04/2013

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 4 - 2013

THEMA: CYBERAANVALLEN

DIAGNOSTIEK VOOR U

ARTIKEL VAN HET JAAR

WAT GAAN WE DOEN TEGEN DE CYBERAANVALLEN?

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

Is er nog privacy? Dit vragen we ons tegenwoordig nogal eens af. Maar laat ik even het volgende scenario schetsen:
Een groep zeeverkenners op Curaçao gaat tien dagen op bezoek bij een padvindersgroep op Aruba. In die tien dagen zijn er een paar ongeplande momenten, met als topper het volgende: Eén avond moet de helft van de verkenners naar het verblijfadres teruglopen, de groep was uit elkaar gevallen door een misverstand over waar de auto geparkeerd stond.
De zeeverkenners zijn in uniform, want ze komen van een formeel diner. De verkenners zelf zien het probleem niet zo, ze hebben wel vaker een dropping meegemaakt. In dit geval weten ze precies waar ze zijn en ze zijn in een groep. Wat kan er misgaan?
Een paar dagen later keren ze terug op Curaçao. Hier worden ze geconfronteerd met een directe schorsing en een mogelijk royement. Ze begrijpen nauwelijks waar het om gaat. Maar al snel wordt het duidelijk. Die bewuste avond laat zijn ze verschillende malen gespot en ondanks het feit dat een telefoontje van het ene eiland naar het andere vrij duur is, zijn er een aantal gepleegd. Er is melding gemaakt van schofterig gedrag, lallend over straat lopend. En dat in uniform. Dit is grote schande! Dat de werkelijkheid anders kan zijn, wordt nauwelijks bij de beoordeling meegenomen. Hoezo wederhoor?
Het heeft weken geduurd en nog een aantal telefoontjes over en weer om het echt recht te zetten: het lallen was gewoon zingen en van alcoholgebruik (laat staan misbruik) was geen sprake.
Dit verhaal heeft zich rond negentienvijfenzeventig afgespeeld. En ja, ik was één van de zeeverkenners. Voor de kenners: lid van de Kon-Tiki groep, groep 11. Maar dus ook in die tijd was er geen privacy. En ik kan me zo voorstellen dat, zoiets als dit verhaal, in ieder plattelandsdorpje in Nederland ook had kunnen plaatsvinden. Ook in die tijd was privacy beperkt, ook al was er geen Twitter en Facebook. Het is één van de oudste herinneringen die ik heb aan privacy. Maatschappelijke discussie hierover was er toen niet.
Inmiddels is die maatschappelijke discussie er wél. Maar daarnaast is een andere discussie gaande: bedrijven worden verwacht bij incidenten volledige openheid van zaken te geven. Hier zit in mijn ogen een tegenstelling: we waarderen onze eigen privacy, maar bedrijven moeten volledig transparant zijn. En wanneer ze dat zijn, lopen ze het risico dat zaken die publiek gedeeld worden nog eens volledig uit verband worden gerukt, net als de tocht naar 'huis' van de zeeverkenners toen. Daar kun je je nauwelijks tegen wapenen.
Ik ben helemaal voor openheid, maar met grenzen. Het moet niet te ver gaan. Ook als bedrijf behoud je recht op privacy en wat je deelt of niet deelt moet je zelf mogen uitmaken, gebaseerd op wat wel of niet goed voor je is. We willen allemaal wel eens een momentje kunnen wegstoppen, of dat nu privé is of bedrijfsmatig.

Lex Borger, hoofdredacteur

INHOUDSOPGAVE

Foto omslag: World Cyber Games Singapore 2005 cc-sa-by Conew

DIAGNOSTIEK VOOR U

André Koot is Senior Consultant bij Strict in Vianen en redacteur van dit blad en bereikbaar via a.koot@strict.nl.

In het afgelopen jaar kreeg informatiebeveiliging flink wat aandacht. Niet alleen doordat ons blad in een behoefte voorziet, maar vooral omdat security problemen publiekelijk bekend werden gemaakt. Er was sprake van Hacken, van Lekken en van Datadiefstal en er werden kwetsbaarheden bekend gemaakt op manieren die we niet gewend waren. De pers was een bekend medium, maar ook op Twitter werd volop melding gemaakt van kritische lekken. Verwarmingsinstallaties van sporthallen, sluizen (de sluis bleek toegankelijk met gebruikersnaam "Veere" en wachtwoord "Veere" en dat leverde heel wat publiciteit in de pers op), verkeerslichten bleken op afstand te beheren door anderen dan de eigenlijke beheerders. En vertrouwelijke gegevens, vaak met een medisch karakter, bleken soms figuurlijk, maar heel vaak ook letterlijk op straat te liggen (als er weer eens een oud ziekenhuis wordt verhuisd bijvoorbeeld, maar ook als een oude back-up server nog gewoon online blijkt te staan).

De maatschappij is echter nog niet helemaal ingespeeld op deze nieuwe manier van transparantie. Hoe moeten we in vredesnaam omgaan met dergelijke meldingen. Daar zijn verschillende redenen voor:

- Ten eerste is onze wetgeving niet toegesneden op het fenomeen hacken, of zelfs 'ethisch' hacken. We kennen wettelijk gezien eigenlijk alleen computervredebreuk. En dat wil al eigenlijk zeggen dat je, tenzij je in opdracht met vrijwaring bij de klant zelf een onderzoek/pentest uitvoert, gewoon in overtreding bent.
- Ten tweede vinden organisaties publiciteit op dit gebied onprettig. Voor veel organisaties is het risico van publiciteit een reden om te gaan beveiligen. Als je dan in de pers komt, dan heeft dat geen positieve uitstraling.
- Ten derde hebben we geen heel sterke historie als het om toezicht en handhaving gaat. Er is wetgeving die eisen stelt aan het omgaan met gegevens, maar handhaving is matig. De business case voor beveiliging bestaat eigenlijk niet.
- En misschien ten vierde: de meeste risico's zijn alleen te doorgronden

Henk Krol

door specialisten. Privacy risico's? Ach, 'ik heb niets te verbergen' dat is een veel gehoorde uitspraak als het om privacy gaat. En mensen die zich druk maken om privacyproblemen bij Facebook worden meewarig bekeken door de gewone enthousiaste Facebook gebruikers.

Wat er in de regel gebeurt met lekken en zo? Wie zal het zeggen. In de regel zijn er verschillende manieren om met meldingen om te gaan. We onderkennen eigenlijk standaard deze werkwijze:

Een maatschappelijk betrokken onderzoeker meldt een lek bij een organisatie. De bedoeling van de melding is om het lek gedicht te krijgen. Als dwang hanteert de onderzoeker het dreigement het lek en de details te publiceren als de organisatie geen werk maakt van het herstel van het lek. In de praktijk wordt een lek na 60 dagen gepubliceerd. Het op deze wijze kenbaar maken van een lek heet Responsible Disclosure, eventueel gevolgd door Full Disclosure als er geen actie door het slachtoffer wordt ondernomen. Deze werkwijze wordt al jaren gehanteerd.

Sommige hackers hanteren meteen Full Disclosure, met name als ze er geen vertrouwen in hebben dat de organisatie verantwoordelijk omgaat met de melding. Of als ze gewoon boos zijn op de eigenaar van het doelwit.

Overigens is dit de werkwijze van ethische hackers die niet in opdracht van een klant werken. Criminelen werken natuurlijk anders. Zij misbruiken een lek en hebben hooguit pech als een ethische hacker het lek ook ontdekt en het meldt om het te laten herstellen.

Verwarmingsinstallaties, sluizen en verkeerslichten bleken op afstand te beheren

Hetzelfde geldt ook voor Zero-day kwetsbaarheden. Zolang zo'n kwetsbaarheid niet is verholpen, blijft het een risico. Ethische onderzoekers melden de kwetsbaarheid, criminelen misbruiken ze.

Hier doet zich natuurlijk wel al een dilemma voor. Als een onderzoeker een lek vindt, dan heeft hij vermoedelijk al meer activiteiten uitgevoerd dan enkel bladeren over een website. Een beetje prikken, CSS scriptje proberen, eenvoudige SQL-injectie poging, inlogpagina opsnorren, commando-prompt zoeken. Testen op aanwezigheid van de OWASP Top 10 kwetsbaarheden behoort niet tot de standaardacties van een argeloze websurfer. En voor de onderzoeker betekent dat al snel dat als er iets gevonden wordt, er grote kans is dat er één of andere wet wordt overtreden met de dreiging van vervolging als resultaat.

Voor de onderzoeker betekent het al snel dat mogelijkerwijs de wet wordt overtreden

Vanuit de maatschappij en dus ook vanuit onze beroepsgroep wordt duaal gereageerd op dergelijke meldingen. De ene reactie is: "Fout, overtreding, aanpakken". De andere: "Goed dat het gemeld wordt, dan kunnen we er tenminste iets aan doen".

Beide reacties kregen we heel duidelijk in beeld bij twee interessante gevallen vorig jaar. Ten eerste de hack van het Groene Hart Ziekenhuis in Gouda. Een hacker meldde een datalek in een back-up server. Werd keurig via de pers aangekaart en iedereen tevreden. Totdat bleek dat het ziekenhuis aangifte deed en het Openbaar Ministerie de hacker ging vervolgen. De hacker bleek nogal wat gegevens uit de server te hebben opgehaald en (vermoedelijk) gebruik te hebben gemaakt van een lek om malware bij het ziekenhuis te installeren. Het lijkt er in dit geval sterk op dat de grenzen van het ethisch hacken werden bereikt en overschreden.

