iB
INFORMATIEBEVEILIGING
Jaargang 14 - 2014
#4

CYBEREDUCATIE

Heartbleed

Cyber Security Academy

INTERVIEW: John McClurg (Dell)

IT en Cars

Kwalificatiestelsel op basis van e-CF



INLICHTINGEN DIENSTEN | SPIONAGE | PRIVACY

17 juni 2014 | De Reehorst in Ede

Black Hat Sessions XII

Op 17 juni 2014 organiseert Madison Gurkha alweer de twaalfde editie van de inmiddels befaamde Black Hat Sessions. Het thema van deze editie van het jaarlijkse event van Madison Gurkha luidt: ***Inlichtingendiensten***, ***Spionage*** en ***Privacy***. Achter die begrippen gaat een complexe wereld schuil.

Zowel voor techneuten als niet-techneuten belooft het een interessante dag te worden! En natuurlijk ook een uitgelezen kans om met vakgenoten van gedachten te wisselen over deze onderwerpen.

SPREKERS

keynote

Marietje Schaake
Europarlementariër voor D66, in de 'Alliance of Liberals and Democrats for Europe' (ALDE). @MarietjeSchaake

keynote

Wilma van Dijk
Met ingang van 1 juni 2014 nieuwe directeur Cyber Security bij de Nationaal Coördinator Terrorisme-bestrijding en Veiligheid (NCTV)

Wolter Pieters
Wetenschappelijk coördinator van het Europese project TREsPASS

Sandro Etalle
CEO SecurityMatters, Professor aan de TU Eindhoven & Universiteit Twente

Ot van Daalen
Oprichter Digital Defence en oud-directeur Bits of Freedom

Wouter Lueks
Promovendus aan de Radboud Universiteit Nijmegen

Arthur Donkers
Directeur en principal security consultant bij ITSX

Sander Degen
Security consultant bij TNO ICT

Frans-Paul van der Putten
Senior onderzoeker aan het Instituut Clingendael

Job de Haas
Principal security analyst bij Riscure

Voor leden van het PvIB geldt een aantrekkelijke korting van 10%. Geef bij uw aanmelding de code BHS14-PvIB op en de korting wordt direct verrekend. Meer informatie over het congres, de geldende groepskortingen en het inschrijfformulier vindt u op www.blackhatsessions.com.

SPONSORS

COMPUTABLE | kahuna managing security | WeSecure | paloalto NETWORKS | TSTC | @ at computing | SCOS TRAINING WIRESHARK | qict | ITSX

KENNISPARTNERS

ISACA Netherlands Chapter | NOREA | PvIB Platform voor InformatieBeveiliging | Ngi Platform voor IT-professionals | CIP

ORGANISATIE

Madison Gurkha
Your Security is Our Business

www.blackhatsessions.com

BROWSER AFHANKELIJKHEID

Internet Explorer had zijn eerste post-Windows XP zero-day[1]. Dit was het moment waar de hele beveiligingswereld op zat te wachten, want hiermee zou de eerste permanent blijvende kritieke kwetsbaarheid op Windows XP ontstaan - voor particuliere gebruikers, die geen patches meer krijgen. Microsoft heeft dit probleem onderkend en heeft wél een patch beschikbaar gemaakt.
Voordat de patch beschikbaar was, heb ik wat discussies mogen meemaken bij bedrijven die worstelden met de aanpak van de kwetsbaarheid. Wat mij in deze discussies verbaasde was dat we zo afhankelijk zijn van één merk browser en dan nog vaak ook één versie. Kennelijk zijn er een heleboel webapplicaties gebouwd die alleen werken op, bijvoorbeeld, Internet Explorer 6. Tevens lees ik als lezersreactie op security-sites dat 'het antwoord' is om naar [Google Chrome | Firefox | Opera] over te stappen. Alsof deze browsers geen last hebben van enig zero-day probleem.
Als ik dan hoor dat er leveranciers zijn die met droge ogen een webapplicatie opleveren die alleen op IE6 werkt 'omdat de klant hier om gevraagd heeft', zijn de grenzen van mijn inleving overschreden. Zelfs als een klant bij de opdracht aangeeft dat iets moet werken op IE6, wil dat niet zeggen dat hier een keiharde beperking ingebouwd moet worden. In mijn ogen zou hier sprake moeten zijn van zorgplicht bij de leverancier.
Maar ik wil verder gaan: in een tijd van ver-cloud-ing van diensten zou het juist een harde eis moeten zijn dat webstandaarden gebruikt worden op een manier die zonder poespas functionaliteit draait op alle gebruikelijke browserplatformen. Als de webapplicatie er daardoor wat minder sexy uitziet, moeten we dat maar op de koop toe nemen. Houd ook de poespas om verschillende cliëntvormen te herkennen en ondersteunen functioneel. Ik kan begrijpen dat een smartphone-versie van de site er soms anders uit moet zien dan de 'gewone' versie, maar schiet niet door. Richt je juist op een ontwerp dat dynamisch schaalt op basis van het vensterformaat.
Uiteindelijk wordt het hier allemaal simpeler door, en toepassing van het KISS (keep it simple, stupid) principe maakt het ook veiliger. We moeten onze intelligentie gebruiken om het product zo te maken dat het domweg eenvoudig in te zetten en te onderhouden is. In de cloud-wereld geldt dit meer dan ooit.

Lex Borger, hoofdredacteur

Links

[1] https://technet.microsoft.com/en-us/library/security/2963983

In dit nummer

HEARTBLEED: DE LESSEN VAN EEN GEBROKEN HART

Heartbleed: een poëtische naam voor een ernstige kwetsbaarheid. De programmeerfout in OpenSSL heeft de gemoederen flink beziggehouden, binnen én buiten(1) de vakmedia. Inmiddels zijn servers gepatcht, certificaten vervangen en betrokkenen geïnformeerd. Maar nu? Gaan kwetsbaarheden als Heartbleed vanaf nu 'business-as-usual' zijn of valt er iets aan te doen? Een terugblik én vooruitblik vanuit het Nationaal Cyber Security Centrum.

Fotografie: Aad Hoogendoorn

Pieter Rogaar werkt als senior adviseur bij het Nationaal Cyber Security Centrum. Hij is de auteur van het factsheet over Heartbleed. Zijn specialisme is cryptografie, en hij heeft een grote interesse in privacy en IT-recht. Als adviseur schrijft hij kennisproducten zoals factsheets, whitepapers en het Cybersecuritybeeld Nederland. Pieter drukt graag op knoppen zonder label, hij is politiek actief en praat veel en vaak over de toekomst van het internet.

Heartbleed in het kort

Op 7 april werd de informatiebeveiligingsgemeenschap opgeschrikt door de onthulling van Heartbleed(2), een ernstige kwetsbaarheid in OpenSSL die al twee jaar in deze software zat. Deze kwetsbaarheid stelt aanvallers in staat om op afstand het interne geheugen van een kwetsbaar systeem uit te lezen. In dit interne geheugen staat allerlei informatie: geheime sleutels van certificaten, wachtwoorden, klantgegevens, broncode van webapplicaties etc. Met behulp van de achterhaalde informatie kan een aanvaller meerdere typen aanvallen uitvoeren. Met een wachtwoord kan hij systemen binnendringen. Met geheime sleutels van certificaten kan hij beveiligde verbindingen openbreken. Met klantgegevens is van alles mogelijk: identiteitsfraude, creditcardfraude of het versturen van spam.

Twee derde van het web draait OpenSSL

OpenSSL is opensourcesoftware het is de populairste programmeerbibliotheek voor het opzetten van beveiligde verbindingen op basis van het SSL/TLS-protocol. Veel andere software gebruikt OpenSSL: Linux-distributies, Android, webservers en firmware van netwerkapparatuur. Tweederde van de actieve websites gebruikte in april 2014 webserversoftware die op OpenSSL steunt(3).

Updaten en zoeken naar mogelijk gelekte gegevens

Het verhelpen van de Heartbleed-kwetsbaarheid bestaat uit het updaten naar een niet-kwetsbare versie van OpenSSL. Daarna begint het opruimwerk: alle mogelijk gecompromitteerde geheime waarden (wachtwoorden en geheime sleutels van certificaten) moeten worden vervangen. Gaat het om klantwachtwoorden, dan moeten ook klanten op de hoogte worden gesteld om hun wachtwoord te veranderen.

Respons: wat weten we eigenlijk wél zeker?

Al snel besloten we bij het NCSC om niet alleen een advisory(4) maar ook een factsheet(5) over Heartbleed te schrijven. Een advisory is een technisch beveiligingsadvies, een factsheet biedt meer achtergrond. We kozen voor een factsheet vanwege de ernst van Heartbleed, de complexiteit van mitigatiemaatregelen en de verwachte aandacht voor de kwetsbaarheid binnen en buiten de informatiebeveiligings-gemeenschap. Er zou, kort gezegd, veel behoefte zijn aan informatie over Heartbleed Informatiebeveiligers gingen op 8 april massaal op zoek naar OpenSSL-installaties binnen hun organisatie. Deze bleken overal te zitten: Linux-servers, Linux-werkstations en Android-smartphones waren belangrijke kandidaten. En dan stonden daar nog die appliances en netwerkapparatuur. Mogelijk gebruikten die ook OpenSSL, maar wie wist dat eigenlijk zeker? En konden die wel zomaar geüpgraded worden? Ironisch genoeg bezorgden op de dag dat Windows XP end-of-life werd, juist de Linux-systemen hun beheerders de grootste kopzorgen.

Was het de NSA?

Ook kwam al snel de geruchtenmachine op gang: had de NSA al twee jaar over deze kwetsbaarheid geweten en deze ook actief misbruikt? Hadden ze deze misschien wel zelf toegevoegd aan de OpenSSL-code? Hoewel er voor dit alles geen aanwijzingen zijn, zorgde het er wel voor dat organisaties met dubbele energie aan het verhelpen sloegen.

Wat een gedoe zeg, dat verhelpen!

Bij het NCSC zijn we die dagen veel gemaild en gebeld om advies. Het vaakst vroegen mensen of het mogelijk was een Heartbleed-aanval uit serverlogs af te leiden. Het antwoord daarop is, helaas, 'nee'. Alleen door het bestuderen van netwerkverkeer is af te leiden dat een aanval plaatsvindt of plaats heeft gevonden. Alleen wie zijn netwerkverkeer langere tijd opslaat, kan achteraf dus vaststellen of hij is aangevallen. Omdat het zo lastig is een aanval vast te stellen, was de volgende vraag ook te verwachten: is het dan écht nodig om al onze certificaten en wachtwoorden te vervangen? Met andere woorden, hoe waarschijnlijk is zo'n aanval nou eigenlijk? Over de periode vóór 7 april valt weinig te zeggen, maar daarna was er geen twijfel meer mogelijk. Enthousiastelingen van over de hele wereld schreven hun eigen Heartbleed-scanner en gingen op zoek naar interessante doelwitten. Ongegeneerd publiceerde men inloggegevens van webdiensten als Yahoo om aan te tonen dat deze kwetsbaar waren voor Heartbleed.

En de gegevens van onze klanten?

De vraag die informatiebeveiligers het scherpst in twee kampen verdeelde, was die van de klantgegevens: moeten organisaties hun klanten instrueren hun wachtwoorden te veranderen, en hen misschien zelfs vertellen dat hun gegevens gelekt kunnen zijn? Elke organisatie heeft hierin haar eigen keuze gemaakt, op basis van het eigen risicoprofiel en de aard van de verwerkte gegevens. Een massale waarschuwing voor mogelijke identiteitsfraude paste niet bij de aard van de dreiging, zo vonden wij. Ook zou een dergelijke oproep mogelijk een paniekreactie oproepen.

Drie lessen van Heartbleed

Inmiddels is het stof rond Heartbleed weer gaan liggen en is het tijd voor reflectie. Stonden de gebeurtenissen rond Heartbleed op zich of zijn dit soort kwetsbaarheden de nieuwe 'business-as-usual'? Kunnen we als informatiebeveiligingsgemeenschap iets leren over de manier waarop we omgaan met software en hoe we reageren op het bekend worden van zulke kwetsbaarheden?

Les 1: Organisaties hebben nog steeds te weinig grip op welke software ze gebruiken

Weten welke software waar draait, is cruciaal voor een organisatie. De respons op Heartbleed toont dat opnieuw aan. Organisaties leggen dat – als het goed is – vast in een Configuration Management Database (CMDB). Ontdekt men dan een kwetsbaarheid als Heartbleed, dan hoeft men slechts op te zoeken in de CMDB waar de betrokken software (i.c. OpenSSL) zoal draait en het daar te verhelpen. De praktijk blijkt keer op keer complexer. Lang niet alle gebruikte software ligt vast in de CMDB: hoe zit het met firmware van apparaten? De gebruikte packages op een Linux-server? Programmeerbibliotheken die meegeleverd worden met de software die ze gebruikt? De software die op een appliance staat? En zijn er misschien apparaten die wel software draaien, maar helemaal niet in de CMDB staan? De les hieruit is tweeledig. Ten eerste: ja, organisaties moeten hun CMDB's netter bij gaan houden. Ze vormen de basis van ons informatiebeveiligingsbeleid. Ten tweede: het is niet realistisch te denken dat een CMDB compleet en perfect is. Actief zoeken naar kwetsbare software, bijvoorbeeld met een scanner, vormt een belangrijke aanvullende maatregel.

