06/2013

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 6 - 2013

MET PATCHEN KUN JE NIET WINNEN

NO FUNCTION CREEP BY DESIGN

BOB LORD OVER SECURITY BIJ TWITTER

LANDELIJKE CAMPAGNE TEGEN IDENTITEITSFRAUDE

TWEE DAGEN ONDER HACKERS BIJ HACK IN THE BOX

FOX IT

for a more secure society

FOX-IT voorkomt, onderzoekt en beperkt de meest serieuze cyberdreigingen met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. Onze aanpak combineert slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. We ontwikkelen producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.

FOX-IT.COM

Fox zoekt nieuwe Foxers

FOX-IT groeit en bloeit. Om deze reden zijn wij over de volle breedte van ons werk op zoek naar hackers, Forensic Experts, Pentesters, Developers (Python / C++), Hardware Engineers en Fraude analisten. Een Foxer is nieuwsgierig, kritisch en talentvol.
Je draagt bij aan de missie van FOX-IT: having fun in making technical and innovative contributions for a more secure society

Interesse om bij ons te komen werken?
Bel of mail Walter Doorduin 06 41901011 of doorduin@fox-it.com.

VOORWOORD

Recentelijk zijn twee emaildiensten gestopt, *Lavabit* en *Silent Circle*. *Lavabit* is duidelijk gezwicht voor de druk van de Amerikaanse geheime diensten. *Silent Circle* wil de eer wat meer aan zichzelf houden, maar lijkt toch wel geleid te zijn door het gevoel als medeplichtige gezien te worden aan het lekken van gevoelige informatie. Het bekend worden van het bereik van het afluisterprogramma van de Amerikaanse geheime dienst, PRISM, heeft twee feiten op de kaart gezet:

1. Alles kan worden afgeluisterd en de geheime diensten schuwen niet om hier grote investeringen in te doen.
2. Als je *end-to-end* encryptie gebruikt ben je al verdacht.

Over dat eerste punt is al veel geschreven en kan nog meer geschreven worden, maar op het tweede punt wil ik wat dieper ingaan. *End-to-end* encryptie is versleuteling waarbij de verlener van de dienst geen mogelijkheid heeft om de encryptie te omzeilen, alleen een *brute force* kraak is mogelijk. Dit is anders dan email met SSL beveiligen, want die versleutelen de email alleen tijdens transport naar de emailprovider.

Bankovervallers hebben auto's gebruikt en valsemunters drukpersen, maar dat betekent niet dat auto's en drukpersen illegaal zijn. Waarom is op deze manier versleutelde email dat dan wel? Briefgeheim is altijd gezien als een groot goed en we bewaren waardevolle spullen in kluizen. Dat is ook niet illegaal of verdacht. De basis van de verdachtmaking ligt in het feit dat geheime diensten het niet kunnen lezen, los van het feit of ze dat wettelijk mogen of niet.

Dat maakt ons, gebruikers van versleutelde email, kennelijk verdacht. Net zoals Trayvon Martin verdacht was. En, zoals we in dat geval gezien hebben, kunnen onterechte verdachtmakingen aardig uit de hand lopen.

De tegenbeweging is ook al begonnen: *Mega's* Kim Dotcom heeft plannen om zijn eigen versleutelde emaildienst op te zetten. Kim schuwt niet om de Amerikaanse overheden op de kast te jagen en heeft daar in het verleden al flink last mee gehad. Ik heb hier een dubbel gevoel over, omdat dit het imagoprobleem dat versleutelde email nu al heeft, alleen maar versterkt.

Wat kunnen we dan doen? Generaal Petraeus dacht veilig te zijn door geen email meer uit te wisselen met zijn minnares, maar alleen conceptberichten achter te laten in een gezamenlijk *Gmail* account. Aapten ze de filmwereld na? Of was hij zo slim om uit te zoeken dat hij daarmee de triggers in PRISM omzeilde? Het heeft in ieder geval niet gewerkt, en geresulteerd in het bekende schandaal. Dit is dus niet het pad om te bewandelen.

Voor het juiste pad hoef je niet lang te zoeken. Dat is een product dat al heel lang bestaat. Het is alleen opvallend stil rondom dat product. Een teken dat de gebruikers doorhebben dat ze nu even beter niet al te hoog van de toren moeten blazen? Ik heb het over PGP (*Pretty Good Privacy*). In 1991 geschreven door Phil Zimmermann in een tijd dat encryptie niet geëxporteerd mocht worden. Toen was het een schandaal dat PGP de exportregels had omzeild. Inmiddels is het een standaard (OpenPGP - RFC 4880) en zijn er meerdere implementaties, zoals bijvoorbeeld het open GPG (GNU Privacy Guard). Het voordeel is dat je het met iedere emailprovider kunt gebruiken. Het nadeel is dat het bewerkelijk blijft: Je moet zelf sleutels uitwisselen met je emailvrienden. Het is nog geen gemeengoed en zolang versleutelde email een crimineel stigma heeft zal het dat ook niet worden.

Lex Borger, hoofdredacteur

INHOUDSOPGAVE

Foto omslag: Sleutelbeheer. CC BY-SA: Ellick

MET PATCHEN KUN JE NIET WINNEN; WEL VERLIEZEN

Ir. Dennis Baaten is information security officer bij de ANWB en bereikbaar via dbaaten@anwb.nl

Het tijdig installeren van updates (het zogenaamde 'patchen') is van cruciaal belang voor de informatiebeveiliging van een organisatie. Het aantal berichtgevingen in de media over kwetsbaarheden en het misbruik ervan, zorgt terecht voor de nodige verontrusting binnen en buiten de ICT-afdeling. Toch zorgen spanningsvelden in een organisatie ervoor dat het doorvoeren van patches niet zonder slag of stoot gaat. Overvolle agenda's bij beheerders, de eeuwige strijd om capaciteit en prioriteit, en een business die het patchen eerder als last dan als baat ervaart. Gelukkig hoef je hier niet in te berusten, maar kun je er ook iets aan doen.

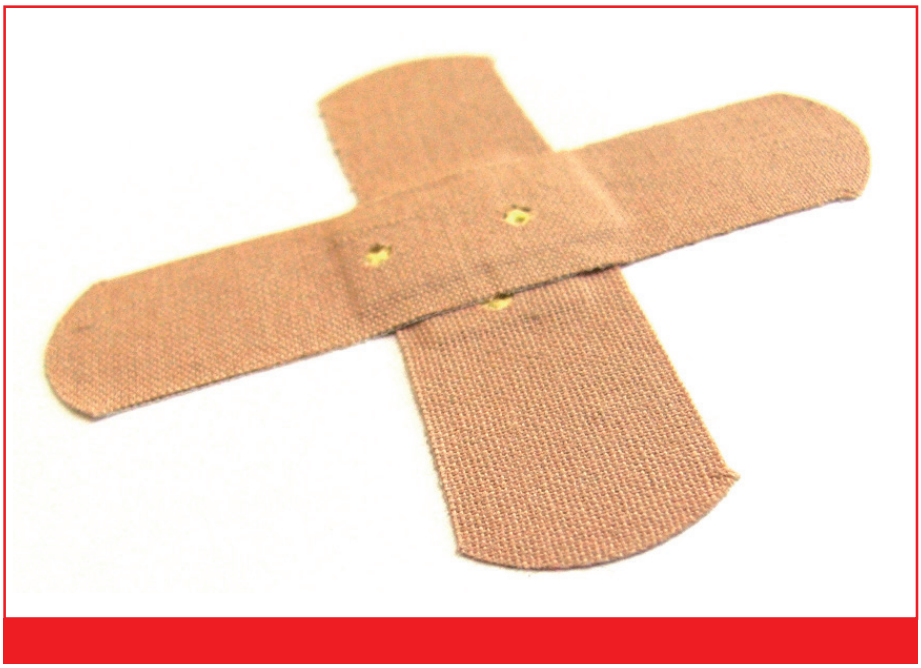
Het ICT-landschap van grote multidisciplinaire organisaties kent doorgaans een hoge complexiteit. Door de constante druk vanuit de business die de concurrentie een stapje voor wil blijven, volgen veranderingen en vernieuwingen elkaar in hoog tempo op. Tegelijkertijd blijft het ICT-budget dalen en lijkt 'meer voor minder' een door de crisis ingegeven noodzakelijke trend. De agenda's van de ICT-specialisten zitten vol met projecten waardoor er voor beheerwerkzaamheden (te) weinig tijd overblijft. Terwijl juist het beheer ervoor zorgt dat het ICT-landschap naar tevredenheid en met acceptabele risico's blijft functioneren.

Het overgrote deel van alle informatiebeveiligingsincidenten vindt plaats als gevolg van misbruik van kwetsbaarheden in verouderde software. Door het installeren van updates worden de gaten in de beveiliging verholpen en verdwijnt het risico op misbruik. Dit risico kan echter nooit tot nul teruggebracht worden, omdat patchen een reactief proces is. Je blijft afhankelijk van de snelheid waarmee een leverancier in staat is om patches voor ontdekte kwetsbaarheden uit te brengen. Hackers maken daarom in toenemende mate gebruik van zero-day-exploits om gaten in software te misbruiken voordat de leverancier van de software op de hoogte is van de kwetsbaarheid. Wanneer de leverancier dagen of weken na het geconstateerde misbruik een patch beschikbaar stelt, is het aan de eigen organisatie om patches snel uit te rollen. Hoe langer je wacht met updaten, des te groter de kans op misbruik. Maar het realiseren van een korte doorlooptijd voor organisatiebreed uitrollen van patches, blijkt vaak niet eenvoudig.

Patch achterstand oorzaak groot deel informatiebeveiligingsincidenten

Focus op het verkeerde risico

Veel organisaties hebben een standaard patchproces dat start bij het beschikbaar komen van een patch. De eerste stap is vaak het bepalen



van de prioriteit van de patch in termen van maximale doorlooptijd waarbinnen een patch uitgerold dient te zijn. Dit gebeurt op basis van (objectieve) externe bronnen en eigen kennis van het ICT-landschap, en is vaak vastgelegd in een beleidsdocument. De resulterende prioriteit kan worden gezien als een weerspiegeling van het risico dat de business bereid is te lopen. Na prioritering wordt de patch verpakt in een installatiescript en wordt de uitrol ervan getest. Bij een succesvolle test wordt het patchpakket (de daadwerkelijke patch + het installatiescript) organisatiebreed uitgerold. Op papier klinkt dat eenvoudig, maar de praktijk is helaas weerbarstiger.

In de praktijk heb ik inmiddels de nodige vertragende factoren de revue zien passeren. Zo komt het voor dat er teveel tijd nodig is om het patchpakket goed werkend te krijgen, maar heb ik ook gezien dat het testtraject te lang duurt doordat er onvoldoende capaciteit en middelen beschikbaar zijn om in korte tijd een representatieve test uit te voeren. Het is echter niet alleen de ICT-afdeling waar de vertragende factoren vandaan komen. Ook de business zorgt voor vertragingen, omdat men bijvoorbeeld niet altijd goed lijkt te begrijpen waarom een patch nodig is. En als je dat combineert met het feit dat de business niet altijd evenveel vertrouwen heeft in de ICT-afdeling, dan snap je wellicht ook waarom soms de hakken in het zand gaan.

Rol vrijgekomen beveiligingsupdates snel uit!

Dergelijke vertrouwenskwesties tussen de business en ICT zijn niet ongebruikelijk. Vaak worden ze veroorzaakt door ontevredenheid over de geleverde diensten en/of de moeizame procesgang die daaraan vooraf gaat. Bij patchen loopt het vertrouwen een deuk op wanneer er te vaak verstoringen worden veroorzaakt als gevolg van fouten tijdens het uitrollen. Vanuit de gedachte "hoe minder patches, hoe kleiner de kans dat er iets misgaat", probeert de business het uitrollen van patches tegen te houden om meer verstoringen te voorkomen. Een begrijpelijke emotie, maar vaak ligt hier niet de juiste afweging aan ten grondslag. De business focust in zo'n situatie teveel op het risico van verstoringen als gevolg van een foutieve patch, en verliest hierbij het oorspronkelijke risico uit het oog. En dat is het risico op misbruik als gevolg van een kwetsbaarheid.

Onzekerheid over bijeffecten patches leiden vaak tot uitstel

Je springt niet hoger door de lat te verlagen

De uitvoerende teams die binnen de ICT-afdelingen verantwoordelijk zijn voor het uitrollen van patches, worden continu met dit gebrek aan vertrouwen geconfronteerd. En doordat er ook de nodige druk ligt om patches snel door te voeren, komen de teams in een tweestrijd terecht. Het is of toegeven aan de druk vanuit de business om niet te patchen, of toegeven aan de druk vanuit het management om (vanuit het belang van informatiebeveiliging) wel te patchen. En omdat druk altijd de makkelijkste weg naar buiten zoekt, barst intern de discussie los aan het bureau van de information security officer.

