iB
INFORMATIEBEVEILIGING
jaargang 15 - 2015
#7

Cloud-mythes - kloppen ze wel?

Voorzitters: de factor mens

Return of the Cyberman

Modelling Threat Scenarios (deel 2)

ISO 21827 steeds belangrijker bij software ontwikkeling

Gezocht: IT security trainees!

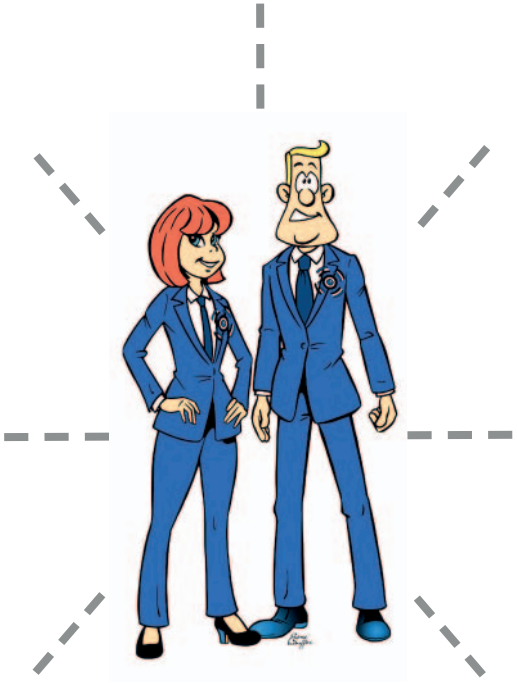
Start begin 2016

"Realiseren van veilige innovatieve IT-infrastructuren."

SecureLink is opgericht in **2003** en heeft **200** enthousiaste SecureLinkers. We hebben **4** vestigingen verdeeld over Nederland en België.

Detail • Klantgerichtheid • Respect • Commitment • Bezieling • Creativiteit • Enthousiasme

Het hoofdkantoor van SecureLink bevindt zich in Sliedrecht (regio Rotterdam). Jouw werkgebied ligt vooral in de Randstad, maar ook de rest van Nederland.



"Breed beginnen en daarna specialiseren in de richting van jouw keuze."

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

Best Workplaces – Great Place To Work – Securelink Nederland B.V.

fd. Gazellen Awards 2011 - 2014

Deloitte. Technology Fast 500

Secure UNIVERSITY

Trainees worden binnen één jaar klaargestoomd voor de functie van Security Specialist!

Een greep uit onze klanten

bol.com, vpro, HU Hogeschool Utrecht, BNN VARA, Mitsubishi, Zi

Interesse in deze vacature?
Neem contact op met Tim Boerakker via T +31 88 1234 200 of mail naar jobs@securelink.nl.
Kijk voor meer informatie op www.securelink.nl.

Go Secure!

GEORGANISEERDE MISDAAD

De 2015-versie van het Europol-rapport over de bedreiging door georganiseerde misdaad op het internet is uit [1]. Dit rapport kijkt naar de hele keten van internetcontentproductie en -consumptie en bevestigt wat we eigenlijk al weten: alle trends van georganiseerde misdaad op het internet zetten weer verder door. Van de ontwikkelaars tot de gebruikers, allen hebben hun eigen bedreigingen om zich tegen te weren en specifieke systematische kwetsbaarheden om bedacht op te zijn.

Cyberaanvallen blijven in het nieuws. Dit belooft wat wanneer volgend jaar de wet Meldplicht Datalekken ingaat. Je kunt beter je meldproces van tevoren inrichten, dan afwachten tot de eerste melding gedaan moet worden, want er zijn behoorlijk wat eisen: je moet weten wat een datalek is, hoe je dat vaststelt, je moet snel kunnen melden, dus moet je ook snel een diagnose kunnen stellen. Verwarrend hierbij is dat een datalek niet per sé een lek hoeft te zijn, elke bewerkersfout kan onder de meldplicht vallen. En dan is er nog de kwestie wie allemaal moeten melden...

Stel dat de recente hack bij Experian, waarbij klantgegevens van T-Mobile-klanten in de VS werden buitgemaakt, onder de wet zou vallen, dan moeten waarschijnlijk zowel T-Mobile als Experian melden binnen de vereiste tijd. In de VS wordt heel snel de zwartepiet naar de bewerker zelf doorgeschoven, er wordt meer gelet op de verantwoordelijkheid dan de aansprakelijkheid.

Ik heb op de COSAC-conferentie eind september nog mee mogen doen aan een gedachte-experiment: stel dat alle informatie op het internet al weggelekt is, wat dan [2]? Je komt dan tot de conclusie dat online-privacy dan weg is. Natuurlijk zouden we wel een weg vinden om door te gaan, maar de wereld ziet er dan anders uit. Dus wat kunnen we daar nu aan doen?

Dat is dus de hamvraag. Iedere beveiliger zal voor zichzelf moeten beslissen wat hij/zij gaat doen. Een aanzet tot inspiratie vinden jullie in dit blad. Cloud-providers in Nederland lijken klaar voor de meldplicht, Rashid Niamat heeft dit voor ons beschreven. Michèlle en Maurice Gittens presenteren deel twee van hun visie op threat-scenario-modelling, wat weer bruikbare ideeën kan bevatten.

Lex Borger, hoofdredacteur

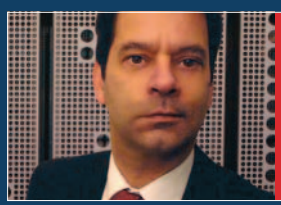
Links

[1] Europol IOCTA 2015 report: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015
[2] COSAC 2015 timetable, sessie 7P: http://www.cosac.net/synopsis.html#7P

In dit nummer

CLOUD-MYTHES KLOPPEN ZE WEL?

Wie nieuws over innovaties volgt, zal het volgende beeld herkennen: er zijn voorstanders, tegenstanders en een groep die afwacht (zie ook Crossing the Chasm [1]). De voor- en tegenstanders maken gebruik van alle middelen om het eigen gelijk aan te tonen en uit de groep die langs de zijlijn staat medestanders los te weken. De twee partijen vallen ook bijna altijd terug op begrippen, incidenten en cases uit het verleden die een eigen leven zijn gaan leiden. Zo worden de broodjes aap, ook wel urban legends of mythes genoemd, geboren.



Rashid Niamat is journalist en werkzaam bij ISPam.
Rashid is te bereiken via rashid@niamatmediagroup.nl

Ook bij cloudcomputing is dit beeld herkenbaar. Hierbij is een bijzondere rol weggelegd voor analisten en uitgevers. Bedrijven als Gartner [2], IDC [3] en IDG [4] koppelen in publicaties cloud meermaals letterlijk aan het begrip mythe. In het begin was de markt (aanbieders en vragers) minder in staat de impact van dit label te overzien en werd er incidenteel minder professioneel gereageerd. Anno 2015 mag worden verwacht dat men in staat is het kaf van het koren te scheiden.

Tijd dus om de vraag te beantwoorden: in hoeverre bevatten de mythes rond cloud een kern van waarheid of kunnen ze worden afgeserveerd? De mythes gaan van A (Aanschaf) tot Z (Zekerheid).
Als we kijken naar de punten die in de lijstjes met mythes van de drie genoemde bureaus het meest voorkomen en die relevant zijn voor de lezers van het PvIB-magazine vallen deze vier op:

- **Fysieke veiligheid**
- **Compliance**
- **Personeel**
- **Leveranciers**

Deze punten worden hieronder afzonderlijk beschreven en daarvoor is aan een bedrijf dat cloudproviders datacenterfaciliteiten biedt (Colt [5]) en een cloudprovider (Fundaments [6]) gevraagd om een reactie.

Fysieke veiligheid

De eerste mythe wordt door zowel voor- als tegenstanders gebruikt. De voorstanders wijzen er op dat als je al off-premise stond in een datacenter dat ISO-gecertificeerd was, het inzetten van clouddiensten op zich geen verandering hoeft te betekenen. Zolang ook dat datacenter maar aan gelijkwaardige eisen voldoet.

De tegenstanders hanteren argumenten voor de off-premise-case en de on-premise-case. In het geval van off-premise wordt vaak gesteld dat in een cloudomgeving de fysieke plek van data niet bekend is en daarmee niet duidelijk is of elke locatie wel veilig is. Toegegeven, dit argument snijdt hout. Zozeer zelfs dat grote cloudaanbieders sinds enige tijd op 24/7 basis kunnen aangeven waar de data staat (zie ook compliance).

Dan de on-premise-veiligheid. Partijen die IaaS- of SaaS-oplossingen bieden, weten dat het met veiligheid van de eigen serverruimtes binnen kantooromgevingen vaak minder goed is gesteld. Om die op een behoorlijk peil te houden, zijn permanente investeringen in zowel kennis als menskracht nodig (zie ook personeel) en dan is er nog het punt van aanpassingen die bij gehuurde bedrijfspanden niet zomaar tot de mogelijkheden behoren (denk naast toegangsmaatregelen aan additionele connectiviteit en stroomvoorzieningen).

De mythe dat fysieke veiligheid van data en processen in een cloudomgeving inferieur is aan on-premise-oplossingen kan gerust worden afgeserveerd.

Compliance

Wie gewend is aan de situatie dat de eigen data in een eigen omgeving staat (wat dan het eigen datacenter kan zijn of in gehuurde dedicated-rackspace) weet daardoor met de grootst mogelijke zekerheid dat hij op dat punt in control is. Vanuit die ervaring is verhuizen van on premise naar naar off-premise een grote stap. Helemaal als het gaat om migratie naar een publieke cloud, waar de resources worden gedeeld met derden en de data over de hele wereld kan reizen, volgt al snel de uitspraak dat men zo nooit meer compliant aan ISO2700x kan zijn.

Is die mythe niet wat kort door de bocht? Is het niet een argument dat elke vorm van migratie wil dwarsbomen? Bedrijven die off-premise diensten afnemen weten dat ze daarmee nog steeds aan de regels kunnen voldoen. Het is zaak gedetailleerde afspraken maken met de leverancier, niet alleen over het type cloud (private, hybride of eventueel public, zie ook deze NIST-publicatie [7]) maar vooral over de SLA's. Hierbij wordt door critici nog wel eens over het hoofd wordt gezien dat als het gaat om zaken als continuïteit en aansprakelijkheid beide partijen belang hebben bij heldere formuleringen.

Is daarmee in elke situatie een clouddienst compliant? Het is geen toeval dat de meeste serieuze cloudaanbieders in Nederland de afgelopen jaren in toenemende mate werk zijn gaan maken van certificering, ze beschouwen het inmiddels als een must. De aanbieders die input leverden voor dit artikel merkten daarbij op dat zij het klantgedrag als gevolg van de certificeringen zien veranderen.

Larik Jan Verschuren van Fundaments verwoordde dat als volgt: “Om de compliancy aan te tonen wil de cloudgebruiker een uitspraak hebben over de compliancy van een leverancier. Dit is waar certificeringen een leidraad kunnen zijn. Normen als ISO27001:2013 en NEN-7510 geven een kader waarbij de maatregelenset voor het beveiligen van informatie worden getoetst. Vaak wordt dit door gebruikers gehanteerd om inzage te krijgen in de processen van een cloudleverancier. Doordat

deze normen extern worden getoetst kan gesteld worden dat dit een goede basis vormt voor een vergelijk tussen leveranciers."

Ben Timmer van Colt merkte hier over op: "Er is geen handboek 'Cloud Certified Datacenter'. Wij kijken daarom zelf naar ASHRAE, dat standaarden omtrent cloud in relatie tot datacenters ontwikkelt. […] We zien de houding ten opzichte van certificeringen veranderen en dan met name wat de audits betreft. Klanten doen veel vaker kleine stukjes in plaats van een 'overall' audit ineens, zoals dat een aantal jaren geleden wel gebeurde. Wijzelf willen in staat zijn om elk moment succesvol ge-audit te worden en houden dus ook een strak regime aan."

De conclusie is dat er sprake is van goede inspanningen. Dat helpt velen te kunnen oordelen of zij compliant blijven als er naar de cloud wordt overgestapt. Echter er kunnen situaties blijven waarin de regels waaraan de beoogde gebruiker is onderworpen niet in een willekeurige cloudomgeving te realiseren valt. Zo is de kans dat een advocaat, die via een reguliere consumentenbreedbandverbinding en gebruik makend van een publieke clouddiensten zonder vastgestelde geolocatie, aan de regels van zijn beroepsgroep voldoet nihil. In die gevallen klopt de uitspraak dat de cloud niet compliant is, maar om daar het label mythe aan te verbinden is overdreven.

