iB
INFORMATIEBEVEILIGING
jaargang 12 2014
#7

SHELLSHOCK

Het begint met goede hygiëne: CSBN4

Open Source: open brief

Medewerkers: Hoe krijg je ze mee?

Maria Genova over identiteitsfraude

Data Risk Management

CYBER SECURITY 2014

The evolving cyber ecosystem

woensdag 12 november - Congrescentrum 1931 | Den Bosch

Keynote Generaal b.d. Dick L. Berlijn, Senior Board Advisor Cyber Security bij Deloitte

Keynote dr. Uri Rosenthal, special Envoy voor de Nederlandse regering voor Cyber Security

Lezing Don Eijndhoven, Principal Cyber Security Architect

Lezing Michiel Steltman, Directeur en Cyber Security Expert bij DHPA

Uw relatiecode: 15527/05

BUSINESS VALUE

Ik word regelmatig gevraagd om een snel oordeel te geven over de gevolgen voor de security naar aanleiding van een situatie of een nieuwsitem. In sommige gevallen kun je snel een algemeen oordeel geven, omdat de situatie zo ernstig is en vergelijkbaar ernstig voor iedereen. "ShellShock" valt wat mij betreft in die categorie. Op conceptueel niveau is de bedreiging duidelijk: Wanneer een web-interface de bash shell gebruikt, dan kunnen er d.m.v. ShellShock ongemerkt commando's toegevoegd worden, die dan uitgevoerd worden op de server, met de hoge rechten van het service proces. Maar daarover in de rest van deze uitgave meer...In de meeste gevallen kun je echter geen duidelijke mening vormen zonder de business beter te kennen. Wat is bijvoorbeeld de consequentie van het geven van root rechten op een server aan functioneel beheer? Dan zijn mijn eerste vragen wat het belang is van de server, hoe de rechten verdeeld zijn, wat functioneel beheer met die rechten doet en waarom dat niet anders kan. In andere gevallen denk ik zelfs wel eens "waar maak je je druk om?" Als je dan gaat analyseren hoe het komt dat men zich druk maakt, dan heeft het te maken met afspraken uit het verleden. Een verleden zonder internet, zonder hackers en zonder online business transacties en met een heel andere dynamiek - veel trager. De afspraken zijn niet meer van deze tijd.

Even terug naar mijn voorbeeld van root rechten voor functioneel beheer. Het is helemaal niet vreemd dat functioneel beheer online de status wil kunnen zien van allerlei infrastructuurelementen, in plaats van iedere keer een verzoek te sturen naar de desbetreffende beheerder of helpdesk. Als de infrastructuur daar niet op is voorbereid, en de beheerder, onder enige managementdruk uitroept dat het alleen kan als de functioneel beheerders root rechten krijgen, dan is de businessbeslissing al snel om die root rechten te eisen. En terecht, ben ik geneigd te zeggen. Je bent op dat moment namelijk als IT-leverancier te kort geschoten. Dit had voorkomen kunnen worden als er in een eerder stadium gekeken was naar het business belang en hoe de IT-dienst daar waarde aan toevoegt.

Om business waarde goed te kunnen benutten is een duidelijke scopebepaling nodig voor de focus en zijn er structurele activiteiten nodig, zoals: verantwoordelijkheden beleggen, vaardigheden bijhouden, samenwerken met je partners, communiceren met stakeholders. Dit zijn kritieke randvoorwaarden, hier moet je eigenlijk dag in dag uit mee bezig zijn. Zwakheden in de uitvoering van deze activiteiten vormen een risico. Aanpakken hiervan vormt de basis van risicogebaseerd werken. Excelleren hierin zorgt dat je klaar bent om elke uitdaging aan te pakken die in dit verband op je af komt.

Lex Borger, hoofdredacteur

In dit nummer

HET BEGINT MET EEN GOEDE HYGIËNE

Vlak voor de zomer verscheen versie vier van het Cybersecuritybeeld Nederland (CSBN), dat in grote lijnen dezelfde conclusies toonde als het rapport van vorig jaar. Het belangrijkste verschil was feitelijk de toonzetting, dit jaar weer iets urgenter van aard. Maar wie moet de handschoen oppakken om structureel de beschikbaarheid van onze IT en de veiligheid van onze data te waarborgen?

Ook in de vierde editie van het CSBN waren woorden als weerbaarheid, vrijheid en veiligheid in het cyberdomein weer prominent aanwezig. Koning Willem Alexander refereerde zelfs expliciet naar cybercrime als onderdeel van de georganiseerde misdaad in zijn Troonrede van 16 september jongstleden. Die verwijzing zal deels gevoed zijn vanuit de wetenschap dat Nederland in 2015 gastheer is van de 4e internationale Cyber Security Conferentie. Dat wordt een interessant meetmoment om te zien in hoeverre we als Nederland tegemoet kunnen komen aan de constatering van minister Opstelten in het voorwoord van 'Nationale Cybersecurity Strategie 2; Van bewust naar bekwaam'.

Wat zegt het Cybersecuritybeeld Nederland?

De belangrijkste conclusie van het CSBN 4 is tweeledig en komt er in het kort op neer dat ICT steeds belangrijker wordt voor Nederland waar het betreft economische groei en innovatie. Daar staat tegenover dat veel vitale ICT-systemen en -applicaties nog steeds zeer kwetsbaar zijn voor aanvallen met als doel gegevensdiefstal, al dan niet in combinatie met het platleggen van de digitale dienstverlening. Als oorzaak wordt genoemd dat veel basismaatregelen nog niet op orde zijn, terwijl dit in feite een gevolg is van een aantal factoren.

Omdat de waarde van 'intelligence' groeit, is er een groter belang bij individuen, bedrijven en staten om toegang te krijgen tot digitaal opgeslagen informatie. Uit een eerder dit jaar verschenen rapport van RAND corporation met de titel Markets for Cybercrime Tools and Stolen Data; Hackers' Bazaar [1], blijkt dat er een volwassen structuur en economische modellen schuilgaan achter online criminaliteit en de middelen die ze beschikbaar stellen en gebruiken. Dit betekent dat er veel rekenkracht en hersencapaciteit gebundeld wordt om de zwakke plek in een systeem te ontdekken en te exploiteren. Deze kennis zorgt er bij veel Europese IT-managers voor dat security topprioriteit heeft in relatie tot hun datacenterplanning, volgens een in opdracht van Colt uitgevoerd 'Planning Anxiety' [2] - onderzoek.

Die zorg wordt ongetwijfeld gevoed door het feit dat er een behoorlijk aantal verouderde systemen in productie draait in Nederland. Een treffende illustratie is het project bij de Sociale Verzekeringsbank (SVB) voor de bouw van het multi-regelingen-systeem (mrs). Daar zal naar alle waarschijnlijkheid een sterk verouderd systeem [3] in productie blijven, dat niet aan de huidige duurzaamheidswens indachtig de Nationale Cybersecurity Strategie 2 voldoet. Bij Defensie zijn de tekortkomingen van de huidige IT-infrastructuur inmiddels onderkend en wordt de komende jaren veertig miljoen euro gereserveerd voor een grondige vernieuwing [4].

Wanneer bij dit project het adagium 'Security by Design' gehanteerd wordt, zoals zeker bij Defensie verwacht mag worden, kunnen er grote slagen gemaakt worden in de strijd tegen malversanten. De technologie en de manier waarop deze wordt ingericht, vormen echter maar een deel van de oplossing. Een ander bestanddeel bestaat uit het security-beleid en de praktische naleving hiervan. Deze is in theorie geborgd door toepassing van methodieken als ITIL en Prince II, maar die verankering blijkt in de praktijk niet altijd een feit.

Tegenover het Security by design-streven, staat namelijk nog steeds de gangbare houding van security als 'afterthought'. Die is ingegeven door het ontbreken van een directe verbinding tussen de business en de information security officer. Lijnmanagers hebben te weinig een directe relatie met een dergelijke functionaris, als al aanwezig, om de risico's van een 'change' te bespreken. Bij voorkeur gebeurt zo'n excercitie door het mogelijk verlies en/of de diefstal van gegevens en de uitval van IT-diensten te ramen en er een kostenplaatje aan te hangen. Een dergelijke risicoanalyse schept veel duidelijkheid bij de bepaling of bijvoorbeeld een 'time to market'-voordeel opweegt tegen eventuele schade. Het startpunt is de CSI en de business-manager structureel bij elkaar aan tafel te krijgen. Dit geldt voor zowel publieke als private organisaties.

Ook op landelijk en internationaal niveau is een dergelijke setting wenselijk. Zo kan in Nederland de samenwerking tussen de overheid, het bedrijfsleven, de belangrijkste opleidingsinstituten en non-profit organisaties nog een stuk intensiever. Dit dient twee doelen:

1. Structurele informatieuitwisseling met daaraan gekoppeld een meerjarenplan, inclusief acties en gevolgen;
2. Consequente informatievoorziening aan de zakelijke en particuliere 'ICT-consument'.

Nico Siebelink is Technical Director Service Provider & Enterprise Northern Europe bij Juniper Networks en is bereikbaar via nsiebelink@juniper.net

In relatie tot punt twee valt namelijk te constateren dat veel ingezetenen van Nederland, anders dan we wellicht zouden denken, hun online hygiëne niet op orde hebben. Eerder dit jaar publiceerde EMC een Privacy Index [5], die concludeerde dat mensen basiszaken als softwareupdates, wachtwoorden op mobiele devices en back-ups niet op orde hebben. Er is dus zogezegd behoefte aan consequente en continue voorlichting, zodat mensen zelf de verantwoordelijkheid kunnen nemen in hun gebruik van apparaten waarmee online informatie wordt uitgewisseld.

Naar schatting komt ongeveer tachtig procent van de gevallen, waar mensen benadeeld worden door een vorm van online criminaliteit, voort uit een gebrekkige hygiëne op het vlak van cybersecurity. Momenteel zijn de educatieve activiteiten om dit te verbeteren, gefragmenteerd over overheden en het bedrijfsleven en gefocust op deelkwesties, zoals veilig bankieren of sociale media en privacy. Beter zou zijn een integrale aanpak, waarbij kinderen van jongs af aan de online mores leren, net zoals ze op de basisschool verkeersles krijgen. Dat is geen overbodige luxe gezien vandaag de dag peuters en dreumesen al op een tablet de wereld verkennen.

Deze algehele bewustwording is feitelijk laaghangend fruit, zeker gesteld tegenover de veel complexere uitdagingen die in de laatste editie van de Nationale Cyber Security Strategie naar voren komen. Koning Willem Alexander gaf in zijn Troonrede al aan dat 'Alles met alles samenhangt' met als gevolg dat cyber-vraagstukken vaak grensoverschrijdend en complex zijn. Dit heeft een enorm vertragend dan wel verwaterend effect op wet- en regelgeving, of we nu naar de Europese Cyber Security Directive kijken of naar de Wet Computercriminaliteit III. Daarnaast kost het bedrijven vervolgens substantieel tijd om te voldoen aan deze wet- en regelgeving; tijd die beter geïnvesteerd kan worden in het anticiperen op aanvallen. In dat opzicht ligt de handschoen bij de private sector om zichzelf en haar klanten te beschermen, daarbij risicomanagement zoals hierboven beschreven te omarmen.

Een goed voorbeeld van een privaat initiatief is de Nationale Wasstraat [6] van de Nationale Beheersorganisatie Internet Providers (NBIP), waarbij een aantal hostingproviders en middelgrote isp's aangesloten zijn. De NaWas is op een centrale plek ingericht, beschikt over geavanceerdere anti-DDoS apparatuur van verschillende merken en biedt ruime bandbreedte om DDoS-aanvallen te counteren. Door deze gezamenlijke aanpak kunnen ook kleinere klanten van de hosters en ISP's een beroep doen op deze dienst en zo hun eigen security-niveau verhogen.

Bij dit initiatief springt vooral de focus op het grotere kader in het oog. Wanneer we dat extrapoleren naar de wereldwijde situatie, dan zien we de Verenigde Staten, de Europese Unie en Nederland werken aan eigen security-standaarden en best practices. Het gevolg is vaak onnodige redundantie en mogelijk worden er zelfs nieuwe conflicten gecreëerd. Er is een wereldwijde harmonisatie nodig om tot gezonde omgangsvormen te komen. Daarbij kunnen specifieke activiteiten veroordeeld en gesanctioneerd worden, bijvoorbeeld wanneer ze duidelijk tot doel hebben om een bepaalde infrastructuur of processen te verlammen. Door een dergelijk document te creëren en te ondertekenen, ontstaat eenduidigheid in welke feiten bedreigend zijn voor een samenleving en internationaal strafrechtelijk vervolgd mogen worden.

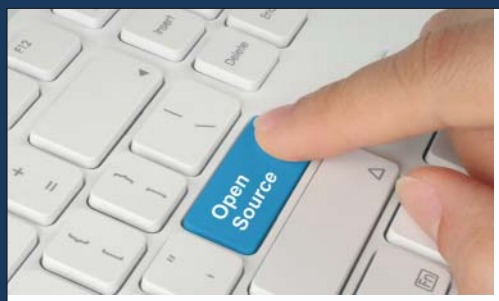
Samenvatting

De meest recente versie van het Cybersecuritybeeld Nederland levert geen verrassingen op en appelleert aan de urgentie van online criminaliteit als bedreiging voor het bedrijfs- en maatschappelijk leven. Dit wordt veroorzaakt door de professionalisering van de kwaadwillenden, de beperkte middelen die individuen en organisaties tot hun beschikking hebben om zich te weren, een tekort aan gekwalificeerde ICT- en security-professionals en onduidelijkheid over verantwoordelijkheden.

Om cybercriminaliteit structureel het hoofd te bieden is een wereldwijde consensus nodig op het gebied van standaardisatie en definities van cybercrime. Tegelijk moeten bedrijven intern en naar hun stakeholders toe de verantwoordelijkheden duidelijk stellen en daarnaar handelen. Tot slot is continue educatie en bewustwording nodig om mensen de basisbeginselen bij te brengen van online veiligheid. Dit moet een gezamenlijke en goed geregisseerde activiteit zijn van overheden, bedrijven en non-profit instellingen.

Bronnen

[1] Het rapport 'Markets for Cybercrime Tools and Stolen Data': http://www.rand.org/pubs/research_reports/RR610.html
[2] Het Planning Anxiety-onderzoek van Colt is te downloaden vanaf http://information.colt.net/planning-anxiety-research-2014
[3] Artikel op Zorgvisie: http://www.zorgvisie.nl/Financien/Nieuws/2014/7/Gemeenten-Uitvoering-pgb-loopt-gevaar-1565224W/
[4] Lees artikel op Computable: http://www.computable.nl/artikel/nieuws/overheid/5173694/1277202/defensie-steekt-komende-jaren-40-miljoen-in-ict.html
[5] Lees het volledige rapport op http://www.emc.com/campaign/privacy-index/index.htm?pid=home-emcprivacyindex-120614
[6] Meer informatie hierover staat op http://www.nbip.nl/anti-ddos/



HEARTBLEED EN HET RISICO VAN OPEN SOURCE SOFTWARE!