Met name in de periodes waarin er in korte tijd veel kritieke patches uitkomen, houdt het patchen de gemoederen flink bezig. Van managers tot beheerders, velen stellen het huidige beleid ten aanzien van de prioritering van patches ter discussie. Er wordt sterk aangestuurd op het verhogen van de maximale doorlooptijd voor patches, maar dat is vanuit informatiebeveiliging zelden een goed idee. Niet omdat het zo leuk is om collega's te dwarsbomen, maar omdat een versoepeling van de norm niet de oplossing is voor dit probleem. Daarmee zou je alleen maar risico's introduceren waarvan de organisatie heeft aangegeven deze niet te willen lopen.

Verkorten van de doorlooptijd

De oplossing tot lage doorlooptijden is gelegen in een goede samenwerking tussen verschillende teams (dus

inclusief de business) vanuit een gemeenschappelijke doelstelling: een functionerend ICT-landschap met acceptabele risico's. Dat klinkt misschien cliché maar daarom, zoals wel vaker het geval met clichés, niet minder waar. Hieronder een aantal tips die je kunt toepassen:

1. *Inrichten van operationeel patchproces* – Richt het patchproces binnen de ICT-afdeling fatsoenlijk in. Zorg dat er voldoende capaciteit en prioriteit is voor het test- en uitrolteam. Vaak is dit een interne aangelegenheid en hoeft de business slechts geïnformeerd te worden.
2. *Leer van je fouten en kijk vooruit* – Fouten maken is niet erg, maar zorg er wel voor dat het er niet teveel zijn en leer ervan. Blijf zo min mogelijk in het verleden hangen en geef elkaar vertrouwen om het opnieuw te proberen. Anders is een poging om het over de inhoud eens te worden bij voorbaat gedoemd te mislukken.
3. *Hanteer een gefaseerde uitrol* – Rol niet uitsluitend uit met een big-bang, maar zorg voor een gefaseerde aanpak waarbij het risico op organisatie brede verstoringen wordt verkleind. Zorg dus voor voldoende mogelijkheden om patches gespreid uit te rollen, zodat de impact van onvoorziene verstoringen kan worden beperkt.

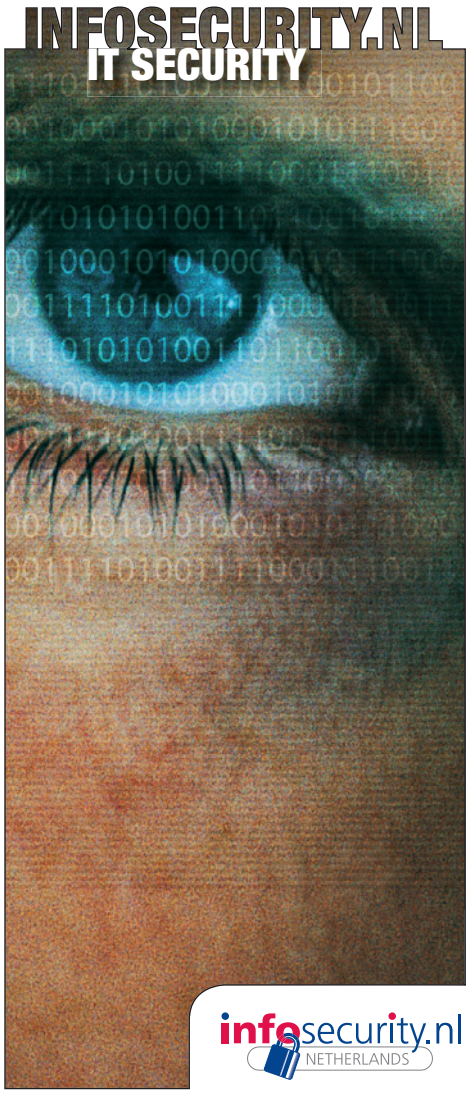
Gefaseerd uitrollen beperkt de patchrisico's

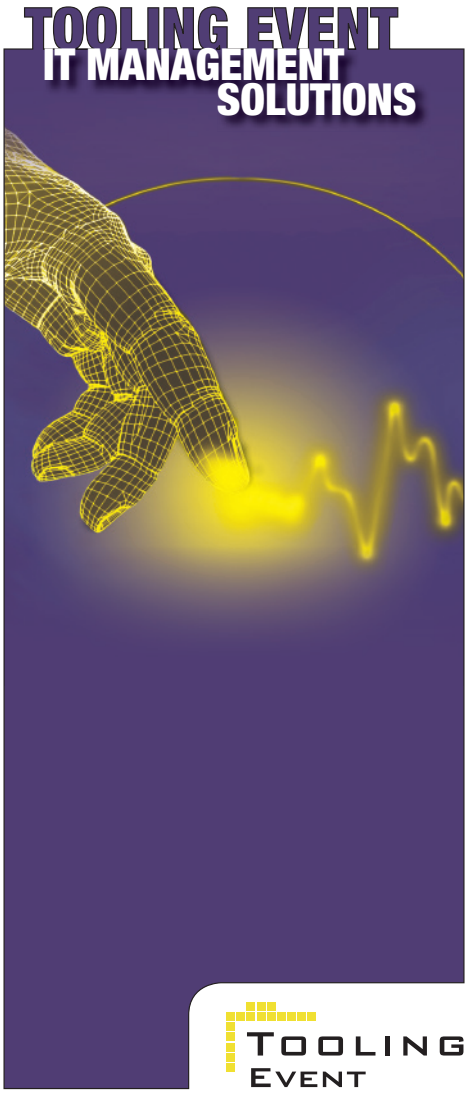
4. *Focus op de risico's* – Zorg dat iedereen begrijpt waarom het belangrijk is dat patches tijdig worden geïnstalleerd. Leg uit welke risico's er zijn, en benadruk dat risico's niet zomaar door specifieke afdelingen kunnen worden geaccepteerd, omdat misbruik van kwetsbaarheden de gehele organisatie treft.
5. *Spreek vaste onderhoudsvensters af* – Plan voldoende momenten in om patches en andere onderhoudswerkzaamheden uit te voeren. Maak met elkaar afspraken over hoe je omgaat met belangrijke patches buiten de vaste onderhoudsvensters.

Patchen is geen rocket science, maar een samenspel waar iedereen zich aan een vastgestelde set met spelregels dient te houden. Bovenstaande tips kunnen helpen de doorlooptijd te verlagen en daarmee het risico verkleinen. Snel en adequaat reageren op een kwetsbaarheid door te patchen vrijwaart je niet van computerinbraken, maar rekent wel grotendeels af met hackers die gaan voor het laag hangende fruit. En dat zijn er veel, heel veel. ●

30 - 31 OKT 2013 JAARBEURS UTRECHT

VAKBEURZEN, SEMINARS EN ONLINE MATCHMAKING VOOR IT-MANAGERS EN IT-PROFESSIONALS





REGISTRATIE VANAF 1 SEPTEMBER OPEN

WWW.INFOSECURITY.NL | WWW.STORAGE-EXPO.NL | WWW.THETOOLINGEVENT.NL

KEYNOTES | SEMINARS | CASE STUDIES | RUIM 150 EXPOSANTEN

Reed Exhibitions marqit vnu exhibitions europe

OPINIE

NO FUNCTION CREEP BY DESIGN

Mr. ing. E.M. Wesselingh, De Haagse Hogeschool (e.m.wesselingh@hhs.nl)

Een populair model voor het beter borgen van privacy is "privacy by design" [1]. Wat ik een beetje mis in het model is het intrinsiek veilige model. Het zit er wel in verwerkt, met name in het principe dat er zo weinig mogelijk data moet worden verzameld, maar dat is niet genoeg. Er wordt niet echt expliciet gemaakt dat je dit moet inbouwen door bepaalde zaken uit te sluiten ofwel onmogelijk te maken. Daarmee wordt privacy toch weer een soort van "on top of" te bouwen module en daar gaat het zo vaak fout, zoals informatiebeveiligers weten.

Er wordt er nog te vaak uitgegaan van de mogelijkheid tot inbouwen van toekomstige functionaliteiten in plaats van het expliciet uitbouwen daarvan. Daarmee wordt de mogelijkheid opengelaten om er later nog meer functionaliteit aan toe te voegen. Dat introduceert twee problemen: er komen steeds meer "nice to haves" in de functionele eisen en "function creep" wordt gefaciliteerd. Voorbeelden waarbij privacy in het geding is zijn de koppeling van databases om sociale zekerheidsfraude op te sporen en het opvragen van gescande nummerplaten door de belastingdienst. Ik pleit daarom voor een systeem dat inherent veilig is qua privacy: er kan gewoon weinig aangebouwd worden, een soort van inherent veilige stand.

> De mogelijkheid wordt opengelaten om later nog meer functionaliteit toe te voegen

Zo'n systeem zou toegepast kunnen worden in het hedendaagse paspoort. In het kader van "als we iets echt niet willen, moeten we het technisch onmogelijk maken" [2] doe ik hier een voorstel tot een ander design. Het paspoort zoals het nu bestaat heeft twee biometrische kenmerken. Dit vloeit voort uit de Europese Verordeningen 2252/2004 [3] en 444/2009 [4] over veiligheidskenmerken en biometrische gegevens in paspoorten en reisdocumenten. De eerste verordening geeft de eisen aan biometrische kenmerken, de tweede een wijziging die is ingevoerd vanwege problemen bij de afname van vingerafdrukken bij jonge kinderen [3].

De verordeningen eisen dat een paspoort of reisdocument twee platte vingerafdrukken bevatten van de houder van het betreffende document. Op dit moment heeft de Raad van State in vier zaken over de onrechtmatigheid van vingerafdrukken prejudiciële vragen gesteld aan het Hof van Justitie van de Europese Unie [5], en ook uit Duitsland liggen vragen bij het hof voor [6]. In die laatste zaak heeft de Advocaat-Generaal op 13 juni 2013 zijn opinie gegeven. Er is dus nog geen uitspraak van het hof, maar in ongeveer 75% van de gevallen volgt het Hof de conclusie van de Advocaat-Generaal.

Verordening 2252/2004
art. 1 lid 2: "Voor deze paspoorten en reisdocumenten wordt een opslagmedium gebruikt dat een gezichtsopname bevat. De lidstaten nemen ook vingerafdrukken in een interoperabel formaat op. [..]"

art. 4 lid 3: "Voor de toepassing van deze verordening mogen de biometrische kenmerken in paspoorten en reisdocumenten alleen worden gebruikt voor het verifiëren van:
a) de authenticiteit van het document;
b) de identiteit van de houder door middel van direct beschikbare vergelijkbare kenmerken wanneer het overleggen van een paspoort of andere reisdocumenten wettelijk vereist is."

Verordening 444/2009
art. 1 lid 2: "Deze paspoorten en reisdocumenten bevatten een opslagmedium dat aan de hoogste veiligheidseisen voldoet en een gezichtsopname bevat. De lidstaten nemen ook twee platte vingerafdrukken in een interoperabel formaat op. De gegevens worden beveiligd en het opslagmedium heeft voldoende capaciteit en is voldoende geschikt om de integriteit, de authenticiteit en de vertrouwelijkheid van de gegevens te garanderen."

Kort door de bocht gezegd zijn de verordeningen niet strijdig met overig EU-recht en kan iedere lidstaat eisen dat een individu vingerafdrukken overlegt om een paspoort aan te kunnen vragen.

> De Raad van State heeft in vier zaken vragen gesteld over de onrechtmatigheid van vingerafdrukken

Maar waarom worden eigenlijk vingerafdrukken geëist? Dat is zo handig voor de opsporing van misdrijven (wat overigens met nadruk wordt uitgesloten in de verordeningen). Waarom geen systeem waarmee opsporing juist buiten het identificatie-proces wordt gehouden? Er zijn ook andere biometrische kenmerken die kunnen worden gebruikt zoals de irisscan (al een aantal jaren in gebruik op Schiphol). Of dit systeem betrouwbaarder is dan vingerafdrukscan weet ik niet, maar ik constateer wel dat het systeem op Schiphol al een aantal jaren klaarblijkelijk naar tevredenheid functioneert. Bij deze dus mijn oproep tot een ontwerp voor een identificatieschema gebaseerd op persoonskenmerken die niet direct inzetbaar zijn bij opsporing. No function creep by design! ●

Referenties:

[1] *Ann Cavoukian, Ph.D., Privacy by Design - The 7 Foundational Principles, https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf*

[2] *Jeroen Terstegge en Klaas Bruin, Het portret – Mireille Hildebrandt: "Als we iets echt niet willen, moeten we dat technisch onmogelijk maken", in Privacy & Compliance 03-04/2012, Baltzer Science Publishers*

[3] *Verordening (EG) Nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten, gepubliceerd 29 december 2004, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:NL:PDF*

[4] *Verordening (EG) Nr. 444/2009 van het Europees Parlement en de Raad van 28 mei 2009 tot wijziging van Verordening (EG) nr. 2252/2004 van de Raad betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten, gepubliceerd 6 juni 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:142:0001:0004:NL:PDF*

[5] *Zaken Willems – Burgemeester van Nuth (C-446/12), Kooistra – Burgemeester van Skarsterlân (C-447/12), Roest – Burgemeester van Amsterdam (C-448/12) en Van Luijk – Burgemeester van Den Haag C-449/12*

[6] *Conclusie van Advocaat-Generaal P. Mengozzi van 13 juni 2013, zaak C-291/12 Michael Schwarz tegen Stadt Bochum, http://curia.europa.eu/juris/document/document.jsf?text=&docid=138362&pageIndex=0&doclang=NL&mode=lst&dir=&occ=first&part=1&cid=5297202*

COLUMN

STERFT JE PRIVACY NA JE DOOD?