Personeel

De mythe dat cloud slecht is voor het eigen personeelsbestand lijkt te kloppen. De komst van cloud betekent het einde van bepaalde IT-functies en daarmee het verlies van banen. Dit kan consequenties hebben voor veiligheid en kwaliteit. Echter IT overdragen aan derden is geen nieuwe ontwikkeling, outsourcing bestaat minimaal sinds het begin van deze eeuw. Het is door de komst van cloud iets dat in principe voor elk type bedrijf, los van sector en omvang, relevant kan worden.

Maar toch moet er ook een kanttekening worden geplaatst. Volgens Verschuren wordt het outsourcen van de oude hardwaregerelateerde zaken naar een IaaS-omgeving door de direct betrokkenen steeds vaker gezien als een last die eindelijk van de schouders wordt gehaald.
"Wij horen keer op keer dat men blij is van de hardware te zijn verlost. IT-afdelingen besteden de tijd en middelen liever aan ontwikkeling en beheer van applicaties dan aan de infrastructuur. Daar zie je dus dat outsourcing leidt tot meer focus, meer tevredenheid en dat zal veiligheid en kwaliteit ten goede komen."

Een andere component van de mythe rond personeel is dat het overstappen naar de cloud nieuwe banen oplevert. Dat kan zijn bij de cloudaanbieder, maar ook bij de afnemer van de dienst. Toegegeven: daar zal de individuele werknemer die zijn baan ziet verdwijnen, weinig aan hebben. In hoeverre deze mythe juist is, is lastig aan te tonen, vreemd genoeg ook omdat er zoveel IT-vacatures openstaan. Daarvan wordt dan weer beweerd dat die bestaan door de mismatch van kwalificaties. Dit laatste verdient de nodige aandacht, want het begrip kwalificaties is breed (kennis van encryptie is een eis, maar van een compleet andere orde dan de eis stellen dat het personeelslid in bezit moet zijn van een VOG).

De twee aanbieders kwamen los van elkaar op het punt personeel en cloud met dezelfde opmerking. Het kwam er op neer dat (onder andere) ISO en NEN feitelijk ook consequenties hebben voor het eigen personeel. Colt nam de financiële sector als voorbeeld om die consequenties te illustreren: "Als DNB oplegt dat banken mensen moeten screenen, dan leggen de banken dat ook aan ons op. Wij screenen dan onze medewerkers én externen die voor deze klanten aan de slag zijn. "

"Dit betekent dat wij onze medewerkers ook regelmatig opleiden. Naast de vereiste certificeringen vinden we daarnaast dat onze datacentermanagers ook de ITIL-principes moeten beheersen, de wettelijke kaders moeten volgen en bijvoorbeeld schakelbevoegd naar NEN3140 moeten zijn [8] . Het heeft ermee te maken dat we een grote organisatie zijn en willen dat de teams in de datacenters zelfsturend zijn, zij moeten dus tot op een behoorlijk hoog niveau autonoom kunnen acteren."

Beide partijen merkten op dat de medewerkers dit als een positieve ontwikkeling beschouwen. De vereiste kwalificaties en aanvullende trainingen vertegenwoordigen namelijk een zekere waarde.

Terug naar de mythe dat cloud slecht zou zijn voor het personeel. Mensen die door een migratie naar de cloud de eigen baan zien verdwijnen zullen het volledig eens zijn met deze uitspraak. Aan de andere kant zijn er ook twee positieve ontwikkelingen te noemen die deze mythe ontkrachten: cloud maakt het mogelijk dat werk uit handen wordt genomen dat velen liever kwijt dat rijk zijn en er is het punt van specialisatie. Tel daarbij het tekort aan IT-medewerkers en de conclusie zou moeten zijn: elke HRM-professional kan bijdragen deze mythe naar de prullenbak te verwijzen.

Leveranciers

Op dit punt aangekomen is er een begrip dat direct genoemd wordt: de keten. Omdat je bij cloud nooit precies weet met wie je allemaal zaken doet (negatiever geformuleerd: van wie je afhankelijk bent) is het onmogelijk alle processen te doorgronden. Feitelijk ben je alleen al daarom nooit compliant.

Een aantal van de nadelen blijkt aantoonbaar ergens op gebaseerd en is daarmee geen mythe

Dat is de kern van de mythe en dat er een link is met compliance lijkt duidelijk. Toch gaat het hier vooral om iets anders. Het gaat om de complexiteit van de keten en de angst van een of een beperkt aantal partijen afhankelijk te zijn. Niet voor niets is vendor lock-in één van de meest gebruikte begrippen door zowel voorstanders (die dit ontkrachten) als tegenstanders van clouddiensten.

En nu de praktijk. Hoe zien aanbieders de eigen rol, hoe gaan zij om met de keten en pareren zijn die vendor lock-in? Verschuren: "Als IaaS-providers leveren wij een exact definieerbaar deel van de IT keten. Dat deel is opgebouwd uit componenten die wij kennen. Zoals elke professionele aanbieder letten we erop niet van één partij afhankelijk te zijn. In het geval van datacenters zetten we in op vier locaties door het land verspreid en die voeren vanzelfsprekend allemaal minimaal dezelfde certificeringen als wij zelf doen. Bij hardware is het aanbod groter dan bij datacenters, dus het is nog makkelijker spreiding van leveranciers te realiseren. De keerzijde van de medaille zou kunnen zijn dat je kiest voor hardware of software die voor ons nog niet het label proven technology heeft verdiend. Wij zullen dat nooit in productieomgevingen inzetten."

Dat is de ene kant van de keten, hoe werkt het de andere kant uit? Verschuren: "We vermelden op onze website en in al onze publicaties waar wij de bouwstenen vandaan halen waarmee we onze diensten bouwen. Daar praten we verder in detail over met onze klanten. Wat je zo bereikt is maximale transparantie en hiermee is de eindgebruiker –dus de klant van onze klanten– in staat een goed beeld te krijgen van de hele keten. Een keten die wat ons betreft ook versterkt wordt door veelvuldige contacten en heldere contracten."

Wat is daarmee de status van de mythe dat cloud gelijk staat aan een ondoorgrondelijke jungle van (sub-)aannemers en leveranciers? Aan de ene kant lijkt het erop dat door transparant communiceren over de opbouw van de keten heel veel onduidelijkheid uit de weg kan worden geruimd. Voor tal van toepassingen zal die keten ook weinig complex zijn, omdat het eenvoudigweg niet nodig is een groot aantal partijen in te zetten. De mythe heeft daar geen voedingsbodem. Aan de andere kant zijn er situaties waarbij de keten zo complex wordt dat schakels in die keten op dat punt voorbehouden moeten maken. In dat laatste geval geldt dat de mythe niet uit de lucht komt vallen. Maar tegelijkertijd geldt dat een té complexe keten ook in een niet-cloudsituatie genoeg aanleiding geeft deze mythe voor IT in het algemeen in stand te houden.

Conclusie

Over cloud is het laatste woord zeker nog niet gesproken. Een aantal van de vermeende nadelen blijkt aantoonbaar ergens op gebaseerd en is daarmee strikt genomen geen mythe. Dat biedt mogelijkheden, want als iets aantoonbaar en meetbaar is, kan er ook gerichter gezocht worden naar oplossingen.

Tegelijkertijd kan niet worden ontkend dat alle discussies hebben bijgedragen aan positieve ontwikkelingen van everything-cloud. De afnemende vraag naar public cloud ten gunste van private cloud is daar evenzo een voorbeeld van als de eigen ISO voor cloud [9]. De discussies hebben er ook toe geleid dat serieuze leveranciers bereid zijn het gesprek met klanten en prospects aan te gaan. Wie weet leidt dat tot een nieuwe mythe die zelfs kan muteren tot realiteit: dat voor het eerst in de geschiedenis van IT er sprake is van grondige samenwerking in de hele keten en dat dit leidt tot innovaties en verbeteringen.

Links

[1] Geoffrey A Moore: Crossing the Chasm. New York 1991-2014: www.harpercollins.com/9780062292988/crossing-the-chasm-3rd-edition
[2] www.gartner.com/newsroom/id/2889217
[3] www.idc.com/getdoc.jsp?containerId=CL54W
[4] www.cio.com/article/2922374/cloud-security/20-of-the-greatest-myths-of-cloud-security.html
[5] www.colt.net/nl
[6] www.fundaments.nl
[7] pagina 3 van deze PDF voor de definities: csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[8] nl.wikipedia.org/wiki/NEN_3140
[9] www.iso27001security.com/html/27017.html

GEGREPEN DOOR DE FACTOR MENS

PvIB-voorzitter Jessica Conquet in gesprek met haar voorganger Fred van Noord

Eén van de eerste IBO-bijeenkomsten die ze bijwoonde, gaf haar de bevestiging: het vakgebied informatiebeveiliging reikt veel verder dan de implementatie van technische maatregelen. Cognitieve psychologische aspecten spelen een rol. De bijeenkomst ging over menselijk gedrag. Waarom voelt iemand zich wel of niet bedreigd? Wat bepaalt wat veilig is of niet? Hoe schatten gebruikers risico's in?

De nieuwe PvIB-voorzitter, Jessica Conquet, kan zich de bijeenkomst in 2009 nog heel goed herinneren. "Informatiebeveiliging is een mooi vak", stelt ze. "Voor mij meer dan een vak. Het is mijn passie. En met terugwerkende kracht durf ik te stellen dat deze bijeenkomst voor mij in dit besef een heel belangrijke rol heeft gespeeld."
"Als student informatica en in de eerste jaren van mijn carrière was ik alleen gefocust op de technische kant van ICT. Pas later, toen ik me ging richten op informatiebeveiliging en risicoanalyse, kwamen hier de aspecten 'Business' en 'Mens' bij."

In het vakgebied van informatiebeveiliging komen volgens Jessica nadrukkelijk alle aspecten samen. "De burger die vooral op zoek is naar een betrouwbaar middel om op elk gewenst moment over de voor hem of haar belangrijke informatie te beschikken. Tegenover bedrijven en organisaties die vaak niets anders willen dan dat de burger hen als eerste vindt op de elektronische snelweg om vervolgens zaken te doen. Daarnaast medewerkers binnen organisaties die tegenwoordig niet meer buiten ICT kunnen en daarmee extreem hoge eisen stellen aan beschikbaarheid en betrouwbaarheid van informatiesystemen. En tot slot technici die allemaal binnen hun discipline het beste weten hoe systemen op te zetten, te beheren en te beveiligen, maar onmogelijk het gehele speelveld kunnen overzien."

Met deze uiteenzetting begint de kersverse PvIB-voorzitter het gesprek dat ze heeft met haar voorganger Fred van Noord. Een wisseling van de wacht die de reden is voor een duo-interview. En al snel blijkt dat Fred net als Jessica is geboeid door de factor mens binnen het vakgebied informatiebeveiliging. Niet zo vreemd, want de achtergrond van Fred ligt in de organisatie-psychologie en bedrijfskunde. Hij benadert informatiebeveiliging daarom veelal vanuit het perspectief van de organisatie- en veranderkunde. "Organisaties ontwikkelen, veilig gedrag van mensen verbetert. En daarmee verandert het besef van veiligheid continu. Iets waarmee wij als informatiebeveiligers altijd rekening moeten houden. Awareness op de werkvloer komt en gaat", weet Fred uit inmiddels ruime ervaring. En juist dat laatste besef heeft Jessica dus gegrepen. "Menselijk gedrag pakt en blijft intrigeren", geeft ze aan. "Het maakt ons vakgebied aantrekkelijk voor mij." En daar sluit haar voorganger zich volledig bij aan.

Vereniging moet groeien

Eens zijn de twee het ook over de potentie die 'hun' PvIB heeft. "Ontwikkelingen in ons vakgebied volgen elkaar snel op. Informatiebeveiliging is niet meer weg te denken uit de samenleving. Bedrijven en organisaties moeten steeds meer informatie beschermen tegen een steeds complexer dreigingsbeeld. Waardoor het aantal informatiebeveiligers toeneemt. De vereniging moet dus ook groeien", stellen Jessica en Fred eensgezind.
"Na de fusie in 2007 hadden we duizend leden. Inmiddels is dit aantal gegroeid naar zo'n vijftienhonderd", weet Fred. En hoewel Jessica zich niet wil vastpinnen op een streefgetal qua ledenaantal geeft ze wel aan gestaag verder te willen groeien. "Waarbij we ons vooral moeten richten op studenten en young professionals", gaat ze verder. "Hen moeten we de kans geven feeling te krijgen met hun toekomstige vakgebied. Ik zie hier echt een rol weggelegd voor ervaren leden binnen de vereniging. Zij kunnen jongeren bij de hand nemen en wegwijs maken binnen PvIB en ons vakgebied. Niet voor niks hebben we onder het voorzitterschap van Fred het tientjeslidmaatschap ingevoerd. De manier om jongeren al vroeg te binden aan ons als vereniging."