Les 2: De informatiebeveiligingsgemeenschap weet nauwelijks welke code kritiek is

Heartbleed ontstond door een programmeerfout in de heartbeat-functionaliteit van OpenSSL. Heartbeat is geen ingewikkelde functionaliteit: het is het SSL/TLS-equivalent van 'ping', het houdt de verbinding open als er verder geen verkeer is. Toch was het mogelijk dat deze kleine fout enorme impact had. Hadden er dan niet genoeg mensen naar de code gekeken? Waarschijnlijk niet, nee. Lang niet alle code is even kritiek voor de beveiliging van systemen(6). De meeste code heeft geen beveiligingsfunctie, of is niet bereikbaar voor aanvallers. Toch krijgt blijkbaar niet alle kritieke code de aandacht die hij verdient. Ja, als je de code voor AES-encryptie in OpenSSL probeert te wijzigen, zul je waarschijnlijk opgemerkt worden. Veel andere code krijgt dat soort aandacht niet, terwijl bijvoorbeeld programmeerbibliotheken als libcurl, libxml of libjpeg ook zeer bereikbaar voor aanvallers kunnen zijn. Het herkennen van zulke kritieke code en het erkennen van diens rol in de beveiliging van het internet, zijn belangrijke stappen in het verstevigen van de fundamenten van beveiliging.

Les 3: Donaties werken nu niet om opensourcesoftware te financieren

Zoals veel opensourcesoftware rekent ook OpenSSL op donaties. Met behulp van deze donaties kan worden gewerkt aan het verder ontwikkelen van deze software. Tot voor kort ontving OpenSSL zo'n US$ 2000 per jaar aan donaties(7). Daarnaast betaalden organisaties het OpenSSL-team nog zo'n miljoen dollar per jaar voor het uitvoeren van programmeerwerk, voornamelijk implementaties op maat voor deze organisaties. Met andere woorden, deze software vervult een belangrijke rol in het beveiligen van netwerken en het internet, maar ontvangt hiervoor nauwelijks financiering. Inmiddels hebben technologiebedrijven een paar ton aan extra donaties voor de komende drie jaar toegezegd(8), maar er is nog geen duurzame oplossing in zicht. Het open karakter en de vrije verkrijgbaarheid van de software maken het lastig om financiële bijdragen van bedrijven en overheden af te dwingen. Toch lijken zulke bijdragen nodig om de kwaliteit van de software op lange termijn te waarborgen.

En nu? Verder.

Heartbleed heeft de gemoederen flink beziggehouden. De kwetsbaarheid heeft een ongekende hoeveelheid aandacht gekregen in technische én niet-technische media. Hoe gaat de beveiligingsgemeenschap de komende tijd aan de slag? Op de vraag of kwetsbaarheden als Heartbleed 'business-as-usual' worden, heeft zij zelf invloed. Als ze het voor elkaar krijgt inderdaad te leren van de lessen van Heartbleed, kunnen we het internet en onze netwerken daadwerkelijk veiliger maken.

Bronvermelding

1. NOS over Heartbleed: http://nos.nl/artikel/633432-beveiligde-internetverbindingen-lek.html.
2. Zie https://www.openssl.org/news/secadv_20140407.txt voor de publieke aankondiging van de kwetsbaarheid. Zie http://heartbleed.com voor meer achtergronden.
3. Volgens de Netcraft Web Server Survey van april 2014 gebruikt ruim 66% van de actieve websites Apache of nginx: http://news.netcraft.com/archives/2014/04/02/april-2014-web-server-survey.html.
4. Ten tijde van schrijven was https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2014-0215+1.20+Zeer+ernstige+kwetsbaarheid+gevonden+in+OpenSSL.html de recentste versie van de Heartbleed-advisory.
5. Zie https://www.ncsc.nl/dienstverlening/expertise-advies/factsheets/factsheet-heartbleed-ernstige-kwetsbaarheid-in-openssl.html voor het NCSC-factsheet over Heartbleed.
6. Dit idee heb ik ontleend aan het blog van Dan Kaminsky: http://dankaminsky.com/2014/04/10/heartbleed/. Ik hoop dat hij het me niet kwalijk neemt dat ik een goed idee van hem leen.
7. Steve Marquess, voorzitter van de OpenSSL Foundation, heeft de situatie in een blog beschreven: http://veridicalsystems.com/blog/of-money-responsibility-and-pride/.
8. Bron: http://arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-finally-agree-to-fund-openssl/.

WAT NU ALS JE INEENS NIET MEER BESTAAT?

Stel dat je er ineens achter komt dat je voor de Nederlandse overheid "niet meer bestaat". Dat ze hoegenaamd niet weten waar je bent en dat je de status VZO (verhuisd zonder opgave) en het label geëmigreerd krijgt. Daar moet je dan natuurlijk wel per toeval achter komen, want als de overheid niet weet waar je bent en je dus niet meer bestaat, kunnen ze je natuurlijk ook niet vertellen dat je niet meer bestaat. Stel nu dat je helemaal niet geëmigreerd bent, maar dat je gewoon nog steeds in je oude vertrouwde stad woont, netjes belasting betaalt, je zorgpremies overmaakt en elke dag naar je Nederlandse baan gaat bij je Nederlandse werkgever. Met het label geëmigreerd ben je dan in een klap stateloos geworden. Want op die toffe buitenlandse locatie, aan een strand met palmbomen en wit zand, woon je immers ook niet…

Ineens stort de zorgverzekering ruim 370 euro terug op de bankrekening. Een telefoontje met de zorgverzekeraar verloopt als volgt: "Oh, maar dat is heel logisch hoor dat dat geld op uw rekening staat, u bestaat namelijk niet en dan mogen wij u niet verzekeren. Dat zijn de premiegelden die onterecht betaald zijn." Na een "maar hoe moet dat nu als ik een ongeluk krijg of medische zorg nodig heb?" en daarop een "tsja, dat is dan jammer, want voor die kosten draait u zelf op" en een verschrikt "maar het is niet mijn fout dat ik niet meer besta, waarom word ik dan nu gestraft?" is het tijd voor een bezoek aan de Gemeente. Na wat speurwerk blijkt dat een (digitaal) doorgegeven verhuizing tot twee keer toe niet is doorgevoerd. Dat de Gemeente nog wel een emailtje had gezonden, maar zo moet de ambtenaar toegeven "We weten dat bij gmail-adressen de email niet aankomt want die wordt automatisch als kwaadaardig aangezien". En dan ben je daardoor blijkbaar al maanden onvindbaar.

Het klinkt utopisch prachtig want ogenschijnlijk ben je ineens aan het wakende oog van Big Brother ontvallen. Vadertje staat kent mij niet! De ultieme vorm van privacy zogezegd. Bij nadere bestudering lijkt het toch echt minder leuk. Zo mag je wel belasting betalen, maar vervalt elk recht op toeslagen. Geen zorgverzekeraar wil je nog aanraken. Je werkt trouwens illegaal want een werkvergunning (sic!) heb je niet. Stemmen mag natuurlijk ook niet, je bent immers geen inwonende van Nederland. Jouw onbekende rekeningen van overheidswege stapelen zich op, want je bestaat niet en je bent klaarblijkelijk wel geld schuldig en je blijft maar niet betalen, maar een factuur en herinneringen daarvan ontvang je nooit. De deurwaarder draait zich inmiddels al warm om bij je aan te kloppen (hoe die jou gaat vinden is een raadsel).

Het overkwam mij. Ik, Privacy Officer, bestond niet meer. Het BRP (basisregistratie personen) gaf dat althans aan. Na veel pressie, persaandacht en interne lobby van lieve vrienden haalde de Gemeente binnen twee weken na ontdekking bakzeil en corrigeerde – met terugwerkende kracht – het BRP. Echter, nog steeds ben ik bezig met het opruimen van de puinhopen van mijn niet-bestaan. De Algemene Rekenkamer doet hier inmiddels onderzoek naar en ik hoop oprecht dat dit anderen in de toekomst bespaard mag blijven.

Mr. Rachel Marbus,
@rachelmarbus op Twitter

INTERVIEW:

AART JOCHEM & KAS CLARK

Wisseling van de wacht. Kas vervangt Aart als lid van de IB redactieraad.

Aart Jochem

Hoe ben je in security terecht gekomen?

Bij toeval: toen ik in 2000 bij mijn vorige werkgever Capgemini bezig was met een intern project voor een authenticatie/-autorisatiesysteem, vroeg de CIO mij een vacature voor security officer voor de Benelux in te vullen. Hij zocht iemand met diepgaande kennis van IT-security en dacht daarbij aan mij. Mijn eerste reactie was dat ik wist hoe je het woord schrijft, maar dat het daarmee ophield. Hij overtuigde me om toch tijdelijk, voor een paar maanden deze rol op me te nemen. Enkele maanden werden jaren, Benelux werd Noord Europa & Asia Pacific en later lid van de Group Security Board; een verslaving was compleet. In het begin heb ik veel voorstellen van collega's direct afgekeurd omdat ze niet voldeden aan de security policies van dat moment. Ik leerde toen al snel dat het niet realistisch was om op alles nee te zeggen. Ik zei dan liever 'ja, maar niet op deze manier' en probeerde met mensen mee te denken om hun project binnen de security richtlijnen toch uit te voeren. Op een gegeven moment begon mijn oude fascinatie voor de publieke sector weer te borrelen en heb ik een functie gezocht op het snijvlak van informatiebeveiliging en de publieke taak. Deze vond ik bij de net 5 jaar oud geworden GOVCERT.NL, nu het Nationaal Cyber Security Centrum.

Welke (grote) ontwikkelingen heb je meegemaakt?

In de bijna 9 jaar bij PvIB is de meest opvallende verandering die ik heb gezien de omslag van informatiebeveiliging naar cybersecurity. Eerst had een organisatie veel controle over hoe goed de data, meestal databases, beveiligd werden door middel van goede procedures, maatregelen en de controle op de uitvoering/implementatie hiervan. Nu is vooral externe component van belang en hoe alert en flexibel een organisatie hiermee omgaat. Je bent nu veel meer afhankelijk van meerdere partijen en niet meer van alleen je eigen organisatie als je het goed wilt doen. Informatie is overal en overal toegankelijk, dreigingen kunnen zich vandaag op morgen manifesteren, vertrouwde maatregelen blijken opeens geen veiligheid meer te bieden (zoals PKI na DigiNotar, of meer recent OpenSSL). De externe component maakt dat beveiligingsprofessionals zich soms moeten gedragen als cyberdiplomaten, zoals bij een responsible disclosure melding of wanneer de oplossingen van een probleem in handen van een ander ligt.

Wat waren/zijn de grootste uitdagingen?

De snelheid waarmee cyber (in)security zich ontwikkeld is zeer hoog. Voor een kleine elite is dit bij te houden, maar een grote groep mensen dreigt af te haken. De verhoudingen tussen publiek en privaat zullen ook gaan veranderen. Hopelijk op een harmonische wijze, in sommige landen zien we dat het wat moeilijker is en de overheid ingrijpt in internetvrijheden.

Wat is je visie? Oftewel, wat is het ideale internet en is het haalbaar?

Het internet zelf heeft ons een blik gegund op hoe 'grassroots' bewegingen en individuen een verschil kunnen uitmaken. Hoe een student in een paar jaar tijd miljarden kan verdienen en kennis razendsnel wereldwijd beschikbaar is. Maar ook hoe iemand aan de andere kant van de wereld een systeem kan hacken en een land of bedrijf op zijn grondvesten kan laten schudden. Het ideale internet geeft ruimte aan deze snelle ontwikkelingen, maar biedt in de basis bescherming voor de grondrechten van personen en kan iedereen erop rekenen dat cybercriminelen uiteindelijk tegen de lamp lopen. Over enkele jaren zit het internet letterlijk in onze haarvaten. Dan heb je dat nodig. Of het haalbaar is? Ik denk het wel. Maar daar moeten we wel keihard aan werken.

Welke trends/uitdagingen zie je aankomen in de komende 5-10-20 jaar?

De belangrijkste uitdaging is cyber security net zo volwassen te krijgen als veiligheid op andere vlakken (zoals brand, verkeersveiligheid of oorlogsdreiging). Dat is nog een zoektocht die net begonnen is. Het NCSC verricht pionierswerk (zelfs internationaal) als het gaat om de rol van overheid en private partijen, monitoring en snelle inschatting van risico's en dreigingen. De komende decennia zal internet en technologie de basis vormen van alle dienstverlening en logistiek in het fysieke domein. De mate waarin een land dit kan faciliteren of een organisatie erop kan inspelen zal bepalend zijn voor hun succes en groei.

Kas Clark

Hoe ben je in security terecht gekomen?

Pas op het einde van mijn masteropleiding in informatica ben ik een keuzevak tegengekomen over netwerk en computer security. Ik had natuurlijk wel eens gehoord over zogenaamde hackers en hacking, maar dat was voor mij iets wat alleen in films gebeurde. Bij dit vak werd het voor mij echter ineens concreet. Er ging een wereld voor mij open. Het was aan de ene kant spannend om te leren hoe ik een systeem zonder toestemming binnen kon komen en aan de andere kant

Kas Clark: "Security was iets dat je tijdens een avondje met vrienden leerde."

ontzettend eng dat het zo makkelijk was. Dit was de benodigde prikkel om mij op het securitypad te zetten. Ik ging in mijn vrije tijd allerlei security boeken lezen en online hacking workshops volgen. Daarna heb ik mijn studie op security gericht en ging diverse security thema's onderzoeken tijdens zowel mijn afstudeerscriptie als mijn daarop volgend promotietraject. In de academische wereld kon ik van een veilige afstand over interessante vraagstukken nadenken maar uiteindelijk wilde ik de theorie toepassen om de praktijk te verbeteren. Met die gedachte ben ik bij het Nationaal Cyber Security Centrum in dienst gekomen.

Welke (grote) ontwikkelingen heb je meegemaakt?