Een tweede casus was net zo interessant: 'Ethisch Hacker' Henk Krol meldde dat hij bij zorginstelling "Diagnostiek voor U" in Eindhoven (hierna #DVU te noemen) zomaar medische dossiers kon inzien en dat hij ze zelfs kon wijzigen. Hij hoefde daarvoor alleen maar in te loggen met een gebruikersnaam en wachtwoord van 5 cijfers. En daar kwam bij dat het wachtwoord en gebruikersnaam hetzelfde waren. Ook Henk Krol werd vervolgd en schuldig bevonden aan computervredebreuk en het illegaal raadplegen van vertrouwelijke gegevens. Het bedrijf was overigens ook voornemens om Krol aan te spreken op de schade van € 80.000 die nodig

waren om het systeem te auditten en beveiligen.

En op dat moment schiet je als security professional even vol. Dat Krol vervolgd werd, ach, dat is niet onlogisch als hij onoirbare dingen heeft gedaan. Maar hoe zit dat nou eigenlijk met dat bedrijf Diagnostiek voor U? Had dat de medische dossiers, met gegevens van GGZ-patiënten, een zeer kwetsbare groep patiënten, alleen maar beveiligd met een wachtwoord van 5 cijfers? En een wachtwoord dat gelijk is aan de gebruikersnaam? Echt waar? Dat kan toch niet? Dat mag toch zeker niet? En zijn die gegevens na inloggen gewoon via het internet toegankelijk? Voor wie allemaal?

Als er persoonsgegevens met een medisch karakter worden bewerkt, dan stelt in ieder geval de Wet Bescherming Persoonsgegevens (WBP) strenge eisen. Dergelijke gegevens worden op grond van de wet tot de meest gevoelige gegevens (klasse 3) gerekend (medische gegevens van een grote groep natuurlijke personen). Het beveiligingsnormenkader voor de zorgsector (NEN7510) geeft aan dat voor een bepaald classificatieniveau passende maatregelen moeten worden getroffen. En nu kan je het vragen aan wie je maar wilt, maar een wachtwoord van 5 cijfers past op geen enkele manier bij deze eisen. 5 cijfers, dat wordt door een beetje hacker in minder tijd gekraakt dan de tijd die nodig is om die cijfers in te voeren. Dat is geen beveiliging. En dan kan er dus ook geen sprake zijn van hacken. In dat geval heeft Krol wel computervredebreuk gepleegd, maar hacken? Nee, dat bestaat niet.

Wat #DVU vervolgens uitspookte, was eigenlijk de reden om zelf actie te gaan ondernemen: #DVU wilde Krol aansprakelijk stellen voor de schade. Maar, er was geen schade, Krol toonde aan dat er ten onrechte een beheersmaatregel ontbrak, een beheersmaatregel waar het management van DVU voor verantwoordelijk is, namelijk informatiebeveiliging. #DVU voldoet naar onze mening niet aan de eisen die aan een professionele organisatie gesteld moeten worden. Niet alleen vanwege het ontbreken van basale beveiligingsmaatregelen, maar zeker wegens het ontbreken van passende maatregelen zoals wet- en regelgeving die voorschrijven.

Het lijkt er op dat de grenzen van het ethisch hacken werden overschreden

Wij als professionals kunnen niet zomaar ingrijpen. Maar er is wel een toezichthouder die dat kan. Het College Bescherming Persoonsgegevens (CBP) is verantwoordelijk voor de handhaving van de WBP. Het CBP is het enige onafhankelijke orgaan dat van buitenaf iets kan doen. Om die reden hebben wij, een aantal professionals (leden van PvIB en Identity.next), ieder afzonderlijk een brief gestuurd

In die zaak bleek het volgens berichtgeving mogelijk dat:

1. artsen beschikten over een inlognummer van vijf cijfers met een gelijkluidend wachtwoord;
2. artsen niet alleen dossiers van eigen patiënten bekijken, maar ook patiënten waarmee ze geen behandelrelatie hebben;
3. medewerkers van het Ministerie van Veiligheid en Justitie inloggen;
4. na inloggen met dit eenvoudige wachtwoord toegang wordt verkregen tot medische informatie;
5. er door gebruikers zo onzorgvuldig met gegevens kan worden omgesprongen dat onbevoegden zich toegang tot gegevens kunnen verschaffen;
6. er wordt ingelogd zonder dat duidelijk is waarvandaan wordt ingelogd.

Daarbij valt op te merken dat:

1. Het systeem toegang geeft tot medische gegevens die volgens de Wbp zijn aan te merken als bijzondere persoonsgegevens.
2. Er naar mijn mening niet wordt voldaan aan artikel 13 Wbp, waarin wordt gesteld dat de beveiliging is voorzien van 'passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking'. Daarbij moet rekening worden gehouden met de stand der techniek. Daarvan is geen sprake als (zoals bij "Diagnostiek voor U"):
   - bij bijzondere persoonsgegevens eenvoudig te achterhalen authenticatie wordt gebruikt;
   - bij bijzondere persoonsgegevens gebruik wordt gemaakt van zogenaamde éénfactor-authenticatie;
   - er onvoldoende waarborgen zijn dat onbevoegden in het dossier van niet eigen patiënten wordt gekeken.
3. Er twijfels vallen te uiten over het beleid van "Diagnostiek voor U" met betrekking tot het inlogbeleid. Zo blijkt er een account te zijn voor medewerkers van het Ministerie van Veiligheid en Justitie om labuitslagen te zien. Volgens de organisatie is dat afgeschermd, maar dat lijkt niet te stroken met een gebrek aan separatie bij het gebruik van accounts door artsen.

Daarnaast is het mogelijk dat de Wet op de geneeskundige behandel-overeenkomst is overtreden.

Inhoud brief

aan het CBP met daarin het verzoek om te gaan handhaven bij #DVU. Onze argumenten, zoals vermeld in de brief waren de volgende:

Het reageren op een handhavingsverzoek is een wettelijke verplichting van een toezichthouder, het verzoek is daarmee een onderdeel van het instrumentarium van een toezichthouder.
Inmiddels heeft elk van ons een reactie van het CBP gehad. Het College merkt op dat wij niet ontvankelijk zijn, aangezien wij niet 'belanghebbend' zijn. Maar, zo meldt het College ook, er is inmiddels ambtshalve een onderzoek gestart.
We zijn er niet bang voor dat het vervolg zich in het duister voltrekt, we zijn immers wel bekend met het optreden van toezichthouders. Andere toezichthouders, zoals NMa en OPTA, maken publiekelijk bekend welke onderzoeken plaatsvinden en welke sancties zijn opgelegd.

Wij vinden het in ieder geval heel belangrijk dat wij, eerzame burgers, de beschikking hebben over een eigen instrument. We hoeven niet meer lijdzaam toe te zien hoe bestuurders ergens een potje van maken. Raden van bestuur, raden van toezicht en directies zijn zelf verantwoordelijk voor de kwaliteit van hun gegevenshuishouding en ze zijn dus ook zelf verantwoordelijk voor het uitvoeren van risico-management en dus ook het treffen van de noodzakelijke, passende maatregelen.

> Het reageren op een handhavingsverzoek is een wettelijke verplichting

Wat ons betreft is het hele proces een triest verhaal. Maar had Henk Krol niet de kat de bel aangebonden, dan hadden we nu geen precedent gehad. Krol heeft niet handig geacteerd, maar dat is niet zo'n wonder, wie weet wel hoe je met meldingen om moet gaan? Moet je melden bij een bedrijf, bij het NCSC, bij de politie, bij de pers?

Deze situatie zal langzaam wel iets gaan veranderen. Er zijn diverse initiatieven om het hacken en melden beter te structureren. De overheid heeft richtlijnen voor ethisch hacken gepubliceerd, er is een model Responsible Disclosure beleid (van Floor Terra) en er zijn al diverse meldpunten, onder andere vanuit Revspace (de hackerscommunity in Den Haag zelf). Ook vanuit het PvIB willen we meedoen, daarover binnenkort vast meer. ●

ARTIKEL VAN HET JAAR 2012

Namens de jury, Leo van Koppen. Leo is te bereiken via l.c.m.vankoppen@hhs.nl.

Na vijf jaar mag je zeggen dat het een jaarlijks terugkerend fenomeen is geworden, "het artikel van het jaar" van het blad Informatiebeveiliging. Zonder de waardevolle bijdragen van het leger van vrijwillige auteurs zou Informatiebeveiliging niet zijn wat het nu is. Het is mooi als je kennis kunt nemen van andermans ervaringen, expertise of mening en zeker als dat de magische grens van 140 karakters te boven gaat. U krijgt het bijna elke maand in uw (fysieke) brievenbus. Een groot goed dat voortgezet en aangemoedigd dient te worden, vandaar dat de reactie destijds besloten heeft tot deze verkiezing. Voor de winnaar een mooi bedrag van 500 euro en ook een kleinere prijs voor de nummers twee en drie. Omgerekend een mooi uurloon, maar het gaat natuurlijk vooral om de roem. Dat je naam in deze fraaie lijst staat, is natuurlijk met geen goud te betalen.

jaar	auteur	titel
2008	Wolter Pieters	De monsterlijke trekjes van beveiligingsproblemen'
2009	Saïd el Aoufi	De rol van audits
2010	Jan de Boer	De misleider te werk.
2011	P. Schimmel	Succesvolle integriteitsbeheersing door beïnvloeden menselijk handelen
2012	……..	……..

Prijswinnaars "Artikel van her jaar"

Ook dit jaar kreeg de jury van de redactie een shortlist toegestuurd van maar liefst twaalf artikelen en, voor alle duidelijkheid, een vijftal beoordelingscriteria. De redactie blijft volledig "in control"….