Heartbleed maakt de risico's van open source software duidelijk herkenbaar. Het is een van de grootste risico's van dit moment. Heartbleed is een lek waarbij hackers gebruik maken van een fout in de software om de beveiliging van een systeem te omzeilen. Het geeft direct toegang tot bijvoorbeeld login gegevens van gebruikers, of privacygevoelige informatie. Zelfs smartphones zijn ermee besmet. Bring Your Own Device is daarmee een net zo groot veiligheidsrisico geworden. Een lek op een lek, je zou voor de aardigheid het risico daarvan eens moeten berekenen. Durf er zelf niet eens aan te beginnen.

20 InformatieBeveiliging MAGAZINE

heartbleed en het risico van open source software!

Nu kunnen we onze schouders ophalen en zeggen dat het niet zo'n vaart loopt, waarschijnlijk breken ze alleen bij mijn buurman in! Heartbleed laat duidelijk zien dat er zeer grote risico's verbonden zijn aan het gebruik van open source software.

Wat is open source software?

Een toeëppplicatie ontstaat uit een idee. Dit kan een idee van een of meerdere mensen zijn. Dit wordt omgezet naar een eerste rudimentaire versie van de software en uitgezet op het internet. Via fora en dergelijke wordt het idee met versie 0.1 van de software opgepikt door de massa. Op de website van de oorspronkelijke ontwikkelaar staat de applicatie met de sourcecode van de software. Deze wordt door velen gedownload en geprobeerd. Is noem het hier proberen, want meer is vaak niet mogelijk. Op de website staat ook een oproep voor donaties. Deze donaties kunnen gedaan worden door geld te storten en/of door mee te helpen aan de verdere ontwikkeling van de oplossing. Laten we even het maar helpen met de ontwikkeling verder onder de loep nemen.
Een gemeenschap ontstaat, deze wordt onderverdeeld in teams die onderdelen verder ontwikkelen. Op deze manier ontstaan de vervolgversies. Deze software kan op een aantal manieren aan de markt aangeboden worden. De eerste waar iedereen aan denkt is dat het volledig gratis is, en ja uiteraard is het mogelijk een donatie te doen. Daarnaast zijn er business modellen waarbij er services aangeboden worden of dat er een bedrag betaald moet worden. Allelai variaties zijn mogelijk. Uiteraard moet natuurlijk altijd zijn dat de makes er meer of minder geld mee verdienen. Ik bedoel hier niet dat de doelstelling altijd is om er veeelijk rijk mee te worden. Een belegde boterham wordt ook al vaak als goed resultaat gezien.

Het ontstaan van Heartbleed

Laten we nu eens kijken hoe Heartbleed is kunnen ontstaan. Er zijn een aantal oorzaken. OpenSSL is zeer populaire software. Het wordt letterlijk door honderdduizenden organisaties gebruikt. Deze organisaties hebben bij elkaar afgelopen jaar bijna ? 2.000 aan donaties overgemaakt! In totaliteit wat te verstaan. Dit is dus de jaaromzet van OpenSSL. Deze software beveiligt het hele hebben en houden van organisaties en individuen. Inclusief de zwaar bediscussieerde en bevochten privacy.
De eerste oorzaak is hier al uit op te maken. Er was domweg niet voldoende kapitaal een fatsoenlijk product op de markt te zetten en anderzijds is de markt totaal niet geïnteresseerd in een goed product. Als iedere gebruiker ? ? had gedoneerd waren er wele honderdduizenden of zelfs miljoenen euro's aan kapitaal beschikbaar geweest om een fatsoenlijk product op de markt te zetten. Dit probleem is dus niet alleen de maker(s) aan te rekenen maar ook onszelf. Dit is een uniek probleem. Dit is bijzonder populaire software, je kunt dus niet stellen dat er te weinig interesse is. Het gezegde dat je krijgt waarvoor je betaald, doet hier zeker opgeld.
Dit was echter niet het enige probleem! Een product wordt ontwikkeld door een team. Je hebt ontwep, bouw en kwaliteitscontrole. Als je naar de sourcecode kijkt van OpenSSL kun je vaststellen dat het een spaghetticode is. Het is zeer moeilijk te lezen, documentatie is niet van een makkelijk begrijpbare soort! Allemaal zaken die het moeilijk onderhoudbaar maken. Er was gewoonweg niet voldoende mankracht. Conclusie is dat de software niet of nauwelijks te onderhouden is. Het lijkt heel veel op software waar voortdurend aan bijgebouwd is, zonder de overtollige delen eruit te halen. Dit lijkt meer op het weld dus afblijven principe dan professioneel en structureel dagelijk werk. Dit is kunnen ontstaan omdat er gewoonweg te weinig mensen in het ontwikkelteam van OpenSSL zitten/zaten. Daardoor is een kleine softwaretuut met zeer grote gevolgen twee jaar lang ongemeld gebleven. Onbekend is hoevelen van dit lek op de hoogte waren en er misbruik van hebben gemaakt.
Het dogma eiven uit te gaan dat als het mogelijk is, het ook werkelijkheid is, is een goed dogma. Ga eivan uit dat ook uw organisatie het slachtoffer is van dit lek. Neem maatregelen! In het geval van Heartbleed is het simpel. De eerste stap is de software te controleren en indien nodig te patchen. Tweede stap is de vervanging van alle certificaten. Derde is het gebruik van Hardwear Security Modules waarin de certificaten opgeslagen worden. Deze vallelen van een smartkaart met cryptochip en kaartlezer tot en met een HSM voor inbouw. Een en ander afhankelijk van de performance die nodig is. De HSM moet wel minimaal voldoen aan Common Criteria EAL4+ level. Dit is dus een eenvoudige oplossing voor Heartbleed en andere lekken/inbraken die gebruik maken van zachte certificaten (certificaten opgeslagen in software).

Frans Bolk is algemeen directeur bij Uniq-ID en bereikbaar via frans.bolk@uniq-id.nl

21 InformatieBeveiliging MAGAZINE

OPEN BRIEF AAN FRANS BOLK

Frans Bolk heeft in IB magazine 2014 #5 een 'marketing' artikel geplaatst, getiteld 'Heartbleed en het risico van open source software'. Helaas bevat dat artikel flink wat onwaarheden die wij proberen op te lossen door een eigen artikel te schrijven met behulp van open source software.

Arnim Eijkhoudt, docent en onderzoeker in IT Security en Digital Forensics, Hogeschool van Amsterdam. Hij is te bereiken via Twitter: @zaanpenguin

Jeroen van der Ham is docent en onderzoeker System and Network Engineering bij de Universiteit van Amsterdam. Hij is te bereiken via Twitter: @1sand0s

Oscar Koeroo is werkzaam bij KPN in het CISO Strategy & Policy team op de hoofdstukken cryptografie, identity en netwerkbeveiliging. Hij is te bereiken via @okoeroo

Rashid Niamat, journalist. Hij is te bereiken via @rniamat

Michiel Klaver is Linux/Unix expert bij internetprovider Luna.nl. Hij is te bereiken via Twitter: @MichielKlaver

Jo Lahaye is voorzitter HollandOpen, directie IRP.

Menso Heus is coördinator Internet Protection Lab. Hij is te bereiken via Twitter: @mensoh

Beste Frans Bolk,

Met grote interesse hebben wij je artikel gelezen in het InformatieBeveiliging Magazine van juni jongstleden. Je uitleg en begrip van de Heartbleed-bug en Open Source software baart ons grote zorgen en door middel van deze ingezonden reactie willen wij een en ander rechtzetten, verklaren en aanvullen.

Heartbleed is een bug in de oudere versies van de OpenSSL softwarebibliotheek. OpenSSL wordt bijna overal gebruikt, omdat OpenSSL lange tijd een van de weinig vrij beschikbare, maar volledige implementaties van cryptografie functies is geweest. De licentie van OpenSSL (de 'OpenSSL'- of 'SSLeay'-license) staat vrij gebruik toe; zelfs het opnemen van OpenSSL in gesloten commerciële software en hardware (zoals je browser, smartphone of auto!). Het is daarmee echter niet altijd duidelijk dat OpenSSL onderdeel is van de software of een apparaat, met als gevolg dat kwetsbaarheden niet altijd direct worden opgemerkt. De omzet (of het budget) van OpenSSL bedraagt daarnaast niet "? 2000", maar zo rond de $1 miljoen per jaar, onder andere door donaties van privégebruikers en grote bedrijven/organisaties als de Amerikaanse Department of Homeland Security en de Department of Defense [1].

In je artikel komt het duidelijk naar voren dat je geen hoge dunk hebt van Open Source software. Dat bevreemdt ons, aangezien het Internet gebouwd is op Open Source software en Open Standaarden (bijvoorbeeld protocollen: afspraken over/voor communicatie). De open implementaties uit de begintijd vormen ook tegenwoordig nog de uitgangspunten voor software, diensten en netwerken, inclusief die van commerciële bedrijven als Microsoft, Apple, enzovoorts. Bovenop deze basis is het World Wide Web ontwikkeld (door Tim Berners-Lee). Wederom gebeurde dat niet op basis van gesloten software en protocollen, maar door het openbaar specificeren en vrij beschikbaar en implementeerbaar maken van de de onderliggende standaarden. Open Source software-implementaties van webservers, zoals Apache en Nginx webservers, vormen daardoor verreweg het grootste deel van de webservers op het Internet. Van alle webbrowsers die we op dit moment kennen, is het grootste deel eveneens Open Source: Chrome, Firefox en zelfs delen van Safari, ondanks dat zij worden ontwikkeld door commerciële teams (zie bijvoorbeeld Apple [2]).

Het is eigenlijk een principiële vereiste dat implementaties van cryptografische functies voor veilige communicatie 'Open Source' moeten zijn. Alleen bij dergelijke implementaties kan men onafhankelijk van de ontwikkelaars verifiëren dat cryptografische functies op een correcte wijze zijn geïmplementeerd, zodat men zeker weet dat informatie onderweg niet kan worden afgeluisterd of aangepast. Dit is ook wel bekend als het Kerckhoffs' principe [3], genoemd naar een belangrijke Nederlandse cryptografisch expert. Alle gangbare implementaties van cryptografie zijn om die reden Open Source (en vaak Open License): niet alleen OpenSSL, maar ook LibreSSL, GnuTLS, PolarSSL (oorspronkelijk van het bekende Nederlandse commerciële beveiligingsbedrijf Fox-IT), NSS, CyaSSL en axTLS. Sterker nog: als de Heartbleed-bug één beveiligingsprobleem heeft blootgelegd, is het de risico's van gesloten software. Open Source pakketten die gebruikmaken van OpenSSL zijn na bekendwording van de Heartbleed-bug snel bijgewerkt om het probleem op te lossen. Bij gesloten software kun je als derde partij slechts hopen dat deze problemen tijdig en correct worden opgelost; echte verificatie volgens het Kerckhoffs' principe blijft echter niet mogelijk.

Wat je schrijft onder "Risico's Open Source software" bevreemdde ons eveneens. Je schuift 'goedkope' gesloten software onder dezelfde noemer als Open Source software. Tevens noem je allerlei doemscenario's van lekkende software, die alleen maar op te lossen zijn door je telefoon in een koekblik te stoppen. Open Source geeft je juist de mogelijkheid om te inspecteren wat er nu precies gebeurt, het probleem eventueel op te lossen of onschadelijk te maken, al dan niet een eigen variant te maken en gebruiken. Die zou je daarna zelfs kunnen verspreiden om zo de originele versie uit de markt te drukken of de aanbieder ervan te dwingen de implementatie te verbeteren.

Je onderstreept daarnaast het belang van digitale certificaten: "De meest eenvoudige [...] is deze software te ondertekenen met een echt certificaat, dat wil zeggen van een erkende Certificate Authority (CA), bij voorkeur eentje van Nederlandse bodem onder Nederlands recht.". Het principe van digitale ondertekening heeft echter een ander doel dan je schetst in je artikel: een digitale ondertekening zorgt namelijk dat de manipulatie van informatie is te detecteren. Zogenaamde 'Digital Signature Algorithms' verzorgen deze functionaliteit met behulp van een certificaat dat door een erkende CA is ondertekend.

Hierdoor is de identiteit van de ondertekening te herleiden naar een natuurlijk persoon en kan de integriteit van de informatie worden gewaarborgd. Anders gezegd: digitale ondertekening wordt gebruikt ten behoeve van het controleren van de identiteit en integriteit van informatie. Versleuteling, waar de rest van je artikel echter over gaat, is een onderdeel van de bewaking van vertrouwelijkheid van informatie. Het mechanisme en principe achter digitale certificaten is niet gegarandeerd foutvrij: Certificate Authorities als DigiNotar en TURKTRUST gaven onterecht ondertekende certificaten uit, met ernstige gevolgen.

Je stelt tenslotte voor om de Heartbleed-bug te lijf te gaan door de inzet van zogenaamde Hardware Security Modules (HSMs). HSMs bieden een aantal functionaliteiten, zoals het beschermen van de sleutels die bij cryptografie worden gebruikt en het ondertekenen van digitale certificaten. De impact van de Heartbleed-bug is echter groter: dit zorgt voor een klein venster naar het werkgeheugen van een computer. Via dat venster heeft men een rudimentair inzicht in wat zich afspeelt in de computer op dat moment, waaronder mogelijke gevoelige informatie als netwerkverbindingen, wachtwoorden of cryptografische sleutels zou kunnen worden bemachtigd. Een HSM zal hierbij dus geen totaaloplossing kunnen bieden: hij zal slechts de cryptografische sleutels beschermen. Dat is weliswaar een begin, maar ook het lekken van de overige informatie kan een grote impact hebben op de veiligheid van gebruikers en organisaties.

Certificeringen op het gebied van informatiebeveiliging bieden eveneens geen absolute veiligheidsgarantie. Er zijn ook Nederlandse auditbedrijven geweest die -naar later bleek- onterecht een dergelijke certificering hebben afgegeven. Een certificering is uiteindelijk niets meer dan een momentopname; veiligheid is een continu proces dat onderdeel van het functioneren van een bedrijf moet zijn. Zo was het grote Amerikaanse retailbedrijf Target weliswaar in het bezit van relevante certificeringen (zoals PCI-DSS), maar is Target desondanks het slachtoffer geworden van een enorm datalek [4]. Nog recenter blijkt hetzelfde aan de hand te zijn geweest bij Home Depot [5].

Een punt waar we het roerend met je eens zijn, is dat je er gerust van uit kunt gaan dat elke organisatie vatbaar is (geweest) voor dit lek. Het is essentieel dat alle benodigde stappen worden doorlopen om een organisatie door te lichten en te beveiligen. Als er één ding is wat de Heartbleed-bug ons echter heeft geleerd, is dat een continue doorontwikkeling en verbetering van software (welke dan ook) essentieel blijft. Juist in deze tijd van diefstal van persoons- en betalingsgegevens, schandalen over het afluisteren door beveiligingsinstanties en het lekken van privéfoto's wordt het belang van goede beveiliging nog eens extra onderstreept. Daarom willen we via deze weg meteen een oproep doen aan alle lezers: doneer vandaag nog aan de ontwikkelaars van veilige, open cryptografische software!