Ik vind dat security steeds zelfstandiger wordt. Daarmee bedoel ik dat security steeds meer als een zelfstandig onderwerp wordt behandeld in plaats van als een onderdeel van iets anders, zoals communicatietechnologie. Dit heb ik voornamelijk in de academische wereld ervaren. Toen ik met mijn bachelor in informatica was begonnen, was security geen onderdeel van mijn studie. Security was iets dat je tijdens een avondje met vrienden leerde. Er waren toen nog geen professors die gespecialiseerd waren in cybersecurity. Sterker nog, de systeembeheerder van de universiteit wist waarschijnlijk veel meer over security dan de rest. Tegen de tijd dat ik mijn masters aan het afronden was, kon ik keuzevakken volgen over cryptografie en informatierubricering. Tegenwoordig zijn er zowel professors als hele studies die gespecialiseerd zijn in cybersecurity. Dat laat zien hoe belangrijk dit vak is geworden.

Wat waren/zijn de grootste uitdagingen?

Eindgebruikers blijven voor mij de grootste uitdaging. Je kan het perfecte systeem bouwen met allerlei security maatregelen maar één eindgebruiker kan alles omzeilen en het systeem in gevaar brengen. Er zijn genoeg voorbeelden van gebruikers die een verdacht linkje volgen omdat ze een grappig filmpje te zien krijgen of vertrouwelijk stukken in de trein achterlaten of via een onbeveiligd, privémailadres naar huis sturen om in het weekend eraan te kunnen werken. We kunnen ze blijven opvoeden met de zoveelste bewustwordingscampagne maar persoonlijk vind ik dit een verkeerde aanpak. We moeten systemen kunnen bouwen die robuust, veilig en tegelijkertijd gebruiksvriendelijk zijn. Een eindgebruiker moet geen reden hebben om bewust of onbewust de security maatregelen te omzeilen.

Wat is je visie? Ottewel, wat is het ideale internet en is het haalbaar?

Volgens mij is het grootste voordeel van het internet ook het grootste nadeel, namelijk anonimiteit. Aan de ene kant biedt anonimiteit op het internet allerlei bescherming voor mensen die iets willen onderzoeken of bespreken zonder dat zij daarvoor vervolgd of gepest worden. Aan de andere kant maakt zulke anonimiteit het juist mogelijk om vreselijke dingen te doen, van pesten tot fraude en nog veel ergere dingen. In mijn ideale internet zouden we een sterk onderscheid moeten maken tussen anoniem internetten en 'gewoon' internetten. Als iemand anoniem wil internetten, krijgen ze toegang tot een beperkt internet met beperkte functionaliteit, een 'read-only' internet, als het ware. Dezelfde aanpak zien we nu bij sommige online fora waar men anoniem mag lezen maar in moet loggen om iets te schrijven. Misschien is het technisch mogelijk om dit te realiseren maar volgens mij zou het nooit sociaal haalbaar zijn. Mensen genieten juist van de pseudo-anonimiteit op internet en zouden dat niet zo snel willen opgeven zelfs als het minder fraude en dergelijke zou betekenen.

Welke trends/uitdagingen zie je aankomen in de komende 5-10-20 jaar?

Volgens mij gaan we afkicken van de 'alles-is-gratis' mentaliteit. We zijn het al jaren gewend dat we op internet alles kunnen zien, beluisteren en lezen zonder ervoor te moeten betalen. iTunes, Spotify en NetFlix hebben bewezen dat, in sommige gevallen, 'makkelijk' beter is dan 'gratis'. Men is wel bereid om een klein beetje geld uit te geven om toegang te krijgen tot hoge kwaliteit media. Dan is het niet meer nodig om iets te downloaden van een verdachte website. Volgens mij zullen we dezelfde verandering zien bij andere diensten, zoals onlinediensten rondom email, agenda, documenten en foto's. De gratis varianten van deze diensten tonen advertenties en delen onze (persoonlijke) informatie met derde partijen. Net zoals bij de media diensten, verwacht ik dat we binnenkort goedkope alternatieven zullen hebben die betrouwbare diensten voor een redelijke prijs leveren zonder onze privacy te schenden.

OPLEIDEN ANNO 2014

In dit artikel beschrijft Vincent Jentjens, CEO van de Security Academy, zijn visie op het vakgebied beveiliging en opleiden (vincent.jentjens@securityacademy.nl).

Visie op het vakgebied anno 2007

In 2007 ben ik samen met mijn businesspartner Hans de Vries de Information Security Academy gestart. Eigenlijk begon dit uit onvrede over het toenmalige opleidingsaanbod. Zeker in 2007 was het vakgebied informatiebeveiliging nog lang niet zo populair als tegenwoordig. Qua opleidingen waren er korte cursussen van 1 tot 2 dagen, veelal op de Amerikaanse markt gericht en vaak product gerelateerd. Voor de informatiebeveiliger in spé dus weinig aanbod aan productonafhankelijke, op de Nederlandse markt gerichte, IT-Security opleidingen.

Onze visie was dat er praktisch toepasbare kennis beschikbaar moest komen op MBO+/HBO-niveau. Met dit idee zijn wij destijds onze opleidingen gaan ontwikkelen. Rond 2010 zagen wij eenzelfde beweging in het vakgebied Business Continuity & Crisismanagement ontstaan. Het vakgebied werd langzaam populairder. Wel was het erg verkokerd in de eigen silo van BCM-ers en crisismanagers. Om deze doelgroep te bereiken en aan te sluiten bij de BCM/ crisiswereld zijn we de Business Continuity Academy gestart. Ook hier pasten wij dezelfde visie toe: praktisch toepasbare kennis leveren.

Visie op het vakgebied anno 2014

Anno 2014 zien we een verschuiving plaatsvinden. Door de vele cybercrime incidenten groeien de werelden van IT-Security en Business Continuity /crisismanagement in rap tempo naar elkaar toe. Immers, je kunt met informatie-beveiliging preventief vele maatregelen treffen om cybercriminelen buiten de deur te houden, maar als ze willen dan komen ze toch wel binnen. De vraag is dan hoe je als organisatie hiermee omgaat (crisismanagement). Beide vakgebieden zijn dus onlosmakelijk met elkaar verbonden. Een integrale aanpak is noodzakelijk.

Per 1 juni 2014 zullen daarom de Information Security Academy en Business Continuity Academy onder een entiteit, genaamd de Security Academy verder gaan. Door de Academy's onder te brengen in de Security Academy wordt een meer integrale aanpak van beveiliging en continuity mogelijk en zal er veel meer kruisbestuiving tussen de docenten, studenten en opleidingen plaatsvinden.

Visie op opleiden anno 2014

Het aanbieden van een opleiding alleen is niet meer voldoende. Studenten zijn op zoek naar ontwikkeltrajecten en carrièrepaden. De Security Academy heeft hiervoor een driestappenmodel ontwikkeld waarbij de student op basis van een ontwikkeltraject opgeleid wordt tot een specifieke functie. Een student kan bij ons kiezen uit een 7-tal ontwikkeltrajecten welke bestaan uit drie stappen:

1. Generieke opleidingen
2. Specifieke opleidingen
3. Intervisie / coaching

De generieke opleidingen zijn breed in opzet en leggen de basis voor de specifieke functie van het ontwikkeltraject. De specifieke opleidingen zijn specialisaties binnen een ontwikkeltraject en focussen op één deelaspect van de functie. Wanneer je als student na de opleiding aan de slag gaat zal de opgedane kennis in de praktijk toegepast moeten worden. Hier ontstaat dan vaak een specifieke opleidingsbehoefte die ingevuld wordt met de laatste stap uit het ontwikkeltraject: de intervisie/ coaching. In deze stap kan je de daadwerkelijke implementatie toetsen en evalueren met één van onze top-docenten. Met de ontwikkeltrajecten en de 3-stappenmethodiek wordt hierdoor dus niet alleen kennis overgebracht, maar wordt de opgedane kennis ook praktisch toepasbaar ingezet.

www.securityacademy.nl

IT & CARS

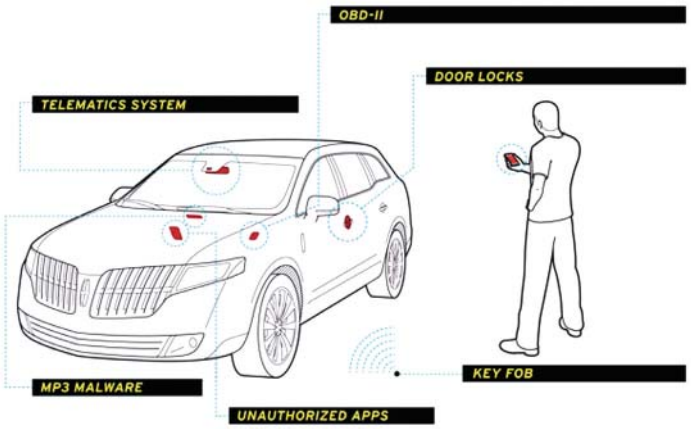
Dat IT onze manier van autorijden sterk gaat beïnvloeden wordt als ontwikkeling inmiddels breed herkend. De tijd dat onze auto's puur mechanisch waren ligt ver achter ons. De boordcomputer bepaalt of onze auto er klaar voor is of niet. En zijn er serieuze problemen met de boordcomputer? Dan kun je beter een IT-specialist zoeken dan een automonteur die hooguit de resetknop weet te vinden.

Diverse specialisten zien de steeds verdergaande computerisering van auto's als een grote stap vooruit in de veiligheid van automobilisten. De computer kan immers binnen de auto vroegtijdig een onderhoudswaarschuwing afgeven en buiten de auto de omgeving in de gaten houden. Stel je eens voor dat alle bestuurders hun vertrek, bestemming, snelheid en huidige weglocatie met elkaar zouden delen? Dit zou enorme voordelen rondom verkeersplanning en het voorkomen van gevaarlijke situaties moeten kunnen bieden. Hetzelfde geldt voor sensoren die bestuurders helpen om voldoende afstand te bewaren of die aangeven (of ingrijpen) op het moment dat je een zebrapad of school nadert. De toename van IT in auto's heeft echter ook een keerzijde. Ze maken auto's kwetsbaar voor allerlei bedreigingen die we tot nu toe alleen op onze computers tegenkomen.

Blue screen of death

Iedereen heeft het op zijn PC wel eens meegemaakt: een blauw scherm, een blokkerend toetsenbord of een spontane

Maarten Hartsuijker is redacteur van het magazine IB en bovendien werkzaam bij Classity en de ANWB en bereikbaar via de mail op m.hartsuijker@classity.com



Bron: http://www.caranddriver.com

herstart. Je bent je werk kwijt, kunt een aantal minuten niets met je PC en je zit in spanning te wachten of de PC weer opnieuw opstart. In relatie tot PC-gebruik is dit gedrag van computers redelijk geaccepteerd. Het hoort er gewoon bij: computers zijn nou eenmaal kwetsbare apparaten. Maar een auto die er midden op de snelweg (of erger nog: een bergweggetje) ineens mee ophoudt… daar moeten we toch niet aan denken. Op dat moment kan een "blue screen of death" ineens wel een hele letterlijke betekenis krijgen.

Computerkwetsbaarheden maken auto's diefstalgevoelig

Dat criminelen relatief makkelijk in computers kunnen inbreken is inmiddels ook wel bekend. Onze persoonsgegevens worden massaal van websites gestolen. En consumenten die iets minder handig met een computer zijn lopen grote risico's op computervirussen, met alle gevolgen van dien.
In het Verenigd Koninkrijk bleken nieuwe BMW's met computersloten in 2012 een geliefd doelwit van autodieven. De dieven hadden een trucje gevonden om de computersloten te hacken en konden in een paar minuten een gloednieuwe auto stelen. Het bleek kinderspel om via de OBD (de on-board diagnose poort) een nieuwe sleutel te programmeren. De dieven plaatsten via een hack een digitale sleutel van zichzelf in een blanco 'keyfob' om daarna met de auto weg te rijden. BMW had blijkbaar nagelaten om de toegang tot de sleutelmodule in de autoprogrammatuur via de OBD goed te beschermen. Resultaat: honderden auto's verdwenen in 1 maand in 1 regio in het Verenigd Koninkrijk via een slimme hackerstool die op de Bulgaarse zwarte markt te koop werd aangeboden. Overigens zijn ook veel draadloze sleutels tot op wel 10 meter af te luisteren op het moment dat ze gebruikt worden om de auto te openen en/of te starten.

Andere hackers slaagden er in om de boordcomputer van een nieuwe auto te kraken via een MP3 die op de autoradio werd afgespeeld. Berijders die dachten op internet een paar leuke nummers voor in de auto te downloaden plaatsten in werkelijkheid een computervirus op hun boordcomputer.

Computervirussen kunnen ongelukken veroorzaken

Vorig jaar maakte Hyundai bekend dat ze het mogelijk willen maken dat berijders via hun smartphone informatie uit hun boordcomputer kunnen ophalen. Op de CES van 2014 toonden ze hun 'CloudCar' en lieten ze zien hoe je via MirrorLink-technologie je smartphone aan het infotainment systeem kunt koppelen. Diverse bedrijven hebben al oplossingen ontwikkeld die het mogelijk maken om via een smartphone ramen en portieren te openen/sluiten en om de auto te starten. Hiervoor dient de auto uiteraard in verbinding met internet te staan. Handig om op afstand te kunnen controleren of je de ramen wel dicht hebt gedaan. Voor hackers zijn de apps (en de interfaces) natuurlijk net zo interessant om op afstand de auto mee open te maken. We zagen op BlackHat 2013 al hoe beveiligingsonderzoekers er (bekabeld) in slaagden om vanaf de achterbank een Toyota Prius te bedienen. De stap naar draadloze controle is minder ver weg dan we denken.