En wat Jessica betreft zou de vereniging nog veel eerder in het proces van beroepskeuze van zich kunnen laten horen. "Kinderen en jongeren moeten steeds vroeger kiezen welke richting ze op willen. Hier kunnen we ook als vereniging op inspelen. Door een bijdrage te leveren aan bootcamps voor jonge hackers bijvoorbeeld, maar ook door kinderen al op jonge leeftijd enthousiast te maken voor het vakgebied. Door het geven van gastlessen."
Ook meisjes hoopt Jessica zo enthousiast te maken voor het vak. Want, meer vrouwen zijn wat haar betreft zeker welkom binnen het vakgebied. "Daarop inzetten, kan wat mij betreft niet vroeg genoeg beginnen", stelt ze enthousiast.

Acties zoals genoemd, hoeft de vereniging volgens de kersverse voorzitter echt niet allemaal zelf te organiseren. Er zijn volgens haar initiatieven genoeg waarbij PvIB kan aansluiten. Als voorzitter ziet zij het dan ook als haar taak en die van het bestuur om dit soort initiatieven op te zoeken. Contacten te leggen en vervolgens linken te leggen naar de verschillende commissies binnen PvIB.

Sandra Kagie is freelance tekstschrijver/journalist (website: www.sanscriptproducties.nl; twitter @SanSanscript). Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst & taal. In het verleden is zij als eindredacteur nauw betrokken geweest bij 'Informatiebeveiliging'.

Menselijk gedrag pakt en blijft intrigeren; het maakt ons vakgebied aantrekkelijk voor mij

Faciliteren en enthousiasmeren

Jessica: "Wij als bestuur zijn er voor onze leden. We moeten onze vrijwilligers in de verschillende commissies de ruimte geven om nieuwe wegen te bewandelen. Wat wij als bestuur moeten doen, is hen faciliteren en enthousiasmeren. Energie geven!" Wat dat betreft gaat de nieuwe voorzitter dingen niet ineens heel anders aanpakken dan haar voorganger. "Fred heeft ingezet op nauwe samenwerking tussen het bestuur en de verschillende commissies. Een samenwerking die ik nog verder wil versterken."

"Onze commissieleden vormen het fundament van de vereniging", haakt Fred in. "Professionals die de juiste keuzes weten te maken en snel kunnen schakelen. Dat zie je bijvoorbeeld binnen de activiteitencommissie. Zij presteren het keer op keer bijeenkomsten te organiseren die aansluiten bij de praktijk van onze leden. Ze weten risico-aspecten uit de maatschappij op te pakken en collega's hierover op het juiste moment te informeren. Een prestatie van formaat. Dat blijkt ook wel uit de bezoekersaantallen van de avonden. Honderdvijftig bezoekers op een avond is echt geen uitzondering."

Zelf heeft Fred ook zo'n vijf jaar deel uitgemaakt van de activiteitencommissie. "Misschien wel het leukste dat ik ooit heb gedaan binnen de club", kijkt hij terug. "Vaak is het gewoon een kwestie van durven", herinnert hij zich. "Nieuwe dingen doen en brutaal zijn. Je steeds weer afvragen wat nodig is om tot beter opgeleide professionals te komen. Relevante thema's benoemen en hier de juiste sprekers bij zoeken."

Bron van informatie én inspiratie

De activiteitenavonden van de PvIB. Het eerste wat bij veel leden opkomt wanneer je volgens Jessica vraagt naar de betekenis van de vereniging voor hen. Focus op een divers aanbod van dit soort bijeenkomsten is in haar ogen dan ook van levensbelang om als vereniging interessant te blijven voor (nieuwe) leden. Iets dat volgens haar en haar voorganger ook geldt voor het blad dat u nu leest. Volgens beiden absoluut een belangrijke bron van informatie én inspiratie voor collega's in een heel breed vakgebied.

Informatie bieden, kennis overdragen en kennis die elders, maar zeker ook binnen de vereniging, beschikbaar is op een eenvoudige manier ontsluiten. Dat is en blijft ook onder de nieuwe voorzitter een belangrijke pijler onder PvIB. Wat Jessica betreft zal er daarom zeker worden gekeken naar manieren om deze kennis steeds beter en op nog meer manieren toegankelijk te maken. Via de website, maar ook middels de inzet van social media. Een speerpunt wat haar betreft.

Advies: 'Denk groot'

Bij de overdracht van het voorzitterschap hoort traditioneel ook een advies van de oude voorzitter aan zijn opvolger. Zo ook in dit geval. Fred adviseert zijn opvolger 'groot te denken'. "Een idee niet bij de minste of geringste tegenslag op te geven, maar dingen waar je oprecht in gelooft de kans te geven. Wanneer het belang van de vereniging hiermee gediend is." Alleen op deze manier kan PvIB zijn rol als autoriteit in het domein van de informatiebeveiliging volgens Fred waar blijven maken. Een advies dat Jessica zeker ter harte neemt. "Ik heb immers gezien waar dit 'groot denken' toe kan leiden", geeft ze aan. "Denk maar aan de totstandkoming van een uniform kwalificatiestelsel binnen ons vakgebied waarmee kennis en ervaring van professionals inzichtelijk wordt gemaakt. Iets dat er mede door de inspanningen van Fred echt lijkt te komen. Een prestatie van formaat waarbij PvIB de rol van initiator heeft." "Met de beschrijving van de verschillende beroepsprofielen en bijbehorende competenties hebben we een belangrijke stap gezet", beaamt Fred verwijzend naar de Whitepaper Beroepsprofielen Informatiebeveiliging, gepubliceerd in mei 2014. Een document dat inmiddels wereldwijd is verspreid. "Maar hiermee zijn we er nog niet", waarschuwt hij. "De profielen moeten zich nu gaan bewijzen door breed geaccepteerd en toegepast te worden. Iets waarvoor ik me samen met anderen binnen de werkgroep Kwalificaties zal blijven inzetten. Een uitdaging, want zo'n kwalificatiestelsel is natuurlijk niet statisch. In een tijd van permanente educatie moet zo'n stelsel onderhouden worden."
Waarbij PvIB volgens Jessica natuurlijk de samenwerking zal blijven zoeken met alle betrokken partijen: opleidingen, werkgevers en professionals. "Samen zijn we immers verantwoordelijk voor een verdere professionalisering van de beroepsgroep", benadrukt zij. "Een streven dat we als vereniging hoog in het vaandel hebben staan. De brede acceptatie en toepassing van een uniform kwalificatiestelsel zou wat dit betreft zonder meer een kroon op het werk zijn. Het ultieme bewijs dat we als vereniging van vrijwilligers ertoe doen. Door in de woorden van mijn voorganger 'groot te denken'."

VOLDOEN AAN DE WET IS NIET MEER VOLDOENDE

Nog niet zo lang geleden had ik het genoegen met Neerlands "slimme privacy-koppen" aan tafel te mogen zitten. Uiteraard zitten we daar met een opdracht: met inzichten over Big Data en privacy mogen we onze politici hopelijk beter informeren over mogelijkheden en onmogelijkheden voor innovatie. De heren en dames aan tafel waren het over een aantal zaken roerend eens. Zo hebben wij als Nederland NU de mogelijkheid voorop te lopen in privacyvriendelijkheid, maar ook de angst zit er bij bedrijven goed in en juist dat remt innovatie.

De publieke schandpaal wordt de afgelopen tijd veelvuldig benut voor bedrijven die "iets" proberen te doen wat in beginsel op gespannen voet staat met het grondrecht op privacy. Banken die analyses willen doen op het gegevensverkeer, verzekeraars die lagere premies aanbieden voor goed gedrag en pizzabezorgers die met camera's door de straten rijden zijn slechts enkele voorbeelden daarvan.

Nu is dat publieke debat uiteraard niet verkeerd, na jaren aandringen op het belang van privacy is dit eindelijk doorgedrongen tot het bredere maatschappelijk debat. Maar zoals met alles wat nieuw is, hebben we samen ook wat te leren. Niet op de laatste plaats over hoe we met dat debat omgaan en waar we innovatie kunnen stimuleren zonder meteen de privacyplank mis te slaan. Het publieke debat slaat de plank mis door ieder nieuw idee meteen als slecht te bestempelen. Niet elke innovatie leidt tot een big-brother-staat. De ondernemende sector slaat de plank mis door ieder nieuw idee slecht voor het voetlicht te brengen. Een enkel "we voldoen aan de wet" volstaat absoluut niet voor acceptatie door de maatschappij.

Voldoen aan de wettelijke vereisten is een no-brainer. Elk idee dat niet aan de wet voldoet is een idee dat geen kans van slagen heeft. Het gaat dus echt niet meer over die wet. Er zit een vraag voor: hoe willen wij als bedrijf bekend staan, wat zijn onze waarden over privacy? Pas als die vraag beantwoord is, kan verder gedacht worden. Nu wij dit idee hebben, hoe gaan we dan met privacy innoveren? Ofwel: kan het beter, met minder gegevens, kunnen wij ons doel op een privacyvriendelijke manier bereiken? Ga een idee ook niet meteen helemaal breed uitrollen. Probeer het in een kleine setting uit met medewerking en feedback van klanten. Laat hen vertellen wat zij ervan vinden en neem het ongezouten commentaar over eventuele privacyproblemen ter harte. Laat de klant meedenken en denk zelf ook alvast na over die klanten die het echt niet willen. Ga je hen ook goed kunnen bedienen?

Communiceren is net zo belangrijk als die privacyinnovatie en innovatieve privacy. De schandpaalvoorbeelden kenmerken zich namelijk allemaal door een gebrek aan open communicatie. Leg uit wat je doet, waarom je dat doet, welke persoonsgegevens je daarvoor gaat gebruiken en welke waarborgen je allemaal in plaats hebt gebracht om de inbreuk zo minimaal mogelijk te maken. Nut je privacyvriendelijkheid uit. Ik, als klant van vele bedrijven in Nederland en als privacyfundamentalist, wil een goede keuze kunnen maken. En dat kan ik alleen maar als ik weet wat er gebeurt.

Mr. Rachel Marbus
@rachelmarbus op Twitter

RETURN OF THE CYBERMEN...
OR PERHAPS THEY NEVER REALLY LEFT!

There is no doubt that Cyber Threat is the topic of the moment. It is featuring on the agenda of pretty much every board, audit committee and regulator.

The Financial Conduct Authority (FCA) has published its 2015/16 business plan and has identified technological challenges as one of the key risk drivers, whilst recognising that of course innovative uses of technology bring benefits to consumers. Cyber-crime is highlighted as one of these challenges and in particular the risk of such activity causing serious disruption to financial markets. The growing reliance upon the internet as the channel by which consumers provide personal data increases the risk of this data being compromised. It is recognised that firms with older and more complex IT systems can find it more difficult to implement adequate security measures and that this is a real risk factor. The FCA has confirmed its commitment to work with the Prudential Regulation Authority (PRA) and the Bank of England on visibility of IT resilience and risks at board level, and with Treasury and regulatory partners on addressing cyber risk.

It is encouraging to see that the FCA is taking the risks posed by cyber-crime seriously, although it may be that the topic warranted more than three paragraphs of an 80-page document. Cyber-crime in its many forms is one of the biggest risks faced by both firms and consumers today and many people may be looking to the regulator for leadership on this issue.

Even the politicians are jumping on the "cyber bandwagon". Former Home Secretary David Blunkett warned in April 2015, *"The biggest threat to the UK way of life will come from cyber terrorism rather than traditional attacks on cities and people."* US President Barack Obama characterised foreign cyber-threats as a "national emergency". During the 2015 State of the Union address, he said if the US government does not improve cyber defences, *"we'll leave our nation and our economy vulnerable."*

Cyber security has been defined as a Tier 1 threat to the nation and has become a strategic risk management issue for all organisations. MI5 wrote to the board of every FTSE350 in mid-2013 urging them to ensure that their businesses were taking adequate steps to protect themselves.

Questions such as "What are we doing about the Cyber Threat?" or "Can we be hacked?" or "Should we get our security tested?" are being asked around Boardroom tables across the land. Executives might perceive that they are under siege.

In our opinion, looking beneath the headlines and media hype, there is definitely good reason for asking the question "Is the Cyber Threat really anything new?"

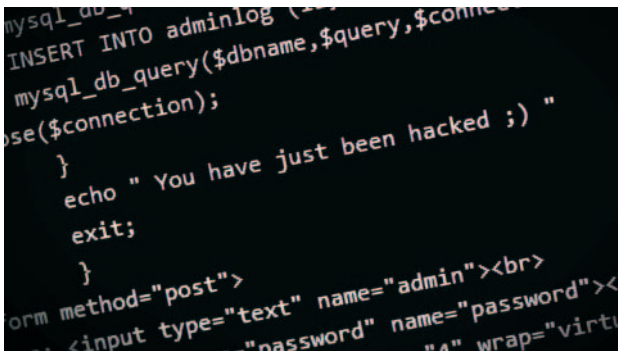
There is no doubt that as organisations and individuals, we are more reliant upon technology and our information assets than ever before – information really is the life-blood of organisations

these days. In reality, threats to corporate information or data have existed for many years. To a certain extent, Cyber Threat is just a new marketing label being used to sell government policies or commercial security software and services.

