte voor leren van elkaar, samenwerking en creativiteit. Bij aanvang komt de hele groep deelnemers samen, en wordt ieder begeleid door het maken van een agenda. Het IDnext-event is opgezet om deelnemers te helpen de tijd en ruimte te vinden met elkaar te praten en van elkaar te leren.
Aan het eind van het Unconference-programma werd de Identity Innovation Award toegekend aan het beste nieuwe concept of product op het gebied van digitale identiteit. De winnaar van dit jaar is Trulioo. Trulioo levert een sterke service voor de online verificatie van identiteiten. De klanten van Trulioo hebben toegang tot ruim 140 databronnen waarmee de identiteiten van drie miljard mensen in meer dan veertig landen op hun echte waarde kunnen worden ingedeeld.

Naast Trulioo waren er nog twee andere innovatieve oplossingen genomineerd voor deze prijs. Moby Face biedt een kostenbesparende en veilige oplossing voor out-of-band verwerking op basis van sterke authenticatie. Bio-pin maakt het mogelijk een uniek e-ID te creëren via uniek lichaamsmateriaal. Bij verlies is het mogelijk een nieuw uniek ID te genereren met dezelfde informatie.



Aan het eind van de dag gaf David Goodman (executive-director EEMA) een inspirerende afsluitende presentatie over het identificeren van de toekomst. Hij stelde dat de zorgen rond identiteit zijn gegroeid: organisch, onvoorspelbaar en zonder enige heldere strategie. Daarom liet David zijn gedachten gaan over de mogelijke relaties tussen de door mensen geconstrueerde en gebruikte identiteiten, online en offline. Deze lange dag werd afgesloten met een informele netwerkborrel voor de deelnemers van IDnext en NVVB.

Op de tweede dag hadden IDnext en NVVB een gezamenlijk plenair programma. Na de opening door Humberto Tan gaven Dagmar Winkelhorst (vice-voorzitter NVVB) en Robert Garskamp (oprichter IDnext-platform) een korte introductie waarin de eerste dag en de hoogtepunten van de tweede dag werden samengevat.

Openingspreker Hans van der Stelt (directeur van het Nederlandse bureau Nationaal Commissaris Digitale Overheid) gaf een inzicht in het Digitaal 2017-programma van de Nederlandse overheid. Hans en zijn team zijn verantwoordelijk voor de realisatie en het effectieve gebruik van de Generic Digital Infrastructure (GDI). Hans merkte op dat digitale transacties met de Nederlands overheid veilig, betrouwbaar en eenvoudig moeten zijn. Het is duidelijk dat de doelen van het programma ambitieus zijn maar hoe dan ook noodzakelijk.
Aansluitend gaf Joost van der Vleuten (beleidsmedewerker binnen DC-connect van de Europese Commissie) zijn inzichten in de Europese ontwikkelingen. Joost noemde dat Nederland het goed doet op de Digitale agenda, met een derde plaats tussen EU-landen, na Zweden en Denemarken. Maar toch is één van de zwakheden van Nederland het gebrek aan elektronisch factureren en online verkopen. Joost concludeerde dat het creëren van eenheid en het nemen van beslissingen over tal van onderwerpen op de Digitale agenda met 28 verschillende bestuursmodellen een uitdaging blijft.

Daarna was het tijd voor een speciale gast van het IDnext-event: Marie Johnson (Managing Director en Chief Digital Officer van het Centre for Digital Business). Marie beschreef de

digitalisering in Australië, en verschillende strategieën die waren gekozen om alles bijgewerkt te houden. Volgens een rapportage over identiteitsfraude en -diefstal in 2014 kost identiteitsfraude de Australische economie meer dan 1.6 miljard Australische dollars per jaar. Digitalisering van de identiteiten van natuurlijke personen en organisaties in Australië (met haar meer dan 23 miljoen inwoners) is gaande, maar nog steeds vinden talloze transacties met de Australische overheid alleen op papier plaats. Marie gaf een voorbeeld van hoe iemand die een kapsalon wil starten minstens 27 formulieren nodig heeft voor de daadwerkelijke opening. Menno Lanting besloot dit gezamenlijke plenaire programma met zijn blik op organisaties – en hoe te veranderen. Volgens Menno is de gevaarlijkste zin "Zo hebben we het altijd al gedaan".