Veilig nieuw rijden

Car tech kan een geweldige boost geven aan de berijderservaring. De mogelijkheden rondom verkeersplanning en gemak zijn eindeloos. Maar elke computeringang (draadloos of bedraad via een connector of een hifi set) introduceert ook nieuwe risico's. Wat gebeurt er als auto's bewust verkeerde informatie met andere auto's gaan delen? Zijn de boordcomputers van elke autofabrikant hier straks tegen bestand? En hoe zorgen we ervoor dat auto's met een internetverbinding straks geen nieuwe prooi voor hackers worden? Als we auto's voor het gemak even vergelijken met procesautomatisering zoals we die in fabrieken kennen, dan weten we dat de bouwers van dergelijke automatiserings-oplossingen niet gewend zijn om met IT-veiligheid rekening te houden. Hoe lang zou het duren voordat iemand ontdekt hoe hij zijn computervirus draadloos van auto naar auto kan kopiëren? En hoe kwetsbaar zijn wij als dat virus vervolgens besluit om de remmen uit te schakelen en gas te geven?

INTERVIEW

JOHN McCLURG

Chief Security Officer van Dell Global Security

John McClurg is sinds drie jaar global chief security officer bij Dell en is medeverantwoordelijk voor de nieuwe strategie van Dell op het gebied van security. Tijdens een rondje Europa hadden we een uurtje de tijd om met hem te spreken over security en privacy, de samenhang ervan en de nieuwe bedreigingen.

Dell

Dell is als leverancier van hardware in de jaren tachtig bekend geworden door de directe verkoop van maatwerkapparatuur. Zo kon iedere klant bijna tot op bitniveau een eigen pc laten samenstellen. Just-in-time productie zorgde voor optimale voorraadniveaus en mede daardoor voor lage kosten. Dell levert pc's, laptops en servers. Maar dat dozenschuifimago is Dell in rap tempo aan het veranderen. De afgelopen jaren heeft het bedrijf enkele grote strategische overnames gedaan en daarmee is het in een ander speelveld terechtgekomen. Belangrijk, omdat de investeringen van Dell sinds 2011 eigenlijk vooral investeringen in security-bedrijven betroffen. Het leveren van een uitgebreid spectrum aan security-producten en -diensten is één van de nieuwe speerpunten.

John McClurg

John's security-carrière is begonnen bij de FBI. Als FBI medewerker was hij medeverantwoordelijk voor het opsporen van dubbelspionnen en hackers. Een bekende zaak was die van Harold James Nicholson. Nicholson was een CIA medewerker die in ruil voor geld spioneerde voor de Russische geheime dienst. Bij het opsporen van deze dubbelspion heeft John een aantal lessen geleerd, met name dat monitoren een belangrijk security-instrument is. Na zijn FBI-tijd en voordat hij bij Dell aan de slag ging was McClurg werkzaam bij Honeywell, eveneens in het werkveld security.

Visie op security

We spraken met John McClurg over zijn visie en voorspellingen over security en privacy en al snel kwamen we uit op de

John McClurg
Chief Security Officer van Dell Global Security

Nuclear Security Summit (NSS) en de perikelen rondom Snowden en de NSA. Gevraagd naar zijn ideeën rondom de beveiliging van het NSS belandden we zomaar bij zijn stokpaardje. "NSS is veel meer dan alleen 'nations coming together'. Het is niet alleen fysieke beveiliging waar we overlast van ervaren, maar net zozeer de cybersecurity-aspecten die daarbij horen. McClurg stelt: "Een belangrijk uitgangspunt bij beveiliging is dat de oude, vertrouwde grensvlakken niet meer als zodanig

Interview: door André Koot is security en IAM consultant bij Strict Consultancy in Vianen en redacteur van het magazine IB. Hij is per e-mail bereikbaar via a.koot@strict.nl.

fungeren. De fysieke wereld en de digitale wereld kennen steeds meer raakvlakken en 'boundaries become more and more poreus'. Het zijn niet langer separate werelden. 'Traditional boundaries are naive in the global networking space'. Dat wil zeggen dat security breder moet worden opgevat. Fysieke beveiliging en logische beveiliging komen steeds meer in elkaars verlengde te liggen, of eigenlijk net andersom, beide krijgen steeds meer last van nieuwe ontwikkelingen als cloud en BYOD en andere nieuwe bedreigingen. We zijn te zeer gewend aan een security architectuur gebaseerd op incidenten en toepassing van silo's. De context is grotendeels afwezig, wat leidt tot steeds grotere chaos, complexiteit en 'conundrums' (raadsels, puzzels, red.)." Dat samenspel aan complicerende factoren moet volgens McClurg worden aangepakt door een versterking van de kerncapaciteiten, een verbeterde verbinding en convergentie van security-middelen. Sinds de koerswijziging kan Dell die hele aanpak ondersteunen met een 'full spectrum of Security Services'. "End to end security is needed."

Security en privacy

Wat vindt Dell's beveiligingsbaas van de huidige ophef rondom de onthullingen over de NSA?

"Niet alleen gewone burgers, maar ook criminelen maken gebruik van internet. Het monitoren ervan is een belangrijke maatregel om te komen tot indamming van de risico's."

Hoe ver mag je daarbij gaan? Wat de NSA allemaal doet, mag dat? Is 'collateral damage', in de vorm van inbreuk op de privacy van gewone burgers, noodzakelijk en niet te vermijden?

Volgens McClurg is privacy belangrijk, maar niet het hoogste goed. "In de grondwet van de Verenigde Staten wordt niet naar privacy als een grondrecht verwezen. Dat wil niet zeggen dat het niet belangrijk of noodzakelijk is, maar voor de VS weegt in bepaalde situaties de bescherming van de staat en haar ingezetenen zwaarder. Er is altijd een bepaalde spanning tussen security en privacy, maar er bestaat 'no privacy without security'. En hoe belangrijk is privacy als je er rampen mee kunt voorkomen? Vraag een weduwe van 11 september of ze het erg vindt dat in de jacht op terroristen haar e-mail wordt gelezen en je weet het antwoord."

Onlangs is bekend geworden dat de NSA ook grote bedrijven afluisterde. Dat ging toch niet om security, of terrorismebestrijding? Mag de NSA dat ook doen? Mag de NSA afgeluisterde informatie delen met commerciële partijen?

John geeft aan dat hij persoonlijk geen kennis heeft van een dergelijke ontwikkeling en dat hij dat nog niet heeft kunnen afleiden uit de onthullingen van Snowden. Wel geeft hij aan dat, in tegenstelling tot in de rest van de wereld, er in de Verenigde Staten geen commerciële staatsbedrijven bestaan. Daar staat tegenover dat sommige buitenlandse bedrijven in handen van de staat zijn en dat betekent dat zij het belang van hun overheid voor ogen hebben. Die betrokkenheid zou kunnen resulteren in een mogelijke bedreiging van de Amerikaanse economische belangen. "National security implies economic security", zegt McClurg daarover. In die context zou optreden van de NSA binnen de geldende Amerikaanse wetgeving moeten passen.

Edward Snowden

John McClurg is open over zijn ideeën rond de onthullingen van Edward Snowden. "Snowden had niet uit zichzelf zomaar de publiciteit moeten zoeken", stelt hij. " Nu worden allerlei staatsgevaarlijke onthullingen ongecontroleerd gepubliceerd. Door die publicaties krijgen terroristen de beschikking over informatie die het ze mogelijk maakt zich te onttrekken aan staatstoezicht. En daardoor worden geheime diensten 'deprived from techniques to intercept terrorists'. Snowden had de geëigende wegen moeten bewandelen om wat hij als misstanden beschouwt aan te kaarten." En die wegen zijn er, volgens McClurg, voldoende.

Voorspellingen

We hebben ten slotte John McClurg gevraagd om een blik in de toekomst te werpen. Dit zijn enkele van zijn security-voorspellingen.

- Social media monitoring. Social media vormen een bron van kennis. Het monitoren daarvan zal van groot belang blijken te zijn.
- Reputatie wordt een steeds belangrijker aandachtspunt voor bedrijven om zaken te kunnen doen op het wereldwijde web. Het managen van identiteiten is dan ook van een steeds groter belang. In dit kader moet ook de overname van Quest Software worden gezien, identiteiten vormen immers de basis voor reputatie.
- Spearfishing is een grote nieuwe dreiging. De criminelen worden ook steeds professioneler in de manier waarop ze hun slachtoffers vinden en benaderen. Ze maken gebruik van de kennis die ze opdoen uit sociale media om hun slachtoffers te leren kennen en hun zo aan te spreken dat er een vertrouwensband ontstaat die misbruikt kan gaan worden.
- Viable insider threat prevention zal een nog groter thema worden, omdat de grootste fraudes nog van binnenuit plaatsvinden.
- Analysetechnieken zullen steeds geavanceerder worden. In die zin moeten dan ook de investeringen van Dell in Kitenga worden gezien.

Als besluit kregen we van John McClurg een fraaie Coin, waarmee we, als we hem weer eens ontmoeten, hem een biertje kunnen ontfutselen.

Verantwoorde onthullingen #7

STUDENT GEEFT UNIVERSITEIT DURE LES

Hoe @XS4me2all de servers van de Rijksuniversiteit Groningen overnam (2007-2014)

Deze keer een case met een hacker wiens identiteit nog onthuld moet worden. @XS4me2all kreeg in 2007 via enkele kwetsbaarheden toegang tot servers van de Rijksuniversiteit Groningen. Hij deed het voor de kick, maar ziet het nu als een jeugdzonde. Hij wil alsnog opbiechten, mits hij niet vervolgd wordt. Frank Brokken, security manager bij de RUG, heeft hier begrip voor en is ook benieuwd wie hen toen gehackt heeft. Op 4 juni zal ik tijdens het NCSC congres de heren aan elkaar voorstellen. Hier alvast hun verhaal.

Het is begin februari 2007 als Brokken een alarmerende mail binnen krijgt: er zouden meerdere van hun computers zijn gehackt. De afzender wil anoniem blijven, maar Brokken vermoedt dat het een van zijn studenten is. Hij roept het crashteam bij elkaar: de interne specialisten bij computerincidenten. Al snel komen ze erachter dat op de webserver illegale software en video's draaien. Ook de image- en installserver blijkt besmet met malware. Die server is normaal gesproken een hulpmiddel voor systeembeheerders om via het netwerk back-ups of updates te laden. Nu besmet hij automatisch elke computer die hier inlogt. Dat zijn er inmiddels meer dan 250. Op een van de PCs staat zelfs een keylogger: de hacker kan dus de toetsaanslagen volgen om zo nog meer wachtwoorden of zelfs credit card gegevens af te vangen.

De universiteit doet aangifte bij de digitale recherche Noord. Brokken kent ze goed en heeft regelmatig contact met hen. Team High Tech crime van de Nederlandse politie wordt er ook bij betrokken. De zaak strandt echter bij het OM. Die besluit niet tot vervolging over te gaan omdat er te weinig concrete aanwijzingen zijn wie de mogelijke dader is. De hacker heeft gewoonweg te weinig sporen achtergelaten. Nader onderzoek wijst wel uit dat een van de systeembeheerders op verschillende plekken hetzelfde wachtwoord gebruikte. "Echt een stommiteit" zegt Brokken en ze hebben de betreffende man op het matje geroepen.

De universiteit neemt nog meer maatregelen. Er wordt een strikt wachtwoordensysteem opgelegd, soms met 2-factor authenticatie. De servers worden opgeschoond, firewalls opgetrokken en alle beheerswerkzaamheden gelogd. Zo kunnen ze in het vervolg beter zien of, waar en wanneer iets mis gaat. "Niet dat we nu bullit-proof zijn, maar zo kunnen we wel alles beter in de gaten houden." Een extern bedrijf doet vanaf dat moment regelmatig pen tests.

Brokken had al eerder de beveiliging willen opschroeven, maar kreeg daar bij het management de handen niet voor op elkaar. Nu wel. Het incident, dat vanaf dan bekend staat als 'de februari hack', heeft hem in die zin geholpen. Hij vond het daarom ook belangrijk om het naar buiten te brengen. "Organisaties worden gehackt, dat is een fact of life. Niet omdat ze hun beveiliging niet op orde hebben, maar door een mentaliteit onder de medewerkers. Als je ziet hoeveel mensen er nog in phishing mails trappen... En dan zo'n mentaliteit van: dat moeten ze bij ICT maar oplossen. Dat is fundamenteel fout."

Chris van 't Hof (www.cvth.nl)

Op 7 maart komt woordvoerder Jos Speekman via het ANP naar buiten met het bericht dat de computers van de RUG zijn gehackt. Op de getroffen systemen zou software zijn geïnstalleerd, waarmee cybercriminelen persoonlijke informatie kunnen stelen, zoals wachtwoorden en creditcardgegevens. Ze zouden de computers bovendien op afstand kunnen bedienen, bijvoorbeeld om illegaal films en software aan te bieden of spam te versturen. De universiteit vermoedt dat de computers van binnenuit door een medewerker of student zijn gekraakt. De schade wordt geschat op 100.000,- euro. Het bericht wordt overgenomen door de Volkskrant, Trouw, Nu.nl, Webwereld en security.nl. Zo komt het bericht ook terecht bij de hacker.

@XS4me2all is dan een jongen van twintig. Formeel is hij op dat moment nog wel student, maar niet aan de universiteit Groningen. Eigenlijk doet hij niets meer aan zijn studie, omdat hij dagelijks tot in de late uren het internet afstruint, op zoek naar nieuwe hackmethoden en steeds grotere targets. Voor de kick. Hij leert zo veel meer dan bij zijn studie. Nu hij leest hoeveel schade hij heeft toegebracht schrikt hij zich rot. Eigenlijk had hij de systeembeheerder willen bellen om te vertellen wat hij had gedaan – dat deed hij wel vaker – maar nu lijkt het hem wijzer zijn mond te houden. Toch blijft de zaak aan hem knagen. Vijf jaar later hoort hij over mijn onderzoek. Hij wil alsnog, via mij, opbiechten wat hij heeft gedaan.