What is the Cyber Threat?

The million dollar question - but you won't get the same answer twice! This is simply because 'Cyber' (whatever that might be) isn't really a threat at all. The Cyber Threat is at best a convenient label to apply to the many and varied risks to data, information and the systems which store and process it.

Cyber threats or crimes can be orchestrated in various ways. Targets can be aimed at critical infrastructure, manufacturing, power grids or water supplies. They could be aimed at disrupting the availability of websites and networks or at stealing trade secrets and financial information. Others could be driven by espionage, vandalism, terrorism, sabotage, political motives or any form of criminality.



These threats could be precipitated by events or actions as varied as external hacking, social engineering, a compromised third party supplier, an employee leaking information via webmail or so-called "hacktivists" hell-bent on causing as much disruption as they can. Such diverse activities are likely to require very different responses to remediation and ongoing management.

So, is this really new?

In the immortal words of Public Enemy *"Don't believe the hype, it's a sequel."*
Whilst an American hip hop group appears an unlikely source to reference regarding Cyber, and whilst they didn't realise it at the time, perhaps a more poignant lyric from the track in question is, *"They claiming I'm a criminal, by now I wonder how, some people never know the enemy could be their friend, guardian."*

Whilst a breach or a hack can result in a range of outcomes - including unwelcome disruption, cost, media attention - it is then, by default, visible and can therefore be remediated and/or mitigated against. Whilst the average hacker can cause you a serious headache, this is not even close to the "migraine" posed by a cyber-terrorist.

Beneath the marketing gloss, should we be concerned about Cyber Threat? The answer is categorically "Yes!" Security incidents globally are on the rise and the level of threat to organisations from data theft, espionage and website attacks has never been higher. Your reputation, regulatory status and financial well-being are more at risk now than they have ever been.

Latest UK government figures indicate that 81% of large corporations and 60% of small businesses reported a cyber-breach, with each breach estimated to cost between £600,000 and £1.15m for large businesses and £65,000 to £115,000 for smaller companies. One London-based business lost £800m following a single incident in 2012!

This elevated threat brings with it a whole new set of considerations for those tasked with determining the risk and subsequent acceptance levels within their organisations. On the plus side, there is plenty of "event data"; these types of incidents aren't new to us and we have experienced first-hand the damage they can do.

BUT …. in the inimitable words of former United States Secretary of Defense Donald Rumsfeld, *"Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones."*
We find ourselves asking the question "Can you truly calculate the cost of downtime? Reputational impact? Loss of intellectual property or competitive advantage?"

Back to basics

Organisations clearly need to respond to the threat. But where to start? Technology companies will tell you that you should buy their software and it will keep you safe. IT service companies will tell you that outsourcing your IT to them will solve all of your problems. Let us be clear, there are some excellent services and technical solutions out there; however, none of them are free of charge and applied in isolation there is a very real risk of completely missing the point.

Technology is, of course, a key enabler. But investment in people, skills and robust policies and procedures are crucial too. This is a problem for the entire business to solve – not just IT.

Technology and tools of the highest quality can be undermined by weaknesses in basic security practices or by a flawed corporate culture. Today's cyber criminals recognise this and exploit it by adopting a range of approaches which step away from the purely technical and exploit weaknesses in the way that organisations manage, control and interact with their information.

The threat of the 'inside job', for example, is definitely on the rise. The corporate approach therefore also needs to shift from one of 'implementing security' to one of 'information risk management'.

Fundamentally, addressing the Cyber Threat means going back to basics, looking again at your organisation and the controls you already have:

- Understanding your people - what threats do they pose? After all there is no patch for stupidity!
- Understanding your organisation's information, where it is and how it is used;
- Identifying the main risks to information assets; and
- Ensuring that the right measures are adopted to mitigate risk to within acceptable levels – balancing cost versus risk.

Understand the risks

Software and tools may be part of the solution, as may be transferring some of the risk by outsourcing services to a third party or conducting a regular penetration test. But unless the foundations of good information and security governance are working well, the investment will most likely be wasted.
These foundations include:

- User access management
- Clear policies on security, acceptable system use and social media
- Staff security training and awareness
- Oversight of third party suppliers; and
- Timely application of software security updates.

Perimeter? What perimeter?

Like it or not, IT globalisation is here to stay. Chief Information Officers are increasingly pursuing globalisation, seeking to improve operations across geographic and organisational boundaries. But globalisation is both an emerging and complicated change and there are few signposts to tell CIOs which way to turn.

With the advent of mobile technologies, we have been treated to 127 new acronyms and abbreviations!! A few examples include: Bring Your Own Device (BYOD), Bring Your Own Software (BYOS), Advanced Mobile Phone Service (AMPS), Electronic Data Interchange (EDI), Universal Mobile Telecommunications System (UMTS) and Wireless Local Area Network (WLAN). In short, a whole new set of challenges to those tasked with protecting your prized possessions and an entire new product suite for the vendors to sell to counter the risks presented.

Return of the ..... layered security!!

It would be wrong not to leverage the internet for an opinion. The Wikipedia definition is as follows:

"Layered security, also known as layered defence, describes the practice of combining multiple mitigating security controls to protect resources and data.
The term bears some similarity to defences in depth, a term adopted from a military strategy that involves multiple layers of defence that resist rapid penetration by an attacker but yield rather than exhaust themselves by too-rigid tactics. As the incursion progresses, resources are consumed and progress is slowed until it is halted and turned back. The information assurance use of the term "defence in depth" assumes more than merely technical security tools deployment; it also implies policy and operations planning, user training, physical access security measures, and direct information assurance personnel involvement in dealing with attempts to gain unauthorized access to information resources. Within a defence in depth security strategy, layered security is regarded by some as merely a delaying tactic used to buy time to bring security resources to bear to deal with a malicious security cracker's activities."

Defence in depth is undoubtedly the way to go!!

The sheer complexity of the challenges Cyber presents should not be underestimated. Please don't delude yourselves into thinking that "it won't happen to me". It is not just the 'big boys' that are targets. Cyber criminals are opportunists and will leverage a soft target to achieve their wider aims. Larger firms with bigger budgets have better detection capability than smaller organisations – they are more likely to spot and deal with breaches of security before they escalate. Another source of exposure are your third parties. Increasingly, organisations' defences are being breached when external service companies become compromised providing criminals with a trusted base from which to attack. Lack of governance and management of trusted third party arrangements introduces a significant security and information management 'blind spot'.

We accept that not everyone can afford a multi-layered solution, staffed by dedicated professionals actively monitoring their networks "24x7" for the next exploit. If you revert "Back to Basics" and "Understand the Risks", though, this will go a long way towards making sure that when the time comes to invest, it will be an informed, risk-based and well considered decision. This will hopefully help you remove and/or mitigate the issues which present the greatest threat to your organisation.

Steps to effective governance

We never tire of banging the governance "drum." Unfortunately no matter how loud it's played, there are those who still choose to ignore it.

The core principles of good governance are essential if organisations are to effectively address the cyber threat no

matter how large or small. These include:

- Setting, maintaining and continuing to evolve the "tone at the top"
- Monitoring by the Board of Directors
- Training and awareness
- Independent assurance
- Regular risk-based testing – internally and externally
- Internal control procedures and internal audit; and
- Regulatory controls

So what's next?

Without any shadow of a doubt the problem is going to get worse before it gets better. We have heard it described as an epidemic. Whilst this might be debatable, we do concur with the view that the problem is unlikely to go away anytime soon. It will, to an extent, need to be "tolerated" as a risk of doing business and mitigated where possible.

In our opinion there needs to be a more robust framework of cyber security regulations driven by governments and the regulators. This needs to appropriately consider the associated risks. For example a large financial services firm is likely to be far more susceptible to attack on a regular basis than a small convenience store. The results of an attack, however, could be equally devastating to both.

Our next article will explore what frameworks are currently available, the pros and cons of each and what the Cyber Threat landscape will look like in the future.

Neil May (left) is Senior Manager (nmay@kscllp.co.uk) and Mark Child is Partner (mchild@kscllp.co.uk) at Kingston Smith Consulting.

BOTNETS OPSPOREN IN DNS-VERKEER
ABUSE INFORMATION EXCHANGE

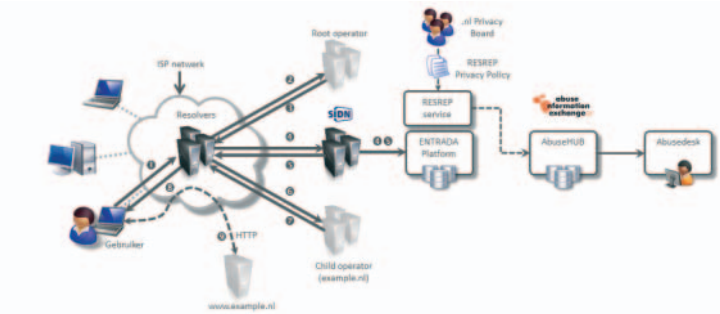
De Vereniging 'Abuse Information Exchange' is een initiatief van KPN, SIDN, Solcon, Tele2, XS4ALL, Zeelandnet en Ziggo/UPC. Het doel is om de informatievoorziening over botnets en andere vormen van internetmisbruik in Nederland te stroomlijnen en zo te verbeteren. Dit gebeurt door abuse-meldingen te ontvangen in een centraal systeem, de AbuseHUB, en deze te correleren.

De AbuseHUB is sinds juni 2014 volledig operationeel. Gegevens over botnetbesmettingen komen geautomatiseerd binnen, via zogenaamde reliable notifiers. Dat zijn partijen met wie een overeenkomst is afgesloten en waarvan is vastgesteld dat ze over betrouwbare, actuele informatie beschikken van botnetbesmettingen en andere informatie in relatie tot internetveiligheid. Shadowserver is een voorbeeld van zo'n reliable notifier.

Op een slimme manier analyseert de AbuseHUB de meldingen (dat wil zeggen: geprioriteerd en zonder 'ruis', zoals dubbele meldingen). Vervolgens worden ze verstrekt aan de desbetreffende providers, zodat die actie kunnen ondernemen.

ENTRADA

Het R&D-team van SIDN, de beheerder van het .nl-topleveldomein, beschikt over een onderzoeksplatform, dat we ENTRADA noemen. Dat is een op Hadoop gebaseerd 'big data'-systeem, waarmee we DNS-data analyseren. Dagelijks worden er ruwweg 166 miljoen DNS-queries toegevoegd aan dit cluster.

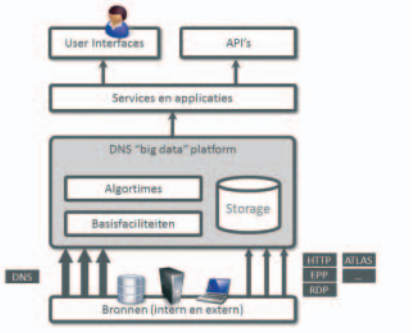


Het merendeel van deze DNS-verzoeken is natuurlijk volstrekt legitiem en voor abuse-preventie nauwelijks interessant. Maar verscholen in deze berg data zit ook informatie die wijst op phishing of een malware-besmetting. En dat laatste delen we tegenwoordig actief met de eerder genoemde AbuseHUB.

De ENTRADA-feed als reliable notifier

Het SIDN Labs-team heeft, op basis van de data in ENTRADA, een algoritme ontwikkeld, waarmee we bepaalde botnets kunnen opsporen. Het onderzoek hiernaar was onderdeel van het 'ResRep'-project, wat staat voor: 'Resolver Reputation'. Zoals de naam al suggereert, wordt aan de DNS-resolvers die voorbij komen op de autoritatieve nameservers (van .nl) een bepaalde reputatie toegekend. Dat gebeurt op basis van hun gedrag. Het is als het ware een vorm van 'profiling' of 'fingerprinting, waarbij overigens de nodige zorgvuldigheid in acht wordt genomen op het gebied van privacybescherming.

Door gedetailleerd het gedrag van het DNS te bestuderen, bleken we in staat om bepaalde patronen in het verkeer als verdacht aan te merken. Hoe dit exact gaat is geheim, omdat we natuurlijk geen slapende honden wakker willen maken. Maar in elk geval kan ENTRADA heel precies constateren wanneer een bepaald botnet actief wordt op een IP-adres. Als dat een Nederlands IP-adres betreft, rapporteren we die informatie vrijwel meteen aan de AbuseHUB. De betrokken isp kan dan direct in actie komen, bijvoorbeeld door contact op te nemen met de klant en hem te helpen met het verwijderen van de betreffende malware. Dit proces van opsporen en signaleren verloopt geheel geautomatiseerd, 24 uur per dag en 7 dagen in de week.