Tussen de presentaties door werd er een drone geschonken door de Oxford Computing Group (OCG), één van de sponsoren (maar ook NETIQ, Forgerock, NotarisID en Experian) van IDnext. Hij werd gewonnen door één van de deelnemers die een visitekaartje hadden achtergelaten bij de OCG-stand.

Direct na de lunch startten de breakout-sessies rond verschillende thema's. Zoals 'eCitizen' (waarmee burgers hun digitale identiteit krijgen) met Freek van Krevel (Ministerie van Economische Zaken), die vanuit een nationaal perspectief sprak over de regulatie van elektronische identiteiten en beveiligingsdiensten. Erik van Zuuren (Trustcore) besprak de situatie van de Vlaamse overheid en haar stichtingen rond e-Identiteit. Bernadette Verberne (Manager ICT van de Koninklijke Notariële Beroepsorganisatie was de volgende spreker. Ze sprak over betrouwbare digitale identificatie waarin de notaris een duidelijke rol kan spelen. Ze noemde ook de ontwikkeling van NotarisID, waarmee problemen zoals identificatie, authenticatie en vermindering van aansprakelijkheid opgelost kunnen worden.

Na een korte pauze besloten Rob Laurence (Innovate identity) en Bart Renard (Vasco) deze lijn. Rob gaf zijn blik op de digitale

economie of Burgermanagement. Bart stelde het nationale eID-schema centraal in de levering van beveiligde digitale identiteiten.

Parallel, in de 'Social Consumer'-track (rond ontwikkelingen van de sociale consument c.q. eindgebruiker), gaven Eefje van der Harst (Surfnet) and Nick Smaling (Deloitte) hun presentaties over veilige toegang tot cloud-applicaties voor het hoger onderwijs en onderzoek. Samen met zijn collega Marcel van Kleef stelde Nick zich de toekomst van de digitale identiteit voor: hoe voorwerpen geloofsbrieven zullen vervangen, en hij gaf een voorlopig resultaat van het onderzoek door Deloitte en IDnext. Hugh Steed (Experian) sprak over de verborgen gevaren van inbreuk in verband met de persoonsgegevens (en hun waarde), wanneer de gemiddelde consument beschikt over 26 online accounts en een gemiddeld aantal van slechts vijf wachtwoorden om deze te beveiligen.

Privacy is onontbeerlijk in de wereld van de digitale identiteit. De 'Privacy Eye'-track (privacy is geen eenduidige informatie meer) omvatte presentaties van Jelte Jansen (SIDN) over het privacy-framework van DNS Big Data-applicaties, en Erwin Bomas (Kennisnet), over of de student centraal moet staan in een gebruikersgerichte identiteitswereld. De laatste toonde zich een voorstander van het verplichtstellen van de UMA-standaard (geïnitieerd door Kantara Initiative).

Dit vormde de afsluiting van twee volle dagen van het delen van kennis en ervaring, en netwerken tussen experts van de digitale identiteit. We willen nogmaals graag onze partners danken. Zonder hen hadden we dit evenement niet kunnen laten plaatsvinden.

Links

Presentaties zijn beschikbaar via: http://idnext.eu/en/events/the-european-digital-identity-event-2016/report-idnext-2015/

VERSLAG

CISO 5, de jaarlijkse Esmeralda-lezing op 3 juni 2015

ETHICS AND BIG DATA

Over het nut van ethische vragen rond de toepassing van technologie zal niet veel misverstand bestaan. De centrale rol van technologie in de maatschappij is iedereen duidelijk net als het feit dat er te vaak vergeten wordt fundamentele vragen te stellen rond technische ontwikkelingen. Jeroen van den Hoven, hoogleraar ethiek en technologie aan de TU te Delft, is er helder over: het gaat erom zorgen te vertalen in requirements in plaats van zwartgallig te gaan doen over nieuwe ontwikkelingen. De professional, de deskundige zal geconfronteerd moeten worden met ethische aspecten. Dat zorgt voor nuance in de discussie en helpt de ontwerper van technologie.