In zijn studentenkamer vertelt hij mij hoe hij te werk ging. Het eerste wat hij aantrof op het universiteitsnetwerk was een printserver die online stond. Het wachtwoord was versleuteld, maar hij kon wel de hash van het wachtwoord zien. Op internet circuleren allerlei lijstjes – rainbow tables - van dergelijke hashes waarmee je het wachtwoord kunt achterhalen. En ja, hij vond een match. Met gebruikersnaam "admin" en wachtwoord "S4k1nt0s!" kon hij erin. Nu kijken of deze administrator nog meer systemen online heeft staan. Dat bleek het geval. Maar hij kon niet overal in want de admin was van een bepaalde studierichting en kon niet inloggen buiten zijn eigen domein.

Hij herhaalde de truuk met de hashes en rainbow table bij andere systeembeheerders en kwam erachter dat er veel overlap was in hun beheersdomeinen. Via die overlap kon hij makkelijker overstappen van de ene naar de andere. Hij zag ook dat ze allemaal een ConsoleOne van Novell gebruikten om het systeem te beheren en die was ook via internet benaderbaar. Dat zal makkelijk zijn geweest voor de systeembeheerders als ze van een locatie alle systemen willen updaten. Maar ook voor @XS4me2all. Via de beheerdersingang, poort 1761 van de console, kon hij nu vanaf zijn studentkamer het hele netwerk van de Rijksuniversiteit Groningen besturen.

Om niet elke server stuk voor stuk te hacken had hij een ander plan bedacht. Hij nam de image en installserver, daar installeerde hij zijn eigen malware in de gereedstaande images. Iedereen die nu inlogde, besmette dus zo zichzelf. Binnen een maand had hij toegang tot alles. Op een enkele computer zette hij ook wat malware die leek op een keylogger, gewoon om te zien of het kon, zonder hem te gebruiken want hij kon toch al overal in. Het leukste vond hij de wake on LAN functie, waarmee je op afstand computers aan kan zetten. Dat deed hij dan 's nachts. "Stel je voor, is daar zo'n schoonmaker aan het werk, gaan ineens alle computers aan… Kicken!"

Daarmee was zijn missie geslaagd. Het ging hem er niet om de universiteit schade toe te brengen. Het was puur de kick ergens in te komen. Vol enthousiasme vertelt hij erover aan andere hackers op een gesloten chatforum waar hij lid van was. Die geloven hem niet en willen bewijs zien. Dat kan: geef mij een film en dan laat ik die vanaf hun server draaien. Als hij dit doet, kijkt er waarschijnlijk iemand mee die het waarschuwende mailtje naar de universiteit stuurt. Anders kan niet, want hij heeft tegen niemand verteld hoe ze er in konden. Hij was, dacht hij, de enige.

@XS2all4me blijft de zaak volgen in de media. Gaandeweg krijgt hij meer respect voor security manager Frank Brokken die openlijk vertelt over het incident en zelfs zegt dat ze er veel van geleerd hebben. Hij ziet tot zijn verbazing op fok.nl ook een video van Studenten TV, met daarin een interview met de zogenaamde RUG-hacker. Dat vond hij minder leuk. "Staat er zo'n gozer in het donker met vervormde stem… die zei echt onzin en maakte het probleem veel groter dan het daadwerkelijk was." Hij had liefst zelf met Brokken willen praten, om te vertellen wat hij heeft gedaan en waarom, maar wil uit angst voor represailles niet naar buiten komen. Totdat hij in 2013 mij ontmoet. Zijn geweten knaagt, hij wil schoon schip maken. Ik stel voor te bemiddelen tussen beiden.

Ik stuur Brokken een mail waarin ik vertel over mijn onderzoek en hem vraag om meer documentatie. Ik stel ook voor een ontmoeting te arrangeren tussen hem en de hacker, mits de universiteit afziet van strafvervolging. Hij reageert positief. "In het delen van ervaringen ben ik altijd geïnteresseerd, ik zie geen reden om op het bekend maken van een kwetsbaarheid te reageren met juridische acties. De hacker hoeft wat dat betreft niet bevreesd te zijn en kan denk ik zelfs wel rekenen op een kopje koffie ;-)" Zijn mail is gesigneerd met PGP. Ik weet dan nog niet wat dat is en begrijp ook niets van al codes onderin zijn mail, maar voor @XS4me2all is dit voldoende als vrijwaring. We kunnen van start.

In mijn gesprek met Brokken merk ik geen wrok of frustratie, maar eerder bewondering voor hetgeen de hacker heeft gedaan. "Ik vind het geweldig dat die jongen het op deze manier heeft gedaan. Als jij toegang hebt tot de server die software installeert op andere machines, wordt het werk door de organisatie gedaan. Dat is prachtig." Brokken moet zelfs hartelijk lachen als ik vertel hoe 's nachts de computers werden aangezet. Na beide heren te hebben gesproken, schrijf ik dit stuk en zie uit naar 4 juni. Dan zijn we samen in het Worldforum voor een verantwoorde onthulling.


ЩО-1
7,366
ЩО8505-0415
ЩО-3
8,674
ЩО8505-0415
ЩО3-Н-8,674-15,0-25-375-0,3
NYM-5x10 L=25м
ЩС-2
Ру=36,6кВт
Рр=34,77
Iр=60,16А
ЩО-2
3,242
ЩО8505-0415
ЩО-4
9,222
ПР 8503-3093
222-15,9-20-318,-0,3
L=20 T 32=4м
Резерв
AE2046
Iр=40А
AE2046
Iр=31,5А
AE2046
Iр=31,5А
ЩС1-Н-10,4-18,0-25-450-0,4
NYM-5x16 L=6м
ПВ1-5(1х 50)
ЦЭ6803В 2Т, 5А
N1
250
150
ВВОД N2
Ру2= 71,754 кВт
Рр2= 63,6 кВт
Iр2= 110,00А
АВАРИЙНЫЙ РЕЖИМ
Ррав. = 32,8 кВт
Iрав. = 55,0 А
КЗ

Auteursinformatie: *Prof. dr. ir. Jan van den Berg is hoogleraar Cyber Security aan de Technische Universiteit Delft. Jacqueline van Zoggel is senior adviseur Hoger Onderwijs. Samen vormen zij sinds dit voorjaar de directie van de Stichting Cyber Security Academy The Hague, een samenwerkingsverband van de Technische Universiteit Delft, Universiteit Leiden en De Haagse Hogeschool.* ***Voor meer informatie: www.csacademy.nl***

CYBER SECURITY VRAAGSTUKKEN

Den Haag, stad van vrede, recht en veiligheid, heeft de ambitie geformuleerd uit te groeien tot een internationaal toonaangevende veiligheidsregio. Daarom is afgelopen zomer de netwerkorganisatie The Hague Security Delta (HSD) opgericht, waarin inmiddels zo'n tweehonderd partners uit de gouden driehoek (overheid, bedrijfsleven, kennis-instellingen) zijn verenigd.

In een snel digitaliserende samenleving is goed functionerende en veilige IT (kortweg cyber security) cruciaal voor het reilen en zeilen van de samenleving als geheel. Betrokken HSD-partners zoals ministeries, banken, telecombedrijven, energieleveranciers, adviesbureau's en (inter)nationale koepelorganisaties zoals Europol/EC3, NCTV en kennisinstellingen, voorspellen een groeiende behoefte aan specialisten op het terrein van cyber security. De Technische Universiteit Delft, de Universiteit Leiden en de Haagse Hogeschool hebben hun kennis en kunde gebundeld in de dit voorjaar opgerichte stichting Cyber Security Academy, The Hague (CSA). Op initiatief van de CSA werken enthousiaste wetenschappers en docenten vanuit diverse disciplines samen met experts uit de beroepspraktijk, aan een vernieuwend programma aanbod. Een gloednieuwe wetenschappelijke masteropleiding Cyber Security voor professionals, die dit najaar van start gaat, vormt het eerste concrete resultaat van deze werkzaamheden. Deze postinitiële opleiding leidt op tot een MSc in Cyber Security [1] en kent, als één van de eerste opleidingen in Europa, een integrale benadering van cyber security. De opleiding brengt de technische, juridische, bestuurlijke, economische, politieke en psychologische dimensies van digitale veiligheid met elkaar in verband en gebruikt geïntegreerde benaderingswijzen voor het oplossen van de snel in complexiteit toenemende vraagstukken rond cyber security.

Cyber risico's in perspectief

De groeiende aandacht voor cyber space en cyber security is niet verwonderlijk in een samenleving die in rap tempo nagenoeg al haar vitale processen afhankelijk heeft gemaakt van ICT. Het aantal toepassingen en gebruikers groeit gestaag (bijna drie miljard gebruikers wereldwijd [2]. De technische mogelijkheden kennen een autonome vlucht en de vraag van gebruikers is nagenoeg onbegrensd. Cyber space is daarmee in enkele decennia uitgegroeid tot een complex, manmade

Bowtie model

system met grote afhankelijkheden en tal van dimensies die veel verder reiken dan de technische aspecten alleen.

De ermee gepaard gaande dreigingen en kwetsbaarheden zijn talrijk en leiden tot een gestaag groeiende reeks van incidenten: er gaat vrijwel geen dag voorbij zonder dat een of ander cyberincident de krantenkoppen haalt.

Incidenten zijn vaak het gevolg van bewust uitgevoerde aanvallen die resulteren in incidenten in de sfeer van cyber crime (creditcard fraude, digitale spionage) en cyber warfare (militaire aanvallen met drones, Stuxnet). Ook treden er incidenten op door technische of persoonlijke fouten, als neveneffect van natuurrampen, door bestuurlijk onvermogen, door onvoldoende adequaat toezicht en/of door naïviteit van eindgebruikers.
De concrete impact is verschillend van karakter en kan variëren van economische schade, verstoring van bestuurlijk en politieke verhoudingen, milieuschade tot schendingen van grondrechten en privacy, dan wel combinaties daarvan.

Als gevolg van een complexe verwevenheid van boven-genoemde dreigingen, kwetsbaarheden, incidenten en impact, manifesteren cyber incidenten zich steeds meer als een veelkoppig fenomeen. Het begrip 'risico' als resultante van de kans op incidenten en de impact daarvan op de samenleving is, binnen het door ons gecreëerde nieuwe domein van cyber space, toe aan een grondige herijking.

De constatering lijkt gerechtvaardigd, dat de beheersbaarheid van via het Internet gestuurde systemen en de weerbaarheid van actoren in cyber space (overheden, bedrijven en burgers) momenteel geen gelijke tred kunnen houden met (de enorme snelheid van) de hedendaagse digitale innovaties.

Nog veel (te) weinig aandacht gaat uit naar doordachte preventie en regulering zoals het definiëren van politieke en bestuurlijke verantwoordelijkheden (rol van overheden). Ook preventieve bedrijfsstrategieën (cyber security als onderdeel van ieder van IT- afhankelijk bedrijfsproces) komen nog maar aarzelend tot ontwikkeling, en ten slotte laat de bewustwording en educatie van (eind)gebruikers (de bedrijfscultuur) vaak nog veel te wensen over.

Kortom, er is groeiende noodzaak om gezamenlijk acceptabele cyber risico's te formuleren en toe te werken naar meer integrale vormen van cyber risicomanagement, inclusief adequate wet- en regelgeving, over de volle breedte van de digitale samenleving.

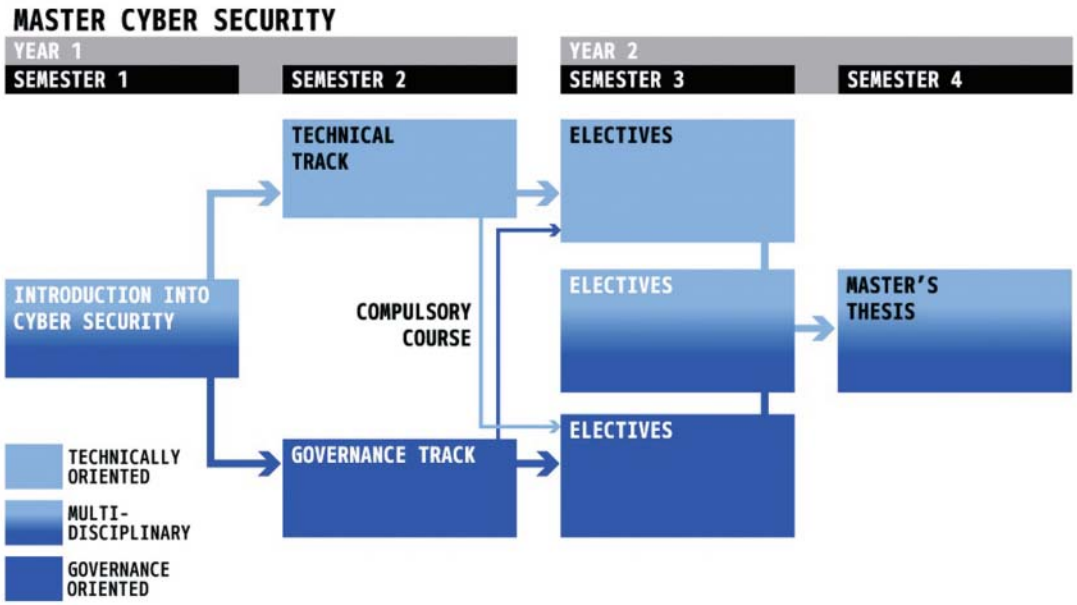
De zich ontwikkelende vraag naar CS-specialisten

Het is niet verwonderlijk dat momenteel de vraag van werkgevers in uiteenlopende sectoren vaak uitgaat naar technisch gekwalificeerd personeel die de werking van IT begrijpen. Deze vraag, naar technisch talent, dat binnen organisaties en bedrijven een zichtbare bijdrage levert aan beter beveiligde (primaire processen) is begrijpelijk. Het is echter

wel een eenzijdige aanpak van problemen, die weinig recht doet aan de complexiteit en de afhankelijkheden die cyber security inmiddels kenmerken. Een aanpak die op termijn mogelijk zelfs een meer visierijke (lees: noodzakelijke nieuwe) benadering in de weg staat. Het is de verwachting van overheidsinstanties [3], kennisinstellingen en experts verenigd in de Cyber Security Academy dat naast de groeiende vraag naar technisch geschoold personeel ook de vraag naar een nieuw type professional met geïntegreerde kennis van en met een visie op het vergroten van de digitale weerbaarheid zal toenemen. Het gaat dan om professionals met overzicht over en (basis)kennis van zowel technische, juridisch/ethische, bestuurlijk/politieke als culturele/psychologische aspecten samenhangend met digitale veiligheid, die in staat zijn op strategisch en tactisch niveau sturing en richting te geven aan nieuwe strategieën en concepten voor de regulering van complexe digitale processen en digitaal verkeer.