De jury, dit jaar bestaande uit Lambrecht Nieuwenhuize, Remco Bakker en auteur, is in deze setting aan de slag gegaan. Ieder heeft individueel en onafhankelijk een beoordeling opgesteld om vervolgens de oordelen met elkaar te delen en te bediscussiëren. Ook in deze vijfde verkiezing was het opvallend en tegelijkertijd veelzeggend dat alle drie de jury leden dezelfde auteur op de eerste plaats hadden staan. Het kiezen van de winnaar was dus geen probleem. Ook het bepalen van de tweede plaats was redelijk eenvoudig. De derde plaats kostte wat meer moeite, hierover liepen de meningen wat meer uiteen.

In zijn algemeenheid is de jury zeer tevreden over het niveau en de leesbaarheid van de gehele shortlist. Van alle nominaties kan gezegd worden dat het duidelijk stukken zijn, dat wil zeggen heel goed leesbaar, taalkundig verantwoord en alle artikelen hebben zeker iets te melden.

IB1 - Virus in je noodstroomgenerator - Jeroen Aijtink en Jan Wiersma
IB2 - De impact van BYOD - John Grüter
IB3 - Het lekken van data - Johan Pater
IB4 - Lean Business Continuity Management bij VGZ - Thérèse van Vliet
IB4 - Hebt u ze op een rijtje? - Rob van Gansewinkel en Aaldert Hofman
IB5 - Vergeten gegevensrisico's - Ronald Koorn en Jeroen van Kerkhof
IB5 - Pincode voor je pacemaker - Jules Prast
IB6 - Schaap of Herder - Jurgen van der Vlugt
IB6 - Open Einde - Henk-Jan van der Molen
IB6 - Feit of fictie – De realiteit van cyber war - Don Eijndhoven
IB7 - Kwantificatie van herleidbaarheid - Matthijs Koot
IB8 - Eigen schuld, dikke bult? - Nicole van der Meulen

Shortlist artikelen

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

Beoordelingscriteria

De jury heeft de eerste drie beoordelingscriteria min of meer gezien als absolute randvoorwaarden en vervolgens het gewicht van het oordeel vooral gelegd bij de laatste twee criteria.

De winnende artikelen uit de voorgaande jaren muntten uit in het vernieuwende gehalte en/of dat de doelgroep aan het denken werd gezet. Ook dit jaar is dat zeker weer het geval.

Hierbij het resultaat:
1. **Schaap of Herder**
   Jurgen van der Vlugt
2. **Open Einde**
   Henk-Jan van der Molen
3. **Kwantificatie van herleidbaarheid**
   Matthijs Koot

Juryrapport

Ook dit jaar is de jury ingenomen over het niveau van alle ingezonden artikelen. Alle artikelen brengen een boodschap die helder is verwoord, taalkundig is verantwoord en de doelgroep in brede of minder brede zin aanspreken. Bij een aantal artikelen wordt een actueel overzicht van de stand van zaken gegeven op een specifiek aandachtsgebied. Dat kan voor een deel van de doelgroep zeer bruikbaar zijn. Een ander deel van de artikelen opent je vooral de ogen door nieuwe inzichten te verschaffen. De echte winnaars maken je niet alleen wijzer, maar doen dit op een zodanige wijze dat het in je gedachten blijft, dat je het gaat *herkauwen* en dat je er op de één of andere manier iets mee doet in je dagelijkse praktijk.

Kwantificatie van herleidbaarheid van Matthijs Koot is een wetenschappelijk artikel over de privacy. Het maakt op zeer uitgebreide wijze duidelijk op welke wijze privacy heel snel geschonden kan worden. Op basis van een reeks van constateringen komen vervolgens design rules naar voren die de boodschap *privacy by design* gestalte geven. Een pittig artikel dat door de detaillering wellicht wat minder eenvoudig leest, maar de beroepsgroep wel kan helpen bij implementatie van privacy.

Het artikel *Open einde* van Henk-Jan van der Molen leest als een roman, fictie, maar met een fraaie boodschap over nut en waarde van open standaarden. Een zeer bijzondere stijl die je niet verwacht in een zo degelijk blad als Informatiebeveiliging. Heel verrassend dus, waardoor je een volgende keer met meer verwachting een nieuw exemplaar zal openslaan. Wellicht is een feuilleton een optie Henk-Jan? Mooie en zeer goed gekozen titel, heel boeiend geschreven, je leest het als een thriller in één adem uit.

Schaap of herder geschreven door Jurgen van der Vlugt geeft op bijna literaire wijze weer wat velen van ons ervaren en denken. Het zet de lezer te denken over de vraag of alles wat we doen en ook de wijze waarop, nu werkelijk wel bijdraagt aan het uiteindelijke resultaat. Het is op een heerlijke wijze doorspekt met quotes, zegswijzen en oneliners en aangevuld met zeer passende afbeeldingen, waardoor het een uitstekende mix is geworden van humorisme en cynisme, dat leest als een trein. Last but not least daagt hij de lezer uit toch vooral te reageren op zijn stellingname. Het is de jury niet bekend of hij veel reacties heeft gekregen. Een vervolgdiscussie bijvoorbeeld via sociale media zou gebruikt kunnen worden als verlengstuk van een dergelijk artikel. De stijl van Jurgen was ons min of meer bekend vanuit een rol als dagvoorzitter. Met dit artikel geeft hij aan dat hij met deze stijl op papier nog beter tot zijn recht komt. Dit type artikelen geeft een extra dimensie aan het blad Informatiebeveiliging doordat het de lezer uitdaagt in denken en doen. De jury spreekt de wens uit dat we hiervan in 2013 meer artikelen gaan zien. Het is een verfrissende afwisseling van de weliswaar zeer informatieve, maar soms ook wat al te brave en minder spannende artikelen.

Tot slot

Na vijf ronden zit mijn termijn erop. Het was iedere keer weer een genoegen om te doen en ik wil André Koot hierbij danken voor het feit dat hij het nodig achtte dat iemand uit het onderwijs deel uit moest maken van de jury. Aan mijzelf nu de uitdaging om ook te gaan meedingen naar een plaats in dat fameuze rijtje. Er gebeurt ook in het onderwijs genoeg dat vermeldenswaard is en wellicht kan ook ik, naast mijn studenten, ook de lezers van Informatiebeveiliging uitdagen in denken en doen. ●

OPINIE

WAT GAAN WE DOEN TEGEN DE CYBERAANVALLEN?



Prof. dr. Pieter Hartel en prof. dr. Marianne Junger zijn verbonden aan de Universiteit Twente. Dr. ir. Jan van den Berg is verbonden aan de Technische Universiteit Delft. Zij houden zich bezig met onderzoek naar cyber security en zijn respectievelijk te bereiken via pieter.hartel@utwente.nl, m.junger@utwente.nl en J.vandenBerg@tudelft.nl.

Een aantal bedrijven, zoals ING, de Telegraaf, en de NS hebben de afgelopen maand last gehad van Distributed Denial of Service (DDoS) aanvallen. Enigszins gesimplificeerd zijn hierin de volgende stappen te onderscheiden: 1) de PC van een gebruiker loopt een computervirus op, bijvoorbeeld omdat de gebruiker een email aanhangsel van dubieuze herkomst opent. 2) De geïnfecteerde PC gaat daardoor deel uitmaken van een 'botnet', waarbij de PC op afstand bestuurd wordt door een crimineel, ook wel bot-herder genoemd. Hoe meer PC's er in het botnet zitten, hoe meer schade de bot-herder kan aanrichten. 3) De bot-herder besluit om het botnet in te zetten om berichten naar een bepaalde website, bijvoorbeeld van een bank, te sturen. 4) Als dat wordt gedaan, dat wordt de website door overbelasting – nagenoeg – onbereikbaar. Wereldwijd worden er per dag honderden van dergelijke DDoS-aanvallen geregistreerd [1]. Soms pakt de politie een bot-herder op, maar meestal niet, omdat ze zich goed kunnen verstoppen.

Omdat de voorbereiding voor een DDoS-aanval uit verschillenden stappen bestaat, is de bestrijding daarvan het meest kansrijk als op meer fronten preventieve maatregelen worden getroffen. Hieronder beschrijven wij een aantal maatregelen die op korte termijn mogelijk zijn om de situatie te verbeteren.

1. De ISPs gaan samen werken om botnetbesmettingen aan te pakken

De Nederlandse Internet Service Providers gaan binnenkort op grote schaal botnetbesmettingen aanpakken via de Abuse Internet Exchange. Dat is een verzamelpunt waar allerlei informatie bijeen komt over besmette PC's in de netwerken van de providers. Die informatie wordt vervolgens doorgesluisd naar teams die contact opnemen met de getroffen klanten en hen informeren over hoe de computer opgeschoond kan worden. De providers doen dit al enkele jaren, maar onderzoek van de TU Delft toonde aan dat ze maar een beperkt deel van de besmettingen wisten op te sporen en op te ruimen. Het nieuwe initiatief gaat het probleem grootschaliger aanpakken.

> De kans bestaat dat u medeplichtig bent aan een van de recente DDoS-aanvallen

2. De gebruiker gaat de thuis PC beter onderhouden

Als gebruikers maken wij zelf deze kans op besmetting groter wanneer we onzorgvuldig omgaan met onze PC, bijvoorbeeld als we niet de laatste versie van de programma's gebruiken, of als we de virusscanner

of de firewall uitzetten. Uit onderzoek van de TU Delft is gebleken dat ongeveer één op de twintig PC's besmet is. Dit betekent dat de kans bestaat dat u, lezer, 'medeplichtig' bent aan één van de recente DDoS-aanvallen op onze banken of - op dit moment - meedoet aan de DDoS-aanval op een bedrijf elders in de wereld. Daarom lijkt het ons verstandig dat gebruikers nadrukkelijk op hun verantwoordelijkheid wordt gewezen om hun PC en daarmee het Internet gezond te houden. Vanzelfsprekend geldt dit ook voor PC's en computersystemen van bedrijven en andere organisaties.