Sneller, dus efficiënter

Het voordeel van dit systeem ten opzichte van andere systemen, is vooral de snelheid en de volledigheid. Het botnet-gedrag wordt vrijwel meteen op het moment dat het plaatsvindt geconstateerd. Andere 'reliable notifiers', zo ze al wat opmerken, detecteren het misbruik met een aanzienlijk grotere vertraging. De ResRep-feed aan de AbuseHUB is daarmee een mooi voorbeeld van de veelzijdigheid van het ENTRADA-systeem en de waarde van DNS-data.

Auteur: *Marco Davids, research engineer* | ***Mail:*** *marco.davids@sidn.nl*

MODELLING THREAT SCENARIOS DEEL 2

Het artikel Modelling Threat Scenarions (IB 6-2015) introduceerde een aantal concepten die ten grondslag liggen aan dit vervolgartikel. We streven naar alignment tussen risk control requirements en risk control objectives. Het Business Model Canvas zetten we in dit artikel in om tot een schets van een business aligned threat scenario modelling methodiek te komen. Een belangrijke deliverable hierbij is de Threat Scenario Map. De structuur van een Threat Scenario Map zal in dit artikel gepresenteerd worden.

Recap van de belangrijkste concepten

In het voorgaande artikel is het concept van een threat gedefinieerd in termen van Equity, Prospect en Material Events. Het uitgangspunt is de bekende balansvergelijking:

$$Equity = assets - liabilities$$

Prospect is gedefinieerd als:

$$Prospect = opportunity * probability_{opportunity} - risk * probability_{risk}$$

Met andere woorden, de verandering in de prospect is gelijk aan de verandering in de opportunity minus de verandering in risk. Als de geldende probabilities gelijk zijn aan 1 dan zijn equity, assets en liabilities respectievelijk synoniem met prospect, opportunity en risk. Een material event wordt gedefinieerd als een toekomstige gebeurtenis die de waarde van de prospect beïnvloedt en een threat is een material event type die de prospect in negatieve zin beïnvloed. Met behulp van deze concepten gaat dit artikel dieper in op Business Aligned Threat Scenario Modelling.

Business aligned threat-scenario modelling

In dit artikel is het uitgangspunt dat de toegevoegde waarde van een Threat Scenario Model afhangt van de mate waarin het model aansluit bij de verwachtingen, belevingswereld en taalgebruik van betrokken stakeholders. Zoals eerder aangegeven zullen we in dit artikel het Business Model Canvas (BMC) inzetten om de gewenste aansluiting te helpen realiseren. Een ander hulpmiddel zou evengoed door dit doel ingezet kunnen worden. Het gaat erom dat we waarborgen dat risk control objectives aansluiten op risk control requirements.

Michèlle Gittens studeert Economie en Bedrijfskunde aan de Universiteit van Amsterdam met de keuzerichting Financiering en Organisatie. Zij is te bereiken via michellegittens93@gmail.com.

Een voorbeeld van een Business Model Canvas wordt in Figuur 1 getoond.

Figuur 1 - Voorbeeld Business Model Canvas. Bron Business Model Generation

Het toont de negen building blocks van het Business Model Canvas. De succesvolle exploitatie van een business-model zal telkens afhangen van de effectiviteit waarmee de verschillende aandachtsgebieden worden gemanaged. Derhalve zal een onderneming er waarde aan hechten dat er geen materiële afbreuk wordt gedaan aan (onder meer) deze bedrijfsaspecten. Voor de doelstellingen van dit artikel is het BMC een geschikt instrument om de strategische belangen van een (deel van een) bedrijf op een rijtje te zetten.

Basic modelling dimensions: stakeholder interests vs threat sources

De eerste stap in het opstellen van een Threat Scenario Model is het bepalen van de scope van het model. Dit scopingsvraagstuk zien we initieel langs twee dimensies:

- Welke belangen verklaren we in scope?
- Welke threat sources worden gehanteerd in het model?

In dit artikel stellen we dat de scope zich zal beperken tot de volgende aandachtsgebieden:

- Customers Segments
- Key Activities
- Key Assets

Voor de threat sources spreken we af dat we alleen threat sources beschouwen waarbij er sprake is van een perpetrating threat agent. Met andere woorden, we beperken ons tot scenario's waarbij een dader is aan te wijzen. De threat agents die we in scope van dit artikel verklaren zijn:

- Employees
- Hactivists
- Organised Crime

Op basis van de gekozen scope introduceren we in Tabel 1 een eerste Threat Scenario Map. Deze matrix zet de in scope verklaarde belangen uit tegen de threat agents die voor ons voorbeeld relevant zijn.

	Key Assets	Key Activities	Customer Segments
Employees			
Organised Crime			
Hacktivists			

Tabel 1 - Threat agents vs. belangen

Terwijl dit Threat Scenario Model niet zonder waarde hoeft te zijn willen we het verrijken met meer specifieke informatie. Tabel 2 laat zien dat we de in scope verklaarde belangen classificeren om specifieker bedreigde belangen te kunnen onderscheiden. The threat agents worden aangevuld met generieke modi operandi die in het algemeen een aanduiding van de aanpak van de threat agent geven.

		Key Assets		Key Activities			Customer Segments	
		IT	IP	Sales	Operations	Finance	Retail	Wholesale
Employees	steal-the-goods							
	fix-the-books							
	blame-the-butler							
Organised Crime	steal-the-goods							
	fix-the-books							
	blame-the-butler							
Hactivists	steal-the-goods							
	fix-the-books							
	blame-the-butler							

Tabel 2 - Modus operandi vs. klassen belangen

Iedere cell in de Threat Scenario Map noemen we een scenario. Volgens het voorbeeld in tabel 2 worden de belangen van de concern onder meer bedreigd in scenarios waarbij employees die steal-the-goods als modus operandi hanteren. Tabel 3 toont een aantal additionele modi operandi waar de lezer plezier aan zou kunnen beleven.

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

Mnemonic	Omschrijving
steal-the-goods	risk event types waarbij de dader waarde steelt
fix-the-books	risk event types waarbij de dader zijn sporen verdoezelt door administraties te compromiteren
blame-the-butler	risk event types waarbij de dader laat een ander op laat draaien voor zijn misdaden
dupe-the-process	risk event types waarbij de integriteit van een bedrijfsproces b.v. gegevens manipulatie gecompromiteerd wordt
denial-of-service	risk event types waarbij de dader een denial of service variant inzet
damage-reputation	risk event types waarbij de dader de reputatie van een stakeholder schaadt
rig-the-report	risk event types waarbij de dader rapportages in eigen belang

Tabel 3 - Modus operandi

NB deze lijst is niet onze volledige lijst maar volstaat voor de doelstellingen van dit artikel.

Threat scenarios en material event types

In het eerste deel van dit artikel is gesteld dat een material risk event een gebeurtenis is die de prospect van een principal minder maakt. Threat Scenario Modelling is een instrument dat we inzetten om event-types in beeld te brengen die afbreuk kunnen doen aan de belangen van de principal. Dus voor ieder threat scenario in een Threat Scenario Map willen risk-event-types in kaart brengen die met het betreffende scenario te associëren zijn. De impact en de waarschijnlijkheid van de afbreuk is afhankelijk van verschillende factoren betreffende de threat agents en de verschillende kenmerken van de principal. De motivatie van de threat agent zal van invloed zijn op de waarschijnlijkheid van een risk event van een bepaald type. Maar ook de effectiviteit van het risk control framework van de principal zal invloed hebben op impact en waarschijnlijkheid van een risk event van een bepaald type. Het is evident dat ook omgevingsfactoren zoals geldende wetgeving en regelgeving van invloed zijn op impact en waarschijnlijkheid van risk events.

Risk events vs loss events

Het is belangrijk om te appreciëren dat een (1) risk event kan lijden tot verschillende loss events. Bijvoorbeeld een omgekochte medewerker kan over een lange periode en in verschillende situaties afbreuk kan doen aan de belangen van de principal. Zo onderkennen we dat ons Threat Scenario Model per risk-event-type vastlegt welke loss-event-types met de betreffende risk-event-types te associëren zijn.

Uit de risk events types en loss event types die we onderkennen kunnen we risk control requirements afleiden.

Control requirements en risk control objectives

Ook in dit artikel benutten we concepten uit de Principal Agent Theory als leidraad. We stellen dat risk control requirements door de principal worden bekrachtigd om de impact van risk events en loss events op zijn prospect tot een acceptabel niveau te beperken. Dat wil zeggen dat de principal de risk control requirements stelt en zijn agents de taak hebben deze risk control requirements te realiseren. Wie beoogd een business aligned risk control framework te ontwerpen zal telkens willen dat zijn risk control objectives op de risk control requirements afgestemd zijn. Deze afstemming, met andere woorden deze alignment, is te realiseren door de inzet van een Threat Scenerio Model dat op gestructureerde wijze dreigingscenario's identificeert en koppelt aan bijbehorende ze risk-event-types en loss-event-types.

Zo komen we tot een belangrijke stelling voor een business aligned risk control framework: Risk control objectives should align with risk control requirements

Het belang van root cause analysis

We nemen een kleine degressie en merken op dat onze defectieve controls over het algemeen niet risk events maar loss events detecteren. Anders gezegd: loss events zijn de "incidents" die door (Security) incidentmanagementprocessen worden gemanaged. Onze stelling is dat een gedegen root cause analysis vereist is om in het algemeen de risk-events-types uit de loss-event-types kunnen herleiden. Een Threat Scenario Model van voldoende maturiteit is hierbij een belangrijk hulpmiddel.

Prospective risk management en threat scenario modelling

Laten we terug gaan naar af. We stellen dat alle stakeholders gemeen hebben dat ze hun eigen belangen behartigen. In ons jargon geformuleerd wordt dat: alle stakeholders trachten, gegeven hun doelstellingen en specifieke situatie, hun prospect te verbeteren. Threat Scenario modelling biedt ondersteuning bij het ontwerpen en onderhouden van een business aligmed een risk control framework. Het ondersteunt management bij het maken van beslissingen die de prospect optimaal ondersteunen, gegeven de scenario's die in het betreffende verband gelden. De auteurs zullen, gegeven tijd en gelegenheid, deze materie verder uitwerken in toekomstige artikelen.

Samenvatting deel 2

In dit artikel is een aanpak voor Threat Scenario Modelling geschetst. Deze aanpak streeft business alignment na en in dit artikel is het Business Model Canvas gebruikt om bedrijfsbelangen te identificeren. Scenarios, risk-event-types en loss-event-types, risk control requirements en risk control objectives zijn in de context van business aligned threat scenario modelling als ondersteunende concepten gepositioneerd. Threat scenario modelling is als een belangrijke bouwsteen voor prospective risk management gepositioneerd en helpt om op gestructureerde wijze misuse cases te identificeren.

Referenties

[1] Economics of Organizations and Markets. S. Onderstal (2014)
[2] Business Model Generation, A. Osterwalder, Yves Pigneur, Alan Smith, and 470 practitioners from 45 countries, (2010)
[3] Artikel in Informatiebeveiliging: "Management Risk Prospectively in IB1 2015.
[4] Artikel in Informatiebeveiliging: "Tethering Enterprise Interests", gepubliceerd in IB1 2015.
[5] Artikel in Informatiebeveiliging: "Accual Based Risk Management" gepubliceerd in IB1 2015.
[6] Artikel in Informatiebeveiliging: "Threat Scenario Modelling I" gepubliceerd in IB3 2015.

POLLUTION CONTROLLED

The Attributer tries to choose subjects that are topical, so it is important to choose a 'title attribute' that is self-explanatory. When it was agreed that the VW scandal would be a good topic, finding a suitable title/attribute was at first puzzling. In calling it 'pollution controlled' there is explicit intent to explore the wider meaning of 'polluted'. Not just atmospheric pollution, but pollution of corporate values and trust in technological industry in general. There are many aspects of 'pollution' to be explored with this SABSA attribute.

Cyber crime and cyber security are popping up in new and unexpected places. Who would have thought that cyber fraud would be committed by one of the world's most famous car manufacturers? What is perhaps more surprising is that they clearly expected to get away with it. Otherwise why would they have invested their entire reputation in this outrageous scam? Here is a quotation from The New York Times on 23rd September 2015, by contributing writer, Zeynep Tufekci, which nicely sums up the situation [1].

'For the past six years, Volkswagen has been advertising a lie: "top-notch clean diesel" cars — fuel efficient, powerful and compliant with emissions standards for pollutants. It turns out the cars weren't so clean. They were cheating.'