Het huidige aanbod aan cyberopleidingen

Een nadere analyse van de hierboven geschetste frictie tussen vraag en aanbod van specialisten cyber security laat het beeld zien van een tot nu toe te gefragmenteerd en op onderdelen tekortschietend opleidingenaanbod in Nederland zowel in kwantitatieve als kwalitatieve zin. Uit een onlangs op initiatief van enkele hoogleraren cyber security opgestelde inventarisatie naar (wettelijk erkend) opleidingenaanbod in het hoger onderwijs in Nederland komt naar voren dat diverse hogescholen (zoals de Noordelijke Hogeschool Leeuwarden, Hogeschool Zuyd, Fontys hogescholen, De Haagse Hogeschool en Saxion Hogeschool) bachelor- en masteropleidingen aanbieden op het terrein van veiligheid, informatiemanagement en ICT en recht met cybergerelateerde specialisaties. Veel van deze opleidingen zijn gepositioneerd in het informaticadomein.
Universiteiten , zoals de Universiteit Twente, Technische



Opleidingsconcept postinitiële master Cyber Security

Universiteit Delft, Radboud Universiteit Nijmegen, Vrije Universiteit en TU-Eindhoven bieden (al dan niet in combinatie met elkaar) technische tracks aan (zoals binnen het Kerckhoff's instituut), veelal als specialisatie van uiteenlopende opleidingen Computer Science. Andere universiteiten bieden tracks en masteropleidingen op het grensvlak van disciplines zoals Law and Technology (de Universiteit van Tilburg en de Universiteit Leiden) Forensics en inlichtingenstudies (Universiteit van Amsterdam) en Safety & Security (Universiteit Leiden) en Cyber and Business (Nyenrode Business University). De drie technische universiteiten hebben het initiatief genomen om in samenwerking met elkaar (mogelijk aangevuld met derden) een nieuwe (overwegend technische) master Cyber Security te ontwikkelen (beoogde start in 2015).
Naast het bachelor- en masteraanbod van universiteiten en hogescholen bieden tal van private bedrijven en organisaties gespecialiseerde korte cursussen, leergangen, workshops e.d. op het terrein van Cyber Security. Bekende aanbieders zijn Deloitte, FOX-IT , ENCS, Thales, VKA, KPMG, TNO, Security Academy e.a.
In Europees verband verdienen University College Dublin en diverse universiteiten in de UK vermelding (University of Warwick, Royal Halloway London, University of Oxford en Lancaster University). Ook eerste open online onderwijsvarianten (MOOC's) zijn in ontwikkeling (University of Maryland). Veel van deze opleidingen kennen een sterke focus op technische knowhow met een enkele keuzemogelijkheid in het domein Recht en/of Bestuurskunde.

De multidisciplinaire executive master Cyber Security

Nog vrijwel nergens blijken vraagstukken rond cyber security vanuit holistisch perspectief bestudeerd te worden. Mede in het verband van het beschikbare netwerk van bedrijven en instellingen verenigd in The Hague Security Delta deed zich voor kennisinstellingen voor hoger onderwijs in de Haagse regio de unieke gelegenheid voor om een multidisciplinair opleidingsconcept te ontwikkelen en aan te bieden.

In deze parttime eenjarige Engelstalige MSc opleiding (verspreid aangeboden over twee jaar) voor zowel technisch als juridisch en sociaal wetenschappelijk geschoolde deelnemers, wordt vanuit een gemeenschappelijk framework (introduction into cyber) in twee (verdiepende) specialisaties (technical en governance track) met behulp van uiteenlopende verbredende en verdiepende keuzemodules (variërend van o.a. cyber forensics, cyber espionage en tot cybercrime and law enforcement) en een individueel uit te voeren onderzoek (de masterthesis) toegewerkt naar een nieuw type cyber security-professional voor functies van de toekomst.

Referenties

[1] De opleiding is inmiddels door de Universiteit Leiden ter accreditatie voorgelegd aan de NVAO.

[2] http://www.internetworldstats.com/emarketing.htm

[3] Nationale Cyber Security Strategie 2, oktober 2013

[4] Prof. dr. Wouter Stol, prof. dr. Pieter Hartel en prof. dr. Jan van den Berg, e.a.

ARTIKEL VAN HET JAAR 2013

Namens de jury, Renato Kuiper. Renato is te bereiken via renato.kuiper@vka.nl

TOP 3

1) **Agile in Informatiebeveiligingsprojecten van T. van Vooren**
2) **Brede meldplicht datalekken van M. Elferink en M. Kortier**
3) **Van risicomanagement naar succes governance van Rieks Joosten**

Juryrapport

In 2014 is de jury weer aan de slag gegaan met het beoordelen van de aangereikte artikelen die door de redactieraad waren genomineerd. Als jury hebben we acht artikelen ontvangen, deze hadden allen een verschillende scoping op het onderwerp Informatiebeveiliging: enerzijds juridische aspecten, anderzijds procesmatige aanpak voor het borgen van informatiebeveiliging, maar ook diepgaand technische onderwerpen.

Bij het beoordelen van het artikel van het jaar hebben we de 5 criteria gehanteerd die voor de beoordeling van toepassing waren:

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

De jury heeft onafhankelijk van elkaar een top drie uit deze acht artikelen gekozen. Voor deze artikelen gold dat ze alle drie voldeden aan de vijf bovengenoemde criteria. Als jury hebben we opnieuw dieper gegraven in de artikelen om tot onze conclusies te komen.

Enkele opmerkingen m.b.t. de (top) drie artikelen:

- **Van risicomanagement naar succes governance:**
  Het artikel triggert je al direct in de inleiding, mede omdat er ook hulp wordt geboden. Het stimuleert ook om een terugkoppeling te geven aan de auteur. De auteur is tamelijk sceptisch over de efficiëntie en effectiviteit van het huidige risicomanagement (RM) en de mate waarin het wordt gedragen door de business. Hij onderbouwt zijn scepsis aan de hand van verschillende signalen (8 stuks) die hij in de praktijk is tegengekomen en die aangeven hoe er gedacht wordt over de oorzaak daarvan. Het artikel roept zeker om een vervolg met verdere praktijkervaringen daarin verwerkt.

- **Agile in Informatie-beveiligingsprojecten:**
  Een zeer leuk geschreven artikel, in heldere bewoording neemt de auteur je mee in zijn praktijkervaring in het toepassen van informatiebeveiliging in agile projecten. Informatiebeveiliging in projecten en in bijzonder applicatie ontwikkeltrajecten is doorgaans al een lastig onderwerp waar de IB-er regelmatig veel moeite moet doen om het geadresseerd te krijgen. Laat staan in een ontwikkelomgeving die zeer dynamisch ingericht is. Het artikel vraagt naar een vervolg: met name meer concretere toepassing in IAM-trajecten, het werkveld waar de auteur actief in is.

- **Brede meldplicht datalekken:**
  Het artikel heeft bij een aantal juryleden al gelijk het bewustzijn verhoogd om het e.e.a. al te gaan regelen. Het artikel geeft ook duidelijk aan, dat de nieuwe regels in de meldplicht ook aangeven, dat de verantwoordelijke de plicht krijgt om dit ook expliciet op te leggen aan de bewerker om de verplichtingen ook na te komen. De consequenties van het niet voldoen worden zeer duidelijk uitgelegd en toegelicht, wie niet acteert neemt risico's!

INFORMATIEBEVEILIGERS DEFINIËREN HUN KWALIFICATIE-STELSEL OP BASIS VAN E-CF

PvIB is sinds 2003 bezig met het structureren van het onderwijs voor informatiebeveiligers. Het begon met de eerste Opleidingenmarkt bij de TU/ Eindhoven met een congres en een informatiemarkt van opleiders met hun actuele opleidingen. Sindsdien wordt de Opleidingenmarkt elke twee jaar gehouden bij een opleidingsinstelling. In 2006 publiceerde PvIB het boekje 'Functies in de Informatiebeveiliging'. Het werd de 'de facto' standaard voor het vakgebied bij bedrijfsleven en overheid. In 2009 werd kwalificatie van informatiebeveiligers opgenomen in het Algemeen Beleid van PvIB. In mei 2014 heeft PvIB het whitepaper 'Beroepsprofielen Informatiebeveiliging' gepubliceerd op haar website. Nederlandse en Engelse versies zijn beschikbaar.

In eerdere artikelen (zie Beveiliging #11, 2011, Informatiebeveiliging #5, 2013, iB #2, 2014) kwamen de stappen aan de orde die gezet zijn om te komen tot beroepskwalificatie. In die artikelen kwamen respectievelijk aan bod: het onderzoek naar het kwalificatiestelsel (CPNI.NL, april 2011), het brede maatschappelijk draagvlak dat aanwezig is en de structuur van de beroepsprofielen. Dit artikel doet verslag van de bijeenkomst in Hilversum op 8 april jl. waarbij professionals de beroepsprofielen aan een brede toetsing hebben onderworpen.

Breed maatschappelijk draagvlak voor het kwalificatiestelsel

In september 2013 is de publiek-private samenwerking Stuurgroep QIS (Qualification of Information Security professionals) gestart, die een uniform kwalificatiestelsel voor Nederland gaat inrichten. Sponsoren van dit project zijn: Rabobank, ING, ABN-AMRO, AkzoNobel, Rijksoverheid, Cyber Security Raad, EY, ECP/Digivaardig&Digiveilig en PvIB.

Organisaties van de Stuurgroep QIS

De deelnemende organisaties in de klankbordgroep zijn koepelorganisaties van werkgevers (VNO-NCW, MKB, CIO Platform, CIP (IB-expertisecentrum van, voor en door overheidsorganisaties), kennisinstellingen (ECABO (=mbo), HBO-i,

Auteurs: *Fred van Noord, voorzitter van het Platform voor Informatiebeveiliging (PvIB) en zelfstandig adviseur informatieveiligheid. Fred is te bereiken via fredvannoord@pvib.nl.*
Marcel Spruit, lector Cyber security & safety aan de Haagse Hogeschool en senior consultant bij Het Expertise Centrum/PBLQ. Marcel is te bereiken via marcel.spruit@inter.nl.net

het wetenschappelijk onderwijs, VOI, SPIH) en beroepsorganisaties (Ngi, NOREA).

Organisaties van de Klankbordgroep QIS

Kwalificatie anno 2014

In de huidige situatie voldoen bestaande certificaten niet, is er gebrek aan goede opleidingen en is er een tekort aan goed opgeleide professionals. Straks moet het opleiden van professionals sneller en gerichter gaan, zijn er meer opleidingsmogelijkheden en zijn kwalificaties uniform, geaccepteerd en transparant. Een belangrijke eerste stap hierin zijn beroepsprofielen die door professionals zelf worden herkend en erkend. Een kwalificatie is een formeel resultaat van een beoordelings- en validatieproces, dat wordt verworven wanneer een bevoegde instantie bepaalt dat de leerresultaten die een individu heeft bereikt, aan gegeven normen voldoen.

Beroepsprofielen op basis van e-CF 3.0

Om professionals in informatiebeveiliging te kunnen kwalificeren, is door de PvIB-werkgroep Kwalificaties in een whitepaper vastgesteld welke beroepen binnen het vakgebied informatiebeveiliging worden onderscheiden en wat deze beroepen inhouden. De beroepen zijn beschreven door middel van beroepsprofielen op basis van het Europees e-Competentie Framework 3.0. Een beroepsprofiel geeft een formele beschrijving van een beroep. Het beschrijft de missie, taken en verantwoordelijkheden van een beoefenaar van het betreffende beroep en specificeert de competenties (kennis, vaardigheden en houding) die de beoefenaar dient te bezitten. Voor vier beroepen is het beroepsprofiel beschreven.

A. aan de kant van de business (Information Risk Management):

- Chief Information Security Officer (CISO)
- Information Security Officer (ISO)

B. aan de kant van de ICT (ICT security):

- ICT-beveiligingsmanager
- ICT-beveiligingsspecialist.

Een eerste conceptversie van het whitepaper is door de organisaties van de Stuurgroep en de Klankbordgroep gereviewed, waarna een brede consultatie met de beroepsgroep informatiebeveiligers heeft plaatsgevonden.

Consultatiebijeenkomst beroepsgroep

Met het CIO Platform Nederland is afgestemd over de aanpak en de werving van deelnemers voor de consultatiebijeenkomst. Om een zo breed mogelijke toetsing te krijgen van de IB-profielen waren bij de bijeenkomst vertegenwoordigers van andere beroepsorganisaties betrokken: Ngi (ict'ers), NOREA (IT auditors), NNK (kwaliteitsmanagers), (ISC)^2 (security professionals) en L-SEC (security professionals uit België). De vier beroepsprofielen stonden centraal en de relaties met 5 andere e-CF beroepsprofielen zijn getoetst.