3. Bedrijven gaan de thuis PC gebruiker beter helpen

De banken vertellen ons al sinds jaar en dag hoe je je thuis PC zo gezond mogelijk kan houden [2]. De benodigde software kun je kopen bij bedrijven zoals Symantec, Microsoft en Kaspersky. Maar die software kan beter; zo kost het vaak te veel tijd om nieuwe virussen te analyseren en de software zodanig bij te werken dat die virussen worden herkend en onschadelijk gemaakt.

4. De overheid gaat werken aan een APK voor PC's

Gebruikers moeten aanvullende hulp kunnen krijgen in de vorm van extra kennis en hulpmiddelen. De overheid zou bijvoorbeeld een veiligheidspakket (à la het Duitse veilige e-mail encryptiepakket) kunnen aanbieden, waarmee de gebruiker een simpele "APK-controle" op zijn of haar PC, MAC, én smartphone (en eerdaags ook de digitale TV) kan uitvoeren. Vindt het APK pakket geen problemen, dan ben je grotendeels gevrijwaard van digitale onveiligheden.

5. Er komt een internationaal certificeringssysteem voor software

Virussen maken misbruik van fouten in computerprogrammatuur. Het opzetten van een certificeringssysteem voor programmatuur kan helpen om fouten te voorkomen en daarmee het probleem kleiner te maken, want hoe minder fouten hoe beter.

Succes tegen botnets kan bereikt worden, indien de Nederlandse overheid samen met private partijen bovenstaande punten voortvarend aanpakt. Daarmee is de kous zeker niet af. Het ligt in de lijn der verwachting dat DDoS aanvallen ook steeds vaker gaan gebeuren via de smartphone (waar zijn de veiligheidspakketten?) en de digitale TV. De overheid zal zijn sturende en wetgevende rol rond cyberspace nog serieuzer moeten nemen en bovenstaande initiatieven op elkaar moeten afstemmen, mede in de internationale context. Dit klemt des te meer daar criminelen niet stilzittend zullen afwachten wat wij gaan doen, maar, als reactie op bovenstaande, hun tegenmaatregelen nemen. Kortom, we zullen alert moeten blijven om cyberspace ook in de toekomst voldoende veilig te houden, door inspanningen van ons allen. ●

> De overheid zal zijn sturende en wetgevende rol rond cyberspace nog serieuzer moeten nemen

Links

[1] *Atlas Global DDoS Summary Report: http://atlas.arbor.net/summary/dos*

[2] *NVB campagne Veilig Bankieren: http://www.veiligbankieren.nl*

TSTC – de Security Opleider van Nederland

- Diginotar, Facebook, KPN 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!

TSTC TSHUKUDU TECHNOLOGY COLLEGE

Want security start bij mensen!!

WWW.TSTC.NL

COLUMN

PRIVACYSCHENDING DOOR DE OVERHEID EEN THEORETISCHE DISCUSSIE? LAAT IK HET DAN EENS HEEL CONCREET MAKEN

Onlangs debatteerde men in de Tweede Kamer over het invoeren van automatische herkenning van nummerplaten. Die worden dan vervolgens in een database opgeslagen. Dat is handig, want dan kun je later nog even kijken of er een boef tussen zat. Het CDA ziet hier geen enkel probleem in voor de privacy van burgers, want privacyschendingen door de overheid… dat is toch immers slechts een theoretische discussie? Laat ik het dan voor het CDA eens heel concreet maken met slechts een paar voorbeelden van privacyschendingen door onze Big Brother.

Zo was er bijvoorbeeld dat geval van die mevrouw met een uitkering. Die kreeg een huisbezoek, zodat de overheid tandenborstels kon tellen om te zien of ze wel echt in haar eentje woonde. In het vonnis van de rechtbank staat het huisbezoek als volgt omschreven: "Tijdens dat huisbezoek is de woning getoond en hebben appellante en E. verklaringen afgelegd. Daarbij kwam onder meer naar voren dat bij aanbellen de deur werd geopend door E., dat door de gehele woning antieke meubels en voorwerpen van E. verspreid stonden, dat de kast op de slaapkamer van E. deels zijn kleding en deels spullen van appellante bevatte en dat de achtertuin geheel door E. onkruidvrij was gemaakt en opnieuw door hem was beplant." Nu zult u denken: dat is een uitgemaakte zaak! Dat was het volgens de rechter dus zeer zeker niet. Er was geen enkele sprake van een redelijke verdenking. En doordat deze ontbrak was er geen reden voor het huisbezoek en was er dus sprake van een inbreuk op het huisrecht (het huisrecht is onderdeel van het grondwettelijke recht op privacy).

En mag ik u er dan misschien ook op wijzen dat er op dit moment maar liefst 11 rechtszaken tegen de Nederlandse overheid lopen in verband met privacyschendingen inzake de Paspoortwet? In alle 11 de gevallen gaat het over burgers die vanuit principieel oogpunt weigeren hun vingerafdrukken af te geven. In 7 van deze zaken loopt inmiddels een hoger beroep bij de Raad van State. Alle beroepen zijn echter stilgelegd en zullen pas weer hervat worden als het Europese Hof van Justitie uitspraak heeft gedaan over de betwistte rechtmatigheid van de EU verordening die aan de Paspoortwet ten grondslag ligt. Ook hier is er dus zeker nog geen sprake van een uitgemaakte zaak. "The Dutch Council (*red: de Raad van State*) referred the question of legality to the ECJ, arguing that the restrictions on privacy do not outweigh the ostensible aim of fraud prevention, and questioning the RFID technique. The Council also questioned whether fingerprints could be safeguarded so that they would only be used in passports or identity cards and not in databases for other purposes (known as function creep)."

Misschien heeft u ook wel het recente jaarverslag van het College Bescherming Persoonsgegevens gelezen? Ik citeer: "Het CBP constateert in zijn terugblik op 2012 dat de overheid in toenemende mate persoonsgegevens verzamelt en aan elkaar koppelt. Hierdoor neemt het gevaar van een onzorgvuldige en met de Wet bescherming persoonsgegevens (Wbp) strijdige omgang met persoonsgegevens door de overheid toe. Juist omdat burgers in veel gevallen verplicht zijn om persoonsgegevens aan de overheid af te staan, is het essentieel dat burgers erop kunnen vertrouwen dat met die gegevens zorgvuldig en in overeenstemming met de principes uit de Wbp wordt omgesprongen. Uit de praktijk blijkt echter dat de overheid - aangemoedigd door de technologische ontwikkelingen in combinatie met de wens om efficiënt en klantvriendelijk te zijn - steeds meer persoonsgegevens uit de verschillende databases aan elkaar koppelt om deze gegevens vervolgens te gebruiken voor geheel andere doeleinden dan waarvoor zij oorspronkelijk werden verzameld."

Bent u al wakker dames en heren van het CDA? Privacyschendingen door de Nederlandse overheid zijn namelijk praktijk van alledag. Er is bijzonder weinig theoretisch aan de bovenstaande voorbeelden. En dan betreft het nog slechts een paar voorbeelden die ik zo even voor u uit de losse pols schud. De realiteit is namelijk nog veel schrikbarender, maar zoveel plek heb ik hier niet. Als ik werkelijk alle privacyschendingen zou kunnen benoemen alhier, zou u namelijk heel hard gaan huilen en zou u het niet meer in uw hoofd durven halen om privacyschendingen door onze overheid slechts "een theoretische discussie" te noemen. ●

Mr. Rachel Marbus, @rachelmarbus op Twitter

OPINIE

BASEER DE AANPAK VAN CYBERAANVALLEN OP EEN REALISTISCH SCENARIO

Dr. Nicole S. van der Meulen is werkzaam als universitair docent Internet Governance bij de Faculteit Rechtsgeleerdheid van de Vrije Universiteit Amsterdam. Zij promoveerde in 2010 aan de Universiteit van Tilburg met een vergelijkend proefschrift naar identiteitsfraude in Nederland en de Verenigde Staten. Zij is te bereiken via n.s.vander.meulen@vu.nl.

Het gaat inmiddels van kwaad tot erger, als we de berichtgeving over cyberaanvallen mogen geloven. De afgelopen maand lagen meerdere Nederlandse banken onder vuur door een zogeheten Distributed Denial of Service-aanval (DDoS-aanval) en ook was onder andere De Telegraaf aan de beurt. Dat deze aanvallen de dienstverlening verstoren en daardoor als hinderlijk ervaren worden, zal niemand tegenspreken.

Dat vervolgens een grootse oproep wordt gedaan om deze aanvallen te voorkomen, is echter wel een reden voor kritiek. Terwijl winkeliers schreeuwen om meer actie vanuit de banken om problemen te voorkomen, hebben Detailhandel Nederland, Koninklijke Horeca Nederland en de belangenbehartigers van de tankbranche een beroep gedaan op de Nederlandsche Bank om in actie te komen.

In beide gevallen tonen de partijen hun ondeskundigheid op dit gebied aan. Wijnand Jongen van Thuiswinkel.org erkent zelf dat hij geen technisch expert is. Een gebrek aan technische expertise is echter geen carte blanche om kritiek te uiten en eisen te stellen die weinig aansluiten op de realiteit. Jongen roept om grensoverschrijdende afspraken. Men hoeft geen technisch expert te zijn om te constateren dat die al enige tijd bestaan. Maar zelfs met grensoverschrijdende afspraken zijn opsporing en vervolging op het internet lastig. De uitdaging om een aanval te attribueren - om vast te stellen waar deze vandaan komt en wie erachter zit - heeft weinig te maken met een gebrek aan afspraken, maar eerder met het pallet aan technische mogelijkheden om de herkomst van aanvallen te verdoezelen.