Tegenwoordig is alles slim, overal is data, de opslag- en verwerkingscapaciteit lijken geen grenzen te kennen. De 'big data society' onderscheidt zich door de mogelijkheden van toepassingen die data gebruiken om patronen te herkennen en te voorspellen op allerlei gebieden. Dat heeft gevolgen voor de maatschappij. Jeroen gaat daar nu niet op in maar verwijst naar het boek van Alex (Sandy) Pentland, 'Social Physics.'

Jeroen van den Hoven

Jeroen wijst erop dat 'spullen' de maatschappij en het leven structuur geven, iets waaraan de mens behoefte heeft. De ethische problemen die hij ziet bij 'big data' zijn:

- **Kennis**
- **Gelijkheid**
- **Democratie**
- **Privacy**

Bij het aspect kennis is complexiteit een belangrijk element. Overziet de gebruiker nog wat er in het wereldwijde net omgaat? Snapt hij/zij de onzuiverheid van zoekmachines, fouten in algoritmes? Is betrouwbaarheid van aangeboden gegevens controleerbaar? Zijn er nog bruikbare getuige-deskundigen? Jeroen stelt dat expertise onderdeel is van het probleem en niet meer de oplossing.
Gelijkheid: Wie beschikt over de informatie? Met moderne middelen kan een fractie van een seconde het verschil maken.
Democratie: Jeroen wijst op het boek 'The Wisdom of Crowds' van James Surowiecki, maar waarschuwt dat dit alleen opgaat voor een verzameling mensen die onafhankelijk van elkaar een mening kunnen en mogen hebben. Dit vraagt om een maatschappelijke structuur waarvoor aandacht moet zijn bij ontwerpers en opleiders.
Privacy: Dit aspect is voor de 21e eeuw van groot belang. Persoonsgegevens zijn het nieuwe goud. Jeroen toont een aantal voorbeelden van het gebruik van persoonsgegevens die ertoe leiden dat mensen een 'aanbod' ontvangen nog voordat zij zelf de behoefte daaraan hebben gevoeld. Waar ligt de grens van fairness? Is het eerlijk om een bezitter van een Apple-

computer een hogere vliegprijs te berekenen omdat de besteller kennelijk 'voldoende rijk' is? Is het eerlijk om de abonnementen voor mobiele telefonie zo onbegrijpelijk te maken als deze in de praktijk zijn? De psyche van de klant kan worden ge(mis)bruikt met behulp van wat er aan gegevens bekend is. Jeroen noemt twee uitdagingen die het huiswerk vormen voor de 21e eeuw:

- Het oplossen van het filosofische schandaal dat het belang van privacy niet kan worden duidelijk gemaakt. Tegenover degene die bepaalde dingen 'griezelig' vindt, moet niet steeds gesteld worden '.. als je niets te verbergen hebt, ..'. Het wordt tijd dat wij leren uitleggen wat privacy betekent en waarom dat belangrijk wordt gevonden. Jeroen noemde hiervoor een aantal mogelijkheden.
- Er moet een einde komen aan de metafoor van het evenwicht. Privacy en veiligheid worden als grootheden naast elkaar gelegd en zouden 'in evenwicht' moeten zijn. Maar wat wordt daarbij gemeten? En op welke manier? Het is gewenst dat privacy en veiligheid tegelijkertijd en zonder compromissen aanwezig kunnen zijn. Innovatie vergt dus oplossingen die aan beide kanten tegemoet komen en bevredigend zijn als oplossing. Innovatie, het ontwerpen met een oog voor waarden en normen, is volgens Jeroen een morele opgave. "Als je de wereld vandaag door innovatie zo kan veranderen dat je morgen meer van je plichten kunt realiseren, dan heb je de morele plicht vandaag te innoveren.

Discussie

In de discussie werd onder meer de zorgsector genoemd als een gebied waar veel gegevens samenkomen. Governance is daar een groot probleem. 'Big data' is van niemand en er zijn geen regels voor het gebruik ervan. In dat niemandsland zal de professional een extra stapje moeten zetten om als gesprekspartner te kunnen optreden. Normatieve problemen moeten niet uit de weg gegaan worden.