Professionals discussiëren met elkaar (Bron: Lex Dunn)

In zeven groepen hebben 60 professionals van 40 organisaties alle onderdelen van de beroepsprofielen bediscussieerd. Omdat eenzelfde profiel door meer dan één groepje werd beoordeeld kon ook de consistentie en relevantie van de uitkomsten beoordeeld worden. De groepjes zijn begeleid door moderatoren met kennis van het e-CF uit de PvIB-werkgroep en een assistent (studenten van de Haagse Hogeschool). De aangepaste versie is opnieuw gereviewed door de begeleiders. Het whitepaper 'Beroepsprofielen Informatiebeveiliging' is door de Stuurgroep QIS unaniem goedgekeurd om als basis te dienen voor opleidingsprofielen en de kwalificatieschema's.

De resultaten

Voor het beschrijven van de beroepsprofielen is gebruik gemaakt van het document CWA 16458 van CEN. Hierin zijn beroepsprofielen geformuleerd voor beroepen in de ICT-sector. De in de profielen benodigde e-competenties zijn gebaseerd

Grote opkomst tijdens sessie in Hilversum (Bron: Lex Dunn)

op e-CF. In eerste instantie zijn de beroepsprofielen voor ICT Security Manager en ICT Security Specialist overgenomen. De beroepsprofielen voor CISO en ISO zijn niet in CWA 16458 gespecificeerd. Dit is niet geheel onverwacht, want CISO en ISO zijn geen ICT-functies en vallen daarmee buiten de scope van CWA 16458. In het whitepaper zijn de beroepsprofielen van CISO en ISO opgesteld analoog aan de andere twee profielen. Dit heeft geleid tot aanpassingen in de oorspronkelijke profielen van ICT Security Manager en ICT Security Specialist.

Hieronder als voorbeeld delen van de beroepsprofielen van de CISO en de ICT Security Manager. De complete beroepsprofielen staan in het whitepaper (zie www.pvib.nl).

Profieltitel	ICT SECURITY MANAGER	
Samenvatting	Definieert de ICT-beveiligingsrichtlijnen voor de organisatie in overeenstemming met de informatiebeveiligingsstrategie en -architectuur van de organisatie en organiseert en managet de ICT-beveiliging van de organisatie.	
Kerntaken	• Definieert de ICT-beveiligingsrichtlijnen voor de organisatie in overeenstemming met de informatiebeveiligingsstrategie en -architectuur van de organisatie • Managet de implementatie van de ICT-beveiligingsrichtlijnen • Zorgt voor een projectportfolio voor ICT-beveiliging • Definieert het opleidingsbeleid voor ICT-beveiliging • Definieert en implementeert procedures ten behoeve van to ICT-beveiliging • Organiseert ICT-beveiliging en de daarvoor benodigde expertise • Volgt technologische ontwikkelingen op het gebied van ICT-beveiliging • Voert risicoanalyses voor ICT uit • Monitort ICT-risico's en rapporteert daarover • Zet het ICT-continuiteitsplan op • Initieert and managet ICT-beveiligingsprojecten • Borgt de kwaliteit van de ICT-beveiligingsassessments, -tests, -reviews en -audits • Informeert senior algemeen management over de status van ICT-beveiliging en incidenten	
e-Competenties (uit e-CF)	A.7. Volgen van technologische ontwikkelingen	Niveau 3
	E.3. Risicomanagement	Niveau 3
	E.8. Informatiebeveiligingsmanagement	Niveau 4
Algemene competenties	G.2. Projectmanagement	Niveau 3
	G.3. Communicatie en overtuigingskracht	Niveau 3
	G.6. Management	Niveau 3

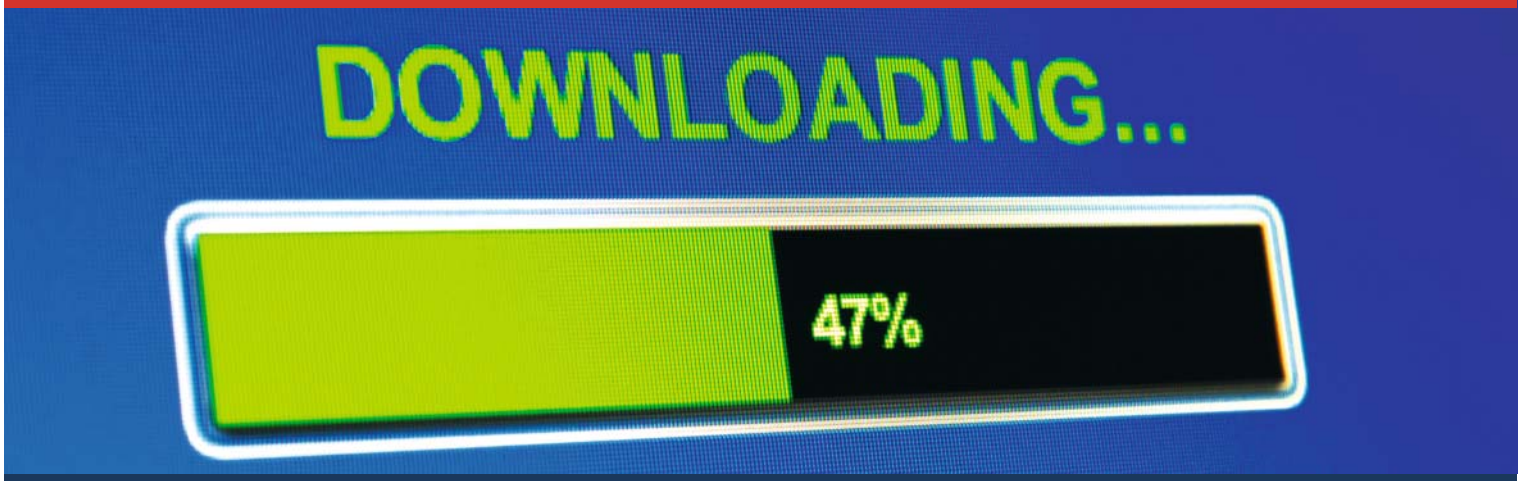
De relatie met andere ICT-beroepsprofielen

Naast de vier IB-profielen is de onderlinge taakverdeling met betrekking tot de aspecten security, risk en compliance van 5 e-CF profielen onderzocht (van CIO, Business Information Manager, Enterprise Architect, Systems Architect en Quality Assurance Manager). Daarbij is de onderlinge taakverdeling onderzocht en of die leidt tot een constructieve samenwerking tussen de professionals.

Europa in

In september 2013 zijn op een bijeenkomst van het CEN (European Committee for Standardization) in Brussel aan vertegenwoordigers van de 28 lidstaten van de Europese Unie, de eerste resultaten van de PvIB-werkgroep Kwalificaties besproken. In mei wordt een terugkoppeling gegeven van de resultaten aan de CEN Workshop on ICT Skills.

Profieltitel	CHIEF INFORMATION SECURITY OFFICER (CISO)	
Samenvatting	Definieert de informatiebeveiligingsstrategie en organiseert en stuurt de informatiebeveiliging van de organisatie overeenkomstig de behoeften en de risicobereidheid van de organisatie.	
Kerntaken	• Definieert de informatiebeveiligingsstrategie voor de organisatie • Zorgt voor een projectportfolio voor informatiebeveiliging • Organiseert informatiebeveiliging en de daarvoor benodigde expertise • Initieert organisatiebrede informatiebeveiligingsactiviteiten en -projecten • Zorgt voor organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging • Borgt de kwaliteit van informatierisicoanalyses, beveiligingsontwerpen en -oplossingen • Borgt het naleven van de eisen en architectuur voor informatiebeveiliging • Borgt informatiebeveiligingsbewustzijn binnen de organisatie • Borgt dat de organisatie voldoende voorbereid is op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's • Borgt de kwaliteit van informatiebeveiligingsassessments, -tests, -reviews en -audits • Zet een informatiebeveiligingscalamiteitenorganisatie op • Coördineert de reactie op ernstige informatiebeveiligings- of ICT-incidenten • Doet aanbevelingen aan senior algemeen management	
e-Competenties (uit e-CF)	D.1. Strategieontwikkeling informatiebeveiliging	Niveau 5
	E.3. Risicomanagement	Niveau 4
	E.4. Relatiemanagement	Niveau 4
	E.8. Informatiebeveiligingsmanagement	Niveau 5
Algemene competenties	G.1. Leiderschap	Niveau 4
	G.6. Management	Niveau 4
	G.3. Communicatie en overtuigingskracht	Niveau 4
	G.5. Organisatiesensitiviteit	Niveau 4



PATCHED

In the previous issue of this article we looked at the SABSA Business Attribute 'Risk Managed', taking the very highest level 'helicopter view'. In this issue we shall examine a detailed technical example – looking from the bottom up, rather than from the top down.

Software patching is a standard security measure for maintaining the integrity of IT systems, and hence the business functionality that they perform and the business goals and success factors that they support. It is a conventional 'control strategy'. We should keep our systems patching up to date. Simple! Or is it?

The primary concern of patching is that there are vulnerabilities in complex software systems that become known as exploits for hacking and malware attacks. Software vendors issue patches and system managers apply the patches. However, there are many more aspects of patch management that bring more complex, unintended, incidental threats and vulnerabilities and therefore put the business at risk.

The standard approach is based up on the assumption that the patches will work perfectly. This is known from experience not to be the case. A patch is a software modification to fix an original flaw in a program, and so it is just another piece of code to be deployed and 'inserted' into the software. It will often delete previous code and previous parameter settings, over-writing them with new stuff. In a complex operating system environment such a change will often touch many parts of the system, parts that are shared with other applications that have a dependency on OS functionality. How will these other applications be affected? Hmmm – now we see that there are potential uncertainties here that may have been overlooked.

This means that patch management is not just a simple exercise in applying the patches. It needs an end-to-end process that takes account of the other incidental risks. Typically there will be hundreds, even tens of thousands of platforms to be patched. The patch management process should begin with creating a state of 'patch-readiness', meaning having the process itself in place and tested for it's own suitability. Some of the key steps to be incorporated into the process should include:

1. Make the patch management process an integral sub-process of business continuity management. Ensure that patch management will enable business and not hinder it.
2. Assess the business criticality of IT systems so that priority in patching can be decided based on critical need.
3. Ensure good vulnerability intelligence from CERT bulletins and the like, so that zero-day attacks can be identified and likely consequences assessed. This is an essential aspect of patch prioritisation – which ones should be applied first and what sequence of patches is the best. Some at least will be recursive patches – patches on patches.
4. Test each patch on a test platform to assess its effects on overall system performance. Assess the risks of patch failure.
5. Always develop a regression plan before applying any patch in a live production environment. This may require having a disk image of the unpatched state, because many patches are irreversible once applied.
6. The regression plan should also be tested thoroughly to ensure that it would work if needed.
7. Roll out the patches in a systematic way according to the priorities identified and monitor the impacts on live production systems in case the patch testing has failed.
8. Give careful thought to the patching of BYOD environments. This means considering the very architecture used to enable BYOD. We shall address this topic in more detail in the next article in this series, to be called 'BYOD Enabled', so watch this space.

The SABSA approach requires us to consider all aspects of risk from a business perspective, not just applying controls in a blind, uninformed fashion. Far too often the application of security controls is done without this type of holistic consideration.

The Attributer

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

HEARTBLEED KWETSBAARHEID

Hier de analyse van een stuk software waar het internet op is gebouwd:

- 300,000 lines of code
- No central architectural authority
- 6,740 goto statements
- Inline assembly code
- Multiple different coding styles
- Obscure use of macro preprocessors
- Inconsistent naming conventions
- Far too many selections and options
- Unexplained dead code
- Misleading and incoherent comments

Die analyse kon worden gemaakt omdat het stuk software een open source programma is, OpenSSL. Het programma dat de afgelopen weken in het nieuws was door de HeartBleed kwetsbaarheid. Maar is dat geen contradictio in terminus? Open Source betekent toch dat iedereen de code kan controleren? Veel ogen kijken toch mee tijdens de ontwikkeling? Dan moet het toch goed zijn? Hoe kon dat lek ontstaan? *(bron analyse: http://queue.acm.org/detail.cfm?id=2602816)*

Maarten Hartsuijker

Hoewel open source je de mogelijkheid biedt om een code analyse uit te voeren, wil dat natuurlijk niet zeggen dat dit op grote schaal gebeurt. Vermoedelijk is het tegendeel waar. Ik ben nog nooit een bedrijf tegengekomen dat elke update van een open source product uitstelt tot de interne code analyse gereed is. Wel zie ik bij klanten dat open source code naar behoeven wordt uitgebreid. Bijvoorbeeld omdat een CMS framework voor 90% voldoet, maar net dat beetje customizing nodig heeft om goed bij de organisatiewensen aan te sluiten.

Ondanks dat open source een beveiligingsmeerwaarde *kan* hebben, kleven er ook een hoop risico's aan. Ook aanvallers kunnen immers zeer gericht op zoek gaan naar kwetsbaarheden. Een kwaadwillende aanvaller zal de gevonden kwetsbaarheden voor eigen gewin gebruiken en niet melden aan het open source project.

Elk softwareproject bevat beveiligingsfouten. Afhankelijk van het beveiligingsbewustzijn van de programmeurs zullen dat er veel of weinig zijn. Daarnaast bestaat er, net als bij closed source, ook een risico dat er doelgericht beveiligingsfouten aan open source software worden toegevoegd. De meeste open source projecten hebben een schrijnend tekort aan vrijwilligers. Een handige programmeur die de tijd neemt om eerst wat waarde toe te voegen aan een open source project, zou als vast lid van een team vermoedelijk relatief eenvoudig een bewuste kwetsbaarheid kunnen introduceren. Afhankelijk van de kwaliteitscontrole van een project sijpelt zo'n fout dan via software distributies langzaam door in de op internet aanwezige servers.

De mogelijkheid om programmacode te kunnen controleren is een groot goed. Maar als we er echt de meerwaarde van willen ervaren zouden we er als IT industrie meer gebruik van moeten maken.