> Onmacht is een gegeven in de digitale samenleving

De oproep om de pakkans te vergroten en meer actie te ondernemen om dergelijke aanvallen te voorkomen, leidt tot een weinig vruchtbare discussie. Er moet immers een afweging gemaakt worden over de investering van een maatregel en de daaraan gekoppelde effectiviteit.

De mogelijkheden tegen DDoS-aanvallen zijn beperkt. De hoeveelheid netwerken met besmette computers in de wereld, zogeheten botnets, lijkt omvangrijk. Het inzetten van deze computers om dienstverlening plat te leggen, is relatief eenvoudig. DDoS-aanvallen in hun geheel voorkomen, is mede daarom een illusie. De bestaande mogelijkheden om schade na een aanval te beperken, kunnen ook gepaard gaan met het nodige ongemak. Op basis van IP-adressen kan dataverkeer uit bepaalde landen geweigerd worden, maar dat heeft ook nadelen voor legitiem verkeer. Daarnaast is moeilijk vast te stellen of de aanval vanuit een bepaald land of een bepaalde regio wordt uitgevoerd.

Het Nationaal Cyber Security Centrum spreekt tevens over de mogelijkheid van een 'Notice and Takedown', waarbij aan contacten in het buitenland wordt gevraagd om te helpen door bepaalde IP-adressen offline te halen. Ook dat kan echter negatieve gevolgen hebben als er onzekerheid heerst over het IP-adres van de daders.

De mogelijkheden om DDoS-aanvallen te voorkomen zijn beperkt, net als die om de daders te vervolgen. De afgelopen tien jaar zijn aanvallers slechts twee keer met succes strafrechtelijk vervolgd, blijkt uit onderzoek van internet jurist Arnoud Engelfriet. Ook Engelfriet wijst erop hoe complex het is om aanvallers op te sporen en te vervolgen.

Moet er dan niks gedaan worden? Deze vraag impliceert dat bedrijven, banken en de overheid überhaupt geen actie ondernemen. Onterecht. De vraag zou moeten zijn: wat kan er redelijkerwijs nog meer gedaan worden?

Om die vraag te kunnen beantwoorden, dient eerst geïnventariseerd te worden wat bedrijven, en banken in het bijzonder, allemaal al doen om dit soort situaties en de nadelige gevolgen ervan, zoveel mogelijk te beperken. Dit vereist enige transparantie van de betrokken partijen, die wellicht vanuit hun perspectief niet altijd gewenst is. 'Security through obscurity' is een bekend gezegde; het vrijgeven van informatie over beveiligingsmaatregelen kan ook aanvallers helpen om deze maatregelen effectiever te omzeilen.

Het vrijgeven van informatie over maatregelen kan ook aanvallers helpen

Desondanks werkt gebrek aan kennis van bestaande maatregelen het ongenuanceerd roepen om meer actie in de hand. De vraag blijft echter of, zelfs als deze informatie geheel vrijgegeven wordt, er een vruchtbare discussie tot stand kan komen tussen winkeliers en banken. Wil een waardevolle discussie tussen meerdere partijen mogelijk zijn, dan is een zekere risicoacceptatie een voorwaarde.

De partijen dienen te erkennen dat onmacht ook een plek heeft in de digitale samenleving. Het is een onwenselijk gegeven in het tijdperk waarin alles altijd en overal bereikbaar is. Digitale dienstverlening is nu eenmaal kwetsbaar voor aanvallen en voor uitval. Nagenoeg elke maatregel, zoals het weigeren van verkeer vanuit een bepaalde regio, zal ook nadelige gevolgen hebben. Daar wordt momenteel te weinig aandacht aan besteedt. Een evenwichtigere discussie, die zich niet uitsluitend richt op een wenselijk scenario, maar ook op een realistisch en maatschappelijk aanvaardbaar scenario, zou op haar plaats zijn. ●

Deze opinie verscheen eerder in het Financieel Dagblad.

ARTIKELEN SCHRIJVEN IN DIT PVIB BLAD

De redactie heeft onlangs in combinatie met de activiteitencommissie het publicatieschema voor de rest van het jaar vastgelegd, zie tabel 1. Iedere uitgave heeft een thematische binding gekregen. Dat houdt in, dat de redactie actief op zoek is naar artikelen die onder dit thema vallen. Het is echter nog steeds mogelijk om artikelen buiten het thema ook een plaats te geven, bijvoorbeeld vanwege actualiteit of inhoudelijke kwaliteit.

Het kan zijn dat de redactie besluit om een uitgave tot special te benoemen. In dat geval staat de uitgave *geheel* in het kader van het thema. Op dit moment zijn er nog geen specials aangewezen in het publicatieschema. Voor de invulling van de thema's zijn de volgende ideeën geuit, al moeten deze meer als inspiratie worden gezien dan als inkadering:

- *Consumerization* – BYOD, mobiliteit, informatie governance, compliance-eisen, onbeveiligde data/credentials, "het internet van apparaten"
- *(Cyber)Aanvalsvectoren* – de evolutie van de aanval op IT, aanvallen op clouddiensten en hooggeautoriseerde gebruikers
- *Cloud* – informatie governance, multi-tenant faciliteiten, identity & access management, toegangsbeveiliging als een service, business continuity & disaster recovery
- *Menselijke factor* – beveiliging van mensen (met IT), beveiliging begrijpbaar maken voor mensen
- *Privacy* – bescherming, ethiek, eisen, wetgeving
- *Technologie (beide delen)* – IT security, security monitoring, embedded systems, (het einde van) het wachtwoord, biometrie, data encryptie, digitale watermerken, DRM

Uitgave	kopijdatum	publicatie	thema
IB1	10 dec	26 jan	
IB2	04 feb	09 mrt	Volwassenheid
IB3	11 mrt	13 apr	Consumerization
IB4	22 apr	25 mei	(Cyber)Aanvalsvectoren
IB5	10 jun	13 jul	Cloud
IB6	12 aug	14 sep	Menselijke factor & Privacy
IB7	23 sep	26 okt	Technologie (deel 1, mobile apps)
IB8	04 nov	07 dec	Technologie (deel 2, agile development)

Tabel 1 – Publicatieschema 2013

Auteurs gezocht

De redactie is altijd op zoek naar nieuwe denkbeelden in het vakgebied. En ze zijn er van overtuigd dat die volop aanwezig zijn. Het is verder nuttig om auteurs er op te wijzen dat het schrijven van een artikel wellicht de meest eenvoudige manier is om CPE-punten te vergaren voor het bijhouden van professionele certificaties zoals CISSP en CISA. Het bewijs is eenvoudig te leveren in de vorm van een tastbare publicatie. Hiernaast kun je de wetenschap plaatsen dat je een bijdrage levert aan kennisdeling met en voor professionals, op het gebied van informatie-beveiliging, maar vaak ook breder.
De redactie snapt dat je niet zomaar een artikel in elkaar zet. Dit is een proces, en nota bene een proces waar consultants niet per se goed in zijn. Het is heel anders om een rapport te schrijven voor een opdrachtgever of een artikel voor een professioneel publiek. Mocht je het overwegen om een artikel te schrijven, dan beveelt de redactie aan dat je je aanmeldt bij de auteursgroep op LinkedIn [1]. Hier vind je relevante informatie voor auteurs en kun je ook als auteur (in spé) vragen beantwoord krijgen.

Auteursinstructies

Voor een auteur is het prettig om te weten wat de redactie verwacht wanneer een artikel aangeleverd wordt. Het is voor de auteur eenvoudiger om naar toe te werken en voor de redacteur efficiënter in de begeleiding en beoordeling van het artikel. De auteursinstructies beginnen met een uitleg welk soort artikelen in het blad worden gepubliceerd en wat het publicatieproces is na ontvangst door de redactie. In de ervaring van de redactie zijn vooral de instructies met betrekking tot opmaak van de tekst en illustraties/tabellen heel nuttig, met name het gegeven dat afbeeldingsmateriaal voor drukwerk veel meer resolutie moet hebben dan webpublicaties.

Als je als auteur een bijdrage zou willen leveren aan het blad, neem contact op met de redactie (ibmagazine@pvib.nl). Wij helpen je graag verder. ●

Links

[1] LinkedIn groep voor auteurs: http://www.linkedin.com/groups?home=&gid=4188826 (verzoek tot lidmaatschap indienen)

[2] Auteursinstructies: https://www.pvib.nl/auteursinstructies

VERSLAG

THEMASESSIE INCIDENT RESPONSE

Johan Pater is security consultant bij KPN IT Solutions Trusted Services.
Hij is bereikbaar via johan.pater@kpn.com.

Op dinsdag 29 januari 2013 organiseerde het PVIB de themasessie "Incident Response" wat door meer dan 140 leden is bijgewoond. Het adequaat reageren op security incidenten is een onmisbaar onderdeel van informatiebeveiliging. Maar hoe organiseer je dat? Een (security) incident is per definitie een onvoorziene gebeurtenis. Wat kun je nu doen als een hacker meldt dat hij/zij een lek heeft gevonden en hoe zit dat met die meldplicht datalekken?

Erwin Kooi, security manager bij Alliander opende als voorzitter van de avond, door in te gaan op de vraag hoe je als organisatie moet handelen bij een security incident, zoals een digitale inbraak.

Rence Damming, privacy officer bij KPN nam ons mee in wat KPN heeft gedaan om de organisatie voor te bereiden op de meldplicht datalekken. KPN heeft hiervoor het high level ISF (International Security Forum) framework voor data privacy toegepast. Rence vertelde over de definitie van een privacy incident en gaf aan welke informatie voor de toezichthouder OPTA moet worden verzameld. Hiervoor is het bestaande security incidentenproces aangepast en heel veel aandacht aan awareness besteed. Zo dient iedere KPN medewerker verplicht een e-learning te volgen over privacy en zijn er 1-op-1 management sessies geweest. Rence vertelde dat KPN liever 100 meldingen teveel heeft dan één te weinig.