Als we ten hemel stijgen, ten grave gedragen worden, de pijp aan maarten geven, het hoekje omgaan of niet meer uit de as zullen herrijzen, maakt het dan eigenlijk nog wat uit of je recht op privacy hebt? Ik moest hieraan denken toen ik alle berichtgeving las rond de dood van 'Roelie', de vrouw die in 2012 overleed in een instelling nadat zij minutenlang door vier medewerkers in bedwang was gehouden. Haar zussen zijn boos op de Raad van Bestuur van de instelling. Door een interview te geven aan NRC heeft de Raad de privacy van 'Roelie' geschonden, zo stellen zij.

Wie het nieuws een beetje gevolgd heeft, weet dat dit een zeer verdrietige zaak is waarin heel veel is misgegaan. De instelling was er niet op toegerust om patiënten in bedwang te houden. Vrijheidsbeperkende maatregelen mogen alleen door Bopz-instellingen toegepast worden en dat was deze instelling dus niet. De camerabeelden waren op televisie te zien in *Nieuwsuur* nadat de instelling tevergeefs geprobeerd had dit door een kort geding te voorkomen. De instelling meende dat de privacy van de patiënte geschonden zou worden indien de beelden op tv te zien zouden zijn. De rechter liet echter vrijheid van pers als beginsel prevaleren.

De camerabeelden zouden overigens afkomstig zijn geweest uit het justitiedossier. Als dit echt waar is, dan vraag ik mij oprecht af wie binnen het overheidsapparaat de afweging gemaakt heeft dat de privacy van het op camera stervende slachtoffer ondergeschikt is aan nieuwsgaring en dat de beelden dus wel naar buiten konden. De privacy van verdachten is sowieso vaak stukken beter geregeld dan die van slachtoffers. Het OM heeft bijvoorbeeld een zeer uitgebreide richtlijn over hoe omgegaan moet worden met de privacy van verdachten, waarin ook geregeld is hoe om te gaan met camerabeelden. Voor slachtoffers is niets geregeld door het OM.

Maar, sterft je privacy nou eigenlijk als je dood gaat? Welnu, een beetje, maar gelukkig niet helemaal. De Wet Bescherming Persoonsgegevens is niet meer van toepassing als je dood bent, daar kun je dus als nabestaande geen beroep op doen. De praktijk leert echter wel dat veel bedrijven procedures hebben waarbij nabestaanden de persoonsgegevens van overleden dierbaren kunnen laten wissen. Daartoe zijn ze niet verplicht, maar het is *common sense*. Ze doen het uit respect voor hun klanten. Om te verhinderen dat camerabeelden of foto's gepubliceerd worden, kunnen nabestaanden een beroep doen op het portretrecht (tot tien jaar na overlijden). De rechter zal dan onderzoeken of er een redelijk belang kan zijn tegen publicatie. 'Roelie' was nieuwswaardig, niet in het minst omdat met haar verhaal een beerput werd opengetrokken. Haar postume recht op privacy sneuvelde in de rechtszaal.

Bij 'Roelie' speelt echter nog iets anders. Het medisch beroepsgeheim helpt namelijk ook na de dood van de patiënt diens privacy te beschermen. Een arts of behandelaar dient te zwijgen over de patiënt tenzij er sprake is van een van de volgende uitzonderingen:

- Er is door de patiënt toestemming gegeven (de nabestaanden kunnen niet namens de overleden patiënt toestemming geven)
- Degene met wie de gegevens gedeeld worden is direct betrokken bij de behandeling
- Een wettelijk voorschrift dat eist
- Er een conflict van plichten ontstaat (je kunt iemand anders leven redden met deze informatie)
- Er is sprake van wetenschappelijk onderzoek (maar dan wel anoniem)

De Raad van Bestuur gaf het interview aan NRC nadat hij eerder elk interview geweigerd had en nadat hij de uitzending van de beelden had bevochten met een beroep op het recht op privacy van de overledene. Nu was er nog niet zo heel veel aan de hand geweest indien de Raad zich puur en alleen had beperkt tot uitspraken over het eigen handelen. Maar dat deed hij niet. In het interview werd gemeld dat 'Roelie' last had van psychoses. Dat is medische informatie en dat had niet gedeeld mogen worden.
De zussen hebben dus wel degelijk een punt. Is er privacy na de dood? Jazeker. Er is privacy voor de overledene en diezelfde privacy dient ook de nabestaanden die in beslotenheid willen rouwen om de dood van hun dierbare zonder dat de rest van de wereld daarbij geïnformeerd wordt over de persoonlijke (medische) gegevens en omstandigheden. ●

Mr. Rachel Marbus, @rachelmarbus op Twitter

VERSLAG

BOB LORD OVER SECURITY BIJ TWITTER

Door Matthijs Koot. Matthijs Koot is security consultant bij Madison Gurkha.

Bob Lord, Director of Information Security van Twitter, gaf een keynote op de tweede conferentiedag van *Hack in the Box 2013 Amsterdam*, dat in het Okura hotel plaatsvond. De keynote blijkt een frisse blik op *security awareness* training. Hij trapt af met het "streetlight effect": de valkuil van het zoeken waar zoeken het makkelijkst is, in plaats van waar je eigenlijk moet zoeken. Hij vindt dat we zó op techniek zijn gefocust dat we de mens zijn vergeten.

Uit het "debat" (de aanhalingstekens zijn van Lord) over *security awareness* training haalt hij vervolgens Bruce Schneier aan, die in een recent essay stelt dat *security awareness* training in het algemeen tijdverspilling is. Hij noemt ook Dave Aitel, die vorig jaar al tot de conclusie kwam dat training van *security awareness* weggegooid geld is.

Lord is optimistischer. Hij onderbouwt zijn optimisme met proefondervindelijke uitkomsten van doorlopend intern onderzoek binnen *Twitter* die wijzen op effectiviteit van *awareness* training. Met dit onderzoek wil hij meten hoe effectief hun inspanningen ter verbetering van de veiligheidscultuur zijn. Als onderzoekspopulatie is gekozen voor 'recent aangenomen personeel', omdat:

1. `they have to show up';
2. `they will be a captive audience, eager and impressionable';
3. `over time they will represent a cross section of the company';
4. `we can track them during their entire company career'.

Elke nieuwe groep aangenomen personeel vormt een nieuw cohort. Van elk cohort meet hij vervolgens het gebruik van password managers (via een periodieke enquête), en phishability (via het daadwerkelijk uitvoeren van phishing (test)aanvallen tegen het eigen personeel). Ten slotte is er een feedback loop, bestaande uit het sturen van reminders over het gebruik van password-managers en het (vriendelijk en opbouwend) confronteren van 'slachtoffers' die in de phishing aanval zijn getrapt. Dat laatste creëert 'anti-lichamen', aldus Lord, en cultiveert een "ons"-cultuur. Het onderzoek is longitudinaal: er wordt gekeken naar het effect over langere tijd en niet alleen tussen twee phishing campagnes.

De grafieken uit dit onderzoek suggereren dat er inderdaad winst wordt behaald. Ook suggereren de cijfers dat wanneer een werknemer in de eerste weken na zijn indiensttreding password-managers leert gebruiken, het waarschijnlijker is dat de werknemer deze ook op lange termijn blijft gebruiken. Het sturen van herinneringen voor het gebruik van een password-manager blijkt hier volgens Lord een positief effect op te hebben. De `phishability' blijkt, zoals gehoopt, af te nemen wanneer er een vriendelijke en constructieve confrontatie heeft plaatsgevonden met een werknemer die in een phishing mail is getrapt.

Mij is niet duidelijk of die werknemer dan ook in privécommunicatie meer waakzaam is, of dat het zich beperkt tot *Twitter*. Ook weet ik niet hoe Lord de phishingaanvallen voldoende vernieuwt en voorkomt dat ze worden herkend als gevolg herhaling of patroonvorming.

Op enig moment vraagt Lord aan de zaal: "how many of you have phishing campaigns within your organizations?" Slechts een paar handen gaan omhoog. Wat mij betreft zijn phishing tests "tegen" je eigen personeel een goed idee om digitale weerbaarheid te verhogen. De gewenste "ons"-cultuur eist waarschijnlijk wel dat het bestaan van deze campagnes vooraf is gemeld en dat de persoonlijke levenssfeer van de werknemer niet wordt geschonden. Spear phishing kan arbeidsintensief zijn, maar als de creativiteit eenmaal op gang is dan wordt het schrijven van nepberichten makkelijker - en worden de berichten geloofwaardiger. Ter inspiratie voor het uitvoeren van social engineering, zie bijvoorbeeld de boeken van Kevin Mitnick, Chris Hadnagy en Joe Navarro, en zoek op YouTube naar het "Tactical Surveillance"-praatje van Chris Nickerson (50 min). ●

"Softpedia News (http://news.softpedia.com/news/Hack-in-the-Box-13-Twitter-s-Bob-Lord-Forces-New-Employees-to-Use-Password-Managers-344699.shtml)".

RISICO'S VOOR BETROKKENEN CENTRAAL IN DE CBP-RICHTSNOEREN BEVEILIGING

Rina Steenkamp werkt als technoloog bij het College bescherming persoonsgegevens (CBP). Zij is te bereiken via r.steenkamp@cbpweb.nl.

Artikel 13 van de Wet bescherming persoonsgegevens (Wbp) vraagt van organisaties die persoonsgegevens verwerken dat ze passende maatregelen treffen om de gegevens te beveiligen. In februari 2013 publiceerde het CBP, dat toezicht houdt op de naleving van de Wbp en aanverwante wetten, richtsnoeren waarin het begrip 'passend' nader wordt ingevuld. De richtsnoeren geven weer hoe het CBP de beveiliging van persoonsgegevens beoordeelt. Centraal in de richtsnoeren staan de risico's voor de betrokkenen, de mensen op wie de persoonsgegevens betrekking hebben: welke gevolgen kunnen deze mensen ondervinden als hun gegevens op straat komen te liggen, of niet kloppen, of er ineens niet meer zijn? De richtsnoeren vervangen de publicatie A&V 23 die de voorloper van het CBP uitbracht in 2001.

De techniek ontwikkelt zich steeds verder en biedt steeds meer nieuwe mogelijkheden. De keerzijde is dat zich steeds nieuwe beveiligingsrisico's voordoen, waar vanuit het vakgebied informatiebeveiliging weer op ingespeeld wordt met nieuwe methoden, standaarden en technieken. Dat roept de vraag op hoe deze veelheid aan nieuwe ontwikkelingen zich verhoudt tot de wettelijke verplichting om persoonsgegevens te beveiligen. Wanneer is nu sprake van een passend beveiligingsniveau?

Om deze vraag te beantwoorden heeft het CBP richtsnoeren gepubliceerd voor de beveiliging van persoonsgegevens. De richtsnoeren maken inzichtelijk hoe het CBP bij het onderzoeken en beoordelen van individuele gevallen de open beveiligingsnormen uit de Wbp toepast. De richtsnoeren zijn bedoeld als verbindende schakel tussen de twee domeinen waar het hier over gaat: enerzijds het juridische domein, met daarbinnen de eisen uit de Wbp en wat die betekenen voor de dagelijkse praktijk, en anderzijds het domein van de informatiebeveiliging, met daarbinnen de kennis en kunde die noodzakelijk zijn om daadwerkelijk aan de wettelijke eisen te voldoen.

In de moderne informatie- en communicatietechnologie hebben we te maken met een steeds grotere verscheidenheid aan technologieën en soorten verwerkingen, die allemaal vragen om specifieke beveiligingsmaatregelen. Een *app* vraagt andere beveiligingsmaatregelen dan een backoffice-applicatie, en een webwinkel beveilig je op een andere manier dan een groot ketensysteem waarin overheidsorganisaties persoonsgegevens uitwisselen. In de richtsnoeren ligt de nadruk dan ook op een risicogerichte benadering, en op het toepassen van de expertise die er binnen het vakgebied informatiebeveiliging beschikbaar is. Om zo veel mogelijk houvast te bieden is daarnaast ook een baseline

opgenomen met daarin breed toepasbare beveiligingsmaatregelen zoals toegangsbeveiliging en encryptie.

De richtsnoeren vervangen de studie Achtergronden & Verkenningen 23, Beveiliging van persoonsgegevens. Deze studie werd in 2001 uitgebracht door de Registratiekamer, de voorloper van het CBP, en is in de loop van de tijd steeds verder af komen te staan van de praktijk. A&V 23 blijft beschikbaar op de website van het CBP, maar heeft geen officiële status meer.