Lex Borger


Maarten Hartsuijker


André Koot

Lex Borger

Software produceren van kwaliteit is moeilijk. Software controleren op kwaliteit is nog moeilijker. Daarom wordt vaak gestopt met een programma verbeteren als de testresultaten goed zijn. Maar vele van de hierboven genoemde analyseaspecten vind je niet met testen. Kwaliteit wordt alleen gerealiseerd middels discipline, van de programmeur en van de code-inspector. Bij een aantal taken kan analyse door software handig zijn als maatstaf, maar ook dan bepaalt de programmeur wat de invulling is.

Bepaalde zaken zien we liever niet in software: goto statements en inline assembly code. Bepaalde zaken ontstaan gewoon over tijd, zoals codeerstijlen en 'dode' code. Bepaalde zaken vergen discipline, zoals naamgevingsstandaarden, goed commentaar toevoegen en opties beperken.

Verbaast deze analyse van de OpenSSL code mij dus? Nee. Heeft hier iemand zitten slapen bij de controle? Nee. Mag je verwachten dat open source software kwalitatief goed is? Nee, tenzij er een partij is die hier verantwoordelijkheid voor wil nemen. Bij OpenSSL wordt deze rol genomen door de OpenSSL Software Foundation. En die zijn actief en lijken deze rol serieus in te vullen. Daarmee voorkom je niet dat er een fout insluipt en dat die onopgemerkt blijft.

Het antwoord is niet dat je moet verwachten dat reviewers alle code voor je gaan inspecteren en hun bevindingen netjes gaan rapporteren. Het enige antwoord hierop is defensief programmeren. Dit is te bereiken met de eerder genoemde discipline, en met een goede invulling van de governance door de OpenSSL Software Foundation. Hierbij hoort wél dat als er een bevinding gerapporteerd wordt, er vervolgens iets mee gedaan moet worden.

Was dit allemaal op zijn plaats geweest, dan was Heartbleed in zijn totale omvang niet mogelijk geweest. Dat dit wel gebeurde hoort de OpenSSL Software Foundation zich aan te trekken. En ook alle andere open source governance bodies, want OpenSSL heeft echt niet een uitzonderingspositie hierin.

André Koot

Een paar jaar geleden liep ik op de PvIB stand op Infosecurity een bekende ICT jurist tegen het lijf die mijn een simpele vraag stelde: Is open source software veiliger dan gesloten source software? Mijn antwoord: Ik heb geen idee. Ik zou misschien kunnen (laten...) uitzoeken hoe veilig een stuk open source software is, maar ik zou erop vertrouwen dat een gesloten source pakket veilig is. Wat mij betreft is er ook geen discussie wat er veiliger is. Nee, dat tendeert bijna naar een religieuze vraag, ik denk dan ook dat het een kwestie van geloof is wat veiliger is. Geloof je in het principe van open source, of niet. En van beide stellingen is het bewijs de afgelopen maand weer onderuit gehaald. Heartbleed bewijst dat het feit dat veel ogen mee kunnen kijken niet per definitie inhoudt dat vele ogen dat ook goed doen. Maar een paar dagen later bleek een lek in Internet Explorer, doordat een zero-day (via Flash) in de praktijk misbuikt werd. Het uitgangspunt dat het niet openbaar maken van code de veiligheid verbetert, is daarmee ook weer eens onderuit gehaald. Het is misschien inderdaad een religieuze discussie. Nu hang ik persoonlijk wel de theorie aan dat het feit dat meerdere ogen mee kunnen kijken, in potentie betere software oplevert. Er is enig bewijs voor die theorie. De firma Coverity scant softwareprojecten op de aanwezigheid van softwarefouten (1). En de afgelopen jaren bleken open source producten een betere kwaliteit te hebben dan commerciële tegenhangers. Maar daar valt tegenin te brengen dat we geen idee hebben van welke tegenhangers van Linux, MySQL, Apache Hadoop en nog wat andere open source producten zijn beoordeeld. Dat kunnen ook wel obscure producten zijn. Dat OpenSSL niet tot de toppers hoort mag duidelijk zijn. Maar dat is geen bewijs voor de stelling dat het open source model van systeemontwikkeling daarmee ook onveilige software oplevert. Net zomin als dat een lek in Internet Explorer het failliet van gesloten softwareontwikkeling aantoont.
Wat wel relevant is, is dat je bij inzet van welk product dan ook een risicoanalyse moet uitvoeren en dan kunnen analyses zoals de bovengenoemde wel eens heel relevant blijken te zijn.

Link: http://softwareintegrity.coverity.com/rs/coverity/images/2013-Coverity-Scan-Report.pdf

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)
Ronald van Erven (Timeos Pensioendiensten)
Maarten Hartsuijker (ANWB)
André Koot (Strict)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)
Martijn Veken (SNS REAAL)

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 2014
De abonnementsprijs in 2014 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

BETROUWBARE BEROEPEN

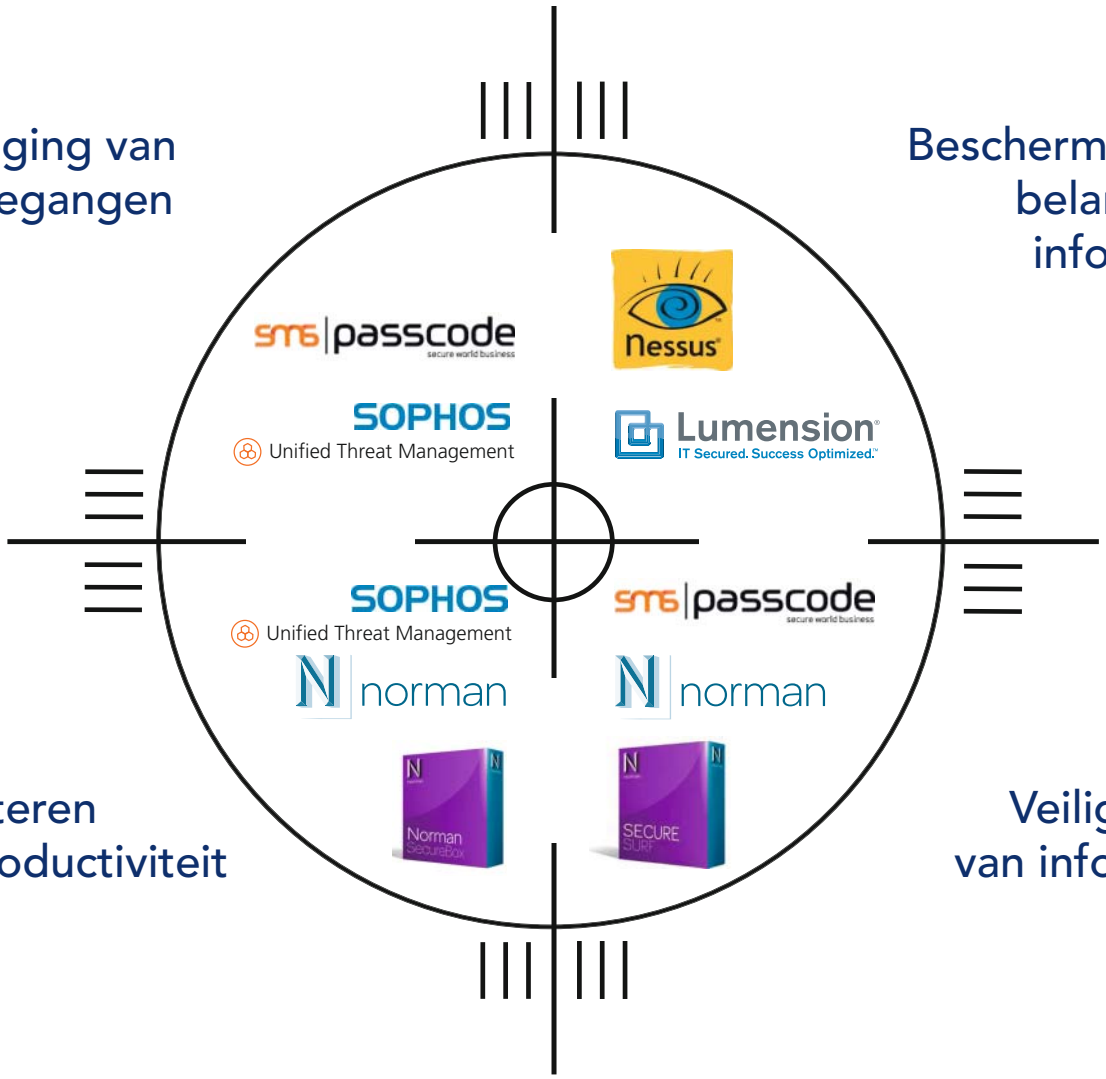
Gistermiddag kwam ik iemand tegen die mij vertelde dat hij melkboer was. Mijn kleinzoon (7 jaar) vroeg mij wat dat was. Ik legde hem dat uit en in mijn verhaal ging ik van de melkboer naar de schillenboer, de kolenboer en zo kwamen er nog een aantal beroepen voorbij die inmiddels al lang uit het straatbeeld zijn verdwenen. Nadat ik mijn kleinzoon naar huis had gebracht bleef mijn brein continu beroepen voortbrengen die er niet meer waren. Bankmedewerkers, videotheekmedewerkers, fotozaakmedewerkers en het bleef maar doorgaan. Mijn vrouw ziet altijd heel scherp als ik weer zo'n bui heb en raadde mij aan om eens aan beroepen te denken die er de afgelopen 25 jaar zijn bijgekomen. Het duurde even voordat mijn hoofd weer beroepen ging voortbrengen, maar uiteindelijk ging het weer los: hackers, marktplaatszwendelaars, pinpasfraudeurs, toeslagenmisbruikers. Mijn vrouw stuurde mij weer bij met de mededeling een positief beroep te bedenken. Ook hier had ik weer wat last van opstartproblemen, maar uiteindelijk lukte me het weer een stroom beroepen voort te brengen, privacy officers, risk officers, compliance officers, information security officers, de stroom Engelstalige beroepsgroepen bleef maar aanzwellen.
Ik werd er flauw van en ging mij bedenken hoeveel van die medewerkers in mijn bedrijf werkzaam zijn. Ik was al snel de tel kwijt en bij de dertig ben ik maar gestopt. Ik denk dat ik de helft vergeten ben van de functies die min of meer rechtstreeks met informatiebeveiliging hebben te maken. Allemaal medewerkers die niet direct onderin de piramide aan het werk zijn, allemaal medewerkers die bekwaam zijn in het opschrijven wat beter kan en wat veiliger moet. Het is ook geen keus van mijn organisatie om zoveel van die medewerkers in dienst te hebben. Dat wordt afgedwongen door onze toezichthouders (weer een nieuwe beroepsgroep) die vinden dat mijn organisatie zich goed moet voorbereiden op het onzichtbare kwaad van buitenaf en van binnenuit. Tegen het kwaad van buitenaf kun je jezelf beschermen middels de aankoop en implementatie van producten. De vele tonnen die daarin gaan zitten beschermen ons tegen aanvallen. Mijn grootste zorgen zitten niet in de aanvallen van buitenaf maar meer in het gedrag van onze medewerkers. Beroemd zijn de verhalen dat er weer eens stukken in de trein lagen die uiteindelijk zeer vertrouwelijke informatie bevatten. De onbeveiligde USB-stick die uit de jaszak is gerold met ons volledige klantenbestand. De CD met klantgegevens die tegen alle werkinstructies in eens een keer als leesbare tekst is gebrand. De aangeschoten medewerker die graag mag vertellen wat er binnen ons bedrijf allemaal niet goed zit, de Facebook-gebruiker die zijn persoonlijke frustratie op dit sociale mediakanaal achterlaat. De medewerker die een net te groot huis heeft gekocht en via zwakheden in onze eigen omgeving zichzelf verrijkt.
Bij het nalezen van deze opsomming verbaas ik mij dat ik nog over een goede nachtrust beschik. Op dit moment zijn de grote accountantskantoren bezig met het voorbereiden van de grote Europese stresstest voor banken. Tientallen miljoenen euro's worden uitgegeven om ons een stuk zekerheid te geven. Om ons een veilig gevoel te geven, met nadruk op gevoel, want het wordt niet betrouwbaarder door een test. Een bank kan alle stresstesten doorstaan, maar als ze er achter komen dat een betrekkelijk kleine groep bankmedewerkers een rentestand probeert te beïnvloeden, zak je als een baksteen van de betrouwbaarste bank naar de meest onbetrouwbare plek op de lijst. Hebben die medewerkers het voor hun eigen gewin gedaan? Ik weet het niet, ik probeer mij zoveel mogelijk van deze perverse hebzucht weg te houden maar ik heb mijn twijfels. De fraude bij banken is door niemand meer te herkennen, laat staan te begrijpen. De melkboer was niet in staat te frauderen, want die werd onmiddellijk afgestraft door zijn klanten. Maar ja, de melkboer komt niet meer terug…

Berry

Human factor and security

Beveiliging van ICT toegangen

Beschermen van belangrijke informatie



Verbeteren van productiviteit

Veilig delen van informatie

Waar zitten uw risico's in het ICT-landschap? Adequate beveiliging door een ervaren, betrouwbare en loyale partner is meer dan ooit noodzaak. Crypsys is toonaangevend op het gebied van security analyse, advies en installatie bij overheden, semi-overheden, gemeenten, grote bedrijven en organisaties.

CRYPSYS secure computing

CRYPSYS secure computing 25 years

CRYPSYS Data Security BV Edisonweg 4 4207 HG Gorinchem **tel** +31 (0)183 62 44 44 **fax** +31 (0)183 62 28 48 **mail** sales@crypsys.nl **web** www.crypsys.nl

CRYPSYS is officieel distributeur van: Sophos, SMS Passcode, Norman, Adyton, Lumension en Nessus