Was getekend, met vriendelijke groet,

Arnim Eijkhoudt, docent en onderzoeker in IT Security en Digital Forensics, Hogeschool van Amsterdam
Jeroen van der Ham, docent en onderzoeker System and Network Engineering, Universiteit van Amsterdam
Oscar Koeroo, beleidsmaker voor o.a. het onderwerp cryptografie, KPN
Rashid Niamat, journalist
Michiel Klaver, Linux/Unix expert bij internetprovider Luna.nl
Jo Lahaye, voorzitter HollandOpen, directie IRP
Menso Heus, coördinator Internet Protection Lab

N.B.: deze reactie is geschreven op persoonlijke titel en niet representatief voor genoemde bedrijven/organisaties.

Contact info: @1sand0s of @zaanpenguin

Links

[1] **http://en.wikipedia.org/wiki/OpenSSL**
[2] **http://www.opensource.apple.com**
[3] **http://en.wikipedia.org/wiki/Kerckhoffs%27s_principle**
[4] **http://www.darkreading.com/risk/compliance/target-pci-auditor-trustwave-sued-by-banks/d/d-id/1127936**
[5] **https://corporate.homedepot.com/mediacenter/pages/statement1.aspx**

Reactie op open brief

Beste Arnim Eijkhoudt, docent en onderzoeker in IT Security en Digital Forensics, Hogeschool van Amsterdam, Jeroen van der Ham, docent en onderzoeker System and Network Engineering, Universiteit van Amsterdam, Oscar Koeroo, beleidsmaker voor o.a. het onderwerp cryptografie, KPN, Rashid Niamat, journalist, Michiel Klaver, Linux/Unix expert bij internetprovider Luna.nl, Jo Lahaye, voorzitter HollandOpen, directie IRP en Menso Heus, coördinator Internet Protection Lab.

Goed vast te stellen dat er met grote interesse gelezen wordt en dat jullie je zorgen maken. Kan mij daar volledig bij aansluiten. Heartbleed is inderdaad een bug in een oudere versie van de OpenSSL softwarebibliotheek die echter zeer veel gebruikt werd. Na het vaststellen van deze bug hebben veel organisaties de bugfix aangebracht. Verder is het gebruik van software, open of niet, altijd verbonden aan risico's. Risico wordt bepaald door de kans dat iets gebeurt en de schade die het kan veroorzaken. De kans dat iets gebeurt is afhankelijk van de technologie zelf, het proces waarmee het tot stand gekomen is en de organisatie. Bij Heartbleed waren alle drie niet goed. "OpenBSD founder Theo de Raadt has created a fork of OpenSSL called LibreSSL. He argues that OpenSSL is full of "discarded leftovers" and unreadable code."
Over de omzet (budget) het volgende. Ten tijde van Heartbleed was het vermogen volgens OpenSSL? 841 en een paar centen. Volgens een blog van Steve Marquess (waarschijnlijk wel bekend) "OSF typically receives about US$2000 a year in outright donations". Momenteel is dit gelukkig meer en zal het inderdaad rond de 1 miljoen zijn. Het in inmiddels inderdaad verhoogd, maar niet alleen door donaties. Grote organisaties en de Amerikaanse regering hebben ingezien wat het risico is van onder andere OpenSSL; zoals een zeer veel gebruikte software die kritisch is voor veel organisaties en slecht onderhouden wordt door "slechte backing". Ze hebben daarom een soort emergency fund beschikbaar gemaakt om dit soort risico's uit te sluiten. "OpenSSL will get a portion of the funding but likely nowhere close to the entire $3.9 million. The initiative will identify important open source projects that need help in addition to OpenSSL."

Steve Marquess bevestigd dit in zijn blog: "but all those donations together come to about US$9,000. Even if those donations continue to arrive at the same rate indefinitely (they won't), and even though every penny of those funds goes directly to OpenSSL team members, it is nowhere near enough to properly sustain the manpower levels needed to support such a complex and critical software product. While OpenSSL does "belong to the people" it is neither realistic nor appropriate to expect that a few hundred, or even a few thousand, individuals provide all the financial support. The ones who should be contributing real resources are the commercial companies and governments who use OpenSSL extensively and take it for granted."

Jullie aanname dat ik geen hoge dunk heb van Open Source software kan de spreekwoordelijke plank niet verder misslaan. Ik en wij gebruiken Open Source software, altijd al gedaan en zullen het ook blijven doen. Onze organisatie maakt dankbaar gebruik van standaarden, zowel dejure als defacto. We zijn alleen voorzichtig met het gebruik daarvan en de risico's; stellen altijd de vraag hoe groot het risico is, wat de consequenties zijn. Wij maken gebruik van o.a. x.500; x.509; ISO29115 en ISO29003 om maar een paar voorbeelden te geven. Als jullie deze standaarden kennen, weten jullie dat wij bewust moeten omgaan met risico's.

Het Kerckhoffs' principe klopt. Mijn vraag aan jullie is dit toe te passen op Heartbleed. Hier hebben wij te maken met te weinig funding en te weinig mensen voor onderhoud. Het Kerckhoffs' principe gaat ervan uit dat alles in voldoende mate aanwezig is. Als dat het geval is klopt het als een bus. Bij OpenSSL was dit niet het geval, dus is de implementatie van de cryptografische functie niet goed uitgevoerd dus "afluisterbaar". Ik blijf erbij dat ondanks het Kerckhoffs' principe door slecht beheerde software er een veiligheidslek ontstaan is. De private key was uitleesbaar bij alle organisaties die deze specifieke versie van OpenSSL gebruiken. Hadden ze gewoon de door jullie geroemde en door ons gebruikte standaarden, zoals bijvoorbeeld de Commen Criteria gebruikt of de ETSI standaarden was de private key NIET uitleesbaar geweest ondanks de bug in OpenSSL.

Jullie reactie op de titel "Risico's etc" geeft precies aan waarom het een risico is. Er vanuit gaan dat open source zonder risico is niet goed en niet waar. Vraag die over blijft is hoe groot dit risico is. Zoals jullie, gezien jullie achtergrond, weten is dit

voor iedere organisatie anders. De kans dat het voorkomt is groter dan in het verleden. Dit door het simpele feit dat het aantal Open Source software pakketten iedere dag groter en groter wordt en het aantal mensen dat onderhoud pleegt niet in dezelfde mate groeit. Daar zit dus een discrepantie die niet zomaar recht te trekken is. Ik stel vast dat er risico's zijn en dat organisaties moeten nadenken over hun risico's en daarmee hun veiligheid. Of het nu open of gesloten software is doet er niet toe. Veiligheid behoort een top prioriteit te zijn voor het strategisch management van een organisatie.
Open source geeft je inderdaad de mogelijkheid te inspecteren wat er precies gebeurt, het probleem eventueel op te lossen of onschadelijk te maken door een eigen variant te maken en te gebruiken. Vraag is echter hoeveel organisaties dit doen? Dat het kan, wil nog niet zeggen dat het gebeurt of een oplossing is. Ervaring leert dat het niet voldoende gebeurt en dan ben ik nog voorzichtig. Zie daarom niet hoe dit het risico verkleind voor organisaties?!

Goed te zien dat bekend is dat je met certificaten meer kunt doen dan alleen ondertekenen. Hoop dat je ook op de hoogte bent van de nieuwe wetgeving die afgelopen 1 juli ingegaan is? Hierin wordt het gebruik van de verschillende soorten certificaten wettelijk geregeld. Het is daarom van belang de Nederlandse of Europese certificaten te gebruiken. Deze vallen onder deze wetgeving. Uiteraard kun je met certificaten ondertekenen, vertrouwelijkheid garanderen, authentiseren en code signing doen. Jullie beschrijving van de HSM klopt helemaal. Wat jullie echter vergeten te melden is dat dit precies het probleem is/was. De impact van de Heartbleed bug heeft betrekking op primair en secundair sleutelmateriaal. De secundaire zijn user credentials en wachtwoorden, session keys en session cookies. Om dit te herstellen is het noodzakelijk eerst de trust te herstellen en daarna pas het secundaire sleutelmateriaal. Als de organisatie persoonsgebonden certificaten gebruikt als authenticatiemiddel en deze zitten binnen een HSM (smartcard), dan was ook het secundaire sleutelmateriaal niet gecompromitteerd geweest.
Binnen een HSM kun je de private keys NIET uitlezen, gebruik je geen HSM kun je het WEL uitlezen. Als een organisatie OpenSSL gebruikt met de bug EN de private keys in een HSM, was en is het NIET mogelijk de private keys uit te lezen. Consequentie is dat als de private keys beschermd zijn de rest ook beschermd is, je komt er via deze weg gewoon NIET in, dus kun je de rest ook niet lezen!!!!!

Jazeker er zijn enkele lekken geconstateerd met certificaten. Dit was en is echter te wijten aan menselijk falen. De techniek, het mechanisme is correct. Het daarop afschrijven is echter te kort door de bocht en een schromelijke vergissing. Vraag je zelf eens af welke lekken de andere methodes hebben. Dit is oneindig veel groter, dat lezen we elke dag in de krant. Waar ik wel blij mee ben is dat het verkeerd uitgeven van certificaten ernstige gevolgen heeft. Dit is bij een beperkt aantal organisaties gebeurt. Is bij jullie bekend bij hoeveel organisaties OpenSSL gebruikt werd met dezelfde ERNSTIGE consequenties?
Inderdaad certificeringen geven geen absolute garantie! Kan ook niet, want er werken mensen. De kans is echter zeer klein. Waar mij de koude rillingen van over mijn rug lopen zijn die veiligheidsvoorzieningen die niet onder dit soort certificeringen en controle staan, dat is een oneindige veelvoud van de circa 30 bedrijven die onder certificering staan waar tot nu toe twee problemen zijn geconstateerd. Het aantal inbraken en dergelijke is echter wederom oneindig groot en niet te wijten aan een gecertificeerde x.509 organisatie. Wijzelf werken daarom met verschillende encryptie technieken om processen waar mensen bij betrokken zijn te beschermen. Wij zijn er voorstander van een infrastructuur te beveiligen met certificaten, maar dan ook volledig! Dit is uitermate gebruikersvriendelijk en veilig. Door het gebruik van certificaten kun je inderdaad de privéfoto's beveiligen (encrypten) op een zodanige wijze dat de beoogde ontvanger de enige is die het kan lezen (pki).

Tenslotte wil ik opmerken dat dit artikel niet bedoeld is Open Source software aan te vallen. We gebruiken het zelf ook. Het is bedoeld mensen bewust te maken van risico's. In de huidige maatschappij waar informatietechnologie een steeds belangrijkere rol inneemt en de privacy/veiligheid steeds verder onder druk komt te staan moeten we ons steeds beter bewust zijn van risico's. Heartbleed is een waarschuwing. Dat is wat ik aangegrepen heb. Het is belangrijk dat (Open) Source software goed ontwikkeld en beheerd wordt. Is dit niet het geval wordt het risico te groot.

Frans Bolk
CEO UniQ-ID

DATA RISK MANAGEMENT

De hoeveelheid bedrijfsdata neemt exponentieel toe. Zo ook het aantal locaties en leveranciers die data voor u in beheer hebben. Door de grote hoeveelheid data is het voor vele organisaties onoverzichtelijk waar de data staat en hoe dat werkelijk is beschermd. De omvang en complexiteit van data vormt een extra dimensie die beteugeld moet worden om grip te krijgen op de beveiliging ervan. Zonder overzicht en goede bescherming van die data loopt de organisatie een groot risico. Tot nu toe zijn we nog niet verder gekomen dan checklists en heatmaps met getallen tussen 0 en 10 voorzien van stoplichtkleuren. In dit artikel neem ik u mee in de wereld van risicomanagement gericht op data, zoals de nieuwe versie van ISO27001:2013 specifiek van ons vraagt.

De inhoudsopgave van de internationale informatiebeveiliging standaard ISO27001:2013 beschrijft in grote lijnen waaraan een managementsysteem voor informatiebeveiliging moet voldoen. Een belangrijke verbetering ten opzicht van de vorige versie (ISO27001:2005) is de verbijzondering van de risicomethodiek die gericht moet zijn op de data. Maar hoe ziet dat Data Risico Management eruit? Vele organisaties worstelen met een data risico-analyses. De toenemende hoeveelheid data, de complexiteit van de verschillende beveiliging-standaarden, de administratieve lasten van checklists, project security reviews en de technische details met nietszeggende 'heatmaps' maken het in de praktijk onmogelijk voor het hoger management informatiebeveiliging op een normale manier aan te sturen. Nog maar te zwijgen van de adviseurs die bijna weten hoe je informatiebeveiliging moet implementeren. De kunst is om maatregelen optimaal af te stemmen op basis van je data risico's, zodat je niet een risico van een dubbeltje met een maatregel van een kwartje verzekerd. Tevens is het vereenvoudigen van informatiebeveiliging een kritische succesfactor, waarbij wel recht wordt gedaan aan de complexiteit van deze risico's. Bedrijven doen wel van alles aan beveiliging, maar de samenhang is zoek. Een één-dimensionale beveiligingsmaatregel om USB-poort af te sluiten op de bedrijfslaptop is weinig effectief als je vervolgens via Dropbox, Gmail en WeTransfer de data thuis op een USB-stick zet. Er is zoveel data, dat bedrijven door de bomen het bos niet meer zien wat ze moeten beschermen. Data Risico Management is de "missing link" die bedrijven nodig hebben om beveiligingsmaatregelen in balans te krijgen met een acceptabel bedrijfsrisico.

De speld in de berg van data

Om te beginnen moet je focus aanbrengen in de grote hoeveelheid data. Alles analyseren is met deze grote hoeveelheden data gewoon niet meer mogelijk. Een logische focus in deze grote hoeveelheid data, is de data van Mission Critical Applications (MCA). MCA ondersteunen namelijk de belangrijkste bedrijfsprocessen en vormen een bedrijfsrisico als het mis gaat. In de regel hebben MCA's een hoofdgebruiker die verantwoordelijk is voor de productiedata. Echter, bij audits blijkt dat productiedata wordt gekopieerd naar andere omgevingen en de nieuwe "data eigenaar" niet wordt benoemd. Dit eigenaarschap is wel nodig. Als de data namelijk wordt verplaatst, veranderen vaak de beveiligingsomstandigheden. Het is daarom van belang om alle databronnen van een MCA

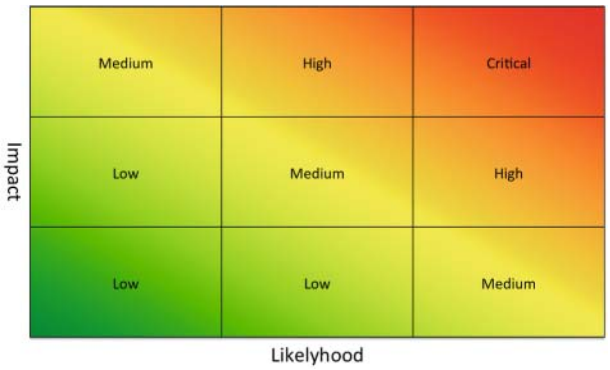
in kaart te brengen, inclusief de bijbehorende data eigenaar. Het risico neemt ook exponentieel toe naarmate de hoeveelheid (vertrouwelijke) data toeneemt. Een databron met alle patiëntgegevens op straat heeft veel meer impact dan een enkel papieren dossier. Een andere reden om alle databronnen van een MCA in kaart te brengen, is dat hackers in de praktijk ook liever de achterdeur gebruiken. Denk aan incidenten met bijvoorbeeld Cheaptickets (testomgeving) en Diginotar (via kantoornetwerk naar productie).