Erik de Jong, werkzaam bij Fox-IT vertelde over de anatomie van incidenten. Hierbij werd een plaatje van een kameel als metafoor gebruikt. Het begint op de kop van de kameel, waarbij er een incident is, directe actie is vereist en er beslissingen moeten worden genomen op basis van vrijwel geen informatie. In het heetst van de strijd is er onderzoek en communicatie en wellicht ook een melding bij een toezichthouder. Als eenmaal de rust is wedergekeerd en alle leerpunten zijn verzameld, is er nog een hele grote to-do lijst, waarbij we de rug van de kameel moeten opklimmen.

Floor Terra, ethisch hacker vertelde over zijn ervaringen en leermomenten na het melden van een security incident bij een bank. Hiervoor heeft hij een website gelanceerd met een voorbeeld van een responsible disclosure beleid, mede om de dialoog aan te gaan met hackers en organisaties. Het belangrijkste wat naar voren kwam, is om de melder en melding serieus te nemen en de kwetsbaarheid niet te negeren. Hierbij werd aangesloten op wat Erik de Jong in zijn presentatie aangaf: 'Wees eerlijk in je communicatie, want er zijn altijd mensen op het internet die de waarheid weten'.

André Beertens, Chief Information Security officer voor vier ziekenhuizen vertelde hoe de organisatie een digitale inbraak heeft ervaren en wat zij allemaal aan communicatie hebben gedaan. Hierbij was er niet meer sprake van een responsible disclosure, want het was al aan meerdere partijen gecommuniceerd. André vertelde dat iedereen in de organisatie gericht was op het oplossen en communiceren en dat er ook snel besluiten werden genomen. André sloot aan bij de presentatie van Erik de Jong, waarbij ook zij hebben ervaren nu op de rug van de kameel te zitten en dat er nog veel werk verricht moet worden.

Erwin Kooij sloot de themasessie af door de sprekers te bedanken, waarna de discussie werd voortgezet onder het genot van een hapje en een drankje. ●

VERSLAG

"BCM IS LEUK"

Lex Borger is een consultant informatiebeveiliging bij Ideas-to-Interconnect en hoofdredacteur van dit blad. Hij is te bereiken via l.borger@i-to-i.nl.

Op 1 April 2013 werd BCM-expert en -auteur Jacques Cazemier een 'pensionado'. De professionele gemeenschap nam op 11 april jl. afscheid van Jacques op een expertsymposium, dat door VKA in DeFabrique werd georganiseerd.

DeFabrique is een aparte evenementenhal in Utrecht-noord. Ooit begonnen als huisvesting voor een olieslagerij is de grote fabriekshal nu een evenementencentrum. Het is een prachtige omgeving om van een icoon afscheid te nemen.

Twee personen vertelden over de inrichting van Business Continuity Management (BCM) in hun organisatie: Erno Kleijnenberg, bestuursvoorzitter bij ONVZ en Thérèse van Vliet, business continuity officer bij VGZ.

Erno beschreef hoe je BCM klein moet houden, dicht bij de business en dicht bij de mensen. Thérèse gaf haar uitgangspunten bloot: Ga uit van vaardigheden die je moet hebben, leg niet te veel vast en denk vooral nú al na wat je bij een crisis gaat doen. Ze vond dat, terwijl de crisis zelf natuurlijk niet leuk is, vooraf bezig zijn met BCM vooral leuk moet zijn, niet moeilijk of formeel.

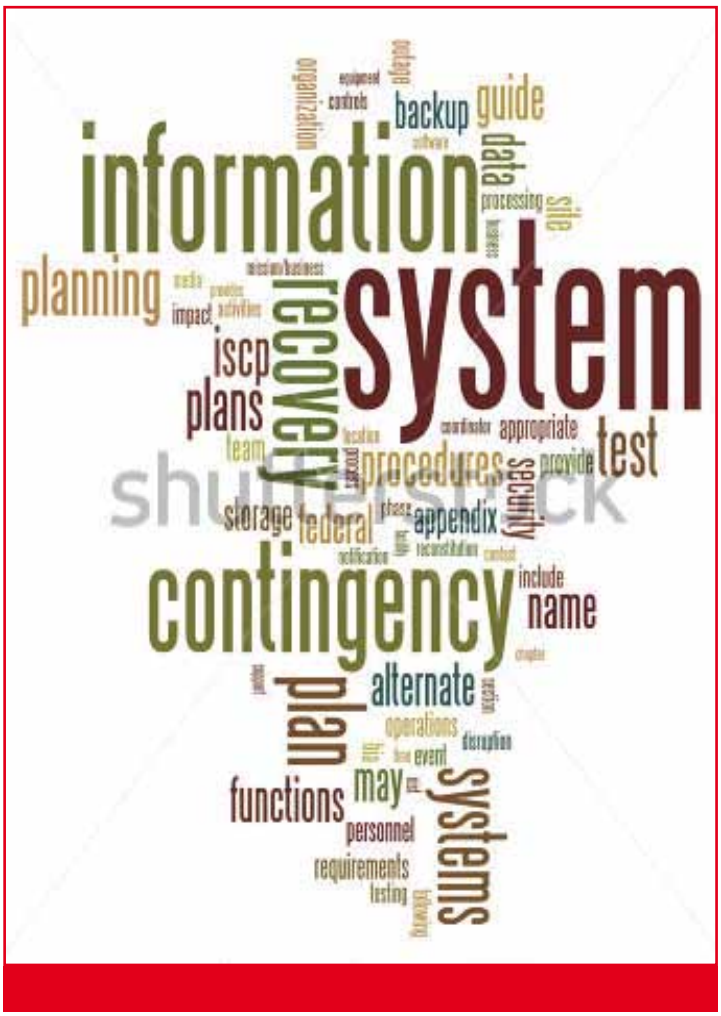
Deze wijsheden hadden ze opgepakt van Jacques. Jacques heeft een lange en mooie staat van dienst en heeft zijn kennis ruim gedeeld met zijn omgeving. Altijd was hij bereid om zijn mening te geven over een dilemma wat je hem voorhield of zijn scherpe analyse te geven van een specifieke situatie.
Jacques is een bekend auteur, recente boeken van zijn naam zijn "Information Security Management with ITIL V3" en "Business Continuity Management". Ook heeft hij artikelen geschreven voor vele tijdschriften, waaronder ook

Informatiebeveiliging. En van ons mag hij dat ook als pensionado blijven doen...

Voor Jacques was er de gelegenheid om het laatste woord te hebben. Hij was de derde spreker van de dag. Jacques had nog twee tips voor diegenen die in zijn voetstappen moeten volgen:

- Focus nóg meer op crisiscommunicatie.
- Werk aan 'lean auditing'. We raken steeds meer in een cultuur van 'vinkjes zetten'. Jacques sprak zijn zorg uit over de checklists die gezond boerenverstand vervangen. Zijn idee: heb aandacht voor het 'typische', niet de norm.

Nu dat hij gepensioneerd is, gaat Jacques zijn tijd besteden aan een andere kunst, meer beeldend. In de receptieruimte stonden kunstwerken van Jacques geëxposeerd. En nu hij daar veel meer tijd voor heeft, zullen daar nog flink wat kunststukken bij komen. ●



DATA BREACH INVESTIGATION REPORT 2013 UITGEBREIDER DAN OOIT

Eerste indruk van de redactie. Vragen en/of opmerkingen kunt u sturen naar ibmagazine@pvib.nl.

Op 23 april dit jaar publiceerde Verizon hun jaarlijkse Data Breach Investigations Report (DBIR) [1]. Het rapport is dit jaar uitgebreider dan ooit, uit 19 bronnen werd informatie over 47 duizend incidenten verzameld. Bij 621 incidenten is het duidelijk dat er sprake is van dataverlies. De meeste cijfers in het rapport hebben deze subset als oorsprong.

De DBIR zou verplichte leeskost moeten zijn voor eenieder die zijn brood verdient in de informatiebeveiliging. Dit rapport bevat de harde cijfers achter de incidenten die onderzoekswaardig waren voor één van de 19 bronnen, waaronder zich ook het Team High Tech Crime van de KLPD bevindt. Analyses op basis van dit rapport kunnen prachtig gebruikt worden om managers en bestuurders te informeren.
Nieuw in dit rapport zijn Microsoft's Broad Street taxonomie en meer demografische analyses. Opvallend is dat data verlies via mobiel of uit de cloud nog nauwelijks een aanmerkelijk aandeel vormt in het geheel.

DBIR Voorpagina

Door de jaren heen heeft het DBIR al bewezen dat de cijfers in het rapport een betrouwbaar beeld geven van beveiligingsincidenten. De geldigheid van de cijfers moet je natuurlijk in de juiste context bepalen: Incidenten uit het rapport zijn incidenten waar een onderzoeksbureau of de wettelijke handhaver aan te pas is gekomen. Simpele diefstallen van mobiele apparaten of laptops komen er dus niet in voor. Ook intern veroorzaakte continuïteitsincidenten hoef je niet te verwachten. Het beeld is dus niet compleet, maar wel zeker breed toepasbaar.

De aggregatie van de cijfers laat een heel duidelijk beeld zien waar incidenten zich voordoen. En hier zit verrassend weinig variatie in: Meest voorkomend is de simpele aanval, met financieel motief op gebruikersapparatuur en servers. Een niet onverwachte nieuwkomer is spionage. De meest universeel gestolen informatie is inloggegevens. En het is duidelijk dat iedereen slachtoffer kan zijn van dataverlies.

