iB

INFORMATIEBEVEILIGING

jaargang 15 - 2015

#3

Interview RedSocks

Requirements dependency analysis

Verliefd op onveiligheid

Cyber damage control

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

MODELLEN EN CONTROLELIJSTEN

De informatiebeveiligingswereld werkt tegenwoordig vrijwel universeel volgens de IEC/ISO 27002 standaard of een afgeleide daarvan, zoals de NEN 7510, BIR of BIG. Ik werk er dus ook veel mee, maar als het moeilijk wordt, grijp ik naar iets anders, een model. Ik ben een conceptueel denker, ik gebruik graag modellen. Ik begrijp complexe zaken door modellen en ik kan de werkelijkheid structureren en inzichtelijk maken met modellen. Dat is anders dan controlelijsten (checklists). Die zijn geschikt voor operationele taken, maar ze helpen mij niet zoals modellen dat doen. Controlelijsten zijn voorgestructureerd naar een standaard, bevatten de feitelijke doelen. Modellen zijn het middel om een reis naar een onbekend doel te maken.
Oftewel: met modellen kan ik de werkelijkheid kneden, met controlelijsten is de werkelijkheid een rigide structuur.
In die zin kun je IEC/ISO 27001 als een security-managementmodel zien en IEC/ISO 27002 als een security-controlelijst. Zij die mij kennen weten dat mijn favoriete IT-procesmodel COBIT en mijn favoriete inhoudelijke security-model SABSA is. Modellen zijn geschikt om onbekende problemen in kaart te brengen en open te blijven voor alternatieve oplossingen. Modellen zijn inherent niet geschikt om exacte, accurate uitkomsten te krijgen. Wil je dat bereiken, dan moet je werken met controlelijsten. Verwacht van een model geen exacte uitkomst, wel een duidelijk pad.
Werk je met controlelijsten, dan dien je jezelf continu af te blijven vragen of je geen schijnzekerheid aan het creëren bent. Een slechte controlelijst geeft onbetrouwbare, onjuiste of onvolledige informatie. Een slecht model geeft geen uitkomst, of een uitkomst die aantoonbaar niet voldoet.
Is de IEC/ISO 27002 een goede controlelijst? Ja. Biedt het de flexibiliteit van een model? Nee. Er is plaats voor beide en gebruik het juiste middel voor het juiste doel, anders lijkt het middel niet te werken.

Lex Borger, hoofdredacteur

In dit nummer

Interview RedSocks - **4**
Requirements Dependency Analysis - **8**
Verliefd op onveiligheid - **10**
Op zoek naar een duizendpoot - **14**
Studierapport 'Algemene beheersing van IT-diensten' - **18**
Column Privacy - Hacking Barbie - **19**
In Memoriam Gert van der Pijl - **20**
OWASP - **21**
Cyber damage control- **22**
Sfeerimpressie ONE Conference - **24**
Hier word ik nou blij van - **26**
Achter het Nieuws - **28**
Column Berry - Ze doen het nog hartstikke goed - **31**

INTERVIEW

Malware-opspoorder RedSocks:

‘WE ZIJN GEEN ROEPENDE IN DE WOESTIJN MEER’

Er is in het hele kantoorgebouw geen naambordje te bekennen. Het enige dat hun aanwezigheid verraadt, is een paar rode sokjes aan de voordeur. De makers van de RedSocks Malware Threat Defender blijven liever een beetje onder de radar. Toch krijgen we een kijkje achter de schermen…

Pim Cornelissen

Pepijn Janssen

Aan het woord zijn de twee oprichters van RedSocks [1]: Pim Cornelissen en Pepijn Janssen. Pim: 'Toen we twee jaar geleden van start gingen met RedSocks hadden we niet verwacht dat het onderwerp zo 'hot' zou worden. Cyber is echt booming. We hoeven helemaal geen moeite te doen om mensen te vinden.' Het beveiligingsbedrijf ontwikkelde een kastje dat via dataverkeercontrole checkt of je systeem is geïnfecteerd met malware (antwoord: ja, ga er maar van uit van wel).

Pim werkte in 2012 voor zichzelf als beveiliger bij een grote Amerikaanse farmaceut toen dat bedrijf gehackt werd. Gegevens van negen jaar onderzoek werden gestolen en verkocht op de zwarte markt. 'De Nederlandse overheid waarschuwde ons, maar deed daarna niets meer. Daarom vloog het bedrijf de FBI in. Ik werkte op dat moment al samen met Pepijn. Hij had dankzij een voorloper van de software waar we nu mee werken al binnen drie dagen een dik onderzoeksrapport klaar waarmee we precies wisten wat er gebeurd was en wanneer.' Pepijn: 'Ik matchte verkeersgegevens bij de klant met malware-intelligence, verzameld door een groot aantal botnets te monitoren. Toen werd duidelijk dat de hackers door spearfishing via een privémailaccount op een zakelijke laptop waren binnengekomen.' Drie dagen was heel erg snel. 'Veel sneller dan de FBI. Omdat ik wist dat andere gehackte bedrijven hier ook behoefte aan zouden hebben, sloegen Pepijn en ik daarna de handen in elkaar,' zegt Pim.

Probleem van ICT

Daarna ging het snel. In december 2012 richtten ze RedSocks op om 2013 achter de schermen het product te verfijnen. En waar komt de naam vandaan? Pim: 'We wilden iets met het woord 'Red', dat doet denken aan 'red alerts', iets met gevaar. En sock komt van socket, de logische poort op je computer waar je informatie naar binnen haalt. De naam blijft hangen en voelde meteen heel natuurlijk.' Ze begonnen met het werven van 'écht technisch talent', in kleine kring. 'Techneuten vinden elkaar op basis van techniek,' zegt Pim. Inmiddels bestaat het bedrijf uit 27 man, waaronder een aantal freelancers.
Ze werken nauw samen met een paar universiteiten in Nederland. Een van de RedSocks-medewerkers promoveert ook op dat onderwerp aan de Universiteit Twente. Halverwege 2014 was het zover en konden ze de boer op. Pim: 'We merkten toen snel dat we een roepende in de woestijn waren. Want hoe krijg je hoger management geïnteresseerd in malware? Dat soort dingen zien ze al snel als 'het probleem van de ICT-afdeling' en veronderstellen ze dat alles bij hen wel onder controle is. Daarom zochten we een distributeur. Binnen twee weken hadden we een contract met Arrow Electronics en konden we de markt benaderen.' Maar hoe?
'De RedSocks Malware Threat Defender is een simpel plug & play kastje met een abonnement. Potententiële klanten mogen het twee weken testen, om te kijken wat ze 'vangen'. Door de simpelheid kost het bedrijven nauwelijks tijd om het in gebruik te nemen.' Het resultaat kan confronterend zijn, bijvoorbeeld voor

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

De analyzers van RedSocks

RedSocks werkt achter de schermen met speciale analyzers aan het verkrijgen van de juiste informatie om de RedSocks Malware Threat Defender zijn werk te kunnen laten doen.
Deze analyzers variëren van wat je zou verwachten dat een bedrijf als RedSocks zou doen, tot aan hands-on-laboratoria waarin uniek analysewerk gedaan wordt. Het zijn:

- Feeds-analyzer - dit zijn gewoon de standaard informatie-feeds die publiek in te kopen zijn, miljoenen regels per dag. RedSocks analyseert deze informatie en dikt het in tot de essentiële kennis voor de Malware Threat Defender.
- High-volume-analyzer - een virtuele sandbox waarin het gedrag van honderdduizenden malware-samples tegelijk bekeken wordt om hun netwerkgedrag te leren (her)kennen.
- Long-term-analyzer - een virtuele sandbox waarin het gedrag van malware-samples die niet aanslaan in de high-volume-analyzer wordt bekeken over langere tijd.
- Basic malware-lab - een real-life sandbox van echte systemen, dus tastbare hardware, waar weer de malware-samples op wordt losgelaten die niet aanslaan in een virtuele omgeving.
- SNMP-analyzer - een analyzer die actieve spambots registreert.
- Open-source-information - bevat de locaties van IP-adressen en bekende Tor-node.

Al deze analyzers tezamen leveren de IPs en gescripte signatures die naar de Malware Threat Defender gestuurd worden, zodat deze appliance daarmee in de netwerkomgeving van de klant zijn detectiewerk kan doen.

bedrijven in de zorg die vanwege de privacy-gevoelige patiëntengegevens drie en soms wel vier securitylagen om hun systemen hebben. 'Die verwachten dan echt niet dat daar iets doorheen komt. Toch gebeurt dat altijd: cybercriminelen zitten niet stil en dat is een ontzettende eye-opener. Het snelste gesprek duurde slechts enkele minuten. We hadden net het proof-of-concept-contract getekend, ik rijd nog niet weg of ik word al gebeld: 'We krijgen nu al threat-level1-meldingen! Daar moeten we mee aan de slag.' Of ik kon omdraaien.'
Verder heeft het bedrijf veel gehad aan de openbaarmakingen van Snowden. 'Dat bracht bewustwording bij het grote publiek.' En blijkt een aanjager voor Europese beveiligingsproducten. Een andere 'grote hulp' wordt de Wet meldplicht datalekken, die organisaties verplicht cyberlekken van informatie te melden. Bedrijven krijgen een sanctie opgelegd als ze bewust niets doen. Onder de Wbp is de maximumboete nog 4.500 euro, met de komst van deze nieuwe wet wordt dit verhoogd naar 810.000 euro of een deel van de omzet. 'Als een bedrijf onze RedSocks-doos in huis haalt, voldoen ze technisch al snel aan die wet.'

We kijken niet naar de inhoud

Pepijn: 'Klanten willen niet al hun verkeersgegevens (flowdata) naar een bedrijf sturen, dat is alsof je het in een Amerikaanse cloud onderbrengt.' RedSocks werkt dan ook precies andersom: klanten hoeven geen gegevens naar buiten te brengen om het bedrijf zijn werk te kunnen laten doen. Ze plaatsen de Malware Threat Defender juist in het bedrijfsnetwerk, de doos krijgt de nodige informatie van RedSocks. 'We kijken niet naar de inhoud van klantsystemen, maar zoeken patronen,' legt Pepijn uit. 'Verdwijnen er gegevens met een bepaalde regelmaat en wordt een connectie gemaakt met een bepaalde IP? Dan kan dat een heartbeat-trojan zijn waarlangs gegevens verdwijnen. We voeren heel veel analyses uit op de malware die we vinden, in onze speciale labs.
Door die labs te gebruiken en de lijsten met verdachte IP-adresssen en malware te verfijnen, maken wij een gigantische kwaliteitsslag op de standaardlijsten en lopen we steeds een aantal jaar voor op de rest.' Pepijn heeft een politieachtergrond. Hij werkte 'als burger' bij de Team High Tech Crime van de KLPD, in 2001. Daarvoor werkte hij op een van de eerste breedbandcomputers in Nederland, bij de Universiteit Nijmegen. 'Bij de politie was altijd discussie of je niet teveel zou uitlokken door naar malware-gedrag te kijken. Uiteindelijk is dat heel normaal geworden.'