Voorbeeld: Een Cliënt Volg Systeem heeft een productiesysteem bij een ISO27001-gecertificeerde hosting partner in Almere, een dagelijkse back up-procedure van de databron met patiënt- en/of medewerkergegevens in de cloud (VS) en een datawarehouse in India. Dezelfde data valt in dit voorbeeld onder verschillende wetgeving, kent verschillende beveiligingsniveau's en het data eigenaarschap is versnipperd. Om dit goed aan te sturen, is een specifieke vorm van risicomanagement nodig.

Risico = Kans x Impact

Risicomanagement is traditioneel kans maal impact. Kans neemt toe als er iets van waarde te halen is en de impact is groter naarmate de organisatie groeit. Context en reputatie spelen daarom een belangrijke factor om de waarde van data risico's in te schatten. Een hoog risico voor een lokale bloemist is nu eenmaal anders dan een hoog risico voor een nationale bank. Het uitdrukken van impact in geld is handiger dan de traditionele indeling "High, Medium en Low". Systemen die namelijk allebei geclassificeerd zijn als 'High', zijn bij de vergelijking gelijk, maar blijken in de praktijk toch een verschillend risicoprofiel te hebben. De impact wordt ingeschat op basis van een schadepost die deze data kan veroorzaken.

De impact wordt uitgedrukt in een realistische schadepost op basis van termen uit de informatiebeveiliging, te weten: beschikbaarheid, integriteit, beschikbaarheid en non-compliance. De maximale schade als alle data uit een databron op straat komt te liggen (Confidentiality), de kosten



Risico heatmap

van een foute beslissing als de data niet juist blijkt te zijn (Integrity), de waarde als data voor maximaal aantal dagen niet beschikbaar is (Availability) en tot slot het niet voldoen aan wetgeving waardoor ik een boete kan krijgen (Non-compliance). De hoogste waarde bepaalt voor deze specifieke MCA de waarde van alle hoge risicoklassen – C,I,A,N – uitgedrukt in geld.

Het Ponemon Instituut heeft op basis van bekende incidenten onderzoek gedaan naar de gemiddelde kosten van een security incident. Deze schade komt internationaal neer op 150 euro per record. Dit bedrag biedt een uitgangspunt voor het bepalen van risico schade op basis van aantal records. Dit schadebedrag heb ik getoetst op incidenten die ik zelf ken, maar ook bij verzekeraars. Het is mijn conclusie dat dit schadebedrag per record naar beneden wordt bijgesteld bij organisaties met een lokale of nationale reputatie. Hierdoor krijg je een realistische inschatting van de werkelijke risico's.

Soms kan ik slechts één High-waarde vaststellen, soms twee en soms allemaal. De impact van deze data is daarom de hoogste waarde van deze vier categorieën (C,I,A,N) en geldt voor alle databronnen die gekoppeld zijn aan deze MCA. De andere risicoklassen Medium en Low worden hiervan afgeleid

Gerco Kanbier is directeur van Trust in People - the information protection company. Hij is te bereiken via gerco.kanbier@trustinpeople.com.

met respectievelijk 50% en 10% van de 'High'.
De kans is gekoppeld aan het aantal ISO27002-maatregelen die deels of niet genomen zijn rond de databron. In deze methodiek starten we dus niet met een dreigingenanalyse, maar starten met een mogelijke maatregel uit ISO27002 die een specifiek risico scenario afdekt. Het niet nemen van een individuele maatregel introduceert een kans dat het op dit punt fout kan gaan. Tegelijkertijd kunnen genomen maatregelen reeds preventief en/of overlappend zijn. Meer maatregelen, hoe kleiner de kans. Minder maatregelen vergroot andersom de kans op incidenten. De hypothese is dan wel dat een "databron" 100% veilig is als alle ISO27002-maatregelen zijn toegepast. Deze hypothese is natuurlijk niet waar, maar wel praktisch toepasbaar en goed bruikbaar als stuurinformatie. Beide grootheden - kans en impact - zijn op deze manier objectief meetbaar en kwantificeerbaar. Als een andere beveiligingsspecialist een inschatting doet, dan zal dat vergelijkbare resultaten opleveren. Dit in tegenstelling tot die risicospecialisten die zich bezig houden met wiskundige kansberekeningen.

Maatregelen (ISO27002)	Toegepast?	Auto Classificatie (C,I,A,N)	Scenario	Schade
Organisatie [Video bewaking]	JA	2C	Aanwezigheid of handeling kan ontkend worden bij onderzoek naar gestolen waar	€1.312.500
Organisatie [Security awareness training voor medewerkers]	NEE	3C	Medewerkers zijn een makkelijk prooi voor social engineer en/of phishing aanvallen	€262.500
Organisatie [Geheimhoudingsverklaring medewerkers]	DEELS	1C	Leverancier of medewerker lekt informatie naar derden	€2.625.000
Organisatie [Functiescheiding]	JA	1C	Gebruiker heeft teveel toegang tot vertrouwelijke informatie	€2.625.000
Organisatie [Uitwijklocatie]	NEE	1A	bij een ramp is er geen alternatieve locatie	€2.625.000
Organisatie [Informatiebeveiligings functionaris is aangesteld]	JA	2N	data eigenaarschap is niet goed belegd en bestuur is daarmee aansprakelijk	€1.312.500
Organisatie [Security is staffunctie van directie]	NEE	3N	informatiebeveiliging kan niet goed en/of volledig worden aangestuurd	€262.500
Processen [Data risico analyses worden periodiek uitgevoerd]	JA	2N	ad hoc aanpak laat echte risico's ongemoeid	€1.312.500
..	..	..	..	..

Risico's per databron in balans

Per databron wordt in kaart gebracht welke ISO27002-maatregelen wel, niet en/of deels genomen zijn. Het management heeft in een oogopslag een gewogen beeld van de huidige informatiebeveiliging per databron. Het management krijgt daarnaast een overzicht met begrijpelijke scenario's die nu nog als rest risico mogelijk zijn. Zo kan het management zelf quickwins definiëren en risico's accepteren op basis van integrale samenhang. Zie het voorbeeld in tabel

Heatmap

Als alle belangrijke databronnen geregistreerd, geanalyseerd en beoordeeld zijn, dan is het belangrijk voor het management een overzicht te krijgen waar de grootste risico's liggen, de zogenaamde 'heatmap'. Het management wil een beoordeling van het geheel. Alle risico's onder een bepaald platfond (bijvoorbeeld 1 miljoen euro), worden volgens beleid niet met hoger management besproken. Boven dat plafond wordt door de directie bekeken welke maatregelen extra genomen moeten worden dan wel als geheel geaccepteerd worden als rest risico. Met een heatmap krijgt het management een goed beeld of de standaard security architectuur over de linie goed is geïmplementeerd. Gemiddeld zijn er x maatregelen per databron genomen, waardoor afwijkingen goed zichtbaar zijn voor het management. De impact is uitgedrukt in geld, waardoor onderlinge risicoverschillen tussen MCA's en databronnen in een oogopslag zichtbaar worden. Zo kan het management besluiten gericht op een specifieke databron maatregelen te nemen (bijvoorbeeld een quick win), of een project te definiëren die de beveiliging van alle systemen verbeterd (bijvoorbeeld de centralisatie van logging).
Met bovenstaande managementinformatie kan het management ook haar bestuurlijke verantwoordelijkheid waarmaken. Het wordt duidelijk welke risico's acceptabel zijn en welke niet.

Statement of Applicability

Tot slot beschrijf ik de relatie tussen Data Risico Management, ISO27001, ISMS en het Statement of Applicability (SOA). Ongecertificeerde bedrijven hebben nog nooit gehoord van een Statement of Applicability. Dit is een document noodzakelijk voor een ISO27001-certificering met onder andere een beschrijving van de scope, de security incidenten en laatste audit findings. Maar belangrijkste onderdeel voor klanten, auditors en management is de vastlegging welke data risico's zijn geaccepteerd. Data Risico Management (DRM) is daarom een onmisbare schakel bij de uitvoering van informatiebeveiliging. De ISO27001 beschrijft een management systeem gericht op informatiebeveiliging (ISMS). Andere ISO-normen worden momenteel herschreven, waarbij elke norm onderscheid wordt gemaakt tussen het management systeem en de maatregelen. Hierdoor kunnen bedrijven in de toekomst makkelijker verschillende normen naast elkaar implementeren zonder verschillende managementsystemen aan te schaffen.

DRM

De afkorting van Data Risico Management, DRM, roept onder vakgenoten vraagtekens op. DRM staat namelijk ook voor Digital Rights Management. Tevens heeft Data Risico Management hetzelfde doel als Informatie Risk Management (IRM). Toch heb ik gekozen voor een andere naamgeving, omdat de methodiek gericht is op de DATA en een geheel andere aanpak heeft dan de bestaande risico methoden. In navolging van Enterprise Risk Management (ERM) wat zich op de enterprise richt, Operational Risk Management(ORM) op de operatie en Credit Risk Management (CRM) op de kredieten, richt Data Risk Management zich specifiek op de data.

HOE OM TE GAAN MET EEN ONVEILIGE HAVEN?

Het Amerikaanse data-uitwisselschip is al een tijdje zinkende. De discussies over de onveiligheid van de Safe Harbour, ontworpen om juist op een veilige manier data te kunnen uitwisselen met Amerikaanse entiteiten, lopen al geruime tijd maar beginnen nu eindelijk ook het nieuws te halen. Recentelijk werd de nieuwe EU-commissaris Jourová aan een vragenvuur onderworpen in het Europees Parlement. Privacyvoorvechters binnen de EU zien de Safe Harbour het liefst verdwijnen. De EU-Commissie heeft nog steeds een onderhandelingstraject lopen met de Amerikaanse overheid om de Safe Harbour aan te scherpen, dit naar aanleiding van de afluisterschandalen van de NSA. Jourová heeft toegezegd dat als dit traject niet succesvol blijkt, het schrappen van de Safe Harbour een reële optie is.

Die datagraaipraktijken van de Amerikaanse overheid zijn echter niet het enige probleem. Het Safe Harbour systeem functioneert niet. Althans, niet naar de strenge Europese normen voor de bescherming van persoonsgegevens en privacy van personen. Het is een zelf-certificerend mechanisme met een zwakke vorm van "toezicht". Bedrijven kunnen zichzelf certificeren en geven daarmee aan dat zij zich aan EU-standaarden van dataprotectie zullen houden. Uit onderzoek van het CDD (Center for Digital Democracy) blijkt dat veel Amerikaanse bedrijven zich helemaal niet houden aan die regels, maar wel "gewoon" data uitwisselen omdat ze gecertificeerd zijn. Onduidelijk is welke persoonsgegevens verwerkt worden, waarom dat gebeurt en met wie die gegevens allemaal gedeeld worden. Naar EU-standaarden een enorme no-go.

Ook het indirecte "toezicht" is een issue. Het CDD heeft ook dit tekort in Safe Harbour aangekaart in haar rapport, de Federal Trade Commission (FTC) zou nauwelijks toezicht houden op de naleving van de Safe Harbour. Het toezichthoudend orgaan zal doorgaans alleen dan actie ondernemen als er een duidelijke klacht wordt ingediend. Het CDD heeft hun onderzoek dan ook ingediend als klacht bij FTC, de 30 met naam benoemde bedrijven kunnen daardoor - als de klacht serieus genomen wordt - visite verwachten.

Maar wat moet je dan nu als bedrijf doen als je gegevens wilt gaan uitwisselen met een Amerikaans bedrijf? Het lijkt een heel erg open deur, maar ik zeg het hier met nadruk: vertrouw nooit zomaar iemand op zijn blauwe ogen. Weet met wie je zaken doet. Kijk op websites, lees privacystatements, doe een google search, vraag bij conculleg's naar hun ervaringen. Lees het CDD rapport (30 met naam benoemd!). Heeft een bedrijf geen of een heel slecht privacystatement? Een rode vlag. Worden ze genoemd in een rapport over slechte omgang met klantdata? Een rode vlag. Stel vragen, ga de diepte in. Kunnen ze daarop geen of moeizaam antwoord geven? Een rode vlag. Kijk ook naar wat je gaat doen met dat bedrijf. Misschien zijn er ook anderen op de (EU) markt die hetzelfde kunnen doen. En vergis je niet, ook EU bedrijven kunnen privacyregels schenden. Onderwerp hen aan eenzelfde kritische blik.

Voel je je comfortabel na dat eerste onderzoek? Kunnen ze ook jouw meer ingewikkelde vragen over privacy en informatiebeveiliging beantwoorden? Zorg dan om te beginnen dat je goed contracteert (de Model Clauses van de EU of een eigen "privacy"overeenkomst). Met alleen papier haal je het niet, zorg ook voor controlemechanismes. Denk aan auditrechten, periodiek overleg, aanspreekpunten, alsook de looptijd van de overeenkomst en mogelijkheden tot tussentijds opzeggen. Ben je dan helemaal veilig? Nee, maar je hebt wel meer kans van slagen op een behouden vaart.

Mr. Rachel Marbus,
@rachelmarbus op Twitter

HOE KRIJG JE ZE MEE?

Veel organisaties gaan over naar 'papierloos werken', waarbij informatie wordt gedigitaliseerd en het opslaan en uitwisselen van informatie via internet of de 'cloud' een steeds grotere rol speelt. Ook maken ze steeds meer gebruik van nieuwe ontwikkelingen, zoals 'het nieuwe werken', 'mobile devices' en social media. Een minder prettige ontwikkeling is de toenemende cybercrimedreiging. Cybercriminelen ontfutselen gericht informatie en gebruiken daarbij professionele en geavanceerde methoden en technieken, zoals social engineering en (spear)phishing. Als gevoelige informatie 'op straat terecht komt', kan dat leiden tot ernstige reputatieschade dan wel financiële schade. Als gevolg van de nieuwe ontwikkelingen en toenemende dreiging zijn organisaties kwetsbaarder voor misbruik van gevoelige informatie. Als gevolg daarvan krijgen medewerkers een grotere verantwoordelijkheid in het zorgvuldig omgaan met informatie.

Lambrecht Nieuwenhuize is Corporate Information Security Officer bij BNG Bank en houdt zich o.a. bezig met informatiebeveiliging, awareness en business continuity management. Daarnaast is hij eigenaar van Cyber Security Scan Europe. Hij schrijft dit artikel op persoonlijke titel. Lambrecht is te bereiken via lambrecht.nieuwenhuize@bngbank.nl.