Wow! VW is an old and respected brand. It takes a long time to build up a brand of such value, an asset that the company trades on for the future of its business. Such a brand can be irreparably damaged by a scandal like this, to the point of no return. One wonders how this damage will affect the future of VW, if indeed VW has a future. Let's see what's at stake here.

It is not uncommon for product vendors to exaggerate the efficacy of their wares in a competitive market. It's part of the game of advertising – up to a point. Anti-aging creams come to mind, but then the sales pitch is to the vanity of the buyer, and so long as she/he feels happier for using the product, the actual performance of skin preservation might not be all that important, because the value proposition is an emotional one rather than material. Maybe. But that certainly does not apply here.

VW broke the laws on atmospheric pollution standards, knowingly and deliberately. They designed into their car software a deceiving device that would fool the test procedure. Automobile production is a highly regulated industry in many ways, mostly to do with driver and passenger safety standards. In this case the regulations have far reaching global effects that concern the health and safety of every citizen in the world, not only the buyers of VW diesel cars. Surely legal proceedings must follow on both a criminal and civil law basis.

Then there are the owners of these 11 million cars, who have, overnight, suffered a huge drop in value of the car they own. One can sense the building pressure of one of the largest civil law class actions ever mounted, because it's hard to imagine a similar case with so many potential litigants. The US Federal Government also has a case to bring, since, according to the New York Times, $51 million in subsidies has been paid to some owners to change to 'clean diesel'. The question of 'is diesel really clean' has also been re-opened, which impacts the entire automobile industry.

So how might SABSA thinking have made a difference? VW saw an opportunity and took a risk. So far, so good. What they apparently did not do was to take a rigorous detailed look at all the potential downside risks embedded in the risk scenario – the threats that were associated with this criminal opportunity. One must also ask how the corporate governance processes were unable to control the 'polluted thinking' at whatever level of management this foolish decision was made. SABSA thinking has application everywhere, because every decision is a risk decision.

The Attributer

Links

[1] http://mobile.nytimes.com/2015/09/24/opinion/volkswagen-and-the-era-of-cheating-software.html

ISO 21827 STEEDS BELANGRIJKER BIJ SOFTWARE ONTWIKKELING

Dag in dag uit verschijnt er reparatiesoftware voor beveiligingslekken, in het jargon "securitypatches" genoemd, gemiddeld verschijnen er ongeveer 7 per dag (bron: security.nl). Alleen al hiermee wordt een hele tak van de IT-security-branche aan het werk gehouden. Het is dus logisch dat de roep om foutvrije software groot is. Hoewel bugs onvermijdelijk zijn, hebben programmeurs wel een verantwoordelijkheid, namelijk het veilig coderen van de software. Uiteindelijk betalen de gebruikers van de software de prijs voor het slechte programmeerwerk.

ISO 21827 kan een oplossing bieden om deze problemen onder controle te krijgen. Wat is ISO 21827 en wat kan de security-gemeenschap er mee? De norm verwijst naar het Systems Security Engineering Capability Maturity Model (SSE-CMM) en beschrijft de kenmerken voor inbedding van informatie- beveiliging in het ontwikkelproces, dit zijn;

- De gehele "trusted product or secure system life cycle" met inbegrip van de ontwikkeling, de exploitatie, het onderhoud en de ontmanteling.
- Is toepasbaar in alle sectoren, organisaties, waaronder management, organisatie- en engineering activiteiten.
- Gelijktijdig interacties met andere disciplines, zoals systeemsoftware en hardware, menselijke factoren, test engineering, systeembeheer, operaties en onderhoud.
- Interacties met andere organisaties, waaronder aankoop, systeembeheer, certificering, accreditatie en evaluatie.
- Best practices zijn nu meetbaar (KPIs)!

De ISO 21827 kan worden gezien als referentiemodel voor "security engineering" en als raamwerk voor assessment van de volwassenheid (Maturity) van een software-ontwikkel-organisatie en ook als raamwerk voor verbetering van het software-ontwikkelproces.

De processen

ISO 21827 kent totaal 22 Process Areas en 5 niveaus van volwassenheid. Van deze 22 Process Areas zijn er 11 zogenaamde "Security Engineering Process Areas" te weten:

PA 01 - Administer Security Controls
PA 02 - Assess Impact
PA 03 - Assess Security Risk
PA 04 - Assess Threat
PA 05 - Assess Vulnerability
PA 06 - Build Assurance Argument
PA 07 - Coordinate Security
PA 08 - Monitor Security Posture
PA 09 - Provide Security Input
PA 10 - Specify Security Needs
PA 11 - Verify and Validate Security

Naast de 11 "Security Engineering" Process Areas zijn er nog 11 Process Areas die betrekking hebben op de organisatie en de projecten Process Areas. Deze laatste 11 kunnen worden gebruikt om afstemming met de ISO 15288 (Systems and software engineering - System life cycle processes) te vergemakkelijken. De ISO 21827 kent de volgende Process Areas:

PA12 - Ensure Quality;
PA13 - Manage Configuration;
PA14 - Manage Project Risk;
PA15 - Monitor and Control Technical Effort;
PA16 - Plan Technical Effort;
PA17 - Define Organization's Systems Engineering Process;
PA18 - Improve Organization's Systems Engineering Process;
PA19 - Manage Product Line Evolution;
PA20 - Manage Systems Engineering Support Environment;
PA21 - Provide Ongoing Skills and Knowledge; and
PA22 - Coordinate with Suppliers.

Maturity-levels

Bijna geheel in lijn met CMM kent de ISO 21827 vijf (5) niveaus van volwassenheid (Maturity-levels). Formeel kent SSE-CMM nog een extra level te weten Level 0 (Not Performed), echter dit wordt verder niet gebruikt.

Het model bevat de generieke processen, (dat wil zeggen, de processen die van toepassing zijn op alle Maturity-levels). Deze generieke processen zijn gegroepeerd op basis van gemeenschappelijk kenmerk en vaardigheidsniveau welke van toepassing op alle levels.

Level 1 - Performed Informally: is het laagste niveau ('initial', geen proces gedefinieerd, de organisatie werkt ad hoc).

Level 2 - Planned and Tracked: dit level focust zich op projectdefinities, planning, en performance-issues. Kortweg een aantal basiszaken zijn geregeld, per project (dwz. nog niet per se uniform voor de hele organisatie). Hierbij moet worden gedacht aan de subprocessen:

- Planning Performance
- Disciplined Performance
- Verifying Performance
- Tracking Performance

Ronald Eygendaal is werkzaam als security consultant bij eygendaals services (www.eygendaals.nl) en is sinds 1990 actief in informatiebeveiliging, elektronische & technisch beveiliging, fraude detectie & bestrijding en bewaking & beveiliging in het bijzonder. Hij is bestuurslid bij de Vereniging Beveiligingsprofessionals Nederland (VBN)

Level 3 - Well Defined: er is een volledig beschreven proces (zowel de primaire software-ontwikkelprocessen, als de managementprocessen) voor de hele organisatie. Dit betreft aanvullende op de processen van level 2 de volgende subprocessen:
- **Defining a Standard Process**
- **Perform the Defined Process**
- **Coordinate Practices**

Level 4 - Quantitatively Controlled: statistische procesbeheersing is ingevoerd. Dit betreft aanvullende op de processen van levels 2 en 3 de volgende subprocessen:
- **Establishing Measurable Quality Goals**
- **Objectively Managing Performance**

Level 5 - Continuously Improving: processen en technologie worden continu verbeterd op basis van statistische procesbeheersing. Dit betreft aanvullende op de processen van levels 2 ,3 en 4 de volgende subprocessen:
- **Improving Organizational Capability**
- **Improving Process Effectiveness**

Maturity-level

Om het Maturity-level vast te stellen is SSAM (Systems Security Appraisal Method) ontwikkeld. Doel van SSAM is het verkrijgen van de baseline van de actuele situatie met betrekking tot beveiligingstechniek binnen de organisatie of project. Een ander doel van SSAM is het oprichten en/of ondersteunen van een momentum voor verbetering binnen meerdere niveaus van de organisatiestructuur.

SSAM is een onderzoeksproces met een aantal fasen, te weten planningsfase, een voorbereidingsfase, Onsite-fase en uiteindelijk een Post-evaluatie-fase. Het team dat SSAM uitvoert doet dit via de volgende stappen:
- Het verzamelen van informatie (tbv de vragenlijst)
- Voorlopige data-analyse aan te geven wat te zoeken/vragen
- Gegevens verzamelen en valideren met de betrokkenen
- Interviews met de betrokkenen
- Presenteren van de uiteindelijke data-analyse aan de sponsor

Uiteindelijk ontstaat er per proces een Maturity-level en ontstaat er een overall Maturity-level.

Historie

SSE-CMM vindt zijn historie bij de Amerikaanse defensie-industrie waar men op zoek was naar een methodiek om leveranciers te kunnen evalueren. Onder andere door sponsoring van de van de National Security Agency (NSA) is rond 1993 de eerste aanzet gemaakt voor het Systems Security Engineering Capability Maturity Model (SSE-CMM). Onder leiding van het Software Engineering Institute van de Carnegie Mellon University en een bedrijvencollectief, van 42 bedrijven, is SSE-CMM verder ontwikkeld. SSE-CMM vindt zijn oorsprong uit Capability Maturity Model (CMM) en verzorgt een internationaal framework voor evalueren van beveiliging, techniek en middelen. Verder omvat het een methodiek voor het meten van prestaties en het verbeteren van diensten om vitale informatie te beschermen.

In 1996 heeft de eerste officiële versie (v1.0) van het Systems Security Engineering Capability Maturity Model het levenslicht gezien. In 1999 kwam versie 2 en in 2002 heeft de International Standards Organization (ISO) versie 3 van SSE-CMM gepubliceerd als de ISO/IEC 21827 Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM).

In 2004 heeft de International Systems Security Engineering Association (ISSEA) het proces ingeregeld om te komen tot een Appraiser Certification Body conform de ISO/IEC 17024, General Requirements For Bodies Operating Certification Schemes For Persons. Daarmee ontstond de mogelijkheid voor certificering van personen en organisaties tegen de ISO/IEC 21827.
In 2008 heeft er een update van de standaard plaatsgevonden, het is daarmee naast de bekende ISO/IEC 2700X, een mondiaal gedragen industriestandaard geworden.

Conclusie

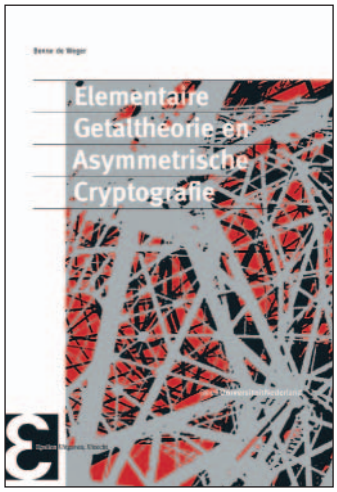
In de praktijk zien we dat ISO 21827 in America, Azië en delen van West-Europa wordt toegepast als procescertificering. Het gaat hier veelal om leveranciers van beveiligingsdiensten, ontwikkelaars van beveiligingsproducten en secure-system-developers/-integrators die dit ten behoeve van het certificeren van softwareontwikkelprocessen toepassen. Mondiaal opererende certificatie-instellingen zoals de ICS Group en Eurotech certificeren bedrijven tegen de ISO/IEC 21827. Bedrijven kunnen tegen verschillende volwassenheidsniveaus worden gecertificeerd, zo is bijvoorbeeld de India's softwarebouwer SRIT gecertificeerd op SSE-CMM Level 5 certified en Tech Mahindra op level 3.

Daarnaast gaat de ISO 21827 een steeds prominentere rol spellen bij het bepalen van de volwassenheid van zowel bestaande information-security-management-systemen als van bestaande Business Continuity Management Systemen. De ISO 21827 wordt steeds belangrijke bij softwareontwikkeling en Maturity-levelvaststelling.

Links

http://www.pqm-online.com/assets/files/standards/iso-iec_21827-2002.pdf
http://www.renaissance-it.com/corporate_factfile.php
http://www.csc.com/ca_en/offerings/54254/54277-security
http://www.cs2consulting.com/about/
http://www.mahindra.com/What-We-Do/Information-Technology/Companies/Tech-Mahindra

"ELEMENTARY, MY DEAR WATSON!"



Soms leer je iets pas waarderen wanneer je het nodig hebt. Ik had 'Elementaire Getaltheorie en Asymmetrische Cryptografie' van mijn oud-collega Benne de Weger al jaren in de kast staan, toen ik zelf deze stof moest gaan behandelen in een college. Ik dacht er niet meteen aan, het was het vierde boek op dit vlak wat ik pakte. Het was de eerste waar ik voor mijn gevoel geen moeite hoefde te doen om het te begrijpen, anders dan gewoon volgen wat er stond.