Vanzelfsprekend zal er naast de ontwerpaanpak aandacht moeten blijven voor repressie. Er gaat altijd wel eens iets mis, ook al omdat niet alles te voorzien is. Alert blijven dus bij veranderingen, het gedrag van systemen en in staat blijven om negatieve gebeurtenissen op te vangen. Op iedere medewerker moet een beroep op de morele kwaliteit mogelijk zijn.

Vertrouwen betekent een reductie van transactiekosten. Daar waar in de toepassing van systemen en de overdracht van data vertrouwen ontbreekt, zal extra zekerheid moeten worden verkregen. Jeroen gelooft niet dat een behoefte aan privacy in de toekomst gaat verdwijnen. De evolutie gaat langzaam en daarom blijven wij mensen gehecht aan vertrouwelijkheid en de mogelijkheid anoniem te zijn.

Jeroen noemt vier redenen voor privacy: voorkomen van inbreuken, eerlijkheid in markten voor persoonlijke gegevens, voorkomen van discriminatie en het respecteren van morele autonomie. De eerste drie zijn ongeveer gelijk als het gaat om voor- en nadelen. Deze krijgen ook de meeste aandacht. Over de vierde, de morele autonomie, bestaan controversiële opvattingen die met culturele achtergronden te maken hebben. Daaraan wordt dan ook de minste aandacht gegeven in internationale debatten.

De naam 'Esmeralda' is ontleend aan de slottekst van de song 'Sprookje' van Jaap Fischer over het selectieproces van een prinses door haar bruidegom:

En toen mocht Hans. En Hans zei: "Ja, ik weet het nog niet, maar het moet een meisje zijn met prachtige kleren en goudblonde lokken met ogen als meren die niet kunnen jokken een mond als van honing en dan weer scherp als een mes en hopelijk is haar vader koning en zij dan prinses. Maar, ze moet Liesje heten."

En toen keek de prinses hem aan en zei: "Ik heet Esmeralda, maar zeg maar Liesje."

Esmeralda als metafoor van een centraal vraagstuk van de IB-er: authenticatie door rollen.

Cees Coumou is sinds medio 2003 gepensioneerd als senior EDP Audit manager bij KPMG. Sindsdien is hij onafhankelijk adviseur en docent aan de IT-Audit Master van de Vrije Universiteit, de opleiding Master of IT auditing van de Universiteit van Amsterdam. Zijn werk op het gebied van organisatieadvisering betrof de laatste decennia met name onderwerpen als risicomanagement, continuïteitsmanagement en informatiebeveiliging. Tussen 2005 en 2012 redigeerde hij voor PvIB 8 boeken over trends in IT-beveiliging op basis van gesprekken met vele verschillende professionals. Hij is bereikbaar via cees.coumou@planet.nl

Achter Het Nieuws

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

VLUCHTEN VAN LOT POLISH AIRLINES GEANNULEERD DOOR CYBERAANVAL

Meer dan 1000 passagiers strandden onlangs op het vliegveld van Warschau nadat hackers op de systemen van het grondpersoneel hadden ingebroken. Door de hack kwamen verschillende vluchten te vervallen en raakten er een aantal vertraagd. Wat betekent zo'n hack voor de passagiers en wie heeft er baat bij om de controle over deze systemen over te kunnen nemen? Onze redacteuren laten er hun licht over schijnen.

Rachel Marbus

Laten we eens verder doordenken waarom een aanval op luchtvaart interessant kan zijn. Stel je nu eens voor dat ze daadwerkelijk een goede ingang vinden. Je gegevens zullen maar zo op straat komen te liggen! Vluchtgegevens omvatten dankzij de verplichte uitwisseling daarvan inmiddels een schat aan informatie. Niet alleen wie je bent (tot in detail), maar ook waar je woont, waar je heen reist, hoe lang, met wie, alsook financiële data. Ik kan me heel goed voorstellen dat dit een zeer gewilde database is om te kraken. In een mum van tijd heb je van honderden mensen alle mogelijke gegevens om zonder enige moeite rekeningen leeg te trekken en identiteitsfraude te plegen. Om nog maar te zwijgen over het feit dat ze weten waar je woont en wanneer je dus niet thuis bent. Over die vertraging zou ik me dan ook niet zo'n zorgen maken.