Hoe werkt het?

De Malware Threat Defender kijkt live naar de verbindingen tussen het bedrijf en 'alles met een IP-adres' op internet en houdt bij of die IP voorkomt op de dynamische blacklist. Pine Digital Security heeft de code in de appliance geprogrammeerd. Pepijn: 'Flowdata is in elke organisatie aanwezig. Wij maken daar dankbaar gebruik van. We kopen net als iedereen lijsten in met foute IP-adressen. Dat zijn er op dit moment ongeveer tien miljoen per uur. Maximaal tien procent daarvan achten wij geschikt. Daarnaast hebben we twee jaar gebouwd aan een gigantisch malware-analyse-netwerk. Daar gaan zo'n 250.000 tot 300.000 stuks malware doorheen. Per

dag. En we monitoren live vele botnets met een focus op deze kant van de wereld. Aanvallers updaten sommige malware wel tien keer per dag. Dat krijgen wij allemaal live mee en de resultaten worden direct doorgezet naar de appliances. Desktop-antivirus wordt doorgaans geen tien keer per dag geüpdatet. Daarmee verlies je die strijd dus.'
Al deze zaken worden op drie niveaus geanalyseerd op de appliance: Hot Storage, Warm Storage en Cold Storage. Hot voor de live-blacklisting, samen met algoritmes. Warm is voor de heuristics-engine die ze met de academische wereld ontwikkeld hebben en kijkt naar gedrag. Cold Storage is voor dataretentie. Voor de wet- en regelgeving slaan ze alle 'flows' op; alle verbindingen in en uit een netwerk. Alleen de officier gegevensbescherming mag deze storage gebruiken, wat gebeurt als men een collega bijvoorbeeld niet vertrouwt.

Alles om onontdekt te blijven

Komt RedSocks malware tegen in een klantsysteem dan gedraagt de software in de labs zich ook alsof het slachtoffer ervan is geworden. Pepijn: 'We doen er alles aan om niet ontdekt te worden. Sommige malware verwacht dat de muis blijft bewegen of dat er steeds wordt getypt. Dus doen we dat ook, niet met de hand natuurlijk. Daarna gebruiken we verschillende omgevingen om malware te checken; dat zijn onze labs. Voor point-of-sales-malware hebben we een kassa gekocht en een pinautomaat. We analyseren een hoog volume aan malware. Het maakt ons niet uit of het encrypted is of niet. Of waar het vandaan komt. Alles draait bij ons om bestemmingen en gedrag van malware. Verder gebruiken we social-media-honey-pots en spamaccounts. Zo vangen we veel spear-phishing-aanvallen gericht op Nederland en branches waar we actief zijn. Die virussen checken we ook meteen in onze labs.'
Het bedrijf heeft verder een Open Source Intelligence-team dat 24/7 de donkere krochten van internet afschuimt. Ze bekijken de 'bad neighbourhoods' van internet, de slechte wijken waar je bijvoorbeeld met bitcoins criminele diensten kunt kopen. Pim: 'We vinden het heel belangrijk om de privacy van onze klanten te waarborgen. We denken hier heel goed over na. Zo kopen we bijvoorbeeld geen buitenlandse beveiligingsproducten, maar bouwen we ze zelf. Klanten kunnen ervoor kiezen om een eigen mirror-server in te richten om rapporten over gevonden malware te raadplegen. Dan weten wij zelfs niet welke klant informatie heeft opgevraagd over welke malware.'

En nu?

Het is duidelijk. Na de internationale schok en interesse over de 'informatievergaring' van de Amerikaanse NSA en andere opzienbarende hacks hoeft het bedrijf niet te vrezen over desinteresse in informatiebeveiliging. De anti-virusbedrijven zelf zeggen dat ze zeventig procent van alle malware niet meer 'aan de poort' kunnen stoppen, de techniek gaat gewoon te snel. Zelfs Gartner zei vorig jaar: 'You're already infected, deal with it'.
Pim: 'RedSocks krijgt veel interesse, ook internationaal, vooral door mond-tot-mondreclame. We bekijken of we ook naar het buitenland kunnen, maar we zijn natuurlijk wel een Nederlands bedrijf. En we werken samen met verzekeringsbedrijven als Crawford en KröllerBoom voor cybersecurityverzekeringen. We voorzien hen van input over waar je je tegen moet verzekeren en RedSocks staat in hun polis opgenomen voor een lagere premie.' Hét verschil met vroeger: 'We zijn geen roepende in de woestijn meer.' Detectie blijkt de toekomst van cybersecurity.

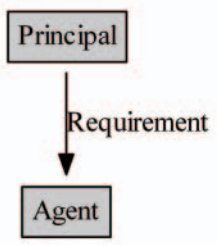
Links

[1] Homepage: www.redsocks.nl

REQUIREMENTS DEPENDENCY ANALYSIS

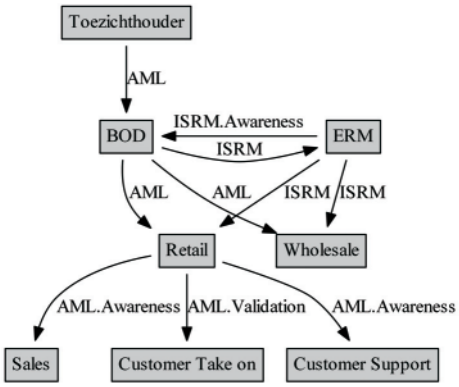
Dit artikel gaat over Requirements Dependency Analysis. We staan stil bij requirements, kenmerken van requirements en verschillende taxonomieën die met requirements te associëren zijn. De stelling is dat effectief requirementmanagement een voorwaarde is voor waardetoevoegend risicomanagement.

Geïnspireerd door terminologie uit de Principal Agent Theory [1], zien we in dit artikel een requirement als een relatie tussen een principal en een agent.



Figuur 1

Om zijn belangen behartigt te zien stelt de principal requirements op die, volgens afspraak, door zijn agents gerealiseerd dienen te worden. De agents accepteren, conform hun rol, requirements en nemen de verantwoordelijkheid op zich voor de realisatie van deze requirements. Requirements kunnen op verschillende manieren worden opgelegd aan agents. Denk hierbij aan beleidstukken, procesbeschrijvingen, referentiearchitecturen en standaarden. Derhalve kunnen requirements verschillend van aard zijn. Denk aan juridische requirements, product-requirements, functionele requirements, technische requirements etcetera. Requirements tussen principals en agents zijn te visualiseren als een gerichte graaf die we een Stakeholder-Requirements-graph noemen. Een voorbeeld dat voor de lezers van dit blad herkenbaar zal



Figuur 2

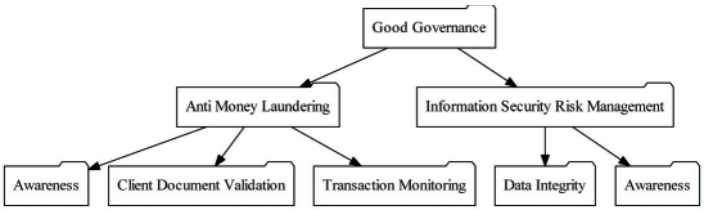
zijn, wordt in figuur 2 getoond. De grijze vlakken zijn stakeholders die principal en/of agent kunnen zijn. De requirements worden aangeduid met pijlen tussen de stakeholders. Volgens het voorbeeld legt de toezichthouder de Anti Money Laundering (AML)-requirement op aan de onderneming vertegenwoordigd door haar Board of Directors. Op haar beurt legt de Board of Directors de requirement op aan de Retail- en Wholesale-business-lines. In het getoonde voorbeeld splitst de principal van de Retail-business-line de AML-requirement in twee delen:

- AML.Awareness-requirement voor de Sales- en Customer Support-afdelingen
- AML.Validation-requirement voor de Customer Take on-afdeling

Maurice Gittens, CGEIT, CISA, CISM. Maurice werkt als consultant met informatiemodelleren, informatieverwerking, informatiearchitecturen en informatiebeveiliging. Hij is momenteel risk-strategieconsultant bij een Nederlandse Bank. Maurice is te bereiken via maurice@gittens.nl.

Requirements Taxonomy

Het onderverdelen van requirements in deelrequirements leidt tot het ontstaan van een taxonomie van requirements. Figuur 3 geeft hier een voorbeeld van en maakt aannemelijk dat we ook requirements als gerichte graaf kunnen visualiseren. Uitgaande van de algemene requirement voor "Good Governance" worden in het voorbeeld de deelrequirements om witwassen van geld tegen te gaan (Anti Money Laundering) en een requirement om aan Information Security Risk Management te doen onderscheiden. Deze requirements worden in het voorbeeld nog verder uitgesplitst.

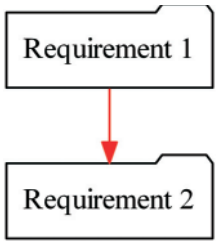


Figuur 3

Requirements-taxonomieën zijn in mijn ervaring altijd te onderscheiden in organisaties, doch zelden in expliciete zin en verspreid over verschillende soorten documenten. Onder benaming als Policy House, Risk Taxonomy, Books of Law, High-level vs Detailed Designs zal de lezer requirements-hiërarchieën kunnen terugvinden. Het komt er telkens op neer dat er een hiërarchie aan requirements wordt ingericht die bij de bedrijfsvoering in acht genomen dient te worden.

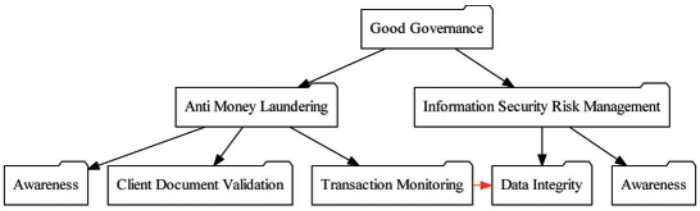
Requirements Dependency-diagram

Een Requirements Dependency-diagram is een requirements-hiërarchie uitgebreid met zogenaamde Requirements Dependency-relaties. Een requirement-dependency tussen twee requirements R1 en R2 gegeven we in dit artikel aan met een rode pijl zoals in figuur 4 getoond wordt.



Figuur 4

De pijl lezen we als: de realisatie van de requirement R1 is afhankelijk van de realisatie van de requirement R2. Dus alleen als er aan R2 voldaan wordt kan aan R1 worden voldaan. Figuur 5 toont een voorbeeld van een Requirements Dependency-diagram dat aangeeft dat Transaction Monitoring in de context van AML slechts effectief mogelijk is als er aan de Data Integrity-requirement van ISRM wordt voldaan.



Figuur 5

Een hiërarchie aan requirements wordt ingericht voor de bedrijfsvoering

Natuurlijk is in een artikel zoals dit de materie flink vereenvoudigd. Toch hoop ik dat de lezer in Requirements Dependency-graphs een instrument zal herkennen dat van waarde zou kunnen zijn.
Toepassingen van requirements-analysis zijn ondermeer:

- Business Impact Analysis; wat is de impact als er aan een requirement niet wordt voldaan?
- Threat Scenario Modeling; welke requirements kunnen we aan een riskmanagementregime stellen?
- De consensusvorming; wat zijn gemeenschappelijke requirements van stakeholders?