De richtsnoeren op hoofdlijnen:

1. *Stem het gewenste beveiligingsniveau af op de risico's voor de betrokkenen*.
   Schat in wat het voor de betrokkenen betekent als hun persoonsgegevens op straat komen te liggen, of niet kloppen, of er ineens niet meer zijn. Bepaal op basis daarvan het gewenste beveiligingsniveau: hoe meer risico voor de betrokkenen, hoe hoger de lat voor de beveiliging komt te liggen.
2. *Tref maatregelen waarmee het gewenste beveiligingsniveau wordt geborgd.*
   Inventariseer de dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen die het beveiligingsincident kan hebben en de kans dat deze gevolgen zich voor kunnen doen. Tref op basis daarvan gericht beveiligingsmaatregelen waarmee het gewenste beveiligingsniveau wordt geborgd.
3. *Maak gebruik van de expertise die in het vakgebied informatiebeveiliging beschikbaar is*.
   Het vakgebied informatiebeveiliging heeft veel te bieden aan methodieken en standaarden die zijn gebaseerd op ervaringen uit de praktijk van mensen die dagelijks met deze materie bezig zijn. Maak daar gebruik van.
4. *Controleer en evalueer regelmatig*.
   Controleer regelmatig of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Beoordeel periodiek of er nieuwe risico's voor de betrokkenen zijn ontstaan en of het bestaande beveiligingsniveau nog steeds toereikend is.
   Kijk ook of de getroffen beveiligingsmaatregelen nog steeds voldoen. Betrek daarbij de stand van de techniek en de nieuwste inzichten binnen het vakgebied informatiebeveiliging, en pas waar nodig de maatregelen aan. ●

Links

[1] *Richtsnoeren beveiliging van persoonsgegevens: http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx*

NOODZAAK LANDELIJKE CAMPAGNE TEGEN IDENTITEITSFRAUDE

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

Met enige regelmaat bericht de pers over gevallen waar burgers het slachtoffer zijn geworden van ID diefstal. Soms zijn dat leerzame gevallen, waar het slachtoffer rationeel kan beredeneren wat er fout gegaan is, zoals een recent artikel van Peter van Eijk [1]. De meeste onderzoeken focussen op de materiële schade van ID-fraude of diefstal, waardoor de indruk kan ontstaan dat dit de enige schadecomponent is. Veel minder aandacht is er voor de immateriële schade. Wat betekent het slachtoffer te zijn van ID-misbruik, bepaalt dat de gedragingen van de getroffen burger en zijn/haar omgeving?

Onderzoek

Een antwoord op die laatste vraag wordt deels gegeven door het onderzoek dat Dynamics Markets Ltd in opdracht van Fellowes medio 2012 deed [2]. Basis is kwantitatief onderzoek, gehouden in negen Europese landen [3] met in totaal 5.507 geënquêteerden van 18 jaar en ouder.
De eerste vraag die bij dit onderzoek beantwoord is, is de omvang van het probleem. Niet minder dan 17% van de ondervraagden gaf aan een keer of vaker (!) slachtoffer van ID-fraude te zijn geweest, waarbij GB met 24% een uitschieter is (NL: 12%).

Definitie

Bij een dergelijk hoge score rijst de vraag: wat is door de onderzoekers gehanteerd als definitie? Temeer daar de huidige campagne die in Nederland wordt gevoerd ('Laat u niet zomaar kopiëren'), meldt dat in 2011 circa 5% van de Nederlanders slachtoffer was van "een vorm van identiteitsfraude" [4]. Het lijkt erop dat de onderzoekers, net als overigens de Rijksoverheid, ID-misbruik en ID-fraude min of meer hanteren als een containerbegrip, waaronder worden verstaan: alle handelingen die er toe leiden dat de ID van een natuurlijke of rechtspersoon door een ander wordt gebruikt met als primair doel financieel, of daarvan afgeleid, gewin.

Hoe groot is de vrees

De genoemde nationale campagne wijst de burger op de noodzaak voorzichtig om te gaan het het verstrekken van kopieën van zijn of haar ID-bewijs. Hierdoor wordt de indruk gewekt dat een groot deel van de bevolking nog moet worden gewezen op het bestaan van ID-fraude. Die zorg lijkt deels terecht. In Europa maken meer burgers zich zorgen om het verlies van de ID (59%) dan om het verlies van de mobiele telefoon (39%). Echter, als we kijken naar de cijfers voor Nederland (bezorgd om verlies ID 48%, telefoon 25%) dan kan worden geconstateerd dat de Nederlander zich minder zorgen maakt, dan wel zich minder bewust is van de risico's.

> ID-misbruik en ID-fraude gehanteerd als containerbegrippen

Alle ondervraagden verschillen niet van mening waarom ID-fraude plaatsvindt. Men vermoedt vooral dat criminelen op die manier bankrekeningen leeghalen (78%), goederen bestellen op andermans naam (59%) of een bankrekening openen, dan wel creditcard aanvragen (50%). Hier is wel een leeftijdsverschil merkbaar: in de groep 18-24 jarigen wordt meer gedacht dat ID-fraude begaan wordt om geld alleen. Ouderen geven vaker meerdere mogelijke motieven voor de daad aan.

Verder zijn er nog twee interessante verschillen waarneembaar tussen niet-slachtoffers en de slachtoffers van ID-fraude. Van de non-victims gelooft 80% dat het gaat om geld, bij de slachtoffers is dat 73%. Hier speelt duidelijk de ervaring een rol. Dat blijkt dan ook uit de score dat 36% van de slachtoffers aangeeft dat ID-fraude een link heeft met georganiseerde misdaad, terwijl die link door maar 31% van de onkundigen wordt genoemd.

Awareness

Alle groepen, los van leeftijd, land en inkomen, zijn ervan overtuigd dat de laatste jaren het aantal pogingen tot ID-fraude is gestegen. De toename wordt wel per land anders gevoeld (perceptie). Nederland scoort met +52% aan de lage kant, uitschieter is hier Duitsland (+78%) waarbij de respons van slachtoffers en niet-slachtoffers bijna gelijk is. Het positieve aan deze trend is, dat steeds grotere groepen zich bewust zijn van pogingen tot ID-diefstal (awareness).

Wat men vreest

Wat de burger vooral vreest als het gevolg van ID-fraude is financiële schade (64%) en het niet kunnen aantonen wie men is (43%). De score van Nederland wijkt hier af van het gemiddelde: 69% vreest de financiële schade en 51% denkt niet te kunnen aantonen wie men is. Een verklaring voor deze verschillen is niet gegeven, maar het kan een extra reden zijn om bij alle voorlichting over dit verschijnsel meer aandacht te besteden aan deze twee aspecten.

De materiële schade

Van de ondervraagden die slachtoffer zijn geweest van één of meerdere succesvolle pogingen van ID-diefstal heeft 46% ervaren dat er geld van bestaande bankrekening(en) is verdwenen. Dit is de meest voorkomende vorm van schade, maar met 27% scoren ook hoog: het openen van nieuwe rekeningen en het bestellen van goederen op de misbruikte naam. Bijzonder: 20% gaf aan dat er iemand door het leven ging met de gestolen naam (NL 22%) en in 15% van de gevallen was er een huis gekocht. Dat laatste klinkt bizar, maar ook 12% van de Nederlandse slachtoffers heeft deze ervaring.

46% van slachtoffers meldt: geld van bankrekening verdwenen

ID-fraude kost vaak geld. 29% van de slachtoffers kan een streep onder de zaak zetten zonder dat het geld heeft gekost. 71% kost het dus geld en het gemiddelde schadebedrag tot nu toe, zaken kunnen nog lopen, is GBP 6299 per persoon. Nederland zit hier met GBP 4987 onder. Het hoge gemiddelde wordt bepaald door de schade omvang in Duitsland (GBP 28k) en Italië (GBP 13k).

Doorlooptijden

Over de zeven landen genomen, duurt het gemiddeld 8,1 maand eer een ID-fraude zaak wordt ontdekt (*"time taken before aware of being a victim"*), 14% wordt binnen 24 uur ontdekt (dat zijn vooral bankgerelateerde zaken). Nederland scoort hier zeer slecht, de onderzoekers berekenden dat het in Nederland gemiddeld 18,5 maanden duurt eer ID-fraude wordt geconstateerd.

Gedragsverandering

38% van de ondervraagden geeft aan voorzichtiger te zijn met geldzaken en de ID actiever te beschermen. 28% zegt de *"ability to trust people"* verloren te hebben en die groep behoort dan ook tot de 10% van alle ondervraagden die aangeeft de activiteiten op Social Media gestopt te hebben als een rechtstreeks gevolg van ID-fraude.

In Nederland is eenzelfde percentage Social Media afhakers gemeten. Op twee belangrijkere terreinen scoren we echter slechter. Dat 29% van de slachtoffers aangeeft voorzichtiger te zijn geworden met bankzaken en eenzelfde percentage zegt meer aandacht te besteden aan het beschermen van de eigen ID, zet aan het denken. In dat licht gezien is de bewustwordingscampagne van BiZa ook hard nodig. ●

Links

[1] *www.computable.nl/artikel/column/infrastructuur/4630875/2379248/de-kijk-van-van-eijk-italianen-wat-nu-weer.html*

[2] *www.fellowes.com*

[3] *Landen: GB, FR,DE, NL, ES,IT,PL,RU,BE*

[4] *www.rijksoverheid.nl/nieuws/2013/01/15/campagne-tegen-identiteitsfraude.html*

[5] *nl.wikipedia.org/wiki/Identiteitsfraude*

COLUMN

HOE @LEGOSTEENTJE EEN WITTE HOED VERDIENDE

MARKTPLAATS.NL ALS VOORLOPER IN ETHISCH HACKEN

Marktplaats is een interessant doelwit voor hackers. De site trekt gemiddeld 1,3 miljoen bezoekers per dag en er gaat veel geld in om. Alleen al de vele inlognamen en wachtwoordcombinaties kunnen interessant zijn voor criminelen. Veel mensen gebruiken immers nog steeds één wachtwoord voor verschillende sites. De beveiliging van Nederlands grootste veilingsite wordt daarom regelmatig getest. Intern, zoals tijdens de *Beer, Pizza & Hacking* avonden, waar ontwikkelaars proberen de zwakke plekken in elkaars code vinden en zo te leren waar men voortaan op moet letten. En van buiten de organisatie, door hackers die gaten in de beveiliging vinden en dat op een verantwoorde manier willen onthullen. Voor hen is er een speciaal Responsible Disclosure beleid [1].

De initiatiefnemers van dit beleid zijn Robin Schuil (medeoprichter en Innovation Program Manager) en Bas Anneveld (Manager Site Operations). Vind je een veiligheidslek dan kun je dat dus melden en zelfs een beloning krijgen. Als je maar wel handelt volgens protocol: meld ons het lek zonder het eerst met anderen te delen, geef ons minimaal 30 dagen om het te dichten, geef de volledige gegevens en veroorzaak geen schade.

Een van de hackers die erin slaagde was Pieter Vlasblom, ook wel @legosteentje, een 19-jarige scholier van het Rijn IJssel MBO. School vond hij eigenlijk maar niks. Geen uitdaging. Stage vond hij leuker. Daar werkte hij met een applicatie die automatisch advertenties plaatste op Marktplaats. Maar hij kwam er al snel achter dat hij beter zelf iets in elkaar kon knutselen, in de open-source taal Ruby. Vervolgens deed hij wat hackers van nature doen: er van alles in stoppen om te kijken wat er gebeurt. Zo zette hij in plaats van gewone tekst HTML code met JavaScript in de advertenties, oftewel Cross-Site Scripting (XSS). Het werkte. De advertentie gedroeg zich als website en @legosteentje zou zo bezoekers van Marktplaats via pop-ups naar een andere site kunnen leiden.

Hij meldde 2 maart 2012 op Twitter dat hij een security probleempje had gevonden. Prompt reageerde @basanneveld: "We komen graag met je in contact indien je een bug gevonden hebt. We hebben een responsible disclosure program tinyurl.com/7orv6ap". Pieter dacht eerst dat hij in de problemen zou komen. Maar Bas wilde vooral uitleg en ze begonnen te mailen. De site was binnen een dag weer gefixed. Pieter kreeg tot zijn verbazing 350 Euro voor zijn vondst en een pakje: een Classified White Hat in a Black Box, oftewel een witte hoed in een zwarte doos. De tegenstelling white hat – black hat komt uit oude cowboy films waar de good guys een witte hoed en de bad guys een zwarte droegen. De term is alom bekend in de hackerwereld. @legosteentje was nu een erkende white hat hacker.

Zijn stage opdracht zat erop maar hij wilde ook niet terug naar school. Hij ging daarom op de koffie bij Bas. Of hij stage kon lopen bij Marktplaats. Jazeker. Vanaf juni 2012 ging hij aan de slag om een applicatie te schrijven die Marktplaats test op zwakheden: SQL injections, poortscan, XSS, etc. Een soort geautomatiseerd @legosteentje. In Ruby uiteraard. En als hij wat vindt, dan meldt hij dit meteen. Zijn stage werd in juli 2013 omgezet in een baan.