André Koot

Het zal je maar gebeuren, heb je 'State of the Art' computer-systemen en dan word je gewaarschuwd door het CERT van je overheid dat je wordt aangevallen. State of the Art wil zeggen dat je het nieuwste van het nieuwste in huis hebt. Als je dan wordt aangevallen, dan is dat niet alleen een probleem voor je eigen organisatie, maar zeker ook voor andere organisaties die minder dan State of the Art ICT in huis hebben. Ja, serieuze problemen. Inmiddels zijn we al een paar dagen verder en is er iets meer duidelijk over de aanval: we weten ook na heel veel onderzoek niet precies wat er is gebeurd. Het lijkt op een DDoS aanval op de grondsystemen. Hierdoor werd het maken van vluchtplannen onmogelijk gemaakt. En het ergste is, het gaat om systemen die ook andere luchtvaartmaatschappijen gebruiken. Dus iedere andere maatschappij is kwetsbaar…

Een DDoS-aanval? The first attack of it's kind? Dan ben ik meteen geprikkeld om een boel rare dingen te zeggen. Een DDoS-aanval impliceert dat heel veel computers tegelijkertijd aanvragen sturen naar een IP-adres of domein. Dat gebeurt alleen nooit toevallig, het is niet zo dat ergens een idioot stuk voor stuk alle IP-adressen aanvalt. Nee, dat gebeurt vanaf het openbare internet naar specifieke domeinen of services. Die moeten ook op het openbare internet beschikbaar zijn. Eerste misschien wel domme vraag is dus: Waarom zijn de grondsystemen op het openbare


Rachel Marbus


André Koot


Dennis Baaten


Maarten Hartsuijker

internet aanwezig? Tweede vraag zou dan zijn: hoe weet iemand dat te vinden? Er zijn zoveel IP-adressen, hoe weet je zoiets te vinden en aan te vallen. Nee, dat geldt dus niet alleen voor deze grondsystemen, dat geldt voor elke service op het internet. Geen DDoS zonder publieke aanwezigheid. Dus wat doet zo'n besturingssysteem op het internet?

Onlangs was er al enige commotie over de dreiging dat passagiers in een vliegtuig toegang zouden kunnen krijgen tot de in-flight systemen van het vliegtuig. Ook hier weer de vraag: Waarom zou dat het geval kunnen zijn? Publieke, onvertrouwde systemen horen niet op interne vertrouwde systemen thuis. Dat heeft niets te maken met cyber, dat is gewoon een gevolg van het hanteren van het need-to-know principe. Maar ja, we weten allemaal dat er veel meer interne systemen gewoon op het internet hangen, de meeste daarvan niet eens beveiligd ("Veere" – "Veere" is een fraai voorbeeld). Voor de meeste van die systemen is een DDoS-aanval misschien niet eens heel spannend, als de nood aan de man komt kun je altijd in plaats van remote beheer, fysieke toegang gebruiken om de besturing over te nemen. Maar waarom een grondsysteem van een luchtvaartmaatschappij open en bloot op het internet? Dan vraag je om ongelukken. Ik vrees dat ze bij LOT nog wel meer (niet State of the Art) security problemen hebben.

Overigens zijn er inderdaad ook berichten dat er ongeautoriseerde toegang tot het netwerk van LOT was verkregen. Ongeautoriseerde toegang? Dat klinkt als een ander probleem. Ik denk dan meteen aan social engineering. En daar is niets State of the Arts aan. Dat is gewoon een teken van onvoldoende awareness. Maar dat past niet meer in mijn reactie.