Het valt op dat medewerkers vaak wel weten dat het belangrijk is om zorgvuldig met informatie om te gaan. Desondanks leven ze richtlijnen onvoldoende na, omdat zij geldende richtlijnen zijn 'vergeten' of kiezen voor gemak. Hieronder een overzicht van oorzaken die wij in de praktijk tegenkomen, waardoor richtlijnen onvoldoende worden nageleefd.

Oorzaken van niet-naleving van richtlijnen:

1. Besef van noodzaak ontbreekt
   - gemakzucht
   - waarom zou ik?
   - er gebeurt toch nooit iets!
2. Richtlijnen worden niet uitgedragen en gestimuleerd
3. Geen structurele aandacht voor beveiligingsbewust gedrag (secure gedrag)
4. Ontbreken van (duidelijke) richtlijnen
5. Communicatie en campagnes sluiten niet aan op de beleving van de doelgroep
6. Onvoldoende faciliteiten
7. Voorbeeldgedrag directie en management ontbreekt
8. Medewerkers spreken elkaar niet aan
9. Effect van awareness-acties wordt niet gemeten en geëvalueerd

Een bekende stelling binnen informatiebeveiliging is: 'de medewerker is de zwakste schakel'. De medewerker is tegelijkertijd een zeer belangrijke schakel omdat hij, in tegenstelling tot technische systemen, goed in staat is om dreigingen en incidenten te beoordelen in relatie tot context en omstandigheden. Van zwakste naar sterkste schakel vereist in praktijk een gedragsverandering, wellicht zelfs een cultuurverandering in de organisatie. In theorie leuk geformuleerd maar in de praktijk een complex en intensief traject. Medewerkers kunnen de sterkste schakel in de beveiligingsketen worden door bewustwordingsactiviteiten structureel en volgens een procesmatige aanpak uit te voeren. Hieronder worden succesfactoren en tips gegeven om de succesfactoren te implementeren.

What's in it for me?

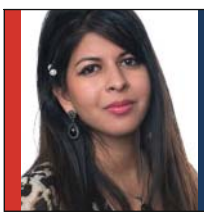
Het besef van noodzaak en urgentie om zorgvuldig met informatie om te gaan ontstaat vaak pas nadat het een keer goed is misgegaan. Het helder maken van de voordelen en consequenties van het al dan niet naleven van richtlijnen draagt bij aan het creëren van het besef van urgentie bij medewerkers. Het besef van noodzaak en urgentie kan gecreëerd worden door onder andere de volgende activiteiten:

- Formuleer boodschappen in voordelen en nadelen en benadruk welke winst veilig omgaan met informatie oplevert;
- Creëer inzicht in consequenties als richtlijnen niet worden nageleefd (verwijs bijvoorbeeld naar sancties);
- Informeer medewerkers over praktijkvoorbeelden of incidenten met betrekking tot informatiebeveiliging binnen de eigen organisatie (bevindingen van de interne audit afdeling of externe auditor kunnen hier bij helpen);
- Wijs medewerkers op nieuwsberichten over organisaties (bijvoorbeeld concullega's) die negatief in het nieuws zijn geweest;
- Organiseer interactieve workshops zodat medewerkers de dialoog met elkaar aan gaan over het belang van het zorgvuldig omgaan met informatie.

Draagvlak en commitment

Een noodzakelijk voorwaarde om gedragsverandering door te kunnen voeren is de aanwezigheid van voldoende managementcommitment en voldoende draagvlak op alle niveaus binnen de organisatie. Vooral het verkrijgen van voldoende draagvlak (zie figuur 1) blijkt in praktijk een lastig, uitdagend en langdurig proces te zijn.
Draagvlak en commitment kunnen gecreëerd worden door:

- Noodzaak en nut (gevolgen en consequenties) te bespreken met het management;
- De Raad van Bestuur of directie een statement te laten formuleren waarom het belangrijk is om zorgvuldig om te gaan met informatie (bijvoorbeeld door middel van een videofragment of een nieuwsbrief);
- Verantwoordelijken (proceseigenaren, systeemeigenaren, afdelingshoofden) bij aanvang van een awareness-programma/plan te betrekken. Zij zijn als verantwoordelijken belangrijke spelers om het gewenste gedrag te stimuleren;
- Verantwoordelijken vervolgens structureel te blijven betrekken om het draagvlak te behouden;

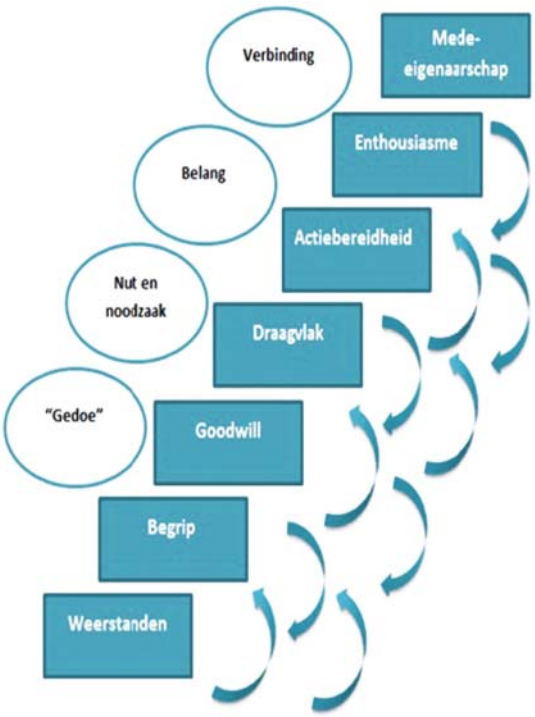


Déjaniera Rampersad is consultant informatiebeveiliging & risicomanagement bij Verdonck Klooster & Associates (VKA). In haar rol als consultant heeft Déjaniera meerdere organisaties begeleid bij het opstellen en uitvoeren van awareness-programma's als onderdeel van de inrichting van informatiebeveiliging. Zij is te bereiken via dejaniera.rampersad@vka.nl.

- Gebruik van serious gaming en simulaties zodat medewerkers op een leuke en pragmatische manier de dialoog met elkaar aangaan.

Heldere communicatie

Medewerkers hebben meestal wel een beeld van het veilig omgaan met informatie, maar vaak is onvoldoende duidelijk wat dit voor hen in de praktijk betekent. Is het verstandig om bijvoorbeeld in de trein gevoelige stukken te mailen via het openbare WiFi netwerk? Met behulp van beleid en gedragscode kunnen heldere richtlijnen worden opgesteld, zodat de medewerkers weten wat van hen wordt verwacht. Een voorbeeld van heldere richtlijnen zijn 'de gouden regels' waarbij de belangrijkste secure gedragsaspecten op een rijtje zijn gezet. Vaak zijn er meerdere richtlijnen binnen een organisatie, bijvoorbeeld op het gebied van integriteit, social media en het nieuwe werken. De richtlijnen over het veilig omgaan met informatie kunnen hier heel goed op worden aangesloten. Het is belangrijk dat alle richtlijnen op elkaar zijn afgestemd en samen een consistent geheel zijn.



Figuur 1 Draagvlakladder

Aansluiten bij belevingswereld

Binnen organisaties zijn verschillende afdelingen, doelgroepen en functies te onderscheiden die vaak verschillende of misschien wel conflicterende doelstellingen nastreven. Deze doelgroepen werken met verschillende soorten informatie en hebben wellicht andere belangen waardoor een standaardboodschap (op bijvoorbeeld een poster) voor de hele organisatie minder effect heeft. Daarom is het belangrijk om aan te sluiten op de belangen en beleving van de medewerker. Het gaat hierbij bijvoorbeeld om aansprekende voorbeelden of casussen die passen bij de dagelijkse praktijk van de organisatie. Taalgebruik en de wijze waarop gecommuniceerd wordt, moeten op de doelgroep worden afgestemd. Dit kan door ambassadeurs binnen verschillende afdelingen aan te wijzen die het belang van 'secure gedrag' binnen de afdeling uitdragen.

Voldoende faciliteiten

Directie en management zijn verantwoordelijk om voldoende faciliteiten (zoals voldoende vergaderruimten, afsluitbare kasten en lades, afsluitbare papierbakken of papierversnipperaar) ter beschikking te stellen zodat medewerkers zorgvuldig om kunnen gaan met informatie. Zij dienen tevens structureel te inventariseren of voldoende faciliteiten geboden worden om de richtlijnen te kunnen naleven. Veel organisaties gaan over naar het nieuwe werken of bieden medewerkers de gelegenheid om op afstand te werken. De behoefte aan een methode om veilig te e-mailen of een veilige cloud omgeving neemt daardoor toe. Bij gebrek aan voldoende middelen is het erg verleidelijk om te kiezen voor een (onveilig) alternatief zoals het opslaan van informatie op een onbeveiligde USB-stick of voor opslag in Google Docs of Dropbox. Medewerkers moeten gefaciliteerd worden in het veilig opslaan en delen van informatie en het verkrijgen van veilige toegang tot informatie(systemen). Periodiek moet worden getoetst of de medewerkers voldoende worden gefaciliteerd.

Voorbeeld gedrag management

Het is belangrijk dat directie en management zich realiseert dat zij een zeer belangrijke voorbeeldfunctie vervullen. Door zichtbaar secure gedrag te vertonen, bevestigen zij dat beveiligingsrisico's een serieus aandachtspunt zijn en 'secure' gedrag als 'normaal' gedrag wordt gezien. Indien directie en management zich niet aan beveiligingsafspraken en procedures houden, zal dat leiden tot vergelijkbaar gedrag in de rest van de organisatie. Met het eigen gedrag kunnen directie en management de organisatie motiveren, dan wel demotiveren. Een voorbeeld van zichtbaar secure gedrag is de mate waarin het management zelf de clear/clean desk of clear screen policy naleeft. Als het management zich goed aan deze policy houdt, straalt dat uit naar de rest van de organisatie. Indien het management zich niet aan de policy houdt, is het niet reëel om van de rest van de organisatie te verwachten dat de policy voldoende wordt nageleefd.
Maak het 'secure' gedrag van management inzichtelijk en koppel de bevindingen vervolgens aan het management terug.

Stimuleren en belonen

Stimuleren is een goed instrument om medewerkers te motiveren

hun gedrag te veranderen. De manager/leidinggevende heeft een cruciale rol als 'motivator'. Door bijvoorbeeld waardering uit te spreken stimuleert de manager de medewerker om het gewenste secure gedrag vol te houden. Ook het persoonlijk en direct aanspreken door leidinggevende/collega's op de eigen verantwoordelijkheid draagt bij aan het stimuleren. Door steekproefsgewijze controles en het direct terugkoppelen van de resultaten, worden medewerkers geconfronteerd met hun gedrag. Ingeval van ongewenst gedrag kan de medewerker direct worden aangesproken op het te verbeteren punt. Een effectieve vorm van stimuleren is dat medewerkers elkaar onderling aanspreken en elkaar scherp houden op richtlijnen. Voorwaarde hierbij is dat er sprake is van een open cultuur, waarin medewerkers elkaar mogen en durven aan te spreken. Bij een organisatie in de zorgsector heerste geen open cultuur waarin medewerkers elkaar durfden aan te spreken. Daar is gekozen het gebruiken van een spelelement in de vorm van een competitie gebaseerd op het TV spel 'Wie is de Mol'? Een aantal medewerkers is maandelijks ´de mol´. Zij houden zich bewust niet aan de richtlijnen. Het spelelement is toegevoegd door de medewerkers zo veel mogelijk ´mollen´ te laten ontdekken. Dit kan een medewerker doen door de ´mol´ aan te spreken en te vragen of hij of zij de 'mol' is. Wie de meeste 'mollen' ontdekt, wint een prijs. In de praktijk zien we dat awareness vaak eenmalig aandacht krijgt door bijvoorbeeld een (poster)campagne of een e-learning traject. Deze 'projecten' dragen uiteraard bij aan de awareness, maar door het tijdelijke karakter blijken de awareness en het secure gedrag ook vaak van tijdelijke aard te zijn. In de praktijk zien we dat een procesmatige aanpak doorgaans het meest effectieve resultaat oplevert, omdat in een proces structureel aandacht wordt gegeven aan awareness. Door structureel het onderwerp 'veilig omgaan met informatie' onder de aandacht van de medewerker te brengen en te evalueren neemt het bewustzijnsniveau niet alleen toe, maar blijft het ook op het gewenste niveau. De kracht van herhaling is ook hier van toepassing. Hieronder is toegelicht hoe een procesmatige aanpak (analoog aan de Deming-cyclus) eenvoudig en praktisch toe te passen is.

Initieer en ontwerp

- Neem secure gedrag expliciet op in het jaarplan, afdelingsplannen, werkoverleggen van directie, management en medewerkers (sluit bijvoorbeeld aan op de planning & control cyclus).
- Stel, samen met de afdeling communicatie, een (communicatie)plan op waarin het onderwerp structureel onder de aandacht van medewerkers wordt gebracht.

Voer het programma uit

- Wijs actiehouders aan om het plan uit te voeren.
- Maak afspraken met de afdeling communicatie over de uitvoering van het plan.

Sluit met het plan zoveel mogelijk aan bij lopende initiatieven. Bewustzijn wordt eenvoudiger vergroot als het onderdeel uitmaakt van een lopend initiatief. De boodschap komt daardoor sterker over. Een voorbeeld van een lopend initiatief is het inrichten van het nieuwe werken. Doordat medewerkers plaats- en tijdsonafhankelijk werken, ontstaan naast voordelen ook risico's. Bij telefoongesprekken of laptopgebruik in openbare gelegenheden kan bijvoorbeeld eenvoudiger worden meegeluisterd/meegekeken door onbevoegden. Door security awareness te benadrukken bij de implementatie van het nieuwe werken komt de boodschap beter en krachtiger over dan de boodschap als apart onderwerp te presenteren. Andere voorbeelden voor aansluiting zijn het integriteitsprogramma, het kwaliteitsprogramma en het introductieprogramma voor nieuwe medewerkers.

Controleer voortgang en progressie

- Controleer of de acties uit het plan worden uitgevoerd.
- Toets het secure gedrag van medewerkers door middel van:
  - Gerichte vragenlijsten uit te zetten binnen de organisatie die kennis, houding en gedrag toetsen.
  - Bestaande meetinstrumenten zoals de Quick Scan Security Awareness aangeboden door het NCTV [1] toe te passen.
  - Steekproefsgewijze onaangekondigde controles tijdens of na werktijd op bijvoorbeeld clean desk en clear screen (facilitair bedrijf kan hier vaak ook aan meehelpen) uit te voeren waarbij foto's de evidence vastleggen.
  - Een mystery-guest actie of social engineering-actie (telefonisch of fysiek) uit te voeren.
  - Structureel in gesprek te gaan met de interne auditafdeling of de afdeling kwaliteit. Deze afdelingen bezitten mogelijk specifieke informatie over het huidige (awareness)niveau. Een gesprek kan extra informatie en inzichten geven.
  - Afspraken met de interne auditafdeling te maken om ook awareness-aspecten mee te nemen tijdens audits.