Ondertussen rommelde het in politiek Den Haag. Er bleken veel gevallen van ethisch hacken, met als bekendste voorbeeld Kamerlid Henk Krol die dossiers van "Diagnostiek voor u" had ingekeken. Het ministerie van V&J kwam daarom in januari 2013 met hun richtlijn Responsible Disclosure. De ambtenaren hadden het protocol van Marktplaats als voorbeeld genomen. Minister Opstelten werd vanuit de kringen van beleid, handhaving en bedrijfsleven geprezen voor zijn kordate optreden. Maar er was ook kritiek op de richtlijn. Zo heeft het OM alsnog de bevoegdheid over te gaan tot vervolging, ook als hacker en getroffene er onderling uit zijn gekomen. Dat bleek voor veel hackers onverteerbaar, maar is wellicht logisch vanuit het perspectief van mogelijk getroffen derden.

Dat geldt dus ook voor de klanten van Marktplaats. Toen Schuil zijn verhaal over @legosteentje op 26 maart 2013 presenteerde tijdens een bijeenkomst van Deloitte, kreeg hij weerwoord van juriste Annika Sponselee. "Stel dat een van jullie klanten zich aangetast voelt in zijn privacy, omdat jullie hackers uitlokken? Die zou een zaak kunnen beginnen." Daar wist Robin niet echt een antwoord op. Maar ja, het gebeurt toch wel en dan kun je dat beter goed doen. @legosteentje gaat in ieder geval door, ook buiten zijn werk. Laatst heeft hij Spotify ge-cross-script. Ook dat leverde hem een mooi pakket met goodies op.

Beleid en richtlijnen voor ethisch hacken kunnen helpen, maar de praktijk blijkt toch altijd weerbarstig. Daarom vanaf heden deze column. Volgende aflevering: "Het geduld van @Floorter en de helpdesk. Ontwerpfouten in de ING Mobiel Bankieren app". ●

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

Links

[1] RD policy: http://statisch.marktplaats.nl/help/responsible_disclosure_policy_en.html

WOENSDAG 9 OKTOBER 2013 ***SECURITY-CONGRES***

Thema: Resilience

i13

Hét congres zonder files,
georganiseerd door
ISACA, NOREA en PvIB

PE 5 – Koninklijk Nederlands Instituut van Registeraccountants

Locatie

Postillion Hotel
Utrecht Bunnik
Kosterijland 8
NL-3981 AJ Bunnik
www.postillionhotels.com

Al ingeschreven op het succesvol terugkerend congres?
Mis het niet en schrijf u nu in en maar hierbij gebruik van de vroegboekkorting!

Het inspirerende programma vindt u op **www.security-congres.nl**
Wederom is getracht een mooi en afwisselend programma op te stellen.

Wat kunt u verwachten:

Dagvoorzitter: André Beerten, Groene Hart Ziekenhuis
Keynote speakers:
> Arno Reuser, OSINT specialist
> René Steenvoorden, Rabobank Nederland
Parallelle sessies:
> Technische track:
- Gerard Klop, MOTIV
- Dennis Reumer, Arché IT

> Maatschappelijke track:
- Ad Reuijl, UWV
- Marc Welters, Ernst Young

> Laatste ontwikkelingen en trends in cloudsecurity
door Cloud Security Alliance, Chapter NL
> Uitreiking Joop Bautz Information Security Award

Dit congres wordt mede mogelijk gemaakt door:

ONSIGHT IT Security Experts

Secure Link Infrastructure Security Solutions

Wij ontmoeten u graag op 9 oktober as.!

Organisatie:

ISACA Serving IT Governance Professionals

PvIB Platform voor InformatieBeveiliging

NOREA de beroepsorganisatie van IT-auditors

Meer informatie:

www.security-congres.nl

VERSLAG

TWEE DAGEN ONDER HACKERS BIJ HACK IN THE BOX AMSTERDAM

Marco Koelmans (CISSP, CISA, CISM) is een onafhankelijke Security Consultant van Xellentis. Hij heeft meer dan 15 jaar ervaring in het vakgebied en is bereikbaar via mkoelmans@xellentis.nl

Woensdag 10 en donderdag 11 april werd in het Okura hotel in Amsterdam het vierde *Hack in The Box Amsterdam* congres gehouden. De twee dagen ervoor waren er technische sessies. Na vier jaar geleden bij de eerste versie van *Hack in the Box* geweest te zijn en daarvan verslag te hebben gedaan in *Informatiebeveiliging* was ik er dit jaar weer bij. *Hack in the Box* Amsterdam is het jongere broertje van *Hack in the Box Kuala Lumpur* in Maleisië en aan het hoofd van de organisatie staat Dhillon Kannabhiran met wie ik vier jaar geleden een interview heb gedaan (ook in dit blad).

Nu moet ik benadrukken dat ik geen techneut ben. Ik zit meer aan de kant van de organisatie van informatiebeveiliging. Dat is belangrijk omdat het een duidelijke tech conferentie is. De conferentie schenkt gelukkig ook aandacht aan niet technische zaken zoals *Security Awareness*.

Okura Hotel Amsterdam

Na een reis met het openbaar vervoer kwam ik aan bij het prestigieuze Okura hotel in Amsterdam. Een vreemd beeld dringt zich aan mij op. Hackers worden door de buitenwereld nog altijd gezien als schimmige figuren met niets goeds in de zin. Binnen de Security community weten wij wel beter. Niet voor niets wordt één van Europa's grootste hackers conferenties georganiseerd in een vijf sterren hotel in onze hoofdstad.

Hackers worden gezien als schimmige figuren met niets goeds in de zin

Er staat een twee dagen durend evenement op het programma met twee tracks aan lezingen, en track lab sessies die staan aangekondigd in cryptische bewoordingen als "General Hack Fu", "Hardware / Embedded" en "Crypto".

Key Note speaker Edward Schwartz, CISO van RSA, trapt de conferentie af. Hij voert een pleidooi om Big Data te omarmen en daar analyses op los te laten. Hij schetst het beeld van een beveiliging die alle toegang dichttimmert maar die nergens anders meer oog voor heeft. Een analyse van alle data van deze "muren" zal wellicht aangeven dat de deur ondoordringbaar is, maar dat de muren van lucht gemaakt zijn.
Hij vergelijkt het met het moment dat je aangevallen wordt door een overvaller. Dan staat de wet je toe om de overvaller te ontwapenen. Maar als je overvallen wordt door cybercriminelen via het internet dan mag je hen niet ontwapenen. Zijn pleidooi om gedrag van internetgebruikers te monitoren en te analyseren om zo de cybercriminelen in een vroeg stadium te herkennen gaat voorbij aan alle privacy vraagstukken.
Hij sluit af met een verwijzing naar een door hem geschreven whitepaper met als titel "Big Data Fuels Intelligence-Driven Security".


Lunch

Ik besluit hierna naar "Security Response in the Age of Mass Customized Attacks" te gaan. De sessie wordt gepresenteerd door Peleus Uhley en Karthik Raman, beiden van *Adobe*. Zij vertellen dat Malware steeds professioneler wordt gemaakt. Het is bijna net zo professioneel opgezet als een project met een project manager en een team aan ontwikkelaars en testers. De malware is modulair opgezet voor verschillende platforms en met verschillende versies. Zo wordt het eenvoudiger om aanpassingen te doen ten behoeve van *customisation* en wordt de *time to market* voor een nieuwe versie korter. Gelukkig is ook de reactietijd van security om lekken te dichten verkort tot gemiddeld twee dagen zodat 0-days snel gepatcht kunnen worden.

De parallelsessie moet ook interessant geweest zijn. Die ging over een onderzoek naar de beveiliging van een type digitale spiegelreflex camera. De onderzoekers kwamen er achter dat het eenvoudig is om (remote) toegang te krijgen tot de camera en waren hierdoor in staat om gemaakte foto's te zien, te downloaden, te wissen en er zelfs andere foto's op terug te zetten. Dit kunnen uiteraard ook hele foute foto's zijn. In theorie stelt het iemand in staat een eigenaar van zo'n camera in een lastig parket te brengen door bijvoorbeeld kinderpornografische afbeeldingen op zijn camera te zetten en vervolgens de politie te tippen. Leg dat maar eens uit aan justitie.


Wilco Baan Hofman

Wilco Baan Hofman liet weer een heel ander lek zien. Zo vond hij verschillende lekken in de protocollen waar de alarminstallaties bij u thuis met de alarmcentrale communiceren. Bij het aanmelden wordt er een eenmalige *handshake* gedaan waarna de alarmcentrale de identiteit van de installatie niet meer controleert. De encryptie is eenvoudig te kraken waardoor Man in the Middle attacks kunnen worden uitgevoerd. Ook kan er op deze manier een DDoS aanval op de alarmcentrale plaatsvinden. Kwaadwillenden kunnen de centrale overvoeren met onterechte alarm meldingen waardoor er niemand meer reageert of waardoor er de kans dat er verkeerde keuzes worden gemaakt groter wordt. Het NCSC blijkt inmiddels te zijn ingelicht en heeft de kwestie opgepakt. Op zich opmerkelijk dat een systeem dat er op gericht is om je huis te beveiligen zelf zo slecht beveiligd is tegen manipulatie van dataverkeer. Fabrikanten schermen met termen als niet te kraken, maar het blijkt kinderlijk eenvoudig te zijn.

Encryptie van alarmcentrales is eenvoudig te kraken

De lunch die volgde was uitstekend en het maakte duidelijk waarom het Okura hotel een fijne plaats is om te vertoeven. Tijdens de lunch werd het ook weer duidelijk op wat voor type conferentie ik was. Een aantal mannen was aan het filosoferen over het kraken van OV kaarten in Duitsland, het kraken van internationale Chipknip varianten en waren de hotelkamer tags aan het lezen om te zien of hier wat mee gedaan kon worden.

Na de lunch bezocht ik de volgende sessies: "Exploiting Hardcore Pool Corruptions in Microsoft Windows Kernel" door Nikita Tarakanov en "Virtually Secure: Analysis to Remote Root 0day in an Industry Leading SSL-VPN Appliance" door Tal Zeltzer. Deze laatste ging over een lek in de F5 Firepass Appliance. In een labsituatie heeft de onderzoeker de controle over de appliance weten te krijgen.

Ik besloot de volgende lezing (na de koffiepauze) over te slaan en ging naar de TOOOL stand waar ik een bliksemcursus Lockpicking kreeg. Heel interessant en redelijk eenvoudig. Veel sloten zijn zonder sporen achter te laten eenvoudig open te krijgen met een setje dat voor een een klein bedrag te koop is.

De lezing van Hugo Teso over kwetsbaarheden in de communicatiesystemen van vliegtuigen heeft eerder al internationaal behoorlijk wat stof doen opwaaien. Hugo is een Security Consultant en commercieel piloot. Vliegtuigcomputers communiceren met ground control en met hun eigen organisatie via ACARS. Een vlucht wordt voornamelijk via de automatische piloot uitgevoerd. Via ACARS kunnen gewijzigde vluchtplannen, correcties en instructies aan het Flight Management System (FMS) worden doorgegeven. Het is in essentie mogelijk om alle systemen aan boord van een vliegtuig middels ACARS aan te sturen. Hugo heeft de systemen van een vliegtuig verzameld. Hij deed dit door componenten op eBay te kopen, op Russische schroothopen en door bijvoorbeeld trainingslicenties voor software te bemachtigen waarvan de fabrikant van de software beweerde dat deze volledig hetzelfde was als de uiteindelijke software die daadwerkelijk in de vliegtuigen gebruikt wordt. In een labsetting thuis is hij erin geslaagd om in te breken in het ACARS systeem en instructies naar het FMS te sturen.

Hugo Teso

Hij kon daarmee bijvoorbeeld een vliegtuig van koers en van hoogte laten veranderen. Potentieel is dat natuurlijk een groot gevaar. Wat zou er immers gebeuren als een terroristische organisatie deze technologie in handen kreeg en een grootscheepse aanval zoals die op het World Trade Centre in New York zou willen uitvoeren. Gelukkig kan de piloot altijd het FMS uitzetten en de controle over het vliegtuig over nemen maar dat is niet altijd een sinecure. Als het mistig is en je hebt niet meer de beschikking over elektronische hulpmiddelen, hoe ga je het vliegtuig dan veilig aan de grond zetten? Nog los van de mogelijke paniek die aan boord van een vliegtuig kan uitbreken als in één keer alle zuurstof maskers naar beneden vallen of als in één keer motoren worden uitgezet en flappen worden bediend waardoor het vliegtuig een duikvlucht gaat maken. Het is dus niet verwonderlijk dat de internationale pers aandacht aan zijn bevindingen heeft geschonken. Ik weet niet of de hack echt zo makkelijk te doen is en of zijn labsituatie de echte situatie benadert. Wel geloof ik dat deze communicatiesystemen nooit gebouwd zijn met mogelijk misbruik in het achterhoofd. Wie had ooit gedacht dat vliegtuigen als wapens ingezet konden worden. Toch is het gebeurd. Dat maakt dat de bevindingen van Hugo niet zo onwaarschijnlijk zijn en ik hoop dat de luchtvaartindustrie hier serieus in gaat duiken.