In het algemeen wil ik stellen dat inzicht in geldende requirements en hun onderlinge afhankelijkheden de sleutel is tot de inrichting van een Corporate-Governance-framework dat op synergetische wijze de belangen van betrokken stakeholders onderkent en accommodeert. Juist door met de requirements van relevante stakeholders rekening te houden kunnen er afwegingen en verandervoorstellen worden gemaakt die op een breder draagvlak kunnen rekenen.

Samenvatting

Requirements zijn in dit artikel gedefinieerd als een relatie tussen principals en agents. Daarnaast zijn respectievelijk een Stakeholder-Requirements-graph, de Requirements-taxonomy en de Requirements-Dependency-graph geïntroduceerd als hulpmiddelen die inzicht geven in requirements en dus waardetoevoegend zijn voor het riskmanagementproces.

Links

[1] Wikipedia: Principal Agent Theory: http://en.wikipedia.org/wiki/Principal-agent_problem.
[2] Artikel in Informatiebeveiliging: "Tethering Enterprise Interests", gepubliceerd in IB1 2015.

MANAGEMENT-SUMMARY
Waarom faalt cyber security steeds? Waarom verkiezen burgers en bedrijven functionaliteit boven cyber-veiligheid? Oftewel: waarom houden we zo van cyber-onveiligheid? Een artikel dat een pleidooi is voor een andere aanpak van cyber security en het maken en gebruiken van veiliger ICT-producten en -diensten.

VERLIEFD OP ONVEILIGHEID

Bij ontwikkelaars en gebruikers in de ICT-wereld staat veiligheid zelden bovenaan als het gaat om de belangrijkste producteigenschappen. Op de eerste plaats moet het gewoon werken. Vervolgens moet het zoveel mogelijk kunnen. En het mag natuurlijk niet te ingewikkeld zijn. Of het ook veilig is? Dat zal toch wel? Nu tegenwoordig zo ongeveer alles en iedereen deel uitmaakt van de ICT-wereld, kan het geen kwaad om eens met een andere bril naar cyber security te kijken.

Tijdens mijn studie, nu ruim veertig jaar geleden, kluste ik bij als programmeur. Zodra het programma geschreven was en in een stapel ponskaarten was omgezet, volgde het functionele testen. Werkte alles naar behoren, dan wilde je graag aan de volgende uitdagende programmeerklus beginnen. De systeemontwerper en -verantwoordelijke dacht daar anders over. Hij haalde een paar honderd ponskaarten uit de afvalbak naast de ponsmachine die je vervolgens moest laten verwerken door je programma. O wee als er ook maar één ponskaart door je programma geaccepteerd werd, dan had je heel wat uit te leggen. Het programma moest zichzelf en daarmee het totale systeem beschermen tegen iedere mogelijke vorm van foutieve invoer.

Crashes

In 1978 crashten mainframes iedere dag wel een paar keer. De kunst was de oorzaak van de meest voorkomende crashes weg te nemen. Er bleek echter een diepliggender oorzaak te zijn. Veel systeemprogramma's controleerden de invoerparameters niet. Vaak werd door een programmeerfout een ellenlange stroom gegevens (bytes) in plaats van een enkel getal aangeboden. Resultaat was een crash van het gehele mainframe door een zogenaamde 'buffer overflow'. Systematisch hebben een collega en ik meer dan honderd van dergelijke systeemprogramma's voorzien van betere invoercontrole en dergelijke fouten uit het besturingssysteem gehaald.

Wachtwoorden

Inloggen op een mainframe was in de jaren 70 eenvoudig. Je ging naar een terminal, verzon een gebruikersnaam en ging aan de gang. Geen wachtwoord was nodig. Pas veel later werden gebruikersnamen en initiële wachtwoorden uitgegeven. Sterke wachtwoorden werden geëist die na korte tijd verversing behoeven. Iedere ICT-innovatie na die tijd zoals midicomputers, minicomputers, PCs, genetwerkte PCs, tablets en smart phones vereiste geen vorm van authenticatie: het waren toch persoonlijke middelen nietwaar? Kort nadat deze systemen grootschalig ingezet werden, bleken er toch veel gevoeliger acties op de systemen uitgevoerd te worden dan eerder gedacht. Bijvoorbeeld opslag van medische gegevens, elektronisch bankieren en een het onderhouden van een verborgen tweede leven. Wachtwoorden met sterkere eisen werden achteraf alsnog toegevoegd.

Onveiligheden

Bij iedere nieuwe ICT-innovatie blijken we echter niet geleerd te hebben van de opgeloste onveiligheden tijdens de vorige ICT-innovatiegolven. Eind jaren tachtig kwamen bijvoorbeeld Unix- en netwerkomgevingen opzetten. In eerste instantie opgezet voor groepsgebruik in een besloten omgeving waren de beveiligingsmaatregelen niet bestaand of ronduit zwak te noemen. Wachtwoorden als klare tekst over het netwerk en geen invoercontrole door communicatieprotocollen waardoor systemen crashten als je er ook maar een byte meer of minder dan verwacht naar toe stuurde. Veel van dergelijke fouten werden achteraf met patches opgelost toen hackers dit type systemen en netwerken gingen openbreken of lieten crashen met bijvoorbeeld de ping-of-death. Pas recent komen de makers van procescontrolesystemen er achter dat ze dezelfde problemen hebben. Raffinaderijen zijn door dergelijke zwakheden plat gegaan omdat een ICT-beheerder per ongeluk een test losliet op het proces¬controle¬netwerk. Inmiddels weten hackers bijna iedere week nieuwe mogelijkheden open te leggen om op dergelijke systemen in te breken.

Vooruitgang

Waarom houden we van onveilige systemen? Ten eerste houden we van vooruitgang. We kunnen we niet snel genoeg nieuwe functionaliteit krijgen die de informatie- en communicatietechnologie (ICT) ons biedt. De verwarming van uw bedrijf vanaf thuis regelen? De bewakingscamera of het hek op afstand via internet besturen? Doen we! Daarnaast willen we gebruikersgemak, geen moeilijk authenticatieproces. We houden ook van de nieuwe gadgets. Het slimme horloge, de slimme bril, bedrijfsgegevens op de eigen slimme telefoon. Informatiebeveiliging? Is dat niet een vage afdeling op het hoofdkantoor?

Briljante ideeën

Ten tweede denken ontwikkelaars van de volgende generatie ICT-innovatie geheel niet aan informatiebeveiliging. Het betreft steeds vaker jonge talenten die al vroeg gescout worden met briljante ideeën om ons geluk, gemak en genot te brengen. Als je bezig bent met het ontwikkelen van apps voor de volgende generatie smartphones, smartwatches, pacemakers [1] of energiezuinige gebouwen, kijk je met een Google Glass op alleen vooruit. Dan kijk je niet terug naar de oude meuk als desktops of, erger nog, mainframes. De eerder lessen van oude beveiligingsfouten in die systemen en hun oplossingen worden daarom niet meegenomen in de ontwikkeling van de volgende generatie ICT-producten. Daarom vinden we in nieuwe producten bijvoorbeeld wederom standaard fabriekswachtwoorden en achterdeuren voor het testen, kunnen hackers opnieuw de code manipuleren door een buffer of stack overflow te creëren en kun je opnieuw cryptografische sleutels onttrekken aan het geheugen. Het is ons onvermogen om te leren van in eerdere generaties ICT geconstateerde beveiligingsfouten waardoor we hier na zo'n vijftig jaar nog steeds last van hebben.

Gebouwbewakingssystemen

Ten derde komt ICT haast ongemerkt steeds vaker in handen van medewerkers van bedrijven die alleen de functionaliteit zien en niet dat ze een te beveiligen ICT-systeem gebruiken. De noodzaak om daarmee veilig om te gaan wordt niet duidelijk uit de installatie-

instructies, de werkinstructies en de context van het gebruik. Denk bijvoorbeeld aan moderne ontruimingsinstallaties, de telefooncentrale, IP-camera's en gebouwbewakingssystemen. Maar bovenal, als dergelijke systemen niet veilig uit de doos komen, gaat het zeker fout. Producenten en systeemintegratoren hebben hier een grote taak.

Lessen

Willen we cyber security aanpakken, dan moeten we eerdere lessen nu eens echt tot ons nemen en daarvan leren. We moeten zorgen dat die lessen ook in de volgende generatie ICT-producten en -diensten terechtkomen. Vooral nu we steeds vaker ketens aan ICT-diensten ontwikkelen, zullen we in de jaren 70 uitgedachte en reeds toegepaste beveiligingsprincipes ter 'zelfbescherming' nu eens echt moeten gaan toepassen. Bijvoorbeeld: controleer alle binnenkomende, maar ook uitgaande informatie op validiteit.

Vitale functies

Nieuwe ICT-toepassingen verstoppen zich steeds vaker diep weg in gebruikersfunctionaliteit. Het aan- of uitzetten van pompen, verlichting, airconditioning en zelf vitale functies voor onze samenleving kan vanaf een tablet gedaan worden. De vraag wordt niet gesteld of dat ook altijd vanaf de keukentafel via internet moet kunnen. Het Shine-project identificeerde in de afgelopen paar jaar al 29.349 procescontrolesystemen in Nederland die rechtstreeks aan het internet gekoppeld zijn… [2].

Glazen bol

Maar we kunnen ook vooruit kijken. Dat doen de hackers en cybercriminelen ook. Ze zien een gouden toekomst tegemoet. Uw wagenpark gaat bijvoorbeeld eerdaags met andere auto's en de weg communiceren. Aan de informatiebeveiligingskant van dergelijke communicatie is er nog weinig ontwikkeling geweest. Hackers hebben allerlei elektronische systemen in auto's al opengebroken [3]. Staan auto's uit uw wagenpark ook op de lijst van onderzochte autotypen? [4] Maar ook bij u thuis hangen spoedig de slimme thermostaat en de slimme meter en rollen de slimme koelkast en de slimme wasmachine eerdaags binnen. Recent kwam naar buiten dat er negen serieuze beveiligingslekken zitten in een bepaald type draadloze thermostaten [5]. Shodan, een 'Google' om bepaalde typen systemen met bepaalde softwaretypen en -versies te vinden, liet zien dat 7000 van dergelijke thermostaten direct op afstand manipuleerbaar zijn. De standaard toegang is user=admin, password=admin, de pincode 1234, geen bescherming tegen het proberen van alle 9999 cijfercombinaties, niet-versleutelde informatie over de Wi-Fi-toegangen tot het privénetwerk, enzovoorts. Zijn uw gebouwbeheer en –bewakingssystemen veiliger? Hoe zeker bent u daarvan?