Evalueer en stuur bij

- Koppel de meetresultaten terug aan de betrokkenen, zodat zowel betrokkene als organisatie inzicht krijgen in het eigen gedrag en worden gestimuleerd en gemotiveerd tot verbetering.
- Koppel de voortgang van het plan en progressie ten aanzien van het secure gedrag terug aan directie en management.
- Pas het plan aan indien nodig.
- Geef aandacht aan awareness tijdens het beoordelingsgesprek van de medewerker.
- Stel, als uiterste bijsturing, een aanvullend sanctieregime in.

Bron

[1] http://www.nctv.nl/pp/zvjz/quickscan-sa/

IDENTITEITSFRAUDE IS KINDERSPEL

Zo'n 540 Nederlanders per dag worden slachtoffer van identiteitsfraude. Inmiddels is dat de snelst groeiende vorm van misdaad. Een paar jaar geleden dacht ik dat het vooral naïeve en onvoorzichtige mensen overkwam. Inmiddels weet ik hoe gemakkelijk het is om iemands identiteit te stelen. Ik heb het zelfs een paar keer gedaan. Niet dat ik iemands bankrekening heb leeggetrokken of spullen op andermans naam heb besteld. Het kon allemaal, maar ik wilde alleen aantonen hoe gemakkelijk het is.

Zo verstuurde ik namens een Tweede Kamerlid e-mails aan andere Tweede Kamerleden om ze te laten zien dat zelfs een digibeet dat kan en dat er meer aandacht moet komen voor het probleem. Hoe identiteitsfraude ontstaat is vrij simpel: de meeste mensen werken met computers maar kennen de gevaren niet. Waar moeten ze leren wat de valkuilen van het internet zijn? Als je een simpele mixer koopt, krijg je er een gebruiksaanwijzing bij, maar bij een computer krijg je niets. Je moet het allemaal zelf uitzoeken, antivirussoftware en firewalls installeren. Bedrijven steken royaal geld in pc-privé projecten, maar een cursus veilig omgaan met de computer hoort er niet bij. Vandaar dat de medewerkers massaal virussen op de bedrijfsnetwerken downloaden of via besmette privé-computers gevoelige informatie lekken. Uit een recent onderzoek bleek dat maar liefst 25 procent van de werknemers op phishingmails klikt, die als zodanig goed herkenbaar zijn. Veel medewerkers verzinnen zwakke wachtwoorden voor hun werkmail, omdat niemand ze geleerd heeft hoe je sterke wachtwoorden kunt maken (en onthouden). Daar zijn ondertussen tal van handige en gratis programma's voor, maar de meeste mensen kennen ze niet. Wat nog erger is: ze gebruiken voor meerdere sites hetzelfde wachtwoord. Tegenwoordig is dat een heel groot probleem, omdat zelfs betrouwbare sites gegevens blijken te lekken. Van Sony tot LinkedIn en van de publieke omroep tot zorgverzekeraars. Digitale veiligheid is blijkbaar het stiefkindje van de begroting bij veel organisaties.

Datalek

Uit een recent onderzoek van SafeNet blijkt dat datalekken bij bedrijven desastreus is voor het klantvertrouwen. Tweederde van de ondervraagden gaf

aan dat ze vermoedelijk nooit meer zullen kopen bij een bedrijf dat hun gegevens gelekt heeft. Uit het onderzoek bleek dat in slechts een kwartaal 175 miljoen gegevens van klanten op straat kwamen te liggen. Getroffen bedrijven waren onder meer AOL, eBay en Spotify.

Beveiligingslekken leiden vaak tot een vertrouwensbreuk en dat zal in Nederland waarschijnlijk toenemen, omdat de bedrijven vanaf volgend jaar verplicht zijn om beveiligingsincidenten rond persoonsgegevens publiekelijk bekend te maken. De nieuwe wetgeving voorziet ook in hoge boetes. Een goede aanleiding om de computersystemen op zwakheden te controleren. De consument beschermen gaat echter niet lukken met alleen een oplettende ICT-afdeling en up-to-date software. De zwakste schakel blijft de gewone medewerker. Tijdens de research voor mijn boek 'Komt een vrouw bij de hacker' stuitte ik op ongelooflijke voorbeelden van medewerkers die de meest privacygevoelige gegevens doorgeven, omdat ze veronderstellen dat ze een collega aan de lijn hebben en niet een oplichter.

Ik nam tijdelijk de identiteit van een vriendin over om te kijken hoe ver ik kom bij een zorgverzekeraar. De gegevens die ze aan de telefoon ter verificatie vragen zijn meestal te googelen, dus ik kwam moeiteloos door de test. De redactrice van mijn boek geloofde niet dat het zo makkelijk kon zijn en belde haar verzekeraar op met het verhaal dat ze haar polismap kwijt was. Hij vroeg alleen haar adres ter verificatie, niet eens haar geboortedatum (die veel mensen trouwens gewoon op Facebook zetten). Binnen de kortste keren wist ze hoeveel ze per maand betaalt, van welke bankrekening het wordt afgeschreven, etc. Ze was geschokt, want voor hetzelfde geld kon iemand anders namens haar bellen en aan al die informatie komen. Een van de mensen die ik voor mijn boek heb geïnterviewd, deed dat jarenlang als 'beroep', de gegevens van honderden mensen bij elkaar sprokkelen, van hun banksaldo's tot hun geheime telefoonnummers. Er was altijd iemand bij de instanties die toehapte en hem verder hielp. Dat deed hij trouwens in opdracht van gerenommeerde bedrijven en organisaties, van verzekeraars tot gemeenten.

Identiteitsfraude de snelst groeiende vorm van misdaad

Riool

Steeds meer databanken worden aan elkaar gekoppeld en dat maakt de burgers (maar ook de organisaties) extra kwetsbaar. Onlangs toonde de Raad van State zich zeer kritisch over de verzameldrift van de overheid. De wet SUWI werd gewijzigd om fraudeurs gemakkelijker op te sporen, maar dat betekent ook dat er volgens de plannen een gigantische hoeveelheid gegevens over de burgers wordt gedeeld en uitgewisseld. Het gaat onder meer om arbeidsgegevens, boetes, belastinggegevens, gegevens over bezittingen, woon- en verblijfgegevens, identificerende gegevens, onderwijsgegevens, zorgverzekeringsgegevens, etc. De Raad van State schrok van deze enorme lijst en sprak van "vergaande beperking van de persoonlijke levenssfeer". Met al die data wordt een risicoprofiel van elke burger gemaakt. Met de decentralisatie van verschillende wetten gaan volgend jaar veel mensen bij de gemeenten toegang krijgen tot nieuwe vertrouwelijke gegevens. Informatieveiligheid spreekt de meeste medewerkers niet vanzelf aan, omdat het een vrij abstract onderwerp is. Informatieveiligheid is net zoiets als de riolering, je merkt er niets van totdat het fout gaat. Volgens de hackers die ik heb gesproken, is het niet de vraag of een organisatie gehackt wordt, maar wanneer. Ze zeggen dat je maar twee soorten bedrijven hebt: bedrijven die al gehackt zijn en bedrijven die dat gaan worden. Eerlijk gezegd geloof ik de hackers wel. Ik heb met eigen ogen gezien hoe ze te werk gaan en hoe ze websites die op het eerste gezicht veilig lijken, via een omweg toch weten te hacken. Veel organisaties hebben het trouwens helemaal niet door als ze gehackt zijn.

De meest voorkomende zwakheden zijn voorspelbare wachtwoorden gebruiken, zoals 'Wachtwoord1' of fabrieksinstellingen van apparaten die niet gewijzigd zijn. Hackers komen ook via ongebruikte servers binnen of via websites met zwakke plekken. Bij drie van de vier beveiligingstests kunnen hackers via het internet de ICT-infrastructuur van bedrijven binnendringen. Onlangs waarschuwde de FBI ook voor ontevreden of pas ontslagen werknemers. Die hebben vaak toegang tot gevoelige informatie en netwerken waar bedrijven afhankelijk van zijn. Volgens

Maria Genova is journalist, schrijfster en spreker over onderwerpen zoals privacy en identiteitsfraude. Ze is per e-mail bereikbaar via genova@casema.nl en via Twitter @genova2. www.mariagenova.nl

de opsporingsdienst is er een toename van het aantal gevallen waarbij insiders toeslaan. De diefstal van gegevens vindt meestal via cloudopslagdiensten zoals Dropbox en persoonlijke e-mailaccounts plaats. Ontslagen werknemers blijken in veel gevallen toegang tot de bedrijfsnetwerken te hebben. Ook passen organisaties de wachtwoorden van hun servers en netwerken na het ontslag van ICT-personeel niet altijd aan.

Crimineel

Bij het lekken van gegevens is de schade niet alleen voor de bedrijven, maar ook voor de burger. Identiteitsfraude is een fenomeen met grote gevolgen, vaak blijft het je jarenlang achtervolgen. De slachtoffers die ik sprak waren in eerste instantie allemaal overtuigd dat het snel opgelost zou worden, omdat ze zelf niets verkeerds hadden gedaan. Toch moesten sommige slachtoffers leningen en spullen van onbekende mensen afbetalen en raakten anderen hun werk kwijt. Ongeveer vijftig mensen per dag komen door identiteitsfraude in aanraking met politie of justitie. Met slechts een kopie van je paspoort kan iemand van alles op je naam doen, want allerlei instanties accepteren kopietjes via het internet als bewijs dat jij het bent. Ga maar vervolgens bewijzen dat je geen contract of koopovereenkomst gesloten hebt als alle sporen naar je wijzen. Dat is ook het lastige van identiteitsfraude. Uiteraard moet je niet zomaar je ID laten kopiëren, maar veel bedrijven eisen dat en de meeste burgers weten niet dat het van de wet niet mag. Als je ergens lid wilt worden of een machine wilt huren, maken nog steeds heel veel bedrijven 'een kopietje'. De consumenten hoor je niet klagen. Pas als ze in de problemen komen, zien ze in wat voor gevolgen zo'n onschuldig kopietje kan hebben. Ik sprak bijvoorbeeld met Linda van wie de gegevens door een onbekend iemand misbruikt werden. Ze betaalde onder meer telefoonabonnementen die ze nog nooit had afgesloten. Ze had in totaal zo'n 11.000 euro aan schulden die niet van haar waren. Ze kreeg psychische problemen omdat ze constant met deurwaarders te maken had. Een ander iemand die ik sprak, Boudewijn, werd opgepakt voor drugs. Hij dacht dat het een foutje was, maar iemand bleek met een kopie van zijn paspoort panden te hebben gehuurd waar wietplantages opgerold waren. Boudewijn was er ruim twee jaar mee bezig om zijn onschuld te bewijzen en al die tijd werd hij als een crimineel behandeld. Hij werd zelfs voor vrijwilligerswerk geweigerd omdat hij een politiedossier had, ook al was het toen allang duidelijk dat het om identiteitsfraude ging.

Veel mensen bewaren een kopie van hun legitimatie in de computer. Dat is ook een van de tips die ik tijdens lezingen geef: niet meer doen. Ik probeer burgers en organisaties wakker te schudden in de hoop dat het tij nog te keren is, want de identiteitsfraude stijgt explosief. Ik merk dat het onderwerp de laatste tijd 'hot' is, want de uitnodigingen voor lezingen stromen binnen: van het ministerie van Binnenlandse Zaken tot de Koninklijke Marechaussee en van KPN tot ondernemersverenigingen: iedereen is op zijn eigen manier met data en privacy bezig. Ik wil vooral met voorbeelden uit de praktijk laten zien hoe gemakkelijk identiteitsfraude is en dat er best veel goede oplossingen zijn om die te voorkomen. Kan niemand meer mijn identiteit stelen? Natuurlijk wel, 100 procent beveiliging is zowel voor burgers als voor organisaties een illusie. Maar vergelijk het met het kopen van goede sloten voor je buitendeur. Inbrekers kiezen meestal de gemakkelijkste weg en dat geldt ook voor hackers.

Over uw online reputatiemanagement

Een toenemend aantal organisaties profileert zich om begrijpelijke redenen steeds nadrukkelijker online. Fungeerde pakweg een decennium geleden de corporate website nog voornamelijk in een bijrol, als digitaal visitekaartje of online promotiefolder; vandaag de dag is vaak sprake van een prominente positie. De consument heeft deze nieuwe ingang tot uw organisatie feilloos weten te vinden en gebruikt deze gretig. En uw reputatie hangt voor een belangrijk deel samen met de manier waarop u zich online profileert. En dus stelt u alles in het werk om te komen tot een fraaie, toegankelijke website en een hoge ranking in de diverse zoekmachines. Met een juiste aanpak zullen tevreden bezoekers uw deel zijn.

Kapers op de kust

Maar met het succes komen ook nieuwe bedreigingen. De creatieve manier waarop profiteurs meeliften op het online succes van anderen en zelfs misbruik maken van de situatie, is een onderbelicht fenomeen. De gevolgen strekken uit van hooguit licht irritant, tot uitermate vervelend. Geen wonder dus, dat goed reputatiemanagement heel nadrukkelijk ook uw online-activiteiten moet omvatten. Helaas is dit echter gemakkelijker gezegd dan gedaan; de meelifters zijn vaak creatiever dan gedacht. Bij SIDN, de registry voor het .nl-domein, zijn we ons hiervan bewust. Speciale teams doen onderzoek naar het ge- en misbruik van .nl-domeinnamen en werken aan oplossingen om misbruik te helpen voorkomen.

Typosquatting

Uw online-activiteiten worden op verschillende manieren bedreigd. Zo is er het het fenomeen 'typosquatting'. Hierbij gaat het om derden, die een domeinnaam registreren die lijkt op die van u. Ze doen dit met uiteenlopende bedoelingen. Soms gaat het om ronduit criminele activiteiten (zoals phishing bij banken), soms gaat het om simpele advertentiepagina's, die omzet genereren als bezoekers een typefout maken. En soms gaat het om partijen die mee willen liften op uw succes, door kopers die een typefout maken terwijl deze naar uw site willen, weg te leiden naar een concurrerende site.

Onbegonnen werk

De wakkere e-marketeer anticipeert hier vandaag de dag al op, door van een domeinnaam ook bepaalde spellingsvarianten vast te leggen. Maar in een aantal gevallen is dat onbegonnen werk. Een voorbeeld: van 'google.nl' bestaan honderden varianten onder .nl en slechts een fractie daarvan is door Google zelf geregistreerd. Voor 'marktplaats.nl' idem dito: 'makrptlaats.nl', 'makrtplaats.nl',' marktlplaats.nl' of 'maqrktplaats.nl' zijn slechts enkele van de vele voorbeelden. Zo zijn er veel domeinnamen die op een of andere manier spellingsvarianten hebben, soms zelfs talloze. Nog een voorbeeld om het af te leren: 'balastingdienst.nl', 'bealstingdienst.nl' en 'beastingdienst.nl' zijn allemaal bestaande .nl-domeinnamen die lijken op 'belastingdienst.nl'.