Dennis Baaten (gastbijdrage)

Security Consultant bij Baaten ICT Security

Wat een hacker motiveert, is vaak moeilijk te achterhalen. Soms wordt de motivatie duidelijk omdat een aanval wordt opgeëist door een bepaalde groepering, maar dat is hier vooralsnog niet het geval. Dan kan ik alleen maar raden naar de motivatie van de hacker, en dan kom ik op fanatisme, activisme of terrorisme. Feit is dat er altijd wel iemand baat heeft bij het hacken van een computersysteem. Het is dus niet de vraag of je slachtoffer wordt van een aanval, maar wanneer. Als het zover is, kan een bedrijf zich alleen nog onderscheiden door de wijze waarop men op een dergelijke situatie reageert. Met name in 'gevoelige' branches zoals de luchtvaartindustrie, is een snelle en adequate reactie misschien wel letterlijk van levensbelang. Doordat dergelijke aanvallen (of pogingen daartoe) een grote impact hebben op de publieke moraal, krijgen ze vaak veel media-aandacht. Als gevolg hiervan kan de reputatie van een luchtvaartmaatschappij behoorlijk beschadigd raken, waardoor het vertrouwen van reizigers snel kan teruglopen. Niemand stapt tenslotte graag in een vliegtuig van een maatschappij die de beveiliging van zijn computersystemen (mogelijk) niet op orde heeft. In een reactie liet de luchtvaartmaatschappij dan ook weten dat "de veiligheid van passagiers niet in het geding is geweest", en dat "er gebruik wordt gemaakt van moderne computersystemen, en de methode van de aanval mogelijk gevolgen heeft voor andere luchtvaartmaatschappijen". Het is onbekend wat er daadwerkelijk is gebeurd, maar marketingtechnisch is de gegeven reactie een slimme zet. Feitelijk ongetwijfeld correct, maar door te stellen dat dit ook bij de concurrent had kunnen gebeuren, wordt het incident gerelativeerd in de hoop dat het vertrouwen voortduurt. Onder de noemer "never waste a good crisis" zou het mooi zijn wanneer dit incident resulteert in meer veiligheid. Medewerkers van de vliegtuigmaatschappij worden weer even op scherp gezet, waardoor momentum ontstaat dat je slim moet gebruiken om noodzakelijke veranderingen door te voeren. Dan is de overlast voor al die passagiers in ieder geval niet voor niks geweest.

Maarten Hartsuijker

Dagelijks hebben vele bedrijven te maken met de gevolgen van computermisbruik. Ze lopen door computerinbraken financiële schade op of hebben te kampen met verstoringen (bijvoorbeeld na de installatie van een Cryptolocker). Een computerinbraak in een netwerk van grondpersoneel op een Poolse luchthaven is eigenlijk geen bijzonder nieuws meer. Maar sinds 9/11 zijn we collectief natuurlijk extra verontrust als er iets misgaat in de luchtvaartsector. De vraag of er vluchten gevaar hebben gelopen, is dan snel gesteld. Het antwoord kwam ook erg snel. Binnen 5 uur was het probleem "verholpen" en konden er weer vluchtplannen verwerkt worden en vliegtuigen vertrekken. Als je zelf wel eens een inbraak in een netwerk hebt moeten analyseren weet je dat 5 uur heel erg snel is. Verder dan symptoombestrijding kom je vrijwel zeker niet, tenzij je ervan overtuigd bent dat het iets kleins is geweest. Op internet waren er dan ook diverse beveiligingsspecialisten die hun twijfels hadden bij deze "cyberaanval". Maar of het nu een cyberaanval is geweest, of een interne medewerker die ongeautoriseerd een domme fout heeft gemaakt: het voorval maakt weer eens overduidelijk hoe afhankelijk we zijn van IT en hoe belangrijk een goede business continuity planning is.

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

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

REDACTIERAAD
Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn (Capgemini)
Maarten Hartsuijker (Classity)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)