Dweilen

Hoe is het gesteld met de beveiligingssystemen die u maakt of koopt, installeert, samenstelt of reeds in gebruik heeft? Levert u de volgende reeks producten en –diensten veilig(er) af? Blijft u onveilige producten kopen of stelt u minimale eisen aan de producten die u eerdaags gaat kopen of laat installeren? Blijft u liever houden van onveiligheid gepaard gaande met veel gebruikersgemak en ongekende functionaliteit (ook voor de hacker)? Dweilen we verder met de kraan open? Is uw strategie die van een Internet of Insecure Things [6, 7]? Dan kan ik nu al voorspellen dat we in 2050 de verjaardag van honderd jaar buffer overflows en standaard¬wachtwoorden gaan vieren.

Links:

[1] http://fusion.net/story/20228/first-cyber-murder-will-happen-in-next-three-months-experts-claim/
[2] http://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014
[3] I. Rouf et al, Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study, USENIX Security'10 Proceedings of the 19th USENIX conference on Security, http://ftp.cse.sc.edu/reports/drafts/2010-002-tpms.pdf
[4] https://www.scribd.com/doc/236073361/Survey-of-Remote-Attack-Surfaces
[5] http://cybergibbons.com/security-2/heatmiser-wifi-thermostat-vulnerabilities/
[6] http://www.channelweb.co.uk/crn-uk/news/2371839/iot-vendors-accused-of-taking-security-back-to-1990s
[7] http://www.networkworld.com/article/2687169/security0/bot-herders-can-launch-ddos-attacks-from-dryers-refrigerators-other-internet-of-things-devices.html

Dit artikel is deels ontleend aan een eerder artikel van de auteur 'Are we in love with cyber insecurity?' in het International Journal of Critical Infrastructure Protection (2014), V7(3), pp. 165–166, september 2014

Eric Luijf is principal consultant bescherming vitale infrastructuur bij TNO. Eric is bereikbaar via eric.luijf@tno.nl.

OP ZOEK NAAR EEN DUIZENDPOOT

De Chief Information Security Officer van morgen

Met de intrede van security 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, komen vooral via de media naar buiten (denk aan RSA, Gemalto, ASML, NZA, Sony, ING) en zorgen daarmee voor de urgentie om meer grip te krijgen op dit fenomeen.
Dat blijkt nog steeds lastig. De belangrijkste oorzaak hiervan is dat de bestuurder nog altijd onvoldoende wordt gevoed met input om een gefundeerde discussie te kunnen voeren. De CISO ofwel de Chief Information Security Officer zal hier in toenemende mate een rol vervullen, enerzijds als adviseur en anderzijds als sparringpartner van het bestuur. De vraag is of de CISO van morgen wel over de juiste kennis en kunde beschikt en of de huidige opleidingen voldoende zijn toegerust op dat wat de moderne CISO moet kunnen en kennen.

De CISO van vandaag

In 2013 heb ik een grootschalig onderzoek uitgevoerd om te verkennen wat de strategische kernvraagstukken zijn waar security professionals mee te maken hebben. Ik wilde vaststellen over welke kennis en vaardigheden CISO's moeten beschikken om de zogenaamde 'knowing-doing-gap' te overbruggen. De bevraagde security experts geven aan dat security veelal wordt gezien als een project, maar meer zou moeten worden opgevat als een proces.
Opvallend is dat de ondervraagden bij de beantwoording van de vragen weinig 'zachte vaardigheden' aanreiken, zoals overtuigingskracht, communicatieve vaardigheden of sensitiviteit ten aanzien van ontwikkelingen in de organisatie. Terwijl ze wel veel waarde bleken te hechten aan zulke 'soft skills' en deze zelfs als een belangrijke succesfactor aanmerkten. CISO's zitten ogenschijnlijk dus wat meer aan de kant van de hard skills (kennis en ervaring) en minder aan de zijde van de soft skills (vaardigheden en competenties). Dit is tegenstrijdig met dat wat bestuurders en toezichthouders verwachten ten aanzien van de toekomstige ontwikkelingen van hun talenten. Zij zien een groeiende behoefte bij zichzelf en hun mensen aan onder andere helikopterview, kritisch doorvragen, beoordelingsvermogen, commitment, resultaatgerichtheid, ondernemingszin en strategisch inzicht.
Dit vraagt om een verschuiving binnen de CISO-capaciteiten en hedendaagse opleidingen. Inhoudelijke kennis zal moeten worden aangevuld met bedrijfsmatige, organisatorische en psychologische vaardigheden, gericht op het aanzetten tot voorwaartse actie. Tenminste, als de CISO de verandering blijvend wil laten zijn en security als een continu proces wil borgen. Al met al kunnen we uit het onderzoek uit 2013 concluderen dat de CISO van vandaag beperkingen heeft. CISO's evalueren en adopteren maar deels de relevante krachten in hun strategie en beleid. Ze weten dat security een continu proces is maar hebben moeite het daadwerkelijk als zodanig te effectueren. Een mogelijke blinde vlek kunnen de sociale vaardigheden zijn. Bijvoorbeeld vaardigheden om doortastend te zijn of veeleisender ten aanzien van het management.

De CISO van de toekomst

De CISO van de toekomst zal doordrongen moeten zijn van het enorme effect dat het vertrouwen van de stakeholders heeft op de continuïteit van de organisatie. Hij zorgt verder voor de noodzakelijke verbinding van de governance (het richten) met het management (het inrichten van processen) en met de operatie (het verrichten van activiteiten). En als er stakeholderbelangen in het geding zijn, dan grijpt hij in. Steeds zal hij hun belangen op het gebied van security verbinden aan de belangen en doelstellingen van de organisatie.
De CISO van de toekomst is dus een verbinder. Hij is in staat om met bestuurders in begrijpelijke bewoordingen over technische onderwerpen te communiceren. Hij is een vaardige verandermanager die psychologisch inzicht paart aan organisatorische sensitiviteit. Hij beschikt over globale kennis van aanpalende disciplines zoals juridische zaken. Hij weet waar de grenzen van de wet liggen en waar die worden overtreden. Hij weet ook waar de aansprakelijkheden van de organisatie liggen. Hij heeft een inschatting gemaakt van de risico's die de organisatie loopt en is in staat om deze in financiële zin te kwantificeren.
Hij heeft verder globale kennis van HR-processen. Hij weet wat de regels zijn waar gebruikers zich aan moeten houden en zorgt ervoor dat deze niet strijdig zijn met hun wettelijke rechten,

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. Bobbert is bereikbaar via yuri.bobbert@b-able.nl.

privacywetgeving. Hij is verder toegerust met globale kennis van architecturen (business-systemen en IT-architecturen) en kan security-architectuurprincipes duiden. Ook heeft hij globale kennis van marketing in huis. Kennis die hij vooral intern benut om bij de medewerkers de juiste houding en het juiste gedrag te bewerkstelligen.
Niet in de laatste plaats heeft de CISO van morgen feeling voor finance. Hij begrijpt waar de organisatie haar geld mee verdient, hoeveel er wordt verdiend en of het op een verantwoorde wijze wordt uitgegeven (security van investeringen in relatie tot risico's). Hij is in staat om business cases uit te werken en toe te lichten om de noodzaak van investeringen in security te onderbouwen. Hij maakt een gedegen afweging van security-uitgaven ten opzichte van te realiseren doelen en kan deze afzetten tegen de industriecijfers (benchmarks).
De CISO van de toekomst weet bovenal wat hij niet weet. Daarom weet hij dat hij moet samenwerken en is hij daardoor in staat samen te werken in multidisciplinaire teams van experts. Hij waakt als een liaison over de juiste teamsamenstelling van kennis, vaardigheden en ervaring.

Permanente educatie

Concluderend kunnen we stellen dat de CISO van de toekomst een duizendpoot is die zich door middel van permanente educatie de kennis en vaardigheden eigen maakt die hij nodig heeft om zijn organisatie blijvend te kunnen (be)dienen. Voor ons vakgebied - waarin veranderingen zich continu voordoen - zijn snelheid en doelgerichtheid van eminent belang.

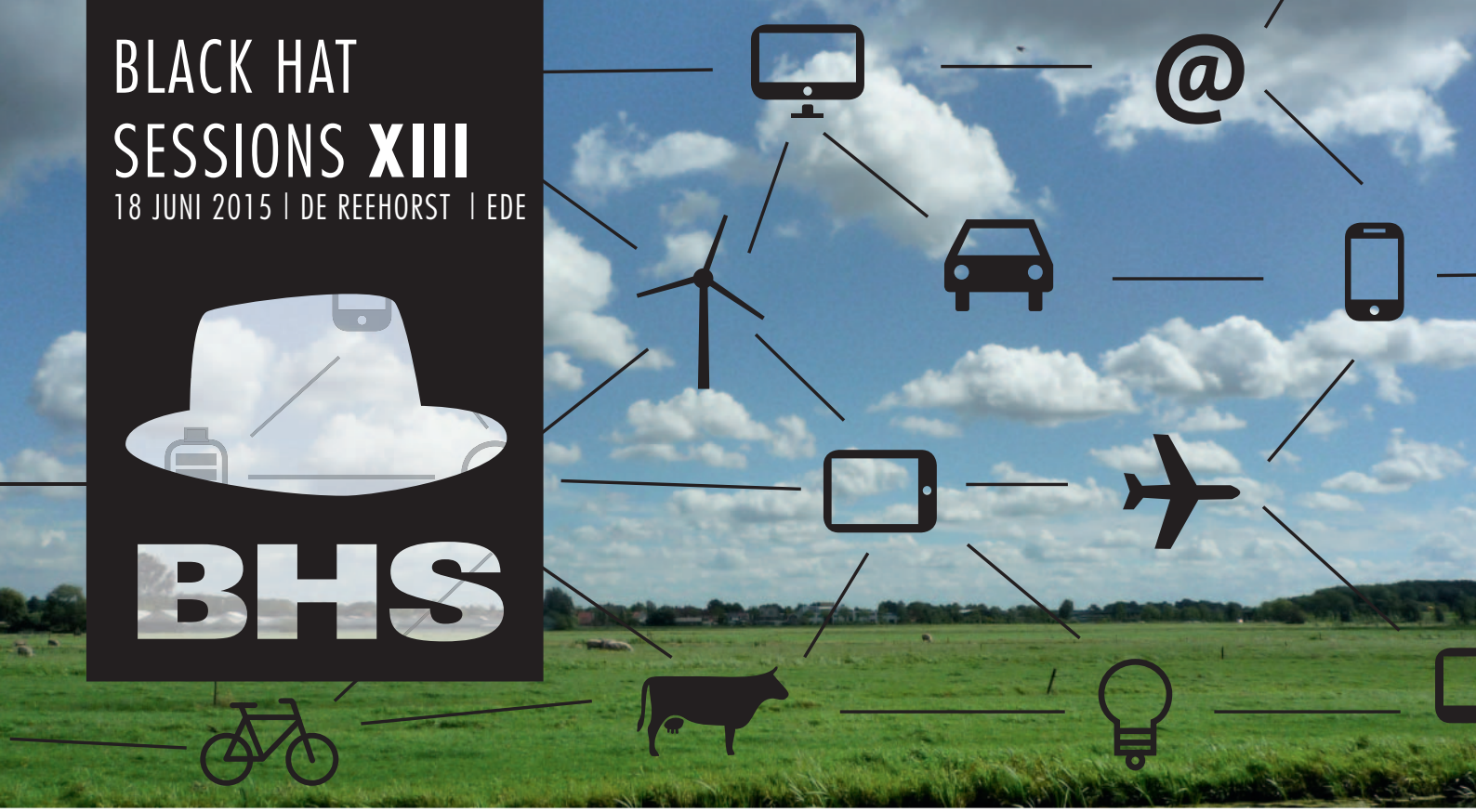
Interventies die nodig zijn om beveiliging naar een hoger plan te tillen, kunnen niet uit louter theoretische zaken bestaan. Er is een voortdurende terugkoppeling vanuit de praktijk nodig. Snelle 'feedback loops' zijn dus essentieel. Daarom is 'action research & learning' zo'n uitermate geschikte methodiek voor ons vakgebied. Juist door deel uit te maken van het te onderzoeken object ontstaat 'levende kennis'. Het is aan hogescholen en universiteiten om hiervoor opleidingen te hebben of te ontwikkelen. Niet alleen om de CISO van de toekomst op te leiden qua (technische) kennis en kunde, maar vooral ook om hem/haar de vaardigheden mee te geven die hij/zij nodig heeft om adequaat te blijven functioneren en zo zijn bestuurders te kunnen blijven adviseren.
Daarom pleit ik ervoor om action-learning en action-research op te nemen in de onderzoekslijnen en leerlijnen van universiteiten en hogescholen. Hogeschool NOVI doet dit al tot grote tevredenheid van de deelnemers. De opleiding ICT van deze hogeschool is recent gekozen tot beste deeltijdopleiding van Nederland. Criteria om deze kwalificatie te verkrijgen waren kleinschaligheid, individuele begeleiding en de intensieve wijze zoals het onderwijs (action-learning) wordt gegeven. Onder andere door praktijkgevallen in te brengen in onderzoek en onderwijs en zo actiegericht tot kennisverbreding en -verdieping te komen. Zowel Hogeschool NOVI als ook LOI Hogeschool hebben een leerlijn 'business information security' gedefinieerd waarin de ISO en de CISO van de toekomst kunnen worden opgeleid.