Benne schrijft zelf in zijn voorwoord: 'De focus van dit boek ligt op de wiskunde, met name de getaltheorie: het boek wil laten zien hoe het begrip van getaltheorie essentieel is voor het begrijpen en goed kunnen gebruiken van asymmetrische cryptografie.'

En dat maakt het boek waar. Daarnaast maakt Benne ook nog een modulaire en cryptografische rekenmachine beschikbaar, MCR [1]. Een krachtige specialistische rekenmachine, geschreven in Java. Ik heb andere boeken bekeken die cryptografie trachten uit te leggen, maar de meesten lijken de berekeningen juist complexer te maken dan te versimpelen. Iets wat Benne wél doet. Je voelt gewoon dat Benne zich dit rekenwerk helemaal eigen gemaakt heeft.

Heel rustig legt Benne modulair rekenen uit, priemgetallen, ontbinden in factoren. En dit alles met goed te volgen voorbeelden, die na te rekenen zijn. Benne's uitleg van modulaire inversen en hoe deze te berekenen met het uitgebreide algoritme van Euclides kan bijna niet duidelijker. En hetzelfde geldt voor de phi-functie van Euler.

Titel: Elementaire Getaltheorie en Asymmetrische Cryptografie
Auteur: Benne de Weger
ISBN: 978-90-5041-108-0
Omvang: 192 pagina's
1e druk: 2009
2e druk: 2011

Op dit alles wordt doorgebouwd, totdat je RSA en Diffie-Hellman zelf helemaal stap voor stap begrijpt en kunt narekenen.

In het boek zijn opgaven opgenomen, met uitgebreide uitwerkingen achterin. En met uitgebreid bedoel ik ook echt uitgebreid. Ruim dertig pagina's uitwerkingen telt het boek.

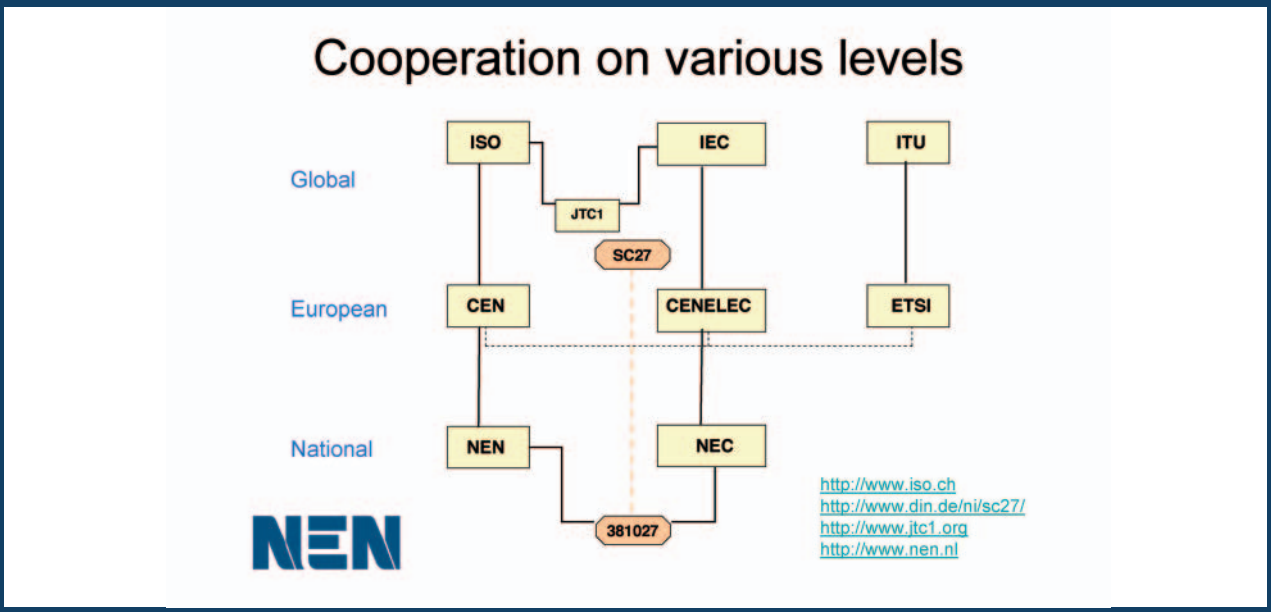
Natuurlijk is een leerboek als dit geen spannend jongensboek, wat je gemakkelijk van voor tot achter wegleest. Maar Benne maakt de wiskunde achter ingewikkelde cryptografie wel zo inzichtelijk als het maar kan. Het maakt dat je eigenlijk maar al te graag ook een boek ziet komen met zijn uitleg over symmetrische cryptografie en hashes.

Heb je een noodzaak om asymmetrische cryptografie en de berekeningen die er achter schuilgaan te begrijpen, dan is dit het boek dat je wilt lezen.

Links
[1] MCR - http://www.win.tue.nl/~bdeweger/MCR/

Door Lex Borger, hoofdredacteur Informatiebeveiliging, security consultant bij i-to-i en docent security aan de Hogeschool Utrecht. Lex is te bereiken via l.borger@i-to-i.nl

LAWRENCE D. EICHER PRIJS VOOR SUBCOMMISSIE SC27



Op 17 september, tijdens de algemene bijeenkomst van ISO in Seoul heeft de subcommissie SC27 de Lawrence D. Eicher-prijs gekregen voor het uitstekende werk dat de subcommissie verricht heeft. De prijs wordt uitgereikt aan ISO-commissies die groot leiderschap getoond hebben, innovatieve aanpakken gebruikt hebben en de deelname van ontwikkelingslanden bevorderen.

Subcommissie SC27, of ISO/IEC JTC1/SC27 zoals de commissie officieel heet, heeft als werkgebied "IT Security Techniques". JTC1 is de overkoepelende commissie van SC27, formeel de Joint Technology Committee 1 "Information Technology".

SC27 is 25 jaar geleden opgericht en verdeelt haar werk onder in vijf werkgroepen (zie figuur 1):

- WG1: IT management systems
- WG2: Cryptography
- WG3: Security evaluation
- WG4: Security controls and services (opgericht in 2006)
- WG5: Identity management and privacy solutions (opgericht in 2006)

SC27 heeft belangrijke internationale standaarden opgeleverd, de meest bekende zijn:

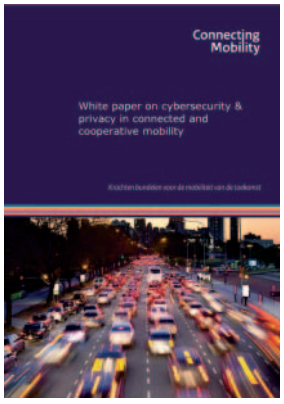
- ISO/IEC 27001 en ISO/IEC 27002, twee welbekende werken in het vakgebied van informatiebeveiliging;
- ISO/IEC 15408 series, de 'Common Criteria';
- ISO/IEC 24760 series, een raamwerk voor identiteitsbeheer;
- ISO/IEC 29100, een privacy raamwerk;
- ISO/IEC 29192 series, lichtgewicht cryptografie.

Verder heeft ISO de inzet van de experts in SC27 genoemd en hun banden met het bedrijfsleven. Dit betrekt bedrijven bij standaardisatie en geeft terugkoppeling over de noodzaak van standaarden. SC27 heeft een grote internationale aanwezigheid, met leden in 71 landen. De subcommissie bestaat al 25 jaar, waarin er veel werk is verzet. Hieruit blijkt de globale behoefte aan IT-beveiligingsoplossingen. In Nederland is SC27 ook vertegenwoordigd, via het NEN (zie figuur 2), onder voorzitterschap van Piet Donga.

De redactie feliciteert alle commissieleden van SC27 met deze prijs, in het speciaal de Nederlandse leden. Door hun inzet blijft Nederland betrokken bij de standaardisatie van informatiebeveiliging, die begon met een Brits/Nederlandse standaard: de BS7799/NEN 'Code voor Informatiebeveiliging'.

SLIMME AUTO'S BRENGEN ZORGEN EN KANSEN

Op 27 november vorig jaar is een workshop gehouden die de basis heeft gelegd voor een whitepaper "Cyber security & Privacy in connected and cooperative mobility" [1].



Een groep van materiedeskundigen, security en privacy specialisten uit Nederland heeft in een interactieve workshop uit een grote hoeveelheid bronmateriaal, waaronder internationale studies en andere relevante documenten, de relevante issues voor security en privacy geïdentificeerd. De workshop stond onder leiding van TNO. De lijst van deelnemers is een who's who lijst van security en privacy deskundigen vanuit de overheid, universiteiten en bedrijfsleven. Dit whitepaper is een vertrekpunt voor het verder vormgeven van security en privacy in dit sterk in ontwikkeling zijnde domein.

De onderwerpen die in deze whitepaper aan de orde komen zijn:

- Veilige ontwikkeling van software componenten
- Een certificatieaanpak en -schema om met verschillende beveiligingsniveaus te kunnen werken
- Veilige communicatie met een PKI oplossing
- De noodzaak voor interoperabiliteit
- Het eigendom, gebruik en de rechten van de eigenaar en de gebruiker

In het whitepaper wordt verder gekeken naar de complexiteit, communicatietechnieken en beveiligingsuitdagingen. Mogelijke oplossingen worden genoemd en er worden aanbevelingen gedaan voor nader onderzoek.

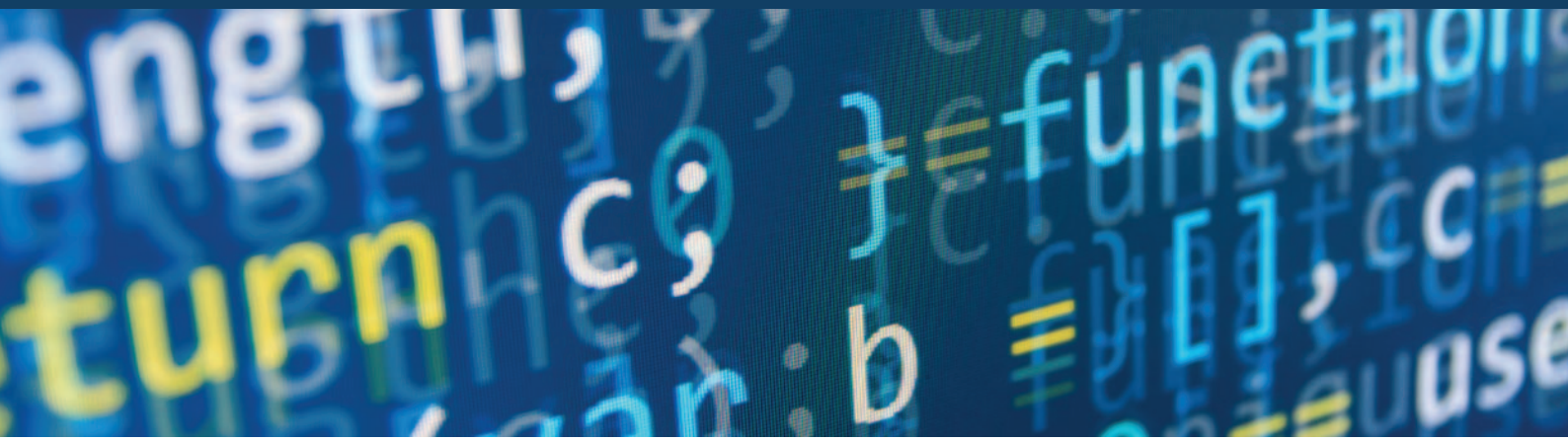
Met name wordt er gekeken naar C-ITS (Cooperative Intelligent Transport Systems), ook wel V2X genoemd, als samenvoeging van V2V (vehicle-to-vehicle) en V2I (vehicle-to-infrastructure). Veiligheid op de weg wordt hiermee gediend, om dit op grote schaal te implementeren is het aan te bevelen de issues uit het whitepaper door te nemen.

Links

[1] Whitepaper:
http://www.connectingmobility.nl/thema_s/security+and+privacy/documenten+security+and+privacy/326242.aspx

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



LIGT DE FOUT BIJ APPLE... OF BIJ DE ONTWIKKELAARS?

Als je als ontwikkelaar snel een iOS App wilt bouwen, kun je niet om de XCode-development-kit van Apple heen. Deze kit kun je downloaden vanaf de site van Apple. Maar wat gebeurt er als kwaadwillenden een kopie van de software over internet verspreiden en van malware voorzien? En wat als deze malware zich ook automatisch verspreidt over alle apps die met de geïnfecteerde development-kit worden gebouwd? Apple kreeg er in september mee te maken en moest alle zeilen bijzetten om kwaadaardige apps uit de store te verwijderen en gebruikers te waarschuwen. Maar hoe ga je hier als bedrijf mee om? Kun je gebruikers zelf nog wel veilig apps laten installeren op mobiele apparaten die bedrijfsgegevens bevatten? Had Apple hier iets tegen kunnen doen? Of ligt de fout hier volledig bij de ontwikkelaars? Hieronder de mening van onze redacteuren.