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

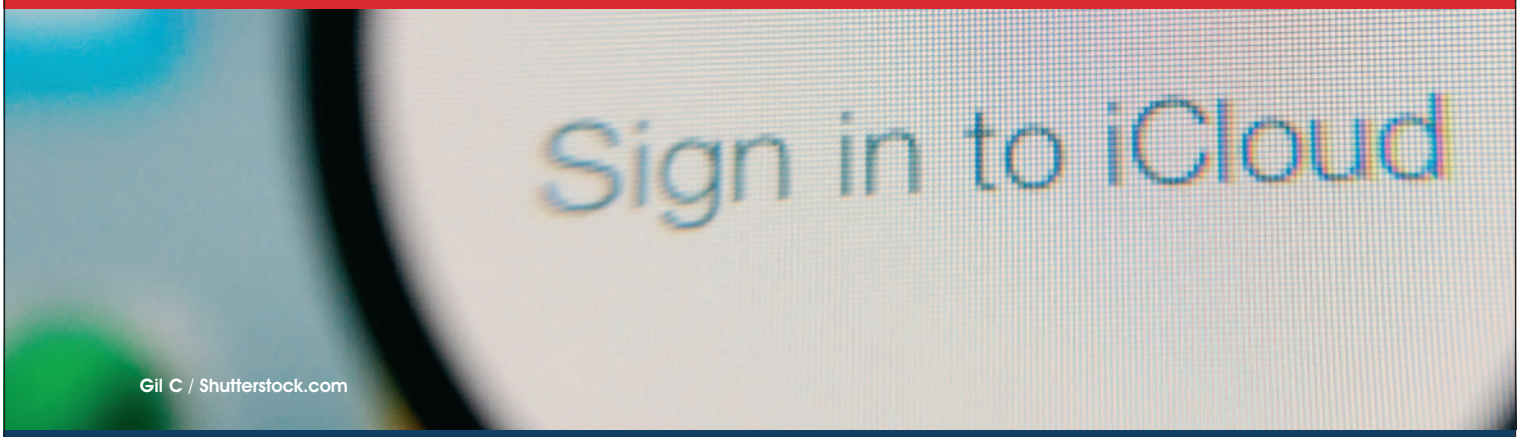
VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

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

ABONNEMENTEN 2015
De abonnementsprijs in 2015 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063



Gil C / Shutterstock.com

ELK KWARTAAL EEN NIEUWE SOAP

Elk kwartaal is er wel een nieuwe soap te ontdekken. Een dag voor de verkiezingen van de nieuwe FIFA-president deed de FBI een inval bij dezelfde club en arresteerde 7 bobo's. Er waren nieuwe bewijzen gevonden tegen de 'Bende van Blatter' en daarom moest er een dag voor de verkiezingen een inval gedaan worden. Niet om de verkiezingen te beïnvloeden maar omdat het kon. Natuurlijk werd de topman (nog) niet gearresteerd en die werd een dag later ook nog eens herkozen omdat al zijn tegenkandidaten zich terugtrokken. Vier dagen later heeft het hoofd van de bende zijn positie alweer beschikbaar gesteld. Momenteel is nog niet bekend waarom maar als uw lijfblad op de deurmat ligt, zal deze soap ongetwijfeld een vervolg hebben gehad.

Toen ik aan het zoeken was op FBI viel mijn oog op een bericht over de iCloud-hack van Apple. In deze column heb ik vaak mijn bewondering uitgesproken over de producten van dit merk maar ook met regelmaat mijn zorgen uitgesproken. Apple maakt natuurlijk producten die gebruiksvriendelijk, mooi, geavanceerd en ontzettend duur zijn. Het beschikbaar maken van al je foto's en al je bestanden op alle toestellen van jou maakt het gebruiksvriendelijk, ideaal om op je iPad je foto's van je iPhone te kunnen zien. En helemaal ideaal is dat je foto's een back-up hebben gehad, helemaal automatisch en je hoeft er niets aan te doen.

Toch zit er wel een risico aan is reeds bewezen. Ineens verschenen naaktfoto's van BA'ers (Bekende Amerikanen) op internet. Nadat het een tijdje onrustig was, bleek dat deze foto's van de iPhones van deze BA'ers kwamen. U mag van mij aannemen dat als mijn foto's gehackt worden dat er geen naaktfoto's tussen zitten maar dat terzijde.

Apple had een zootje gemaakt van zijn beveiliging. Zeer handige tooltjes als "Zoek mijn apparaat" zijn gekoppeld aan je zogenaamde Apple-ID; heel handig om te weten waar je iPhone zich bevindt of waar je iMac staat maar dat terzijde. Op deze dienst kon onbeperkt geprobeerd worden in te loggen: geen blokkades na drie mislukte pogingen maar lekker doorgaan. Als je het password van de Apple-ID kent kun je naar de iCloud om daar de back-ups te benaderen. Niemand merkte dat, inmiddels krijg je als eigenaar van het Apple-ID een mailtje dat een machine je iCloud heeft benaderd, op zich fijn om te weten dat je data wellicht is gestolen.