Meer weten?

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'. Daarnaast heeft Bobbert meerdere wetenschappelijke publicaties op zijn naam. Dit artikel is een bewerking van het hoofdstuk 'Competentiemanagement' dat is opgenomen in het boek 'Hoe veilig is mijn aandeel?'. Dit boek is het resultaat van praktisch en wetenschappelijk onderzoek bij ruim honderd organisaties naar de beveiliging van kritische assets en de wijze waarop bestuurders en managers hun reputatie, vertrouwen en continuïteit kunnen borgen.

BLACK HAT SESSIONS XIII

18 JUNI 2015 | DE REEHORST | EDE



Op 18 juni 2015 organiseert Madison Gurkha alweer de dertiende editie van de inmiddels befaamde Black Hat Sessions. Het thema van deze editie luidt: **Hoe veilig is (IT in) Nederland?** We besteden hierbij onder andere aandacht aan de kritieke infrastructuur, ICS/SCADA, SAP, ERP en anti-DDoS.

SPREKERS

Eric Luiijf (keynote)
TNO

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Hans de Vries (keynote)
NCSC

Teun van Dongen

Alex Bik
BIT

K. Reid Wightman
Digital Bond Labs

Maciej Korczynski
TU Delft

Daniël Dragičević
Madison Gurkha

Ed de Myttenaere
NRG

Alexander Polyakov
ERPscan

Dmitry Chastuchin
ERPscan

Erwin Kooi
Alliander

Paul van der Ploeg
NRG

Voor leden van het PvIB geldt een aantrekkelijke korting van 10%. Geef bij uw online aanmelding de code **GjE6pUHW** op en de korting wordt direct verrekend.

Meer informatie over het congres, de geldende groepskortingen en het inschrijfformulier vindt u op www.blackhatsessions.com.
Zie ook bijgesloten leaflet.

ORGANISATIE

Madison Gurkha
Your Security is Our Business

VOLG ONS VIA

#bhspartXIII
Black Hat Sessions group

LOCATIE

Hotel en Congrescentrum de ReeHorst
Bennekomseweg 24, 6717 LM Ede

Lex Dunn CISA CISSP ISSMP is Security Officer bij een grote, internationale ICT-dienstverlener. Hij is tevens voorzitter van de MSP-ISAC. Hij is bereikbaar via lex.dunn@capgemini.com

STUDIERAPPORT ALGEMENE BEHEERSING VAN IT-DIENSTEN

Verslag van de presentatie van het nieuwe studierapport van NOREA en PvIB op 10 maart jongstleden in Hilversum

Op 10 maart jongstleden was een groot aantal PvIB- en NOREA-leden naar Hotel Lapershoek in Hilversum gekomen om de officiële presentatie bij te wonen van het Studierapport "Algemene beheersing van IT-diensten."

In zijn inleiding memoreerde Bart van Staveren het tot stand komen van dit Studierapport. Het is een vervolg op het bekende boekje "Normen voor de beheersing van uitbestede ICT-processen" uit 2007. De werkgroep "Standaard Normen Beheersing en Beveiliging" heeft niet alleen de opmerkingen en commentaren op het eerste boekje verwerkt, ook wordt een methodiek gepresenteerd om de complexiteit van hedendaagse infrastructuren inzichtelijk te maken. De werkgroep bestond uit Frank Blom, Tjakko de Boer, Bart Bokhorst, Peter Kornelisse, Jan Roodnat en Bart van Staveren. Tjakko de Boer ging in zijn presentatie in op de behoefte aan verantwoording over IT-diensten en aan normenstelsels gebaseerd op de General IT-controls. Als uitgangspunt voor het boekje wordt een werkwijze beschreven om afspraken tussen "business" en IT te maken over de beheersing.

Fotografie: Lex Dunn

Tjakko de Boer
Peter Kornelisse vertelde het publiek dat de klassieke zienswijze, waarbij één systeem wordt beschouwd, niet langer gebruikt kan worden. Door de verregaande integratie van ICT-middelen is een gestructureerde aanpak nodig om de scope voor de audit te bepalen. Dit kan bijvoorbeeld aan de hand van een analyse van de verkeersstromen: hoe komt de gebruiker bij de data, maar ook hoe komt de beheerder bij de beheerde objecten. Met name in die laatste categorie blijken vaak zwakheden aanwezig, die de vertrouwelijkheid of integriteit van het systeem zouden kunnen aantasten.

Peter Kornelisse
Dit nieuwe boek gaat in op de infrastructuurlaag, echter is de applicatielaag natuurlijk ook belangrijk. Wellicht voer voor een volgend boekje? Ter afsluiting van de presentatie werden de eerste exemplaren van het boekje door Bart overhandigd aan vertegenwoordigers van de besturen van PvIB en NOREA, waarna alle aanwezigen ook een fysiek exemplaar kregen.

Uitreiking aan vertegenwoordigers besturen PvIB en NOREA
Het Studierapport is in digitale vorm beschikbaar op de websites van NOREA en PvIB.

Links:
NOREA:http://www.norea.nl/Norea/Actueel/Nieuws/Algemene+Beheersing+van+IT-diensten.aspx
PvIB:https://www.pvib.nl/nieuws/17703002/11-03-2015/Studierapport-%27Algemene-beheersing-van-IT-diensten%27

HACKING BARBIE

Mijn dochter is 7. Ze houdt van alles wat gecomputeriseerd of gerobotiseerd is. De Digibirds vliegen me om de oren en Furby roept de hele tijd dat hij graag snoepjes wil. Ook laat hij tot hilariteit van mijn kleine diva vaak harde winden. Op de iPad kijkt ze naar Netflix en speelt ze met mijn vrienden (want ze was "per ongeluk" met mijn Facebook-account ingelogd) Subway Surfer. Wie dus denkt tegen mij te spelen: nee, je verliest niet van mij maar van een 7-jarige kleine diva.

Ze houdt niet zo heel erg van Barbie. Dat is meer voor prinsessenmeisjes. En dat is mijn kleine diva niet. Ze is namelijk stoer, houdt van blauw en zwart en van doodskoppen op kleding. Ze hockeyt met een rauwe passie waar menig topvoetballer jaloers op zou zijn. Is trots op de hoeveelheid blauwe plekken op haar benen en is fan van Dolfje Weerwolfje. En toch weet ik zeker dat ze de nieuwste Barbie uitermate cool zal vinden.

Mattel (de maker van Barbie) gaat namelijk samenwerken met ToyTalk om een pratende en lerende Barbie in het leven te roepen. Tegen kerst moet het zover zijn. Barbie 2.0 leert doordat een kind tegen haar praat. Barbie vraagt over toekomstplannen, familie en allerhande andere gezellige dingen. Alle gesprekken tussen het kind en Barbie worden opgenomen. Barbie is aangesloten op Wifi. Via Wifi worden alle gesprekken doorgestuurd naar ToyTalk en Mattel. Eh, wat?

ToyTalk en Mattel komen zo dus alles te weten over mijn dochter. Hoogstwaarschijnlijk ook waar ze woont, wie haar mama is, waar ze bang voor is, wat ze leuk vindt, wie haar vrienden zijn en alle andere informatie die kleine diva's aan hun Barbie toevertrouwen. Ik hoef u natuurlijk niet te vertellen dat dit een privacydrama eerste klasse is. De informatie zal – uiteraard!- alleen maar gebruikt worden om het product te verbeteren. Welnu, daarvoor hoeven ze de inhoud van de gesprekken niet te hebben. Ik kan vele manieren bedenken waarmee je een product kunt verbeteren die niet de privacy van kinderen schenden. En wie de wet en de toezichthouder een beetje kent, weet dat minder invasieve manieren om je doel te bereiken altijd verkozen moeten worden boven de privacyschending. En al helemaal als het om de privacy van een uitermate kwetsbare groep gaat.

U begrijpt, in dit huis geen Barbie 2.0.

Hoewel… Barbie is aangesloten via Wifi… Dan is ze dus in theorie hackbaar. Het lijkt mij een uitermate goed idee als white hats deze Barbie 2.0 eens gaan testen op veiligheid. Je moet er toch niet aan denken dat kwaadwillenden alle signalen van Barbie kunnen ondervangen! Ik zou me daarbij ook kunnen voorstellen dat indien deze privacyschendende pop inbreekbaar blijkt een volgende stap het ontwikkelen van privacysoftware is. Een klein laagje bescherming op Barbie 2.0 waardoor niet alle gesprekken zomaar doorgaan naar derden. Lijkt me meteen ook een geweldige kans voor Mattel. Hoe cool zou het zijn als ze laten blijken dat ze om de privacy en veiligheid van kinderen geven door een competitie uit te schrijven voor alle technisch knappe koppen op de wereld en de uitdaging aandurven: Hacking Barbie!