Wie had ooit gedacht dat vliegtuigen als wapens ingezet konden worden

Dag twee

De tweede dag start met de Keynote van Bob Lord, Director of Information Security van Twitter. Hij geeft een warm pleidooi voor *Security Awareness* met zijn lezing “Rethinking the Front Lines”. Daarin komt het gebruik van Password Vaults, het social engineeren van het eigen bedrijf en ultimo, en het wijzigen van de bedrijfscultuur aan bod. Veel security professionals hebben het opvoeden van gebruikers opgegeven. De essentie is echter dat een éénmalige *Security Awareness* training niet zal werken. Na deelname is het eerste wat de medewerker hoort als hij het geleerde in praktijk wil brengen: “Zo doen we dat niet hier”. Het gaat er dus om dat de hele cultuur in een bedrijf verandert. Dat kan met een aantal heel simpele zaken. Een voorbeeld daarvan is om op onregelmatige tijden door je bedrijf lopen zonder pas en de eerste die

je daar op aanspreekt een bon geven voor een gratis kop koffie, een diner of gewoon met geld. Als je dat een aantal keer doet heb je al heel snel en relatief goedkoop resultaat.

Bob Lord

Ook een *phishing attack* op de eigen medewerkers is zo'n voorbeeld. Zorg er wel voor dat resultaten meetbaar zijn. Het aantal meldingen van een dergelijke *phishing attack* of het percentage pasdragers fungeert in bovenstaande voorbeelden als een graadmeter hoe het gesteld is met de *Security Awareness* binnen je organisatie.

De lezing waar ik daarna naar toe ga, heeft de pakkende titel "Abusing Browser User Interfaces for Fun and Profit" en werd gegeven door Rosario Valotta. De spreker gaat in op de verschillende mainstream browsers en de mogelijkheden om een aanval daarop uit te voeren. Met name de modeless notifications waarin een popup in de achtergrond verschijnt waarbij dat venster, ondanks dat het in de achtergrond staat, actief is en waarbij een klik of een enter een OK genereert komen hierbij aan bod. Zo kan een aanvaller een download en installatie forceren waarbij de gebruiker het niet of nauwelijks in de gaten heeft.

Met hooggespannen verwachtingen ga ik na de lunch naar de lezing ´You Can Be Anything You Want to Be: Breaking Through Certified Crypto in Banking Apps" van Andrew Petukhov (Founder/CTO, Solidlab), George Noseevich (PhD Candidate, MSU) en Dennis Gamayunov (Acting Head, Information Systems Security Lab, MSU). Zij hebben gekeken of ze de cryptografie van een Remote Banking System van een grote Europese Bank konden doorbreken. De crypto voldeed aan de eisen van de Russische Centrale Bank en was naar verluid niet te doorbreken. Zij lieten zien hoe de communicatie over een encrypted tunnel verloopt tussen de cliënt en de Crypto Server. Ze vonden een bypass via analyse van het verkeer dat via de tunnel naar de Crypto Server wordt verzonden en wat er vervolgens als antwoord terug komt. De cryptografie was daarmee niet doorbroken maar het bezorgde ze in ieder geval een side channel attack.

Cryptografie niet doorbroken maar wel een side channel attack

De volgende lezing is wat luchtiger. Het gaat over het hacken van IP camera's. U weet wel, een camera die in huis bewegingen vastlegt en waarmee u vanaf uw werk even

thuis kunt kijken of het de kat was die voorbij liep of dat er ingebroken wordt. Sergey Shekyan en Artem Harutyunyan, beiden van Qualys, legden in de lezing “To Watch or Be Watched: Turning Your Surveillance Camera Against You” uit hoe je de camera’s kunt hacken door te doen wat de fabrikant aanbeveelt in zijn handleiding: Een NAT port forward te doen op poort 80. Als voorbeeld gebruikten ze een Foscam camera die op Linux draaide. Deze camera’s zijn erg populair en staan wereldwijd veelvuldig opgesteld op allerlei plekken. Ze bleken in staat om binnen te dringen, een gebruiker aan te maken voor eigen gebruik die niet meer te zien was in het “gebruikers” scherm van de camera zelf. Daarmee was het *user-id* vanuit de normale gebruikersinterface dus onzichtbaar. Omdat de camera met het internet verbonden is en ze hiermee toegang hadden tot de camera konden ze met de camera meekijken, malware hosten, hem opnemen in een botnet, en als proxy gebruiken. Voor inbrekers is het handig dat je ook een DDoS kunt uitvoeren op de camera. Omdat de logs alleen geauthenticeerde verzoeken opslaan kan dit volledig anoniem gebeuren. De heren hebben een toolkit gemaakt voor als je zelf eens aan de slag wilt gaan met zo’n IP camera.

Na de koffie legt Evan Booth uit in de lezing “Terminal Cornucopia” hoe hij wapens kan maken met allerlei materiaal dat hij na passeren van de beveiliging op een luchthaven kocht.

Evan Booth

Hij wilde daarmee slechts aantonen dat dit in de praktijk mogelijk is. Hij was in staat gevarieerde dodelijke wapens te maken met de nodige creativiteit en relatief een korte productie tijd. Zodoende wist hij een “brandbom handbagage koffer” te maken waarmee je brand kunt stichten in een vliegtuig. Het effect van de wapens testte hij uit op een kokosnoot (voor allerhande slag en andere wapens) en in de buitenlucht (voor de brandkoffer). De spullen kocht hij op allerlei luchthavens in Europa en Amerika, waaronder Schiphol. Een sensationele presentatie.

Daarna is de beurt aan de afsluiter van de conferentie: Winn Schwartau over “The History of the Future of InfoSec”. Hij weet zijn publiek op humoristische wijze en met een groot enthousiasme aan zich te binden. Door de snel evoluerende techniek zijn we steeds afhankelijker

Winn Schwartau

geworden. We hebben ook geen alternatieven meer. Dat heeft de spelregels in de maatschappij veranderd maar de maatschappij zelf niet. Dat kan grote consequenties hebben. China heeft dat een paar decennia geleden al ingezien. Zij zijn bijvoorbeeld begonnen om op het gebied van defensie meer in te zetten op Cyberwar. Ondertussen zitten we in het westen nog met onwetende politici. Zij zetten in op inperking van mogelijkheden en privacy terwijl privacy juist een pijler van Security zou moeten zijn. Schwartau schetst een aantal angsten die bewaarheid worden in de hedendaagse aanpak van cybercrime en cyber warfare:

Idiots in politics
Ignorance in business
Apathic about warnings
Arrogance in preparation

Hij daagt de aanwezigen uit om een antwoord op de volgende vragen te vinden:

Why don’t we:
Let hacker communities lead
Teach security history
Embrace failure
Have trusted, self-repellant OS/ Operating environments
Measure security with the time metric
Know how to stop DDoS
Build security in from the start
Do what is RIGHT?

Dat bracht het einde van de tweede dag en daarmee van *Hack in the Box Amsterdam 2013*. Ik ben persoonlijk blij dat ik er geweest ben. Ondanks een heleboel technische lezingen kon ik een voor mij interessant programma samenstellen. Ik had het leuk gevonden als er een aparte, derde track met meer niet technische onderwerpen was geweest. Bijvoorbeeld een lezing over *responsible disclosure*, dat sterke raakvlakken heeft met hacken maar toch minder technisch is. Desondanks was het een leuke en boeiende conferentie op een uitstekende locatie. Tot volgend jaar! ●

Foto’s van de conferentie zijn te vinden op: http://photos.hackinthebox.org/index.php/2013-AMS-KUL/HITB2013AMS/CONFERENCE-DAY-1

De presentaties zijn na te zien op: http://conference.hitb.org/hitbsecconf2013ams/materials/

Video’s zijn na te zien op het Hack in the Box You Tube channel: http://www.youtube.com/user/hitbsecconf

ADVERTORIAL

KAN GEGEVENSUITWISSELING IN DE ZORG VEILIG PLAATSVINDEN?

Uitwisseling van gegevens is een essentieel onderdeel van vrijwel alle processen in de zorg- en welzijnssector. Dit geldt zowel voor de primaire processen van behandeling en verzorging van een individuele patiënt, als voor de financiële afhandeling en de bedrijfsprocessen in een zorginstelling. De eisen die aan de uitwisseling van gegevens moeten worden gesteld, verschillen per proces. Het is voor alle communicatiepartners (tussen zorgverleners en zorginstellingen onderling, met patiënten en cliënten, en met zorgverzekeraars en andere partijen die bij de zorg zijn betrokken) essentieel dat de elektronische communicatie in de zorg op een veilige en betrouwbare wijze plaatsvindt.

De doorstart van het Landelijk Schakelpunt (LSP) ondersteunt de uitwisseling van patiëntinformatie en regionale gegevens tussen zorgaanbieders.
Een aantal koepelorganisaties in de zorg hebben handvatten ontwikkeld ter ondersteuning van de zorgaanbieders: handreiking 'Privacy bij regionale uitwisseling van patiëntgegevens' en de 'Gedragscode Elektronische Gegevensuitwisseling in de Zorg'. De Gedragscode geeft adviezen aan zorgverleners en behandelt de belangrijkste punten waarmee de betrokkenen rekening moeten houden wanneer zij elektronisch gegevens uitwisselen.
De meest bekende norm voor informatiebeveiliging in de zorg is NEN 7510.
Deze norm is een sectorale uitwerking en aanvulling op de internationale normen voor informatiebeveiliging, ISO 27001 en ISO 27002. NEN 7510 beschrijft het proces en de maatregelen die een zorginstelling moet treffen om de beschikbaarheid, integriteit en de vertrouwelijkheid van de bedrijfsprocessen en de informatievoorziening te waarborgen. Naast de door de koepels ontwikkelde handvatten en NEN7510 is de norm NEN 7512 ontwikkeld, getiteld 'Vertrouwensbasis voor gegevensuitwisseling'. NEN 7512 is in 2005 opgesteld en wordt op dit moment herzien.
De herziene norm is in twee opzichten een aanvulling op de richtlijnen die NEN 7510 aan organisaties in de zorg geeft voor hun informatiebeveiliging. In de eerste plaats richt deze norm zich op de zekerheid die partijen elkaar moeten bieden als voorwaarde voor vertrouwde gegevensuitwisseling. Ten tweede levert deze norm een nadere invulling voor een aantal van de richtlijnen van NEN 7510. Dat betreft dan vooral de aanzet tot risicobeoordeling en de uitwerking van de eisen ten aanzien van identificatie en authenticatie die horen bij een bepaalde classificatie van de gegevensuitwisseling.
NEN 7512 geeft de aanpak aan voor het bepalen van de maatregelen die in een gegeven situatie nodig zijn voor vertrouwde gegevensuitwisseling.
Het bevat een processchema om een risicobeoordeling voor de beoogde gegevensuitwisseling uit te voeren.
Als onderdeel hiervan wordt de gegevensuitwisseling geclassificeerd naar de bekende aspecten van informatiebeveiliging: beschikbaarheid, integriteit en vertrouwelijkheid. Ook worden de bedreigingen voor de gegevensuitwisseling geanalyseerd en ingedeeld op grond van een schatting van de kans (zeer klein t/m zeer groot) op een ongewenste gebeurtenis en de ernst van de gevolgen (hinderlijk t/m catastrofaal). Aan de hand van de risicobeoordeling voor een gegeven communicatiescenario levert deze norm de maatregelen die minimaal nodig zijn voor vertrouwde gegevensuitwisseling.
Deze norm volgt hierbij de systematiek van NEN 7510:2011; de risicobeoordeling classificeert de gegevensuitwisseling naar de genoemde aspecten beschikbaarheid, integriteit en vertrouwelijkheid aan de hand van de mogelijke gevolgen van een incident en geeft vervolgens aanwijzingen voor het beoordelen en behandelen van de risico's.
Het is niet nodig dat de individuele communicatiepartners de in NEN 7512 beschreven aanpak voor iedere concrete situatie opnieuw uitwerken. Er mag worden verwacht dat groepen of koepels van communicerende partijen met elkaar afspraken maken over de risico- en maatregelprofielen die bij voorkomende communicatiescenario's passen. Vooral bij elektronische ondersteuning van identiteit en authenticiteit, richt NEN 7512 zich op de specificaties voor zorginformatiesystemen, zowel intern als extern communicerend. Zorgverleners kunnen hiermee de eisen specificeren van de te leveren of te bouwen systemen. ICT-leveranciers kunnen uit de norm specificaties afleiden en achtergrondinformatie vinden voor te ontwerpen zorgsystemen.
Het normontwerp van de gereviseerde NEN 7512 wordt in het najaar gepubliceerd voor een externe commentaarperiode van drie maanden. NEN zal het normontwerp publiceren via www.nen.normontwerpen.nl Alle geinteresseerde partijen kunnen via de website commentaar leveren op het normontwerp. ●

Shirin Golyardi,
consultant NEN Zorg & Welzijn
shirin.golyardi@nen.nl

TSTC – de Security Opleider van Nederland

- Botnets, DDoS, Malware ... Gehackt!
Bent u de volgende?

- En wat is dan uw reputatie- en/of financiële schade?
- Vormt uw Blackberry of iPhone een security risico?
Herkent u bovenstaande vragen?

Deze tijd vraagt om oplossingen en kennis van zaken.