De meest trieste constatering - of de grootste kans voor de informatiebeveiliger, afhankelijk hoe je hier naar kijkt - is dat het grootste deel van de doorbraken pas na maanden ontdekt en door externe partijen gemeld worden. En dat terwijl de doorbraak en uitbraak zelf in uren is gepiept! Of we doen collectief nog niet genoeg aan intrusion detection en log review, of we doen het niet effectief genoeg.

Er is in de eerste weken na publicatie van het DBIR al veel over geschreven door belangrijke autoriteiten op het gebied van informatiebeveiliging [2 … 7]. Naar een aantal van deze reviews verwijzen we hierbij. Ze zijn het lezen zeker waard, net als het rapport! ●

Links

[1] *DBIR 2013 (PDF): http://www.verizonenterprise.com/DBIR/2013/*

[2] *Securosis' review: https://securosis.com/blog/how-to-use-the–2013-verizon-data-breach-investigations-report*

[3] *Forrester's review: http://blogs.forrester.com/rick_holland/13–04–22-observations_on_the_2013_verizon_data_breach_investigations_report*

[4] *Gartner's review: http://blogs.gartner.com/anton-chuvakin/2013/04/29/verizon-dbir–2013-highlights-and-favorites/*

[5] *CSO magazine's review: http://blogs.csoonline.com/data-privacy/2659/nuggets-verizons–2013-data-breach-investigations-report*

[6] *Techtarget's review: http://searchsecurity.techtarget.com/news/2240182198/Verizon-DBIR–2013-Damage-caused-by-simple-attacks-slow-detection*

[7] *Review in de NY Times: http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/*

COLUMN

VALUABLE

In this issue we shall look at a SABSA Business Attribute that is especially slippery in its character: the attribute 'valuable'. Value is measureable, but how reliable are those measurements? That's the slippery bit. The concept of 'value' is closely coupled with risk. The concept of 'risk appetite' is also involved. This is best explored through a series of case studies.

Recently we witnessed a global collapse of the banking system and the world economy. We were wealthy and growing wealthier. Now we're all poor. Questions that have been asked are: where did all the money go? Who finished up with the money? Who's got it now? People think real life can be captured in the form of a game of Monopoly, in which there is a fixed amount of money and it's just a question of who can get hold of it. The game does capture risk-taking, but the model is far too simple as a metaphor for what really happens. The game has a set of rules that constrain the risk levels. In real life these rules don't apply.

The answers to these perplexing questions are simple: there never was any money. There was 'value', in shares, in houses and commercial properties and in material things in general. This gives the impression that value has a materiality – something solid and tangible, but this is an illusion. In reality, value is all in the mind, a psychological phenomenon, and a very slippery fish indeed. Spanish banks invested in property and had healthy balance sheets. The country had a strong economy. Then property prices plunged because there was too much supply and little demand (market forces), and so all the value drained from those balance sheets in a couple of years. Where did the money go? It never existed other than as bookkeeping entries.

Value is driven by human desire to own something. It is an emotional quality. What's valuable to one person may not be valuable to another. Since the earliest days of human society, men have fought wars to acquire desirable things – territory and natural resources such as gold (shiny and rare) and oil (energy needed to keep life going). Value is entirely created by desirability and need. At some point 'the market' invented money, to be a liquid form of value that could easily be transferred from one owner to another in exchange for the things of real (perceived) value. However, money itself is only a series of tokens and only its linkage to the desirable objects that are priced in terms of money underpins its value. The value of money is therefore just as variable as the material objects to which it is linked, as we can see in the money markets. Things became much more risky as we moved on in economic growth, because we moved away from the 'gold standard' (actual gold stored in vaults as the basis for printing bank notes). We printed more money than we had gold, this time underpinned by other material 'valuables' such as property.

Value is created because 'the market' has confidence that these material objects are worth something. The measured value is determined by operation of free market forces. Pricing is based on a 'mark to market' philosophy, which means that something is worth whatever someone else will pay to acquire it. So when someone says that they've had their business or house independently valued, what they have is an expert opinion, which may or may not be validated by putting the asset on the market and finding a buyer.

The inherent systemic risk in this free market is in the form of 'bubbles'. Assets become over-valued because of market enthusiasm that will ultimately collapse. The next one that will hit the global economy is the so-called 'carbon bubble'. Because energy is so desirable, the reserves of oil, gas and coal still in the earth are highly valued. Companies owning these assets have highly valued shares, because the market perceives an opportunity to get rich as these energy reserves are extracted and used.

So where's the threat? Governments around the world (including China) have agreed to limit climate change to a maximum temperature rise of two degrees Celsius. If this plan is implemented then more than half of these reserves are unburnable and therefore worthless, and the global economy will once again collapse. The markets have a risk appetite that is betting on this plan not being implemented. Investors think that there will be warning signals and they will have time to get out as the market peaks, but not everyone can get through the exit at the same time because sellers need buyers, and most will fail because the collapse will be very quick. Maybe the world needs a bit more SABSA thinking injected into it. ●

The Attributer

VERSLAG

PRIVACY EN SECURITY OVER GLASFIBER

Wilfred Hanekamp is IT auditor bij Insite Security.
Hij is te bereiken via whanekamp@insiteadvies.nl.

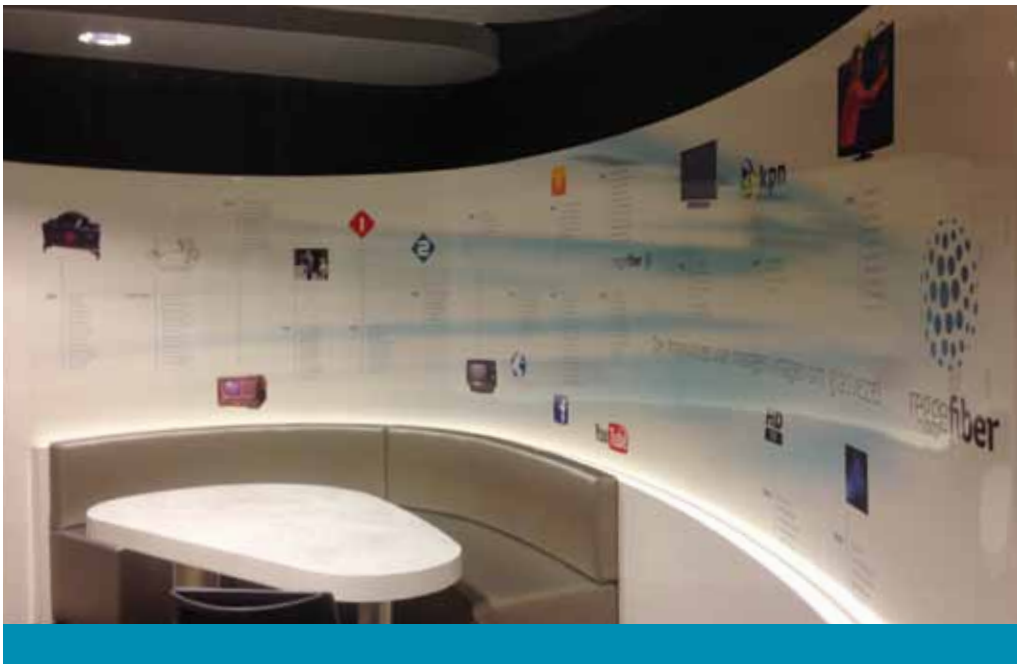
Op 28 februari 2013 jongstleden was het Platform voor Informatiebeveiliging te gast bij Reggefiber in Rijssen. Het bedrijfsbezoek stond in het teken van privacy, cookies en security.

De bijeenkomst werd geopend door de dagvoorzitter, de heer Erik Rutkens, namens het Platform voor Informatiebeveiliging. Hij meldt dat vanuit beveiligingsoogpunt enkele badges van deelnemers op een tweede redundante locatie van een andere PvIB activiteit zijn blijven liggen.
Namens Reggefiber worden de deelnemers aan de bijeenkomst hartelijk welkom geheten door de heer Ben Stortelder. In een bedrijfsfilm 'Innovatief aanleggen' wordt de business van Reggefiber uitgelegd. Reggefiber is een nuchter Twents bedrijf met een gedreven ambitie om zoveel mogelijk huishoudens in Nederland aan te sluiten op glasvezel. De innovatieve aanpak die Reggefiber hanteert, maakt dat Reggefiber sneller en met minder schade kabels kan aanleggen. Dat doet Reggefiber door kabels hoger te leggen dan bestaande kabels en bijvoorbeeld een sleuf te boren in voortuinen en borstelmachines te gebruiken om graafschade te voorkomen. Bijkomend voordeel is dat deze werkwijze zo kosteneffectief mogelijk is.
De visie van Reggefiber is dat glasvezel het netwerk van de toekomst is. Uiteindelijk zal bijna elke woning een aftakking krijgen van de glasvezelkabel wijkcentrale: Fiber to the Home (FttH). De functie van internet verandert – van zoeken, naar delen, naar converseren, naar diensten. Hierdoor is meer en meer bandbreedte nodig. Glasvezel voorziet hierin via optisch datatransport via laserlicht. Reggefiber gebruikt de single mode glasvezel met een onversterkt bereik tot 40 à 50 kilometer. Reggefiber verzorgt de eerste laag: het passieve netwerk. De operators vormen de tweede laag met het actieve netwerk. Service providers zijn met de diensten die ze aanbieden in feite de derde laag.

Na de presentatie van Ben Stortelder nam de heer Henk Lohuis, security officer van Reggefiber, het woord.
Hij ging in zijn presentatie in op het beveiligingsconcept van Reggefiber. Informatiebeveiliging is essentieel voor Reggefiber. Reggefiber heeft daarom een groot aantal technische beveiligingsmaatregelen getroffen en laat zich certificeren op basis van de ISO 27001. Reggefiber maakt in haar infrastructuur bovendien gebruik van geautomatiseerde tooling om de beveiliging van haar IT-omgevingen continu te monitoren. Dit is belangrijk, omdat de IT-omgevingen met enige regelmaat van buitenaf benaderd worden. De IT-infrastructuur is redundant opgezet waarbij de tweede locatie als uitwijk dienst doet.