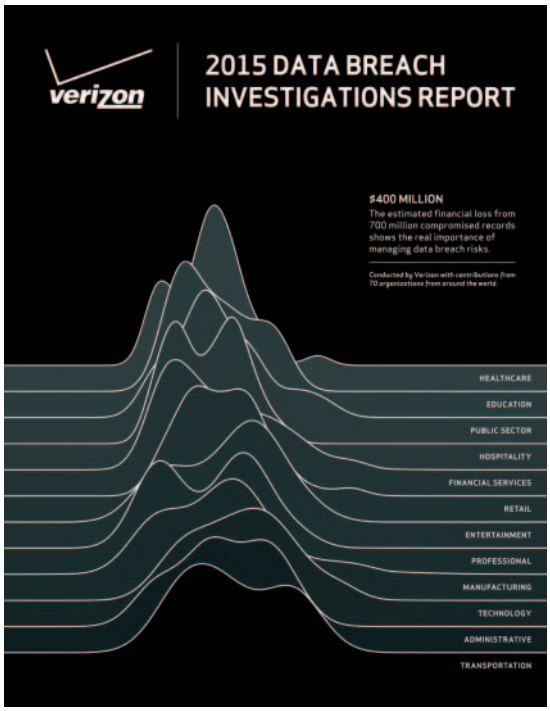
Mr. Rachel Marbus
@rachelmarbus op Twitter

IT-AUDIT-AUTORITEIT GERT VAN DER PIJL

Op 2 maart van dit jaar overleed Prof. Dr. Gert J. van der Pijl RE. Gert was in de periode 1999 tot 2013 hoogleraar EDP-auditing aan de Erasmus universiteit. Voor zijn Erasmus diensttijd was hij, na zijn wetenschappelijke promotie verbonden aan TIAS, waar hij ook docent was aan de Post-doc EDP-auditing-opleiding. Daarnaast was hij, mede door begeleiding van studenten, actief bij ontwikkeling van het vakgebied IT-auditing. Ook was hij jaren hoofdredacteur van het vakblad De IT Auditor van het Norea en als hoofdredacteur verbonden aan de redactie van het Handboek edp-auditing van Norea.

Studenten zullen zich Gert als een vriendelijke leraar met een groot relativeringsvermogen herinneren. En dat vermogen kon hij niet alleen inzetten tijdens het doceren, maar ook als hoofdredacteur. Hij heeft dat ook in zijn proefschrift (over de kwaliteit van informatie) al laten zien. Dogma's pasten hem niet. Het dogma dat een IT-auditor de controles uitvoert ten behoeve van financial-auditors was ook niet zijn dogma. Gert had een bredere blik op kwaliteit van IT dan alleen dat stukje dienstverlening. Kwaliteit, daar was hij dan weer wel van. En informatiebeveiliging is daar natuurlijk een onderdeel van. We zijn dankbaar voor wat Gert voor het vakgebied IT-auditing en voor kennisdeling heeft betekend.

(nu beschikbaar)



(advertentie)

OWASP
AppSec EU 2015 in Amsterdam

Dit jaar vindt de AppSec-EU/Research 2015 conferentie plaats op 19 tot en met 22 mei in de RAI te Amsterdam [1], georganiseerd door de Belgische, Luxemburgse en de Nederlandse OWASP Chapters. Het drietal chapters organiseert al sinds 2008 de jaarlijkse gratis OWASP BeNeLux-Day conferentie.

Het Open Web Application Security Project (OWASP) is een wereldwijde not-for-profit organisatie gericht op het verbeteren van de veiligheid van software. Haar missie is software-security-risico's zichtbaar te maken, zodat personen en organisaties wereldwijd weloverwogen beslissingen kunnen nemen over de veiligheid van software. Jaarlijks organiseert OWASP applicatie-security-conferenties in de USA, Azië/Pacific en, sinds 2005, in Europa. Deze AppSec-conferenties vinden steeds op een andere locatie plaats, zo was de AppSec EU conferentie in 2013 in Hamburg, Duitsland, in 2014 in Cambridge, Engeland en nu dus in Amsterdam.
Er is een uitgebreid programma [2]. Op 19 en 20 mei is het mogelijk verschillende trainingen te volgen, en op 21 en 22 mei zijn de conferentiedagen gevuld met presentaties over applicatiebeveiliging in vier tracks: Dev, Ops, Hack en de nieuwe CISO track. Naast een aanbod van uitstekende presentaties zijn er keynotes van internationaal bekende sprekers, zoals Brenno de Winter, Steve Lorg, Frank Breedijk, Josh Corman en Troy Hunt.
Sinds het begin van de AppSec-conferenties in Europa is hier vooral de verbinding met de academische wereld onderscheidend, waardoor de Europese conferenties zich de naam Research hebben gegeven. Vooraf aan de conferenties zijn er verschillende onderzoekpapers ingezonden waarvan de meest aansprekende zijn gekozen voor het programma van de conferentie. Verder vindt op de eerste conferentie dag de HackPra Allstars plaats, met geselecteerde sprekers uit de research-sector, welke vrij toegankelijk is voor alle deelnemers. Tijdens de conferentie is het voor de deelnemers mogelijk zich via een CTF (capture-the-flag) competitie te meten of bij TOOOL met lock-picking vertrouwd te maken. Awesome Retro bied gelegenheid jeugdsentiment op te halen en masseuses zijn aanwezig om de schouders los te krijgen. Op de avond van 21 mei is er voor deelnemers een social event (in de prijs inbegrepen). Hiervoor wordt er met rondvaartboten van de RAI naar het NEMO Science Center gevaren, waar een buffet op ons wacht en de deelnemers gelegenheid hebben na te praten over de dag en gezamenlijk vooruit te kijken naar dag twee.

OWASP
The Open Web Application Security Project

Registratie voor OWASP AppSec EU is nu mogelijk [3].

Links
[1] http://2015.appsec.eu/
[2] http://2015.appsec.eu/program-overview/
[3] http://2015.appsec.eu/registration/

Martin Knobloch is security consultant, eigenaar van PervaSec en bestuurslid van OWASP NL Chapter.
Hij is te bereiken via martin.knobloch@owasp.org.

CYBER DAMAGE CONTROL: CRITERIA VOOR INFORMATION ASSURANCE

Discussie en het uitwisselen van ideeën en opvattingen staan in CISO bijeenkomsten centraal. Tijdens deze middag ging het over de zoektocht naar een nieuwe eigentijdse onderbouwing van de manier waarop wij IT gerelateerde grootheden beschermen. Een impressie van CISO-3.

Stef Schinagl van Noordbeek BV maakte ons deelgenoot van zijn pogen om criteria te vinden voor een hedendaags antwoord op de bedreigingen waar de informatiemaatschappij zich tegen wil wapenen. Uitgangspunt hierbij is zijn overtuiging dat er gebrek is aan een eigentijds theoretisch model. Zijn inleiding bleek het onderwerp van een promotieonderzoek te zijn waaraan hij is begonnen, een verjongingskuur voor oude modellen.
Stef zei het zelf al, zijn jeugdigheid geeft hem vragen in over de dingen die hij in de praktijk ziet. Zijn motto is:
'Men kan geld voor IB&P-maatregelen maar één keer uitgeven. Daarom is het van belang dat geld te spenderen aan de meest effectieve maatregelen, namelijk de maatregelen die de echte waarde echt beveiligen.'
Stef presenteerde zijn voorlopige model (de Schinagl Kubus) dat op eenvoudige wijze de aspecten van zowel beveiliging als te beveiligen objecten bevat:

- **drie klassen data: Human, Financial, Things**
- **de drie bekende klassen kwaliteitskenmerken: Confidentiallity, Integrity, Availability**
- **de IT-procesfasen: Transmit, Process, Store**

Volgens Stef zijn de wetenschappelijke modellen uit de jaren 1970-80 zoals, Bell-LaPadula, Biba en Clark-Wilson niet meer voldoende voor de moderne informatiemaatschappij. In zijn visie is het aspect Availability het best geregeld in de praktijk, maar dat is natuurlijk een relatieve beoordeling. De bescherming van waarden anno nu vergt meer dan de oude modellen kunnen bieden. Een model van prof. drs. H.C. Kocks RA van rond 1990, dat Stef gebruikt om het IT Audit proces te verduidelijken, onderkent drie gebieden: de gebruikersorganisatie, de systeemontwikkeling en de verwerking- en transportorganisatie. Een overzichtelijke indeling die tegenwoordig vragen oproept. De gebruikersorganisatie is niet meer de hiërarchische bedrijfsopstelling waarvoor in de jaren 1970-80 de modellen werden opgezet. Naast bedrijven en instellingen met hun processen zijn er individuen die zich met private, vaak weinig gestructureerde, processen in de informatiemaatschappij begeven. Het gedrag van de 'gebruikersorganisatie' is dus wezenlijk veranderd. Dat zelfde geldt voor de systeemontwikkeling. In plaats van ontwikkeling onder 'eigen' bedrijfsregie is kant-en-klare-software beschikbaar uit vele bronnen. En ook de verwerkings-en transportorganisatie is door de komst van internet en allerlei 'dingen' die daarop kunnen aansluiten met hun verwerkings- en opslagkracht, danig gewijzigd. Waar ligt de grens tussen intern en extern? Waar ligt de verantwoordelijkheid en de aansprakelijkheid voor activiteiten? Hoe krijgt de communicatie vorm die tussen de gebieden in het Kocks-model worden onderscheiden? De gedachte dat de oorspronkelijke modellen niet geheel eigentijds zijn, ligt voor de hand.
Aan de kant van de bedreigingen, waaraan te beschermen waarden bloot gesteld zijn, is door de technologische ontwikkeling inmiddels ook wel wat veranderd. Handige middelen en technieken staan ook mensen met minder goede bedoelingen ter beschikking. Cybersecurity is mogelijk het begrip dat het beste weergeeft wat de gebruikersorganisaties op het terrein van het beschermen van waarden, tegenwoordig bezighoudt. Stef denkt zijn model toe te kunnen passen door de drie werkprocessen voor Human-, Financial- en Things-data van elkaar te scheiden en voor elk daarvan de relevantie van de kwaliteitskenmerken vast te stellen. Vervolgens kan een risicoanalyse plaatsvinden voor de IT-procesfasen en wel zo dat er voor ieder van de 27 minikubussen een specifiek resultaat wordt gevonden, zowel in termen van risico (gebruikersorganisatie) als van mogelijke maatregelen.

Discussie

In de discussie ging het vooral om definities, over de indeling van de klassen van de kubus, over de vraag hoe het model kan gaan helpen, over het verschil tussen data en informatie. En natuurlijk veel vragen.
De vraag kwam op of het probleem niet meer zit in de effectiviteit van maatregelen dan in de risico's. Als voorbeeld werd de speciale behandeling genoemd die gewenst is bij bepaalde personen in een overigens algemeen bestand. Vanuit het bedrijfsproces geredeneerd komt dit aan de orde, vanuit de risico's vermoedelijk niet.
De gebruikersorganisatie is niet meer eenduidig te definiëren. De veranderingen in de maatschappij gaan snel en dat vraagt om een dynamisch model. Hoe wordt dat in de kubus gerealiseerd?
Hoe kan aansprakelijkheid in het model worden gebracht? Dat is immers de prikkel voor het treffen van maatregelen?
De huidige access-control-systemen zijn van voor de tijd van internet. Is de 'bewezen technologie' nog toepasbaar? Of is de complexiteit bij de invoering van maatregelen te groot geworden?
Ronald Paans benadrukte nog eens hoe belangrijk het is om kennis te delen als er nieuwe ideeën worden uitgewerkt. Het gesprek met vakgenoten vond hij dan ook bijzonder waardevol.