Zorg dat u goed getraind bent, kijk gauw op www.tstc.nl/training/security

---

Een greep uit onze security certificeringen:

Certified Ethical Hacker (CEH)
Computer Hacking Forensic Investigator (CHFI)
Certified Security Analyst (ECSA)
Licensed Penetration Tester (LPT)
Certified Information Systems Security Professional (CISSP)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
Cloud Security Audit and Compliance (CSAC)
Certified Risk Manager ISO 27005/31000

TSTC - 6e jaar op rij de beste EC-Council Security Opleider Europa!

Kom langs op Infosecurity Utrecht 30 + 31 oktober stand D153

TSTC TSHUKUDU TECHNOLOGY COLLEGE

Want security start bij mensen!!

WWW.TSTC.NL

PERSBERICHT

BEDRIJFSGEVOELIGE INFORMATIE NIET VEILIG BIJ ZZP'ER

ZZP'ers lekken bewust en onbewust bedrijfsgevoelige informatie. Meer dan de helft (59 procent) werkt met bedrijfsgevoelige informatie van opdrachtgevers. Echter, 76 procent van de ZZP'ers gebruikt gratis consumentensoftware voor zakelijke doeleinden. Documenten die worden verzonden, gedeeld of opgeslagen met consumentensoftware mogen worden gebruikt, gedistribueerd, weergegeven en gereproduceerd door de aanbieder van de software. 79 procent van de ZZP'ers is zich bewust van deze voorwaarden. Dit blijkt uit onderzoek naar digitaal samenwerken van Woozl, de online document management oplossing voor de zakelijke markt, onder 400 MKB ondernemers en ZZP'ers.

Ook onbewust wordt informatie gedeeld

ZZP'ers hebben niet alle voorwaarden goed op het netvlies. Ook onbewust wordt bedrijfsgevoelige informatie gedeeld met derden. 28 procent weet niet dat de aanbieder van de software de documenten en persoonsgegevens gebruikt voor advertentiedoeleinden. Daarnaast is 53 procent van de ZZP'ers zich er niet van bewust dat dat de eigendomsrechten van documenten worden afgegeven op het moment dat zij gratis software gebruiken om samen te werken.

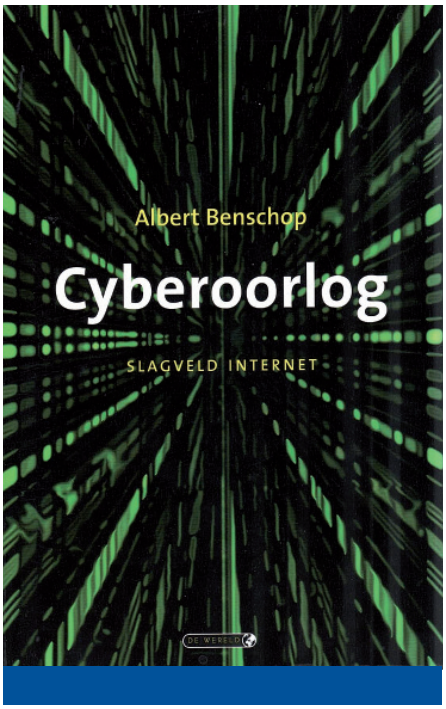
"Niet alleen ZZP'ers maken zich schuldig aan het bewust en onbewust delen van bedrijfsgevoelige informatie. Veel gebruikers van gratis software accepteren de algemene voorwaarden zonder deze daadwerkelijk te lezen. Hier staat echter vaak in dat de aanbieder van de software de documenten bijvoorbeeld mag gebruiken en reproduceren. Het gebruik van gratis consumentgeoriënteerde software hoort dan ook niet thuis in de zakelijke markt. Het is verstandig om, zowel voor zakelijk als privé, op de hoogte te zijn van deze voorwaarden zodat een afgewogen keuze gemaakt kan worden", aldus Joost Bolkenstein, Business Unit Manager bij Woozl.

BOEKVERSLAG

"O JA, DAT WAS WAAR OOK"

door Ronald van Erven

Titel : **Cyberoorlog**
Subtitel : **Slagveld Internet**
Auteur : **Albert Benschop**
ISBN : **978-90-79051-06-9**
Blz : **332**
Waardering: ★★★★☆



Dit is een lekker vlot geschreven boek dat redelijk snel weg leest. Voor de veteranen onder ons zal het boek een hoog "O ja, dat was waar ook" gehalte hebben. Maar voor de starters in het vakgebied of personen die een overzicht willen hebben over het vakgebied informatiebeveiliging levert het boek een goed onderbouwd verhaal door gebeurtenissen, artikelen, vaktheorie, definities en technologieën aan elkaar te verbinden. Het boek bevat verder veel verwijzingen naar onder andere de boeken van Kevin Mitnick en zijn kunst van social engineering [1].

Cyberoorlog heeft voor elk wat wils, van de techneut, de digitaal jurist tot en met de beleidsmedewerker en alles daartussen. Het is een must read voor die mensen die iets in het vakgebied doen of willen gaan doen.

Soms werd er voor mij nog onbekende tooling genoemd of een verwijzing naar een voor mij nog onbekend boek gemaakt. Ik vond de hoofdstukken 6, 7 en 10 het meest interessant. Deze hoofdstukken gingen in op de techniek als een vehikel om doelen te bereiken.

Wat dit boek geschikt maakt als referentie, is dat de techniek op een eenvoudige manier wordt gepresenteerd en dat daarna inzichtelijk wordt gemaakt hoe die techniek wordt ingezet om (cyber) doelen te halen. Het geeft soms een gevoel in een mini cursus *advanced ethical hacking* met motivatie te zijn beland. Je vraagt je af hoe de auteur dit allemaal weet. Zit hij bij een geheime dienst of is hij een ex-cyberspion?

> Op een eenvoudige manier wordt techniek gepresenteerd en hoe het wordt ingezet om (cyber)doelen te behalen

Dan de term cyberoorlog. Een cyberoorlog gaat over het beïnvloeden, controleren of afluisteren van informatiestromen. Cyberspion, cyberoorlog of cyberwarrior zijn marketingtermen. In de Tweede Wereldoorlog hadden we deze beïnvloeding en het afluisteren ook al, denk aan Enigma. Hoofdstuk 2 en 4 gaan dan ook over hoe toegankelijk dit nieuwe "strijdtoneel" nu is geworden.

De Hoofdstukken:

Hoofdstuk 1. Een inleiding: internet als medium en inzet van strijd
Dit hoofdstuk geeft een introductie van het strijdtoneel, een sitrep (militair jargon voor situation report) en de belangen die partijen, als politici, activisten, burgers, bedrijven, hebben. Het geeft een overzicht van de voor- en nadelen van internet en het moment dat er via internet een vorm van status of macht en geld te verwerven viel, dat het belang van internet enkel is toegenomen en dat economieën en maatschappijen hierdoor ook kwetsbaar zijn.

Hoofdstuk 2. Oorlogsvoering nieuwe stijl
Dit hoofdstuk gaat over een nieuwe stijl van oorlogsvoering op het niveau van informatie- en communicatietechnologie. Dit heeft gevolgen in de werkelijke wereld met mogelijk slachtoffers onzichtbaar voor deze cybersoldaten. Het is anders dan een echte oorlog in steden of jungles.

Naar analogie met een echte oorlog beschrijft dit hoofdstuk de doelwitten, de definities en de aspecten van het nieuwe slagveld en hoe laagdrempelig deze te betreden is.

Hoofdstuk 3. Kwetsbaarheden van ICT en de kunst van beveiligen/verdedigen
Een hoofdstuk van actie is reactie. Door de toegenomen complexiteit in de geautomatiseerde verwerking (actie) zijn er meer kwetsbaarheden of punten die benut kunnen worden (reactie) en daardoor moeten er weer tegenmaatregelen genomen worden. Er wordt ingegaan op malware en vormen van malware. Tenslotte gaat de schrijver in op (contra)hackscenario's conform de methode uit de boeken van *hacking exposed* [2].

Door het internet is het strijdtoneel niet meer het exclusieve recht van overheden

Hoofdstuk 4. Nieuwe actoren: cybermilitairen
Alhoewel de auteur in dit hoofdstuk een nieuw fenomeen introduceert (cybermilitairen) en ingaat op cyber-spionage en cyberaanvallen, is er niets nieuws onder de zon. Bewust verkeerd informeren en spioneren of via stoorzenders de informatiestromen onderbreken gebeurd al sinds jaar en dag. Alleen is de drempel voor de benodigde apparatuur nu lager en daardoor meer voorhanden. Tenslotte worden cyber oefeningen van de overheden (cyberstorm) nog krot aangestipt.

Hoofdstuk 5. Cyberspionage: Heimelijk informatieve verwerving
Inbreken, aftappen en natuurlijk een uitvoerige beschrijving van het Digitnotar incident staan in dit hoofdstuk beschreven. Tooling als warvov, wardialing en war driving, shodan, nessus, openvas, core impact, wireshark, metasploit en het commerciële finfisher worden genoemd. Dit hoofdstuk geeft je wederom het gevoel dat je op een ethical hacker cursus zit.

Hoofdstuk 6. Economische en politiek bedrijfsspionage
Diverse objecten worden beschreven in de arena van economische en politiek motieven om spionage te plegen en de afhankelijkheden in dit informatietijdperk. Titan Rain, ShadyRat, operatie Aurora zijn voorbeelden van mysterieuze operaties en netwerken die spionage tot doel hadden. Wat nieuw voor mij was de hack bij Coca Cola. En veel Chinese activiteiten op het gebied van spionage.

Hoofdstuk 7. Cybermanipulatie van financiële markten
Wat gebeurt er op het cybervlak om financiële markten te ontregelen of om geldstromen weg te sluizen door middel van banking trojans? Niet alleen financiële instellingen maar ook de zwendel in emissiecertificaten in de EU wordt in dit hoofdstuk beschreven.

Hoofdstuk 8. Cybotage: van ontregelen naar vernietiging
Een hoofdstuk over kritieke infrastructuren en hoe deze te ontregelen en te vernietigen. Diverse incidenten op proces automatiseringsomgeving worden beschreven en hoe men SCADA systemen kan benaderen en beïnvloeden tot zelfs stil kan leggen.

De cyberoorlog is allang in gang, er zijn vele signalen dat dit zo is

Hoofdstuk 9. De cyberoorlog is al begonnen
Hoe de cyberoorlog allang in gang is en welke signalen er zijn dat dit zo is:

- Website hacking of vandalisme tijdens de onafhankelijkheid van Oost-Timor;
- De situatie in Palestina en Israël of Estland;
- Hoe de NAVO de eerste cyberoorlog in Kosovo voerde;
- Hoe China en de Verenigde Staten actief zijn in Cyberwarfare.

Hoofdstuk 10. Stuxnet: de niet-verklaarde cyberoorlog met Iran
In een boek over Cyberoorlog mag Stuxnet natuurlijk niet ontbreken. Dit was voor mij een interessant hoofdstuk omdat het met een redelijke diepgang Stuxnet beschrijft en hoe dit allemaal in zijn werk is gezet.

Hoofdstuk 11. Cyberafschrikking en oorlogsrecht
Diverse verdragen worden beschreven zoals bijvoorbeeld een uitbreiding op de conventies van Geneve. Daarnaast gaat het hoofdstuk in op hacking en contra-hacking en of dit wel of niet geoorloofd is volgens internationale verdragen.

Hoofdstuk 12. Digitale slagkracht in NL
Hoe staat Nederland nu in het geheel van Cyberoorlogsvoering? De rollen van NCSC, AIVD, MIVD, Defensie expertise centrum, ICT response board, het Team High Tech Crime van de nationale recherche worden beschreven en hoe zij samenwerken. Tot slot wordt er een stand van zaken gegeven van de Nederlands capaciteit op de gebieden van cyber: defensieve mogelijkheden, offensieve mogelijkheden, inlichtingen werk, aanpassend vermogen en innovatie en de internationale samenwerking. Het hoofdstuk sluit af met één ontbrekend element - the rules of engagement.

Hoofdstuk 13. Cyberdoemsdag: een rampscenario
Een hoofdstuk met een hoog "wat zou er gebeuren als… " gehalte. Kortom, scenario-denken. ●

Links

[1] *Kevin Mitnick: http://mitnicksecurity.com*

[2] *Hacking Exposed serie, bijvoorbeeld: http://www.webhackingexposed.com*

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

CISO VERSUS *WHITE HATS*: EEN HAAT-LIEFDE VERHOUDING?

Als (CI)SO volg je natuurlijk de gangbare (en wellicht ook wat minder gangbare) bronnen met informatie over kwetsbaarheden, hacks, malware en dergelijke. Veel van die informatie komt van de zogenaamde "white hat" hackers, de (al dan niet zelfbenoemde) security onderzoekers. Als zij hun bevindingen via *responsible disclosure* bekend maken, kan dit helpen de informatiebeveiliging op het juiste niveau te brengen en te houden. Maar soms zou je willen dat ze het eens wat rustiger aan zouden doen. Na een bezoek aan een security conferentie ben je vaak enigszins gedeprimeerd over wat ze nou weer voor elkaar hebben gekregen, en vraag je jezelf bovendien af of het nou wel maatschappelijk verantwoord is om dit publiekelijk bekend te maken. Bijvoorbeeld: Hoe gebruik je een 3D printer om extra beveiligde sleutels na te maken via een scan of zelfs vanaf een foto [1]? Daarom de vraag aan de redactieleden: hoe kijken de (CI)SO's aan tegen de "white hat" hackers?