Kan het verhaal nog erger worden? Ja, het verhaal is zelfs nog erger. De FBI heeft onderzoek gedaan naar de hack op iCloud en kwam erachter dat een hacker duizenden keren pogingen had gedaan om binnen te komen bij de iCloud dienst zonder dat hij zijn IP-adres wijzigde. Duizenden Apple-ID werden benaderd vanaf één IP-adres zonder dat het Apple opviel. Dat is wonderlijk en erg vreemd en misschien wel een beetje misdadig want ik vertrouw mijn gegevens aan een miljardenorganisatie toe en mag er toch vanuit gaan dat die als een goed huisvader let op mijn spullen.

Misschien wordt het ergens uitgesloten in de 35 pagina's tellende gebruikersovereenkomst die je verplicht bent te ondertekenen bij het in gebruik nemen van de iCloud. Ik moet u heel eerlijk zeggen dat ik hem niet gelezen heb toen ik er akkoord mee ging en degene die dat wel heeft gedaan zal ik overhoren en als het document daadwerkelijk grondig bestudeerd blijkt dan stel ik daar een fijne fles wijn tegenover.

Tim Cook kan iedereen wel doen laten geloven dat Apple privacy en beveiliging in een zeer hoog vaandel heeft staan maar ik moet daar eigenlijk wel een beetje om lachen. Eerst maar eens kijken of Apple zijn goed huisvaderschap gaat uitoefenen. Als je wilt dat je gegevens veilig zijn zet ze dan niet op je telefoon of iPad. Ik zou daarbij graag een passend alternatief willen aandragen maar moet helaas passen.

Berry

Partnership EXIN en Security Academy

Partnership

EXIN en de Security Academy zijn een partnership aangegaan om een volledig portfolio van onafhankelijke security certificeringen te ontwikkelen. De certificeringen zijn gebaseerd op de Security Academy opleidingen en sluiten aan op het e-Competence Framework (e-CF).

Met de wereldwijde release van dit nieuwe examenprogramma versterken EXIN en Security Academy hun partnership in de voortdurende ontwikkeling op het gebied van Security en Cyber-programma's.

Alle examen programma's binnen EXIN's Security en Cyber Portfolio zijn vendor-neutral, onafhankelijk gevalideerd en beschikbaar voor alle partijen. De examens zijn wereldwijd verkrijgbaar, in meerdere talen en via meerdere examenkanalen.

De reeds beschikbare certificeringen zijn:

- Secure Programming Foundation
- Ethical Hacking Foundation

Dit jaar zullen veder ontwikkeld worden:

- Data Privacy
- Business Continuity
- Cyber Crime Essentials

Secure Programming Foundation

In deze opleiding worden de basisprincipes geleerd van het veilig programmeren. De opleiding is bedoeld voor iedere programmeur of softwareontwikkelaar die (web)applicaties ontwikkelt. De cursus bereidt u voor op het internationale Secure Programming Foundation examen van het Exin.
De cursusprijs bedraagt €1.100,- euro exclusief BTW. Dit is inclusief cursusmateriaal en catering maar exclusief het EXIN examen.

Ethical Hacking Foundation

U heeft het misschien wel voorbij zien komen, termen als SQL Injections en Cross-Site Scripting. Maar wat betekenen deze termen eigenlijk? Tijdens deze basistraining kruipt u in de huid van een hacker en leert u de basisstappen van veel voorkomende digitale inbraken. Deze cursus is uitermate geschikt voor personen die over weinig technische kennis bezitten en nieuw zijn in het vakgebied van het ethisch hacken.

De cursus bereidt u voor op het internationale Ethical Hacking Foundation examen van het Exin.

De cursusprijs bedraagt €1.100,- euro exclusief BTW. Dit is inclusief cursusmateriaal en catering maar exclusief het EXIN examen.

BEL ONS +31(0)348-408061

WWW.SECURITYACADEMY.NL
INFO@SECURITYACADEMY.NL