Andere toepassingsvormen zijn bijvoorbeeld parodiesites die eventueel nadelig kunnen uitpakken voor uw reputatie, maar waarvan het in elk geval prettig is dat u er van weet voordat u erover terugleest in de media. Met als relatief onschuldig voorbeeld: http://jumbosupermartken.nl/.

Uiteraard is er ook sprake van veel ernstiger incidenten, met name als er geld te verdienen (of te stelen) valt. Webwinkels en banken hebben hier geregeld last van, zoals zich wel laat raden. De site http://mediamarktoutlet.nl/ was hier een voorbeeld van. Deze site wekte de indruk een officiële online koopjeshoek van de Mediamarkt te zijn, maar was dat uiteraard niet.

Domeinnaambewakingsservice

Organisaties kunnen er baat bij hebben als ze weten dat er domeinnamen worden geregistreerd die hun domeinnaam of merknaam bevatten, of iets wat daar op lijkt. Voor wat betreft domeinnamen die eindigen op .nl is dat relatief simpel met de Domeinnaambewakingsservice (DBS) van SIDN. Wie een abonnement op deze dienst afneemt, krijgt vrijwel meteen een seintje als er een domeinnaam wordt geregistreerd die klinkt als, of lijkt op het origineel (onder meer op basis van een Levenshtein-algoritme). DBS kan een welkome aanvulling op uw cyberverdedigings-strategie zijn. U kunt ervoor terecht bij een .nl-registrar.

Marco Davids, technisch adviseur

Verantwoorde onthullingen #10

TERUGKIJKEN

Verantwoorde onthulling nummer tien alweer… Tijd voor wat reflectie. Ik heb nog een paar cases en een flinke analyse te gaan voor mijn boek "Helpende Hackers" (2015), maar hier alvast een van de conclusies: algemene principes voor ethisch hacken zijn goed, maar casuïstiek is beter. Want of een onthulling verantwoord is, hangt vooral af van de context. En die is voor elk van de betrokkenen weer anders.

Chris van 't Hof
De voorgaande case studies zijn te vinden op www.cvth.nl/vo

Een hacker is ethisch bezig als hij een gevonden kwetsbaarheid netjes meldt bij de eigenaar van het systeem, verder geen gekkigheid uithaalt (malware plaatsen, data downloaden of aanpassen, etc.) en iedereen de tijd geeft het lek te dichten. Gelukkig zijn er steeds meer organisaties die voor Responsible Disclosure beleid hebben om hier goed mee om te gaan: snel de juiste technici inschakelen, communiceren over de voortgang en uiteindelijk credits voor de melder. Zo bereiken steeds meer meldingen de media uiteindelijk niet.

Maar bij veel organisaties is er nog steeds geen RD beleid, of zelfs geen aanspreekpunt. De helpdesk begrijpt niet wat de jongen toch allemaal uitkraamt over vulnerabilities, de systeembeheerder heeft geen tijd, want hij zit al in een lange migratiefase en het management heeft te weinig manuren ingezet op security. Even geduld a.u.b., volgend jaar beter. Dan gaat de hacker met zijn melding maar naar een journalist, of nog erger naar een andere hacker die ermee verder gaat.

Dan is er ineens een CTO of CISO die het incident met open armen ontvangt. Al jaren heeft hij gepleit voor beter patchmanagement en wachtwoorden-beleid. Nu weten ze waarom. Hij weet iemand in het bestuur te overtuigen het gesprek aan te gaan met de hacker en de juridische afdeling op afstand te houden. Een crisisteam wordt samengesteld dat snel werk maakt van het dichten van het lek. De hacker wordt zelfs uitgenodigd een presentatie te houden. Andere organisaties die met hetzelfde beveiligingsprobleem zijn ook uitgenodigd. Mooi!

De geest is echter al uit de fles en er volgen Kamervragen. De oppositie grijpt het bericht aan om de minister aan de tand te voelen: dit lek is geen incident, maar weer het zoveelste voorbeeld dat overheidsinstellingen hun beveiliging niet op orde hebben. Toezicht heeft blijkbaar gefaald. De minister heeft ook het bericht in de krant gelezen. Eigenlijk vindt hij dat de instellingen vooral zelf verantwoordelijk zijn voor de beveiliging, maar hij wil wel het maatschappelijk belang onderstrepen en verschuilt zich achter de toezichthouders die toch echt wat meer tijd nodig hebben.

De politie is ondertussen onderzoek gestart, want het OM wil weten wat er precies is gebeurd. De hacker heeft weliswaar ethisch gehandeld en is eruit gekomen met de instelling, maar er blijken nu meer gedupeerden: de andere organisaties met hetzelfde lek hebben aangifte gedaan. De hacker is dan wel geen verdachte, maar wordt wel gehoord

om uit te zoeken met wie hij de kennis heeft gedeeld. Als hij dit vertelt op een hackersconferentie, ontploft de scene: waarom wordt hij nu gepakt en niet die instellingen die de data lekken?! Weer volgen er kritische mediaberichten en Kamervragen.

Deze fictieve casus is een samenraapsel van dingen die ik tegenkom in mijn onderzoek. Ik kan me goed voorstellen dat ethische hackers zich vaak onbegrepen voelen en natuurlijk hebben journalisten haast met een pakkend verhaal. Ik snap ook dat de ICT-afdeling en het management al genoeg aan hun hoofd hebben, Kamerleden willen debatteren en Justitie wil checken of alles wel klopt. Wie van hen heeft gelijk? Allemaal en daarmee niemand.

Moeten we dan maar lekker relativistisch achterover hangen omdat men elkaar toch niet begrijpt? Nee. Wat we nodig hebben is casuïstiek, zodat we patronen kunnen zien in de handelingen van de betrokken actoren en hun uiteenlopende belevingswerelden. Oftewel: verhalen vertellen. Dat kweekt niet alleen begrip, maar voegt ook een dimensie toe die we nogal eens vergeten bij controversen: de tijd.

De tijdsbeleving van de hacker en systeembeheerder lopen nogal uiteen. De ontdekker ziet meestal vrij direct wat er mis is en hoe het gefixed kan worden, maar ziet niet hoeveel ander werk de systeembeheer nog heeft. Het is niet de enige bug op zijn lijst en bovendien werkt hij met systemen die op een onlogische, maar historisch verklaarbare wijze gekoppeld zijn. Liefst wacht hij op de migratie die over een half jaar plaats vindt. Maar daar kunnen zowel de hacker als de journalist niet op wachten, want ondertussen worden er wel gevoelige persoonsgegevens gelekt.

Of de melding van een lek nieuws is, hangt af van al het andere nieuws en hoe snel het medium is. Nu.nl en Tweakers kunnen binnen een dag publiceren, terwijl EenVandaag soms wel weken nodig heeft om de juiste beelden te vinden voor een TV-item. Dan is er even veel aandacht. Staat kort na de uitzending toevallig een Kamerdebat gepland over ICT, dan is het voorval munitie voor de oppositie en is er meer nieuws. De minister zal moeten antwoorden, maar kan best nog een paar maanden wachten als dat beter uitkomt. Toezichtsorganen komen in de regel ook pas na een paar weken of maanden in actie. Het NCSC is meestal wat vlotter, maar kan uiteindelijk alleen informeren en bemiddelen want zij heeft geen handhavende bevoegdheden. De tijdslijn voor strafrechtelijk onderzoek is nog langer. Dat duurt soms wel jaren.

Als uiteindelijk alle details aan het licht komen, is de media aandacht alweer verdwenen. Door deze wirwar van tijdslijnen springen de meningen alle kanten op. Die blijven hangen in de onderbuik, van waaruit bij een volgende hack weer wordt gereageerd. "Zie je wel dat ze altijd weer de hacker pakken" roept de een. "Nee joh, die hackers zijn gewoon niet te vertrouwen" roept de ander. Wel zijn ze het er over eens dat de overheid altijd te kort schiet. Zo blijven we een ritueel debat voeren. Totdat we terugkijken en zien dat het eigenlijk best de goede kant opgaat met ethisch hacken in Nederland. Steeds meer meldingen worden achter de schermen opgelost. Dat is jammer voor de media, maar goed voor mijn boek.

Rectificatie

In Informatiebeveiliging nummer 5 is bij het artikel "Heartbleed en het risico van open source software" door Frans Bolk een incorrect e-mailadres geplaatst.
Het correcte e-mailadres van Frans is: frans.bolk@uniq-id.com.
Het spijt de redactie des te meer dat deze fout is gemaakt omdat het bleek dat lezers geprobeerd hebben om via het incorrecte adres met Frans in contact te komen. Onze excuses aan Frans en iedere lezer die hier last van ondervonden heeft.

Lex Borger

SHELLSHOCKED

This time we shall look at an undesirable SABSA Attribute, the name of which is, of course, a piece of irony, a way to draw attention to an extensive systemic problem by looking at a recently discovered example of a software bug, nicknamed 'Shellshock'. For those who might have missed the news on this, the nickname applies to a vulnerability discovered in a 20-year old piece of UNIX code, known as the Bourne-Again Shell (BASH for short). The Attributer, ever eager to be topical and relevant, will draw some wider lessons from what is apparently an isolated problem, albeit extensive.

The shock potential of the BASH bug lies in several key points: its 20-year period as an unknown sleeper (how did it get past us for so long?); that so much modern software is built on this low-level code (including LINUX and modern versions of Mac OS X); and finally, that it has been rated by some analysts as vulnerability level 10 out of 10. It couldn't have been much more shocking.

Just at the point at which we are preparing to base our entire domestic and business life management on advanced information technology (the 'Internet of Things'), we are realising that the whole of the software industry output to date is deeply flawed. We 'know' that all complex software contains bugs, but this particular one was 'unknown' until recently. It was a 'known unknown'. Now of course it's a 'known known'. However, it is sufficiently shocking to make us consider how many other 'known unknowns' are lurking in our software assets that are critical to the success of modern society and its economic stability.

We have a great deal of faith in 'open source' software, mainly because it is supposed to be self-regulating in terms of the avoidance of malicious code. Because the entire global community of software engineers gets to poke and prod at the source code in every detail, the likelihood of anyone managing to slip in some malicious code is very small indeed, although not impossible. Even the smartest source code reviewer is incapable of processing a logical trail that has been deliberately designed to have a level of complexity that exceeds their human mental capacity.

Despite the strength offered by extensive public review, the system of open source suffers greatly for the absence of any governance. Coding standards and documentation are often of such poor quality that it is difficult to assess what is actually in the code. The proliferation of interpretive programming languages means that testing is highly dependent on the run-time environment, and even a change of processor can make huge difference to code behaviour. For example, AMD and Intel processors have different default ways to handle exceptions that are unhandled by the application code. Code developed and tested on an AMD chip may not work on an Intel chip. In another example it seems that the published source code for the 'C' language interpreter cannot be compiled to create the same binary object code in the published interpreter. What should we make of such discrepancies?

What's more worrying is that even under this huge public scrutiny of open source, such vulnerabilities as the BASH bug can go undetected for so long, because people don't often find things for which they are not searching.

The Attributer has been told by reliable expert sources that the basic problem is the deeply flawed von Neumann machine architecture (dating from 1945) on which our entire computing capabilities are built. It seems that if we were starting again now, we wouldn't do it that way, but that the global investment in von Neumann architecture is too great to be abandoned.

One day we shall have to grasp this nettle, uproot it and replant with a friendlier specimen. How shall we approach that process? We shall use SABSA Business Attribute Profiling as a means to specify all the desired behaviours of our computing platform architectures. Then we can start again, knowing what we know now, to develop a global infrastructure that is fit for purpose in the modern world.

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, SHELLSHOCK: IS OPEN SOURCE ONVEILIG?

Heartbleed - een kritiek probleem in OpenSSL [1]. Shellshock - een kritiek probleem in Bash [2]. Binnen een paar maanden wordt in een veelgebruikt open source programma een fout gevonden dat zo ernstig is dat systeembeheerders geadviseerd worden alles uit hun handen te laten vallen en éérst deze kwetsbaarheden te patchen. De auteurs verklaren ineens dat het gebruik van hun populaire TrueCrypt programma niet meer veilig is [3]. Strikt genomen zit in TrueCrypt geen open source, maar de source code is beschikbaar voor inspectie. Wat is er aan de hand? Is het zo vertrouwde open source model inherent onveilig? Is het toeval? Moeten we iets veranderen? Kunnen we iets veranderen?


Thomas Sluyter


Ronald van Erven


Maarten Hartsuijker


André Koot

André Koot

Open source en lekken, we zijn er vast nog niet klaar mee wat betreft security dingetjes. OpenSSL, Bash en Truecrypt zijn interessante cases, maar er staat ons vast nog wel wat meer te wachten: OpenStack en CloudStack, beide IAAS platforms. En OpenNebula en Eucalyptus... En wat dachten we van OpenShift, het PAAS platform van Red Hat en wat dacht je van CloudFoundry. Kan allemaal niet goed gaan. Of Docker, een helemaal nieuw veelbelovend containersysteem. En wat te denken van Xen en KVM, daar draait de halve cloud op. En Ceph en Gluster, en Puppet en Juju, Bind, ook allemaal open source. En dus gratis. En allemaal massaal gebruik in de cloud. Er staat ons dus vast nog heel veel meer onheil te wachten. Dan liever closed source oplossingen. Java, Adobe acrobat, Flash spulletjes, Apple Quicktime Internet Explorer, SQL server. Gelukkig allemaal foutloos, geen zorgen voor de security professional... Helaas, zo simpel is de wereld dus niet. Zoals je elders al kon lezen is de aanwezigheid van ernstige kwetsbaarheden niet een diskwalificatie van het fenomeen van open source. Dat de problemen zo ernstig zijn, zegt meer over het succes van open source, of gratis, oplossingen. Voor veel van de hierboven genoemde open source software is echt wel een commercieel alternatief te vinden. Maar daar wordt niet voor gekozen. Vast niet alleen vanwege de prijs. Ook support, functionaliteit en snelheid van ontwikkeling zijn redenen voor de keuze. Belangrijkste boodschap is dat we het change en configuration management op orde hebben, wat voor software we ook gebruiken. En als het om open source gaat, mogen we best een beetje investeren. Geld of tijd, alles helpt.