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

Foto: Tom Bakker

SFEERIMPRESSIE ONE CONFERENCE

Cybersecurists ontmoeten elkaar in Den Haag

Op maandag 13 en dinsdag 14 april was het World Forum in Den Haag weer het toneel van de jaarlijkse ONE Conference van het Nationaal Cyber Security Center. Voor de genodigden was het dit keer wat lastiger om binnen te komen, er was (vanwege de GCCS2015 later in de week) een uitgebreide security check met scanners, security guards, controle van identiteitsbewijzen en zo.

“Live well. Laugh often. Encrypt absolutely everything.”

Inmiddels traditie: de rol van dagvoorzitter was weer in vertrouwde handen bij Nicholas Witchell, die de 900 deelnemers welkom heette. De eigenlijke opening werd gedaan door Klaas Dijkhoff, de nieuwe staatssecretaris van Veiligheid en Justitie. Onder verwijzing naar zijn eerste experimenten met het in elkaar zetten van een computer, die in grote rookwolken eindigde, gaf hij aan de techniek aan de aanwezigen over te laten. Hij benadrukte de noodzaak voor alle partijen (politiek, overheid, bedrijfsleven en wetenschap) om samen te werken, niet alleen nationaal, maar vooral internationaal vanwege het ontbreken van staatsgrenzen in cyberspace.

Als volgende spreker kwam Hans de Vries, directeur van het NCSC, op het podium. Hij betoogde dat het speelkwartier in cyberspace voorbij is, en dat we nu serieus aan de slag moeten om cyberspace op een veilige en verantwoorde wijze te kunnen gebruiken. Daarbij is private-publieke samenwerking absoluut noodzakelijk. Het belang van ICT werd enkele wegen geleden pijnlijk duidelijk door de grootschalige stroomstoring in Noordwest-Nederland. “The game is on, loosing is not an option”.
De eerste plenaire presentatie door de welbekende Jaya Baloo (Chief Information Security Officer van KPN) ging over “crypto”. Enerzijds zijn overheden steeds beter in staat om een totaal plaatje te maken van burgers en hun gedragingen (al of niet met hun instemming), anderzijds zijn er “gaten” in wat de overheden kunnen zien, doordat burgers gebruik maken van “onkraakbare” crypto. Recentelijk is er van diverse kanten een voorstel gedaan om een “golden key” te hebben, zodat de overheden toch in staat zijn gecrypte informatie te lezen. Goed voorstel of niet? Uiteraard roepen diegenen die dit voorstellen, dat alles “op democratische wijze” via de rechter zal lopen, maar hoe controleren we dat? Centrale vraag daarbij is wie je vertrouwd om vertrouwen te geven. De overheid? Een groot bedrijf als Microsoft of Google? Jaya stelt dat het mogelijk is, en zal blijven, om een redelijk compleet beeld van een zaak te bouwen, ook als er versleutelde apparaten gebruikt zijn. Maar in de toekomst ligt de dreiging van kwantum computing boven de crypto horizon. Desondanks: “Live well. Laugh often. Encrypt absolutely everything.”
Vervolgens kwam Jason Healey (Atlantic Council) aan het woord over het bouwen van een “sustainable cyberspace”. Een bron van economische groei, innovatie, maar ook constant onder bedreiging. Het internet is een van de meest ingrijpende technologieën, die de afgelopen zeshonderd jaar door de menselijke geest bedacht zijn. Jason trekt de vergelijking met de uitvinding van de boekdrukkunst door Gutenberg. Wat zou er gebeurd zijn als binnen twintig jaar na deze uitvinding de toenmalige machten ongelimiteerd inzage hadden in wat er door wie gedrukt werd, en aan wie het verspreid werd? Juist omdat dit destijds niet mogelijk was, zagen we de Renaissance ontstaan met alle positieve gevolgen voor de mensheid. Maar wat doen we vandaag met de bedreigingen op, maar ook van, het internet?
In parallelle tracks werd door presentatoren uit overheid, bedrijfsleven en wetenschap ingegaan op actuele thema’s rondom cyber security. Daarnaast werd er ook uitgebreid gebruik gemaakt van de mogelijkheid tot netwerken. De “usual suspects” waren uiteraard aanwezig. Nieuw dit jaar was KIPS, de Kaspersky Industrial Protection Simulation game, waarmee verschillende teams in onderlinge competitie probeerden een waterbedrijf op te zetten en veilig te houden.
In de wandelgangen waren een achttal bedrijven aanwezig om prototypes van innovatieve cyber security oplossingen aan de aanwezigen te laten zien.
NCSC kan terug kijken op een geslaagde ONE Conference, die dit keer ook opmaat was voor de Global Conference on Cyber Space.

Lex Dunn en Tom Bakker, redacteuren IB magazine.

‘HIER WORD IK NOU BLIJ VAN’

Juryrapport ‘Artikel van het Jaar’ 2014

Ook dit jaar kregen wij als jury - Remco Bakker van CQure, Lambrecht Nieuwenhuize van BNG en Renato Kuiper van VKA – een breed scala aan artikelen voorgeschoteld. Uit negen artikelen die de redactie voorgeselecteerd heeft moet een keuze gemaakt worden. Dit betekent dat we alle artikelen nog eens moesten doorlezen. Dit herlezen van artikelen is iets dat we iedereen aan kunnen raden. Naast het blad hebben we gelukkig ook nog de digitale versies van de artikelen beschikbaar op de PvIB website.

Beoordelingscriteria artikelen

Bij het jureren is gekeken naar de volgende criteria:

1. Opzet artikel - Is de opzet van het artikel juist voor de soort (inhoudelijk of opiniestuk)?
2. Leesbaarheid - Is het artikel helder en begrijpelijk geschreven, met passende illustraties? Is de stijl consistent, zoals serieus of satirisch? Of het nu een praktijkbeschrijving is of een wetenschappelijke beschouwing betreft, is de leeservaring prettig?
3. Benadering van de doelgroep - Is het duidelijk wat de doelgroep is voor het artikel? Is het artikel te volgen voor een lezer buiten de subgroep?
4. Vernieuwend gehalte - Heeft het artikel aspecten die getuigen van visie bij de auteur en/of nieuwe gezichtspunten op een onderwerp? In het Engels noemen we dit " thinking out-of-the-box ".
5. Zet het de doelgroep aan het denken? - Ook als de auteur verslag legt van een gezamenlijk gedachtengoed of misschien zelf rapporteert over unieke gedachten van anderen, in hoeverre slaagt hij of zij er in om de rapporteert over unieke gedachten van anderen, in hoeverre slaagt hij of zij er in om de lezer aan het denken te zetten?

Genomineerde Artikelen

#	Titel	Pag.	Auteur
IB1	De CBP-Richtsnoeren nader beschouwd	8	Kersten, F.
IB2	De sterkte van wachtwoorden en hun tekortkomingen	4	Heijningen, N. van
IB3	Big Data: herijking noodzakelijk	10	Verburg, W. e.a
IB4	Heartbleed	4	Rogaar, P.
IB5	De Logius-norm voor DigiD: perikelen bij technisch testen	10	Koot, M.
IB6	Phishing: slinkse manieren om een organisatie binnen te dringen	4	Duijn, R. van
IB6	Klik, klik, klik het geluid van een gezonde werkvloer	8	Niggebrugge, D. e.a.
IB7	Identiteitsfraude is kinderspel	20	Genova, M.
IB8	Vulnerability scanning	8	Vernède, R.

Als juryleden hebben we afzonderlijk een beoordeling met daaraan gekoppelde punten toekend. Het eindresultaat is, zoals dat altijd bij een wedstrijd is, een optelling van de punten.

Het winnende artikel van dit jaar is in eerste aanleg een "technisch" artikel en handelt over de problemen die technische testers tegen het lijf lopen bij het hanteren van de Logius-norm voor DigiD door Matthijs Koot. Zo, dan weet U direct wie de winnaar is. Maar zo eenvoudig was die keuze niet. Want het artikel dat als nummer 2 in onze jurybeoordeling eindigde, van Frans Kersten: "De CBP richtsnoeren nader beschouwd" is vanuit een niet-technisch perspectief een bijzonder leesbaar stuk waarbij ook deze schrijver de moeilijkheid van het vaststellen van hanteerbare normen, in dit geval voor de juiste beveiliging van persoonsgegevens, blootlegt. Als nummer 3 is geëindigd Raoul Vernède met het artikel "Vulnerability scanning".

Bij het beoordelen van de artikelen doen we als juryleden ook wel eens uitspraken, die we nu graag met iedereen willen delen.

1. **Matthijs Koot met "De Logius-norm voor DigiD: perikelen bij technisch testen":**

- Interpretatie van normen is altijd lastig. Iedereen worstelt er mee. De reflectie en alternatieve voorstellen van toetsen moeten m.i. door Logius worden opgepakt. Het advies om beter bij OWASP aan te sluiten kijkt me zeer logisch, ik verbaas me er altijd over dat dergelijke zaken nog te weinig gebeurt binnen de Nederlandse overheid.
- Hier word ik nou blij van :-).
- Zou graag een co-productie lezen van Matthijs Koot en Frans Kersten, daar beiden tegen hetzelfde probleem aanlopen, hoe de "stand der techniek " in toetsbare vorm te gieten zonder vernieuwing en verbetering uit te sluiten.

2. **Frans Kersten met "De CBP-Richtsnoeren nader beschouwd":**

- Geeft een goede analyse van de richtsnoeren en de ontwikkelingen daarnaartoe, inclusief de positieve en negatieve kanten hierin belicht. Ik denk dat dit artikel als eerste in een opleiding security bij het onderwerp privacy als verplicht leesvoer gegeven moet worden. Daarnaast zou de doelgroep van dit artikel ook de informatiemanager/informatiearchitect moeten worden!
- Interessant betoog.
- De auteur hinkt te veel op twee gedachten, iets wat nog eens verder uitgediept kan worden.

3. **Raoul Vernède met "Vulnerability scanning":**

- Het is een artikel dat ik direct aan een beheerder zou geven die belast is met het uitvoeren van vulnerability scanning. Een artikel vanuit praktische ervaring, dit moeten we weer vaker doen in het blad. Het gaat bij het PvIB ook om het delen van praktijkervaringen, naast theorie en beschouwingen.
- Leuk om de ervaringen te lezen met spullen waarmee ik mijn werk in de informatiebeveiliging in 1996 begon :).

Alle auteurs en lezers: hartelijk dank, blijf schrijven, blijf lezen en houd het veilig.