Maarten Hartsuijker

De XCodeGhost-malware toont goed hoe afhankelijk je als afnemer bent van de beveiligingsmaatregelen die de gehele keten achter een toepassing neemt. En hoe handig aanvallers zijn geworden in het verstoppen van malware in door ons vertrouwde kanalen.

Als we kijken naar waarom XCodeGhost zo succesvol was, dan zien we dat de factor gemak een grote rol speelt. De officiële Xcode-ontwikkelsoftware wordt centraal gedistribueerd. Hierdoor was de software in sommige delen van de wereld niet optimaal toegankelijk. De aanvallers sprongen in dit gat tussen vraag en aanbod en boden een geïnfecteerde kopie aan die (bijvoorbeeld in China) wel makkelijk en snel gedownload kon worden. Informatiebeveiligers zien ditzelfde gedrag dagelijks binnen hun gebruikerspopulatie. Daar waar in de IT-infrastructuur vereiste functionaliteit wordt geblokkeerd, zullen veel gebruikers een nog onveiliger omweg vinden. Faciliterend beveiligen is dan erg belangrijk en je ziet dat Apple dat hier ook doet. Na dit incident startte Apple een XCode-mirror in China zodat Chinese ontwikkelaars makkelijker aan officiële software kunnen komen. Wat betekende dit lek voor gebruikers van Apple software? Voor veel gebruikers in Nederland zijn de gevolgen van het lek beperkt. Veel geïnfecteerde apps richtte zich op de Chinese markt. Maar een aantal ervan, zoals WeChat, wordt breder gebruikt. Heb je als gebruiker zo'n app op je apparaat gehad? Dan kun je er van uitgaan dat de malware tot dezelfde


Ronald van Erven


Herman Thijssens


Maarten Hartsuijker

gegevens toegang heeft gehad als de app. Heb je de app toegang gegeven tot je foto's en contacten? Dan kon de malware deze ook kopiëren of muteren. Gelukkig maken de meeste mobiele platformen, inclusief iOS, gebruik van applicatie-isolatie. Dit betekent dat de malware niet zomaar je hele apparaat infecteert of per definitie lastig te verwijderen valt. Het zal altijd van andere kwetsbaarheden gebruik moeten maken om zich dieper in je apparaat te nestelen. Updaten of verwijderen van de app is voor malware als deze daarom vaak voldoende. Niettemin is het voor velen een goede wake-up-call. Instrueer als bedrijf altijd je ontwikkelaars om software van betrouwbare bedrijven te gebruiken. En leg deze instructie ook neer bij derden die voor jou apps ontwikkelen. Indien je zeer vertrouwelijke gegevens op mobiele apparaten verwerkt dan is het net als op normale werkplekken verstandig om de volledige regie over de software op het apparaat over te nemen. Dat vraagt om een zeer goed verhaal en een grondige risicoafweging, want in bedrijfsomgevingen met bring-your-own's en gebruikers die wennen aan steeds meer vrijheid zal je hier als beveiliger helaas weinig begrip mee oogsten.

Ronald van Erven

We leven in een bijzondere tijd. Steeds meer mensen zijn digibeet af en hebben soms meer kennis van ICT dan de in-house ICT-afdeling en modernere apparatuur privé dan op het werk. Daarnaast leven we in een technologiemaatschappij. De technologieën brengen de veranderingen en uiteindelijk efficiencies.

Ook heb je te maken met de "snelle" dames en heren die snel een prototype app in elkaar zetten om hun werk te doen of hun management te overtuigen van de nut en noodzaak voor bepaalde business rules. Mensen wachten gewoonweg niet meer op de ICT-afdeling die na vergadersessies en taskforces met fraaie planningen en architecturen komen en na maanden een prototype hebben.

Deze praktijken ontmoedigen of "alles dicht zetten" is bij veel bedrijven ook geen optie. Naast dat mensen altijd creatief zullen zijn en oplossingen zullen vinden krijgt het bedrijf te maken met onvoldoende jonge en creatieve aanwas in het personeelsbestand.

Dus aan de ontwikkelaarkant moet je het bewustzijnniveau over veilig apps bouwen verhogen. Niet alleen over het bouwen van veilige apps maar ook hen bewustmaken over bedrijfsinformatie en dataclassificatie. Deze laatste is iets wat bedrijfsbreed moet gebeuren. Zodra je het awareness-niveau omhoog hebt, dan hen helpen met technologieën om zaken af te dwingen en te stroomlijnen. Houd de administratieve organisatie zo licht mogelijk. Kortom - "you cannot beat them - so manage them"

Voor mensen in een ISO-rol zijn dit mooie tijden. Je moet bijna realtime mee gaan en on-the-spot je beveiliging inbouwen met dataclassificatie met beheersing in het achterhoofd.

Herman Thijssens (gastbijdrage)

Het is een taak van de ontwikkelaar om officiële software vanuit officiële bronnen te gebruiken voor het ontwikkelen van apps. Dat een onofficiële Xcode gebruikt zou worden om officiële gecertificeerde apps te publiceren in de appstore van Apple had daarentegen ook niemand verwacht. Het is wel enigszins vreemd te noemen dat bijvoorbeeld de ontwikkelaar van WeChat onofficiële Xcode gedownload heeft van de cloudfilesharing-dienst Baidu om een app te bouwen die miljoenen keren is gedownload is. Dit roept wel de vraag op of er van deze ontwikkelaars ook certificaten gelekt zouden kunnen zijn waarmee kwaadwillenden nu apps namens deze ontwikkelaars kunnen submitten. Maar dat is een vraag voor een andere keer. Ik kan bijna met zekerheid zeggen dat bijna elke organisatie met iOS-devices door minimaal één van deze, met malware besmette, apps geraakt is. In veel gevallen zelfs meerdere apps. Voor bedrijven is het altijd de keuze tussen maximale beveiliging en maximale gebruikersvrijheid. In een field service markt waarbij iPads met supervisie worden uitgerold (bij voorkeur via het Device Enrollment Program van Apple, DEP) kan exact bepaald worden welke apps en welke bedrijfsinformatie op deze iPads staat. Gebruikers kunnen zelf dan ook geen apps installeren, alles loopt dan via de EMM/MDM-oplossing. iOS 9 gaat daar nog verder in en schroeft de beveiliging nog meer op. Organisaties waarin mensen meer zeggenschap hebben over wat er op hun eigen device gebeurt hebben deze mogelijkheid niet. Met een EMM-oplossing kan wel inzicht worden verkregen in welke apps een gebruiker geïnstalleerd heeft staan op zijn of haar device en met een gekoppelde anti-malware-oplossing kan hier vervolgens een eventueel geautomatiseerde actie op worden doorgevoerd. Anti-malware voor mobiele devices is relatief nieuw en deze markt is zich razendsnel aan het ontwikkelen, een paar mogelijke kampioenen zijn reeds aan het opstaan. De gebeurtenissen van de laatste tijd met StageFright, XcodeGhost en Masque-attack-vulnerabilities laten wel zien dat het tijd wordt malware op mobile devices serieus te gaan nemen. In een tijdbestek van twee maanden zijn bijna alle populaire devices vatbaar geweest voor malware.

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

MAG IK UW CREDITCARDNUMMER?

In deze rubriek heb ik vaak gesproken over het apparaat dat je overal tegenkomt, wachtend op de trein, fietsend, autorijdend et cetera. Inderdaad, een aantal jaren geleden werd de mobiele telefoon alleen nog maar gebruikt om te bellen en sms'en. Tegenwoordig worden de telefoons daar bijna niet meer voor gebruikt. Degene die mijn rubriek vaker lezen zal het wellicht opgevallen zijn dat ik zowel op het gebied van laptops, PC's, tablets en telefoons eigenlijk altijd voor Apple kies. Die keus wordt eigenlijk alleen maar bevestigd wanneer ik de kranten kritisch lees.

Voor lezers die onbekend zijn op de telefoniemarkt: er bestaat een groot aantal besturingssystemen, maar als je alleen de besturingssystemen telt met een marktaandeel groter dan tien percent blijven er maar twee over: Android en iOS, oftewel Google en Apple. Er is een verschil: Er zijn momenteel duizend verschillende Android-toestelleveranciers, maar een iPhone kun je alleen kopen bij Apple. Er zijn momenteel 24 duizend verschillende Android-toestellen. Apple produceerde minder dan 10 verschillende soorten iPhones. Er zijn 9 versies van Android, waar iedere leverancier weer modificaties op aanbrengt om zich te onderscheiden van anderen. Apple heeft één variant van het besturingssysteem. De nieuwste versie van Android staat op nog geen procent van de toestellen. Op negen procent van de toestellen draait Android 5 en op negentig procent van de toestellen draait een nog oudere software. Aan de andere kant, negentig procent van alle iPhones draait op de nieuwste versie van iOS.

Deze zomer werd de stagefright-hack bekend. Vijfennegentig procent van alle Android toestellen (ongeveer één miljard toestellen) is kwetsbaar en heeft dus een aanpassing nodig. Door de diversiteit van besturingssystemen is er geen eenduidige uitleg te geven hoe de gebruiker het probleem kan verkleinen en is het maar de vraag of de verschillende leveranciers het probleem gaan oplossen. Het probleem is eigenlijk heel beperkt: de hack maakt misbruik van de standaardinstelling in Android om MMS-berichten automatisch af te spelen. De gebruiker hoeft daar geen opdracht voor te geven, het toestel doet dat zelf. Het gevolg van een besmetting met stagefright kan zijn dat je privégegevens van je telefoon gehaald worden, zoals foto's, berichten of creditcardgegevens, of dat alle contacten op je telefoon een MMS-bericht krijgen met het virus erin.

Natuurlijk kunnen er ook lekken in iOS zitten, maar het dichten van deze gaten is veel eenvoudiger omdat Apple de updates direct zelf kan uitrollen. Iedere gebruiker van iOS ziet op zijn telefoon dat er een update is en kan lezen waarom deze geïnstalleerd moet worden. Gezien de eerder genoemde cijfers is Apple wel in staat de gebruikers van iOS te bereiken.

Persoonlijk maakt het mij niet uit welke telefoon je gebruikt, je moet gewoon het toestel nemen dat je het meest plezierig vindt. Persoonlijk maakt het mij wel uit wie mijn creditcard gebruikt, misbruik daarvan vind ik niet zo plezierig.

Berry

PRIVACY THE NEXT BIG THING!

De Security Academy presenteert een tweetal geheel nieuwe privacy opleidingen die zowel de nieuwe Europesche als de nationalte wet- & regelgeving behandelen. Beide opleidingen worden in 2016 door het EXIN geaccrediteerd en geëxamnineerd. U heeft hiermee dus een onafhankelijke, internationaal erkende certificering op zak.

Privacy Foundation

Maak in drie dagen grondig kennis met de Nederlandse en Europese wet- en regelgeving op het gebied van privacy.

Deze cursus is uniek omdat er een voor "gewone" medewerkers (lees anderen dan juristen) begrijpelijke en praktische vertaling wordt gegeven van de relevante wet- en regelgeving. Aan de hand van veel praktijkvoorbeelden vergaart u voldoende kennis en inzicht om adviezen te kunnen geven over privacyvraagstukken binnen uw organisatie. Na deze cursus kunt u als gesprekspartner optreden voor de diverse (management)lagen binnen uw organisatie en voor derden buiten uw organisatie.

Er gelden geen specifieke toelatingseisen om deel te kunnen nemen aan de cursus Privacy Foundation. Na voltooiing van de cursus bent u klaar om deel te nemen aan het examen "Privacy Foundation" van EXIN. EXIN verwacht dit examen begin 2016 aan te gaan bieden.

Prijs: € 1.950,- exclusief BTW

Privacy Advanced

Deze cursus is een vervolg op de Privacy Foundation cursus. In deze drie daagse cursus wordt ingegaan op de zaken die binnen uw organisatie geregeld dienen te worden om aan de eisen die het College stelt te voldoen.

Deze cursus is bedoeld voor iedereen die in zijn werk verantwoordelijk is voor de inrichting, aansturing of controle van de manier waarop met persoonsgegevens wordt omgegaan. U leert daadwerkelijk de pricvacywetgeving te implementeren binnen uw organisatie.

Om optimaal rendement uit deze cursus te kunnen halen wordt aangeraden dat u eerst deel hebt genomen aan de cursus "Privacy Foundation". Indien u al beschikt over een gedegen kennis van de relevante wet- en regelgeving op het gebied van privacy is dat ook voldoende.

Prijs: € 1.950,- exclusief BTW

BEL ONS +31(0)348-408061

WWW.SECURITYACADEMY.NL
INFO@SECURITYACADEMY.NL