Lex Borger

Je kan je druk maken over disclosures, maar dat helpt niet. Je voorkomt het namelijk niet. Daar waar een kwetsbaarheid is, zal altijd een disclosure volgen. Inschatten hoeveel kwetsbaarheden er mogelijk zijn, is vergelijkbaar met de schattingen van de mogelijke hoeveelheid planeten met intelligent leven in ons zonnestelsel.
Je kan je beter druk maken over het gebrek aan disclosures. "Black hats" sporen kwetsbaarheden al op, en overheden en speculanten kopen ze op. Deze komen dus nooit in het publieke domein, tenminste niet totdat ze een volgende keer gevonden worden. En in dat geval is er waarschijnlijk al grootschalig misbruik van gemaakt. Stuxnet gebruikte 4 zero-day Windows exploits, nauwkeurig verzameld door de verantwoordelijke drieletterige geheime diensten.
Een valkuil waar je als security professional niet in moet trappen is de melder aanvallen. We hebben als samenleving de neiging om zo iemand hard te willen aanpakken, bijna net zoals klokkenluiders worden aangepakt. Je zal zeker onder druk gezet worden door bestuurders om de melder hard aan te pakken. Wees hiervoor op je hoede en wapen jezelf hier vooraf tegen. Beoordeel een melder op zijn gedrag en intenties. Het is voor zo iemand al spannend genoeg, zeker als hij in het hol van de leeuw een voormelding wil doen als onderdeel van een *responsible disclosure*.
Wat mij wel opvalt is dat er een klasse "white hats" aan het vormen is die op meer uit zijn dan de ontdekking en melding van de kwetsbaarheid. Het zijn artiesten geworden, die uit zijn op een voorstelling en een applaus. En de topconferenties zijn bij uitstek de plaatsen om hen aan te treffen. Dit heeft effect op het proces van *responsible disclosure*. Het ethisch verantwoordelijke deel wordt zo ondergeschikt aan de show.

Maarten Hartsuijker

Don't blame the messenger. Het is een uitspraak die we allemaal wel eens gehoord hebben en die hier volgens mij erg goed van toepassing is. Als beveiligingsconsultant, ISO en ethisch hacker volg ook ik het beveiligingsnieuws op de voet. Ik zal zelfs niet ontkennen dat er bij een erg creatief uitgevoerde hack zo nu en dan een glimlach van bewondering op mijn gezicht verschijnt. Achter een eenvoudige melding schuilt immers veelal een flinke hoeveelheid werk en doorzettingsvermogen om toch dat ene gat te vinden.
Natuurlijk komen sommige kwetsbaarheden als ik in mijn ISO-schoenen sta niet altijd gelegen.
Maar moet ik het zoveelste *Java* lek een hacker kwalijk nemen? Of neem ik het

Spy vs. Spy; CC by Dave Fayram

Oracle kwalijk dat het deze software zelf niet beter heeft ontworpen en getest? Ik ben er van overtuigd dat we met elkaar alleen verder komen als we bereid zijn om onze kennis te delen. En volgens mij is dit precies wat white hat hackers doen: kennis delen, in plaats van uitbuiten.
Het op passende wijze geven van een *full disclosure* vind ik een lastiger onderwerp. Om de impact van kwetsbaarheden goed te kunnen evalueren en illustreren is het belangrijk om zoveel mogelijk details te kennen. Maar tegelijkertijd verhogen die details de dreiging. Kwaadwillenden (als ze het zelf al niet hadden ontdekt) lezen immers ook mee.
Een haat liefde verhouding is daarom denk ik wel een goede omschrijving. Soms komt een publicatie erg ongelegen, maar we kunnen ook niet zonder.

Tom Bakker
Ik maak me meer zorgen om wat "white hats" allemaal vinden. Als ISO heb je het er maar druk mee. Het volgen van de laatste disclosures en daar weer achteraan gaan. Soms worden er zoveel kwetsbaarheden gemeld dat je er bijna moedeloos van wordt. Dweilen met de kraan open. En dan nog maar niet spreken over wat "black hats" daarnaast nog vinden, stilhouden en gebruiken.
Zou het niet beter zijn kwetsbaarheden eerst te melden aan de betreffende ontwikkelaars? Misschien, maar dan gaan weer andere belangen meespelen. Nee, dan toch maar *full disclosure* en het risico dat kwaadwillenden op ideeën komen voor lief nemen.
Haat-liefde verhouding? Ja, maar een noodzakelijk fenomeen.

Lex Dunn
Het is goed dat er mensen zijn die zoeken naar kwetsbaarheden in (ICT) systemen, daar leren we met z'n allen van en zo kan de industrie veiligere producten leveren. Maar hoe ver moet je gaan? Ik herinner me nog een geval uit een andere branche: de beruchte "Eland" test [2], die de eerste versie van de Mercedes A-klasse vlak na z'n introductie onderging. Deze test is bedoeld om de koers-vastheid van een auto te onderzoeken bij een onverwachte uitwijk manoeuvre. Het is nooit helemaal duidelijk geworden of hier sprake was van "naar resultaten toewerken" (net zolang proberen met steeds hogere snelheid tot het uiteindelijk mis gaat), of dat er structureel iets mis was met dit type auto. Mercedes heeft in elk geval het onderstel van de A-klasse aangepast.
In onze branche valt het me op dat steeds meer onderzoekers gaan voor de glorie, zoals Lex B in zijn stukje ook al aangeeft. Ik vind dat geen goede ontwikkeling, omdat dan meestal de nuance zoek raakt. Simpel voorbeeld: hang- en sluitwerk met het Politie Keurmerk Veilig Wonen (meestal aangeprezen als SKG) biedt betere bescherming tegen inbraak dan goedkopere sloten, maar zijn ook nog steeds te kraken met voldoende tijd en middelen. Dus je kan inderdaad wel een onderzoeker met een koevoet op een voordeur met SKG sloten loslaten. Na tien minuten hard beuken en wrikken zal hij de deur open krijgen om vervolgens op een congres van slotenmakers te gaan vertellen dat SKG sloten te kraken zijn, maar dat was toch al duidelijk. Hetzelfde geldt voor ICT beveiligingen: ook deze zijn met genoeg tijd en middelen te kraken, het is alleen de vraag hoeveel tijd en hoeveel middelen (lees geld) je nodig hebt. "White hats" die zich richten op alternatieve manieren om toegang te krijgen helpen ons als gemeenschap wat dat betreft beter, dan diegenen die maar door blijven drammen. ●

Links

[1] *MIT Students Release Program To 3D-Print High Security Keys: http://www.forbes.com/sites/andygreenberg/2013/08/03/mit-students-release-program-to-3d-print-high-security-keys*

[2] *Eland test met Mercedes A-klasse: http://www.standaard.be/cnt/dmf20110628_050*

COLOFON

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

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

Redactieraad
Tom Bakker (Digidentity BV)
Lex Dunn (Capgemini)
Ronald van Erven (Timeos Pensioendiensten)
Maarten Hartsuijker (ANWB)
Aart Jochem (NCSC)
André Koot (Strict)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)

Advertentieacquisitie
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 2013
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

COLUMN

HOGE BERGEN VANGEN VEEL WIND?

Een aantal jaar geleden mocht ik tijdens mijn vakantie in het prachtige Wales de berg Snowdon bezoeken. Deze berg ligt in een fantastisch mooie en groene omgeving waar het helaas net even te vaak regent. Kortgeleden werd ik weer herinnerd aan deze vakantie door een bericht in de krant (ik ben nog van de generatie die ook het nieuws van gisteren graag tot zich neemt) over ene Snowdon.

Meneer Snowdon had gelekt dat zijn werkgever (de CIA) een grootschalig geheim onderzoeksprogramma PRISM uitvoerde. Inmiddels is bekend geworden dat dit programma zoveel data verzamelt dat je als normaal mens nauwelijks kunt bedenken hoe die hoeveelheden überhaupt te analyseren zijn. Tijdens een verjaardagsfeestje sprak ik iemand aan die bekendstaat om zijn erg uitgesproken mening. Ik vertelde hem dat de data van onder andere *Facebook*, *Google* en *Apple* zouden zijn misbruikt door de CIA. "Maakt mij allemaal niet uit, ik heb toch niets te verbergen" was zijn te voorspellen reactie. Ik probeerde hem uit te leggen dat ik daar toch iets anders over denk. In al deze data banken staan namelijk wel al mijn personalia. Op *Facebook* staat alleen onschuldige informatie, bij *Apple* alleen mijn aankopen van apps, hardware en wat andere administratieve zaken, maar *Google* is een ander verhaal. *Google* heeft heel erg veel gegevens van mij. Ik heb mijn emailaccount al heel lang en de betrouwbaarheid en de Spam filters zijn zo goed dat ik in de toekomst mijn *Gmail*-adres gewoon blijf gebruiken. Mijn surfgedrag is volledig bekend omdat ik *Google* als standaard zoekmachine gebruik en ook nog gebruik maak van de *Chrome Browser* van *Google*. Al mijn mail wordt gescand en ook mijn zoekopdrachten worden nauwkeurig geanalyseerd. Dit blijkt als ik tot mijn stomme verbazing op een nieuwssite een advertentie zie staan van een autoverzekeraar met een foto van een unieke auto die toevallig ook op mijn oprit staat. Toeval? Nee hoor, want als ik de advertenties wat nauwkeuriger bestudeer, zie ik een advertentie van een wasmachine, die ik inmiddels wel heb gekocht maar waar ik op *Google* een aantal weken geleden naar heb gezocht.

Ik bleek plotseling zo verzonken in mijn verhaal dat ik even vergeten was dat ik het verhaal vertelde aan iemand. Ik zag de man verveeld met zijn glaasje bier staan kijken. Inmiddels was er iemand bij komen staan die geboren en getogen is in een ver moslimland maar inmiddels al zo lang in het noorden van het land woont dat hij Martinitoren in zeer goed dialect weet uit te spreken. Hij laat weten ook een *Gmail*-account te hebben. Hij wist al veel langer dat zijn mail niet alleen geanalyseerd wordt door Google, maar ook door de geheime diensten. Door zijn achternaam en zijn emailadressen in dat verre moslimland zou hij ongetwijfeld precies binnen de doelgroep van de geheime diensten vallen. Hij vertelde mij dan ook dat ze door zijn mails ongetwijfeld overuren moesten draaien omdat hij vaak hele onschuldige vragen stelde aan zijn vrouw die heel anders zouden kunnen worden uitgelegd. Als hij in de plaatselijke Albert Heijn ontdekt dat de pindakaas in de aanbieding is en hij dit in een mailtje zet dan zouden de geheime diensten wel eens een uurtje moeten besteden om er achter te komen wat hij nu bedoelde met de mededeling "De pindakaas is in de aanbieding".

Ik vraag me sterk af hoe die miljoenen mailtjes te analyseren zijn. Als ik de bewuste vriend nu een mailtje stuur beëindig ik deze mails tegenwoordig ook steevast met een mysterieuze kreet als "De beer is over de heuvel". Zal wel weer gepeins veroorzaken bij de CIA. Dat Nederland aan deze flauwekul meedoet is helemaal duidelijk nu we weten dat Nederland meer telefoongesprekken aftapt dan de Verenigde Staten. Iedere keer als mijn moslimvriend mij een mailtje stuurt wordt hij wellicht als gevaarlijke terrorist gezien. Ben ik door mijn vriendschap met hem ook staatsgevaarlijk geworden? En al mijn vrienden? En hun vrienden? Ben ik paranoïde? Ja misschien wel, als ik met iemand spreek ga ik midden in de tuin staan en bewegen onze voeten continu over het grind om afluisteraars geen kans te geven. Telefoon, email, tablets, pc's en andere communicatiemiddelen gebruik ik niet meer. Ik spreek vrienden alleen onder vier ogen. ●

Berry

Data Leakage

Bring Your Own Device

Security As A Service

Compliance & Auditing

SECURITY

geen keuze, maar noodzaak!

De toepassingsmogelijkheden van Bring Your Own Device, Security As A Service, Data Leakage en Compliance & Auditing ontwikkelen zich in hoog tempo. Daarmee nemen ook bedreigingen toe in de vorm van Cybercrime, Hacking en Identiteitsfraude. Ook worden deze bedreigingen steeds geavanceerder. Adequate beveiliging van werkomgevingen, data en identiteitsgevens zijn inmiddels geen keuze, maar noodzaak geworden. Security vereist nu ervaren, betrouwbare en loyale partners. CRYPSYS is toonaangevend op het gebied van security analyse, advies en installatie bij overheden, semi-overheden, gemeenten, grote bedrijven en organisaties.

CRYPSYS
secure computing

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

CRYPSYS is officieel distributeur van: Sophos. Lumension. Norman. Cryptzone. Cryptshare. Adyton. Tenable. Kanguru