Renato Kuiper, namens de jury van het "Artikel van het Jaar". Renato is te bereiken via renato.kuiper@vka.nl.

Achter Het Nieuws

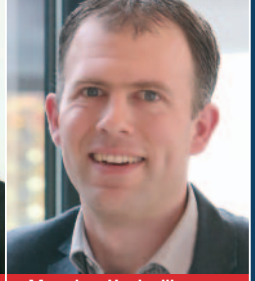
In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over de informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kunt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

RANSOMWARE

Steeds meer bedrijven worden door ransomware getroffen. Het Cryptolocker virus versleutelt werkdocumenten en biedt het slachtoffer de encryptiesleutels te koop aan. Hoe ga je hier als bedrijf mee om? Hoe kun je je voorbereiden? En moet je in gaan op de afpersingsom om je bestanden terug te krijgen, of doe je dat juist absoluut niet? Onze redacteuren geven hun mening.


Lex Borger


Lex Dunn


Maarten Hartsuijker

Lex Dunn

Ransomware: een relatief nieuwe methode in de gereedschapskist van de cybercriminelen. De laatste maanden zijn er herhaaldelijk berichten in de pers verschenen als er weer een organisatie of bedrijf "getroffen" was door een gijzelvirus. Wat maakt dit nou anders dan reguliere virussen of malware? Om te beginnen gaat het vaak om gerichte aanvallen, of in elk geval kleinschalig, waardoor het voor de anti-malware-leveranciers moeilijker wordt om detectie-signatures tijdig aan te leveren. Ook constateren we dat er steeds vaker privézaken op een zakelijke laptop of PC gedaan worden, waarbij vaak zonder na te denken op links of bijlagen wordt geklikt. Een gegeven waar cybercriminelen middels "social engineering"-methoden graag gebruik van maken. En als één gebruiker één keer op de verkeerde link klikt, of een geïnfecteerde bijlage opent, dan is binnen de kortste keren een groot deel van de bedrijfsinformatie op het netwerk versleuteld.
Gelukkig blijkt het in dergelijke gevallen vaak eenvoudig om de versleuteling weer te verwijderen, door de soms knullige manier waarop de malware in elkaar gezet is. Maar hou er rekening mee dat dit zal verbeteren. Moet je dan maar toegeven aan de "chantage" van de cybercrimineel? Persoonlijk denk ik dat je dat niet moet doen, maar ik kan me voorstellen dat er organisaties of bedrijven zijn, die liever maar betalen dan veel moeite te moeten steken in het opruimen van de versleuteling. Je moet dan maar afwachten of de cybercrimineel "eerlijk" speelt, en je de sleutel geeft om de bestanden weer toegankelijk te maken. En hiermee plaats je jezelf natuurlijk wel op de lijst van "easy targets" voor een volgende keer.
Overigens: is dit echt iets nieuws? Nee, in het verleden kwamen "zware jongens" hun bescherming aanbieden aan winkeliers en bedrijven, uiteraard tegen betaling om te "voorkomen dat er iets onprettigs zou gebeuren". Maar ja, toen zaten we nog in het fysieke tijdperk ...

Maarten Hartsuijker

Tien jaar geleden zou het voer zijn geweest voor een goede film. Criminelen die je bestanden versleutelen om er losgeld voor te vragen. Maar vandaag de dag is het helaas de bittere realiteit. Als organisatie is het daarom belangrijk om je goed voor te bereiden. Allereerst richting je gebruikers. Extra bewustwording rondom het risico gerelateerd aan het openen van onbekende e-mailbijlagen kan geen kwaad. Ten tweede binnen de IT organisatie. Het up-to-date houden van software met beveiligingsupdates was altijd al belangrijk. Maar de ransomware-dreiging illustreert daar de noodzaak extra van.

Daarnaast is het goed om de backupstrategie nogmaals goed te herzien. Staan alle belangrijke bestanden centraal? En zijn de backups integer en bewaren we ze lang genoeg? Wat betreft de monitoringomgeving is het het overwegen waard om controles in te richten die detecteren of bestanden onterecht versleuteld zijn. Richting beheerders is het verstandig om nogmaals het belang van het werken onder normale gebruikersrechten te benadrukken. Want een cryptolockervirus dat met beheerrechten zijn werk gaat doen heeft natuurlijk een veel grotere impact dan een virus dat met beperkte rechten acteert. En hoewel antivirussoftware niet zaligmakend is, draagt up-to-date antivirussoftware zeker zijn steentje bij. Net als het door de mailserver laten tegenhouden van versleutelde bestanden uit onbekende bron. Besmet worden met ransomware is geen pretje, maar met goede maatregelen is de impact gelukkig aanzienlijk in te perken.

Lex Borger

Voorkom dat je losgeld moet betalen. Het is niet alleen een financiële schade voor jouw bedrijf; het is ook een aanmoedigingspremie voor de criminele organisatie. En het is wel degelijk te beheersen. Ransomware is in beginsel malware. Dus alles wat je al doet tegen malware werkt ook tegen ransomware, zoals antivirus, gebruikersbewustwording, white-listing van software(locaties), patchen, uitzetten van niet gebruikte diensten (b.v. RDP). Dit is een goede baseline.

Ransomware is echter meer dan gewone malware. Het zit een hele 'dienstverlening' achter. Dat wil zeggen dat er communicatie is met een command & control-server, die de encryptiesleutels aanneemt en de betaalstatus doorgeeft. De communicatie met een C&C-server kan opgemerkt worden. De encryptie is niet instantaan. Maak mensen bewust dat een PC loskoppelen of uitzetten als je een besmetting vermoedt een goede optie is.

Maar de beste optie is om je kroonjuwelen te isoleren - zodat ze niet geraakt kunnen worden bij een besmetting en goede backups te hebben, die niet standaard online staan en waarbij meerdere generaties van bestanden apart gekopieerd worden.
Mocht je tóch overwegen losgeld te betalen, weet dan dat de criminele breinen tegenwoordig een heel klantvriendelijke dienstverlening hebben om je verder te helpen...

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

ZE DOEN HET NOG HARTSTIKKE GOED

Iedereen kent het wel: er staat een tv en een videorecorder in een huiskamer waarvan je aan het model ziet dat deze minimaal ergens in de vorige eeuw van de lopende band moet zijn afgerold. Voordat je gaat zitten slik je de vraag in die je had willen stellen, maar nieuwsgierig als je bent vraag je of het vervelend is dat je even naar het acht uur journaal wil kijken. Mij wordt door de eigenaar van de tv gevraagd onder welke steen ik heb gewoond. Het acht uur journaal kijk je toch niet meer live, dat doe je op je telefoon of je iPad. Ik knik beleefd en voel mij wat warm worden.

Zwijgend drinken wij de koffie en uiteindelijk weet ik toch het gesprek op de tv te krijgen. Het gaat van materialisme naar modern gedoe en eindigt uiteindelijk met de woorden dat ie eigenlijk nog hartstikke goed is. Ja, je kunt de videobanden niet meer krijgen maar hij had ze toch nog niet allemaal gezien.

Zwijgend zaten mijn vrouw en ik in de auto naar huis toen mijn vrouw zei "Wat een oude troep hadden ze daar staan." Ik kan haar daar alleen maar gelijk in geven en vertelde dat dit ook in het bedrijfsleven gebeurde: oude software wordt nog steeds gebruikt omdat het zo makkelijk is en dat het eigenlijk niet goed te vervangen is. Vervangen zou bovendien erg veel geld en tijd gaan kosten. We hebben er zelfs een naam voor gevonden; wij noemen dat legacy. Dus we draaien die oude software nog steeds en eigenlijk zonder enig probleem.

Nou ja, de ICT-club klaagt wel steen over been, want ze vinden het vervelend dat we met een hele oude versie van Internet Explorer moeten werken. Dat is voor de gebruiker ook heel lastig hoor want de websites worden niet meer goed weergegeven en sommige interne programmatuur kan er niet op draaien. Eigenlijk is dat inderdaad wel vervelend maar ja, die software werkt nog hartstikke goed. Als er iets aan verandert moet worden dan lopen er bij ICT nog twee mensen rond die er aanpassingen in kunnen doen. Dus helemaal geen probleem.

Nu denkt u misschien dat het om een beperkt aantal machines gaat bij ons, maar dat valt tegen. Er draaien ongeveer dertig verouderde machines. Bij de rijksoverheid draaiden vorig jaar nog ongeveer dertigduizend verouderde machines.

Ik heb het gevoel dat u denkt "Tja, de rijksoverheid. Berry zal wel bij een bank of een stoffige verzekeraar werken." Ja, dat klopt, maar die stoffige verzekeraar is toevallig wel nog moderner dan de NASA. De NASA (National Aeronautics and Space Administration) werkt met computers uit de jaren zeventig. Dus raketten gaan naar Mars en de maan gestuurd door computers die uw ouders heel lang geleden hadden? Ja, dat klopt dus helemaal en NASA ervaart dat niet als probleem (zeggen ze). Ik probeer me te bedenken wat er door je hoofd heen moet gaan als je beneden bij de raket staat die je straks naar de ruimte brengt. Hij wordt gecontroleerd en bestuurd met een machine en software uit 1973. Dan krab je jezelf toch wel even op je achterhoofd als daar geen helm zat.

Wordt er niemand beter van? Jawel hoor, de leverancier van de legacy is wel bereid om de Cobol-krasser correcties in de software te laten aanbrengen. Microsoft is wel bereid om de machines te blijven patchen. Tenminste, als de eigenaar van de machines bereid is om vierhonderd dollar per systeem per jaar te betalen.

Eigenlijk is het ook erg jammer al die legacy te vervangen door nieuwe systemen. Het is niet alleen een zeer kostbare zaak om die machines te vervangen maar ik moet alle data ook op de één of andere manier in die nieuwe systemen krijgen. Al met al een zeer kostbare zaak. Ik denk dat we dit volgend jaar maar opnieuw moeten bekijken. Dit jaar doen we er even niets aan, want ze doen het eigenlijk nog steeds hartstikke goed.

Berry

Secure Link
Infrastructure Security Solutions



Gezocht!
Security Engineers

SecureLink groeit en is op zoek naar Security Engineers die ons team komen versterken!

Als Security Engineer heb je diepgaande kennis op het gebied van security en networking. De combinatie van enerzijds de security technologie en anderzijds de integratie met networking is iets waar jij al jouw energie en expertise in kwijt kunt. Je krijgt de ruimte zelfstandig complexe security en networking projecten van A tot Z uit te voeren.

Benieuwd? Kijk dan op www.securelink.nl/vacatures



Kom jij ons team versterken?

Sinds de oprichting van SecureLink in 2003 managen en realiseren wij als security en networking integrator met ruim honderdtachtig SecureLinkers, verdeeld over drie vestigingen in Nederland en België, enterprise security architecturen én een hoger security niveau.

Go Secure!

SecureLink Nederland B.V. | Trapezium 224 | 3364 DL Sliedrecht | T +31 88 1234 200 | info@securelink.nl