Maarten Hartsuijker

Het is een beetje Windows vs Linux of IOS vs Android. Het antwoord op of open source veiliger is dan closed source hangt sterk samen met aan wie je het vraagt. De veiligste software wordt naar mijn mening geschreven door de meest beveiligingsbewuste programmeur. En zelfs bij die persoon is een foutje menselijk. Het blijft natuurlijk een feit dat je bij open source software door code-analyse gerichter naar fouten kunt zoeken. Maar het is ook evident dat je in closed source makkelijker een achterdeurtje kunt verbergen. En zo zijn er legio verschillen op te noemen die wisselend in het voordeel van één van beide smaken pleit. Was de bash bug nou zo'n typische "open source" fout? Naar mijn mening niet. Een dergelijke fout kun je zowel in open als closed source programmatuur aantreffen. Dit geldt ook voor Heartbleed. Bij TrueCrypt speelde vooral een vertrouwenskwestie. Wat doe je als bedrijf of beveiligingsbewuste gebruiker als een ontwikkelaar meldt dat zijn product onveilig is, maar verder geen details geeft? Stop je met het gebruik ervan? Ook het antwoord op deze vraag is niet open/closed source specifiek. Aan de bash-bug hadden we in elk geval weer een interessante. Met name omdat de impactanalyse van deze kwetsbaarheid zeer complex was en in elk geval vele malen intensiever dan het doorvoeren van een eenvoudige update. Je moet immers het hele landschap én codebase volledig kennen. En zelfs dan weet je niet of er closed source programmatuur aanwezig is van waaruit deze open source shell wordt aangeroepen. Dus of we nu met closed of open source van doen hebben: het devies blijft patchen, patchen, patchen.

Ronald van Erven

Ik denk niet dat het gebruik van open source meer of minder veilig is geworden. Wat wel duidelijk is, is dat veel van deze problemen (Hearthbleed of Shellshock) diepgewortelde problemen zijn in technologieën die gebruikt worden en waarop volop is doorgebouwd met allerlei diensten. Ofwel we bouwen een huis op een fundament dat fouten bevat. En die fouten in het fundament komen op zijn tijd naar boven toe. Open source kan helpen om dergelijke fundamentele fouten naar boven te krijgen. Ten tijde dat internet enkel gebruikt werd om informatie te delen waren deze issues geen probleem. Maar met de commercialisering van internet zijn de belangen veranderd en moet er iets gevonden worden om fundamentele technische fouten uit het fundament te halen. En dat kost tijd, geld en soms iemand zijn trots.

Thomas Sluyter (gast redacteur)

Dat het roerige tijden zijn in Internetland staat buiten kijf, elk jaar staan we weer te kijken van nieuwe beveiligingsproblemen in de ICT. Waren tien jaar geleden virussen en malware groot nieuws, tegenwoordig lijkt de aandacht te zijn verschoven naar afluisterschandalen, encryptie en het massale stelen van data. Over het aangehaalde TrueCrypt kunnen we kort zijn: de fabrikant heeft dat product end-of-life verklaard. Zij is daarmee niet plotseling onveilig geworden, maar de gebruiker dient zich bewust te zijn dat het niet langer future-proof is. TrueCrypt gaat in wezen Windows XP achterna. Wat betreft de vraag of open source software inherent onveilig is, zal ik ten stelligste "nee" antwoorden: het feit dat broncode openlijk beschikbaar is maakt een product niet onveilig. Ik denk echter wel dat wij het vaak aangehaalde credo "vele ogen kijken mee, dus het is veiliger" moeten ontkrachten. Zo is aan het licht gekomen dat de Shellshock problematiek met de Bash shell al bijna twee decennia mee gaat! [4] De oorzaak ligt hier in de gebruikte programmeerstijlen en de verouderde code van Bash. Let wel: dit soort problemen spelen bij alle software projecten! Bij closed source software zullen wij ze echter nooit zelf kunnen ontdekken. Wat mij terugbrengt bij het eerder aangehaalde credo. Vele ogen die mee kijken kunnen een open source project wel degelijk veiliger maken, zolang men het werk van de voorgangers niet voor lief aanneemt en durft te herschrijven. Het aanpakken van de zogenaamde 'technical debt' is iets dat bij veel projecten lage prioriteit krijgt, maar wat mij betreft continu onder de aandacht moet blijven.

Thomas is Unix & security consultant bij Unixerius.

Links

[1] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
[2] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
[3] http://truecrypt.sourceforge.net/

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 (Classity)
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

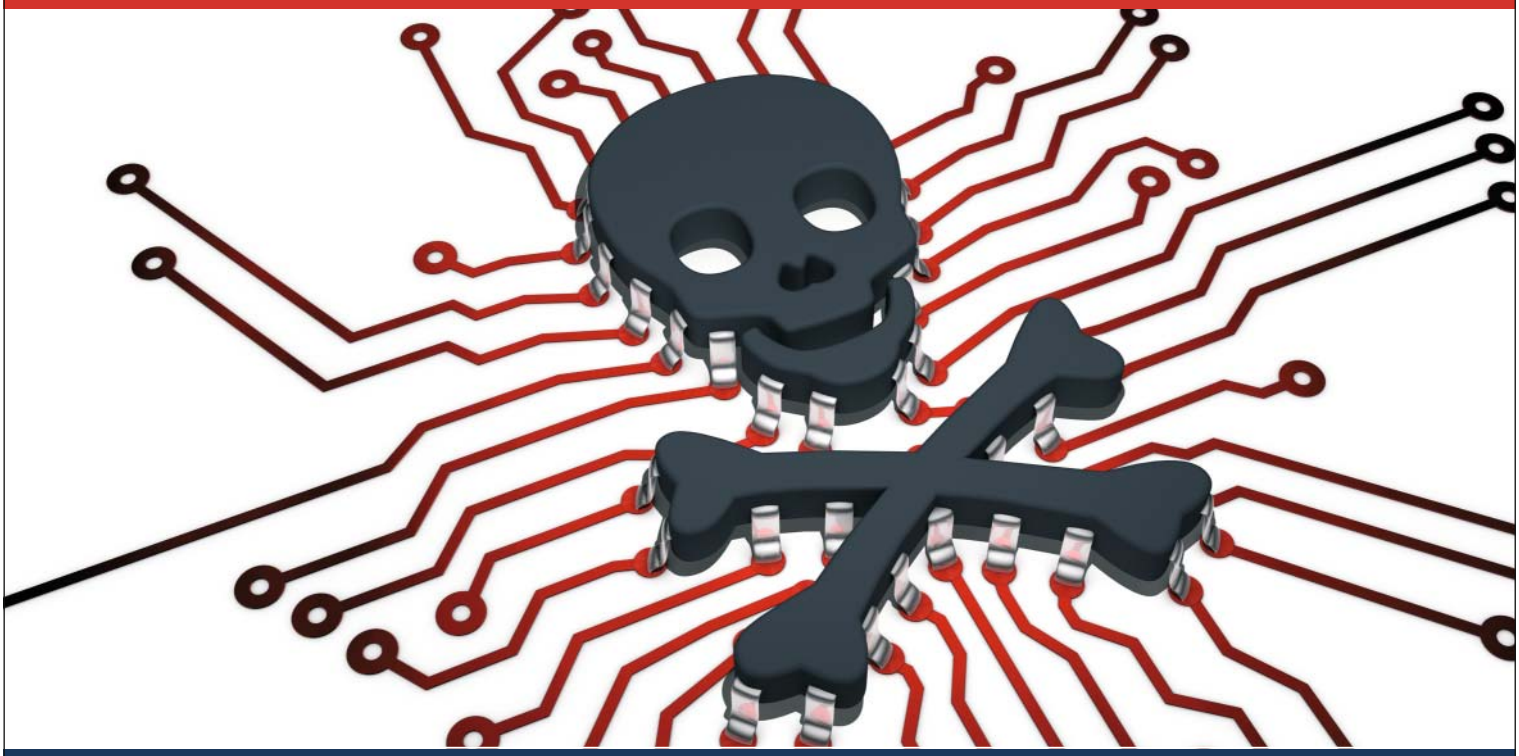
VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

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



DE CYBERCRIMINEEL

Een ieder weet natuurlijk wat het oudste beroep ter wereld is, maar als ik vraag wat één van de jongste beroepen is dan wordt het al gauw stil. Ik zal het maar snel verklappen, een van de jongste beroepen is het beroep van cybercrimineel (CC) die nog maar een jaartje of 25 bestaat. Geleerden hebben uitgevonden dat de CC voor het eerst is ontdekt na het ontstaan van het internet. Goh, wat kun je toch snel als geleerde door het leven gaan. Een beetje een open deur want waarom zou je CC worden als je geen netwerk of websites hebt waarop je kunt inbreken. Overigens heb je als CC een echt beroep, daar waar ze begonnen met lange baarden en liters cola zitten nu in driedelig grijs in chique panden.

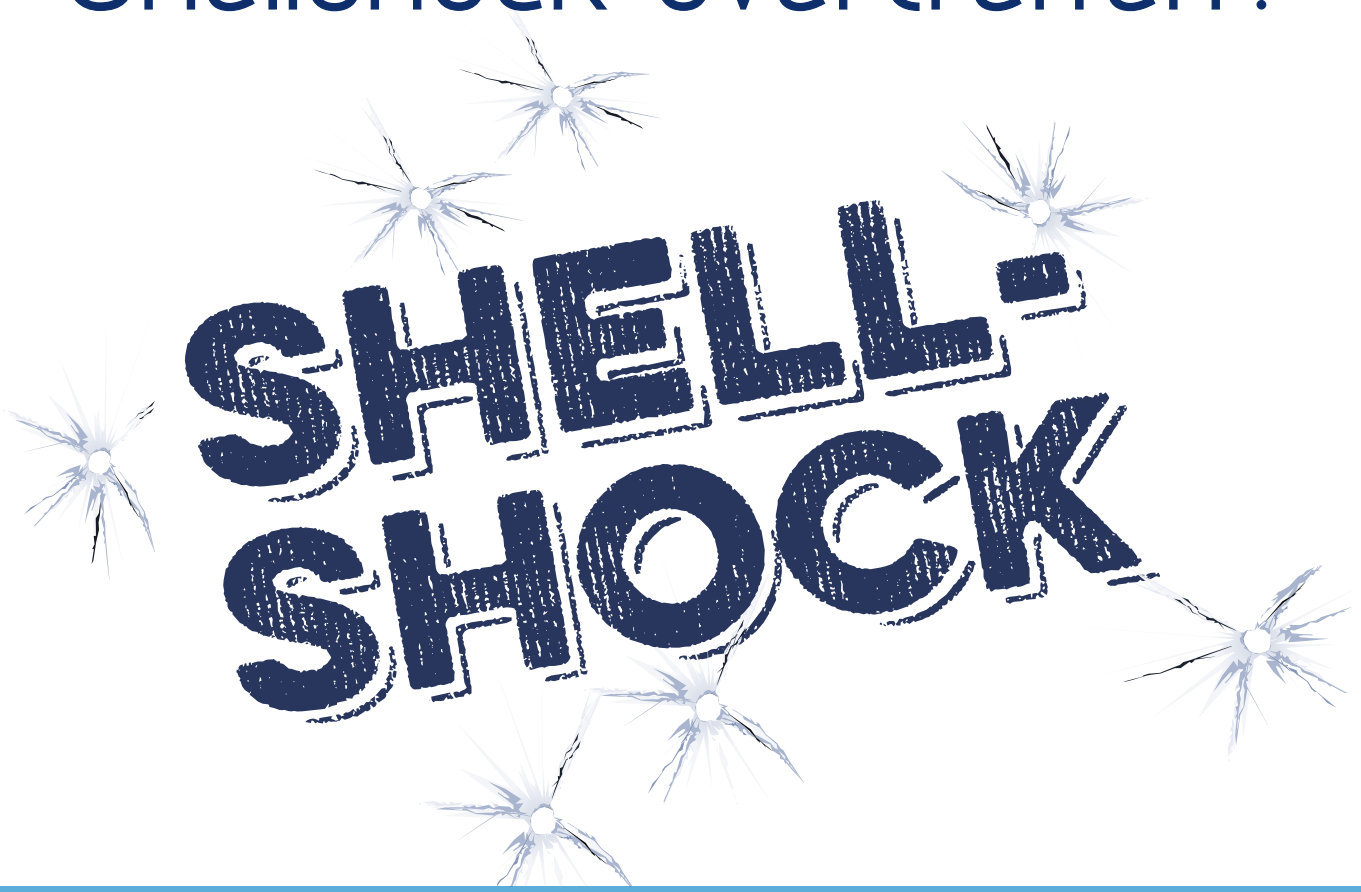
Een ieder die deze column weleens leest weet dat ik een haat-liefde verhouding heb met het internet. Het is geweldig dat de hele wereld vanaf je bureau te benaderen is en dat je een bewering in de kroeg dat een Gierzwaluw in de lucht paart, onmiddellijk kan verifiëren op je telefoon. Je kunt binnen 10 seconden vaststellen dat de Ikea het door jou gewenste kastje op voorraad heeft. U begrijpt dat ik nog tientallen voorbeelden kan noemen van het internet die het leven echt veel plezieriger of moet ik zeggen makkelijker heeft gemaakt. Daar tegenover staat dat die elektronica winkel bij mij op de hoek het hoofd niet boven water heeft kunnen houden, die zag zijn klanten naar de webwinkel verdwijnen. Het bankgebouw waar ik vroeger mijn betaalcheques ophaalde is leeg. Onze postbode komt op zaterdag langs met de folder van de hamsterweken.

Ook in deze categorie zijn tientallen voorbeelden te noemen die het leven wel makkelijker, maar zeker niet plezieriger hebben gemaakt.

Daar waar de CC door het ontstaan van het internet een baantje kreeg, hebben velen of zullen velen hun baan verliezen of ze krijgen een andere invulling van hun werk. De bankmedewerker, vroeger een notabele, tegenwoordig niet in maar op de bank, datzelfde geldt voor de gehele financiële sector. De fotozaken, de videotheken, de zelfstandige detailhandelaar, zelfs de huisarts dreigt in het beeldscherm te verdwijnen. Als schrale troost kan ik aangeven dat ik de boel een beetje gefopt heb, een cybercrimineel is niet het jongste beroep, nog sterker na zijn komst kwamen nog tientallen nieuwe beroepsgroepen. Denk aan de experts die medicijnen voor de computervirussen bedenken en hun oplossingen verkopen aan een ieder die het belangrijk vindt, firewalls die een scheiding moeten geven tussen wie wel en wie niet verder mag, beveiligingsbedrijven, beveiligingsadviseurs, beveiligingsarchitecten, privacy officers, information security officers, compliance officers, security specialisten en ook nu zou ik weer met tientallen beroepen kunnen doorgaan. De strijd tegen cybercriminelen is inmiddels een miljardenindustrie geworden waar vele lezers van deze column ook een fijne boterham mee verdienen. Dus waarom zouden we klagen.

Berry

Welke kwetsbaarheid zal Shellshock overtreffen?



Dit lek is ruim 20 jaar verborgen gebleven voor het grote publiek. Aanvallen op computersystemen worden in versneld tempo gecompliceerder. Zonder gebruik van de juiste software is het vrijwel onmogelijk de huidige bedreigingen buiten de deur te houden en data binnen de deur. Hebt u naast een virusscanner wel zaken geïnstalleerd als multipass authenticatie? Wordt uw netwerk automatisch gemonitord op verdachte activiteiten? Zorg dat u goed voorbereid bent en weet wat er op uw netwerk speelt. De software en diensten van CRYPSYS helpen uw informatiebeveiliging onder controle te houden.

CRYPSYS oplossingen zijn fexibel

CRYPSYS