> Informatiebeveiliging is essentieel voor Reggefiber

Tot besluit van de presentaties van Reggefiber liet Ben Stortelder zien hoe je, zelfs aan je kinderen en schoonmoeder, kunt uitleggen wat glasvezel is en wat je ermee kunt aan de hand van een filmpje van Klokhuis. Ook kwam Humberto Tan nog even vertellen dat hij niet kan wachten tot hij gebruik kan maken van alle toekomstige mogelijkheden die glasvezel biedt. Eindelijk!
Na de pauze was het woord aan Koen Konings. Als eerste in Nederland studeerde hij af in de studie Recht & ICT aan de Rijksuniversiteit Groningen, op het onderwerp privacy.
Koen ging in zijn presentatie in op enkele juridische achtergronden van IT. Privacy



is tegenwoordig vaak in het nieuws, maar is eigenlijk al een stokoud begrip. Het juridische begrip privacy is voor het eerst genoemd in een arrest uit 1834. Privacy bestaat uit ruimtelijke, relationele en informationele privacy. Dit laatste aspect is belangrijk bij automatisering. Privacy werd actueel na afloop van de Tweede Wereldoorlog en werd daarna als grondrecht vastgelegd in diverse internationale verdragen.
Koen schetste dat informationele privacy tegenwoordig vooral actueel is wanneer het gaat over het verwerken van persoonsgegevens. Hierbij ontstaat in toenemende mate een spanningsveld tussen het beschermen van de informationele privacy, een taak die vaak in handen is van (Europese) overheden, en het voortschrijden van technische mogelijkheden die inbreuken op privacy mogelijk maken. Bovendien is sinds de aanslagen van '9-11' in de VS privacy steeds meer onder druk komen te staan in het kader van terrorismebestrijding. Koen stelde echter ook dat privacy niet alleen verticaal, vanuit overheden, onder druk staat, maar ook horizontaal, vanuit grote organisaties, zoals Google. Hierbij speelt het gemak een grote rol; vaak zijn mensen voor 'gratis' diensten bereid hun persoonsgegevens ter beschikking te stellen. Hier treedt het gevaar van 'function creep' op: eerst allerlei persoonsgegevens verzamelen en daarna pas bedenken waar ze voor gebruikt kunnen worden. In de Wet Bescherming Persoonsgegevens zijn, om dit te voorkomen, regels voor 'doelbinding' vastgelegd.
Koen ging vervolgens in op een actuele discussie in het kader van 'doelbinding': cookies. In de diverse regelgeving, zoals de databeschermingsrichtlijn, wordt gewezen op de noodzaak van ondubbelzinnige toestemming voor het verwerken van persoonsgegevens. In dit kader heeft de Nederlandse overheid wetgeving ontwikkeld, waarbij elke gebruiker op een Nederlandse website via een 'opt-in' constructie moet aangeven of deze website cookies mag plaatsen. Nederland is hierbij strenger dan de EU, omdat sinds 1-1-2013 geldt dat elke cookie wordt vermoed een persoonsgegeven te zijn. Recent heeft de OPTA in Nederland tegen deze ontwikkeling stelling genomen. De 'cookiemuren' waardoor websites, zonder acceptatie van cookies, niet zijn te gebruiken, zijn in een aantal gevallen volgens de OPTA niet conform de strekking van de EU richtlijnen, zoals deze bedoeld zijn. Tot slot lichtte Koen toe wanneer een website in de huidige situatie voldoet aan de richtlijnen omtrent plaatsen van cookies. Toestemming voor het plaatsen van cookies is niet nodig in het geval van noodzakelijkheid voor het verzenden van communicatie of om een uitdrukkelijk gevraagde dienst te leveren. Voor alle overige categorieën is toestemming wel nodig, via een uitdrukkelijke 'opt-in' wijze. Stilzwijgende toestemming of slechts informeren is hierbij niet voldoende.
Na de presentatie van Koen Konings bedankte de dagvoorzitter, namens het Platform voor Informatiebeveiliging, de sprekers en alle aanwezigen.
Onder het genot van de borrel werd er nog uitvoerig nagepraat over de ontwikkelingen in de privacy- en cookie-regelgeving. Al met al een geslaagde en leerzame bijeenkomst. ●

> Privacy is voor het eerst genoemd in een arrest uit 1834

BYOD & PRIVACY IN 1995

BLAST FROM THE PAST

Het is goed om vooruit te denken en een visie te hebben over de toekomst en mogelijke ontwikkelingen. Dit is moeilijk, heel moeilijk kennelijk. In 1995 schreef Bill Gates III (ja, de Bill van Microsoft) zijn toekomstvisie op in het boek "The Road Ahead". Er zit een CD bij, maar die is helaas niet meer te gebruiken; niet toekomstvast, dus.

Ik zocht het boek af om verwijzingen naar BYOD en privacy te vinden. Ze staan er in, maar je moet wel met een bril uit 1995 op lezen.
Een duidelijke referentie naar consumerization staat in de volgende passage uit "Implications for Business":
Very soon you'll check your PC, wallet, or television set - the information appliance of your choice - for e-mail, including bills. When a bill comes in, the device will show your payment history. If you want to inquire about the bill, you'll do it asynchronously-at your convenience-by sending e-mail: "Hey how come this charge is so high?"
OK, niet helemaal een zuiver beeld, maar dan lees ik de volgende passage over EDI. Lees XML in plaats van EDI en het beeld is vrij correct:
Tens of thousands of businesses in the United States already exchange information via an electronic system called Electronic Document Interchange, or EDI. It allows companies that have contractual relationships to execute specific kinds of transactions automatically. Dealings are highly structured-reordering products or checking the status of a shipment, which makes conventional EDI unsuitable for ad hoc communications, although many companies are working to combine the benefits of EDI and e-mail into a single system.
The asynchronicity of e-mail and EDI is one of their advantages, but there is still a place for synchronous communications. Sometimes you want to call someone up, talk directly, and get an immediate response rather than leaving a message.

Very soon you'll check your PC, wallet, or television set for e-mail

En dan volgt een complete misser, wellicht het bewijs dat Microsoft de mobiele ontwikkelingen niet voorzag:
Within a few years there will be hybrid communications systems that combine elements of synchronous and asynchronous communications. These systems will use DSVD (and later ISDN) telephone connections to permit the simultaneous transfer of voice and data, even before the full information highway is in place.
Maar de noodzaak van standaarden beschrijft Bill prima:
You won't need to have the same software. The application just has to run on one end of the connection […]. On your end, you would need only an appropriate modem and DSVD software.

Onder "Critical Issues" heeft Bill het over privacy. Hier heeft hij duidelijk meer over nagedacht:
Loss of privacy is another major concern about the highway. A great deal of information is already being gathered about each of us, by private companies as well as by government agencies, and we often have no idea how it is used or whether it is accurate. Census Bureau statistics contain great amounts of detail. Medical records, driving records, library records, school records, court records, credit histories, tax records, financial records, employment reviews, and charge-card bills all profile you. The fact that you call a lot of motorcycle shops, and might be susceptible to motorcycle advertising, is commercial information that a telephone company theoretically could sell. […]

Bill beschrijft hier het business model van Google, een jaar voordat Larry en Sergey begonnen met hun onderzoek op Stanford en jaren voordat ze hier geld mee gingen verdienen. Het privacy probleem is dus duidelijk, maar in de oplossing schiet Microsoft's oprichter mis:
As more business is transacted using the highway and the amount of information stored there accrues, governments will consciously set policies regarding privacy and access to information. The network itself will then administer those policies, ensuring that a doctor does not get access to a patient's tax records, a government auditor is not able to look at a taxpayer's scholastic record, and a teacher is not permitted to browse a student's medical record. The potential problem is abuse, not the mere existence of information.
Het netwerk zelf voert controles uit om misbruik tegen te gaan? Bill heeft duidelijk geen beeld van gedegen bestuur. De term GRC was duidelijk nog niet uitgevonden in die tijd. Bill beschrijft ook niet hoe het netwerk weet wat misbruik is en wie het netwerk dan moet controleren.
Wat ik wel knap vind, is dat hij de opkomst van sociale media wél goed voorziet, want daar was in de negentiger jaren totaal geen sprake van dat zoiets speelde.
These privacy fears revolve around the possibility that someone else is keeping track of information about you. But the highway will also make it possible for an individual to keep track of his or her own whereabouts-to lead what we might call "a documented life". Your wallet PC will be able to keep audio, time, location, and eventually even video records of everything that happens to you.

It will be able to record every word you say and every word said to you, as well as body temperature, blood pressure, barometric pressure, and a variety of other data about you and your surroundings. It will be able to track your interactions with the highway-all of the commands you issue, the messages you send, and the people you call or who call you.

En dan krijg je een voorspelling die uiteindelijk correct is - dat audio en video opnemen en afspelen op computers mainstream wordt. Maar de technische ontwikkeling is duidelijk anders gelopen: we hebben juist meer en snellere opslag, niet grotere compressie, die dit mogelijk heeft gemaakt.

The technology required is not difficult. It should soon be possible to compress the human voice down to a few thousand bits of digital information per second, which means that an hour of conversation will be converted into about 1 megabyte of digital data. Small tapes used for backing up computer hard disks already store 10 gigabytes or more of data-enough to record about 10,000 hours of compressed audio. Tapes for new generations of digital VCRs will hold more than 100 gigabytes, […]

An hour of conversation will be converted into about 1 megabyte of digital data

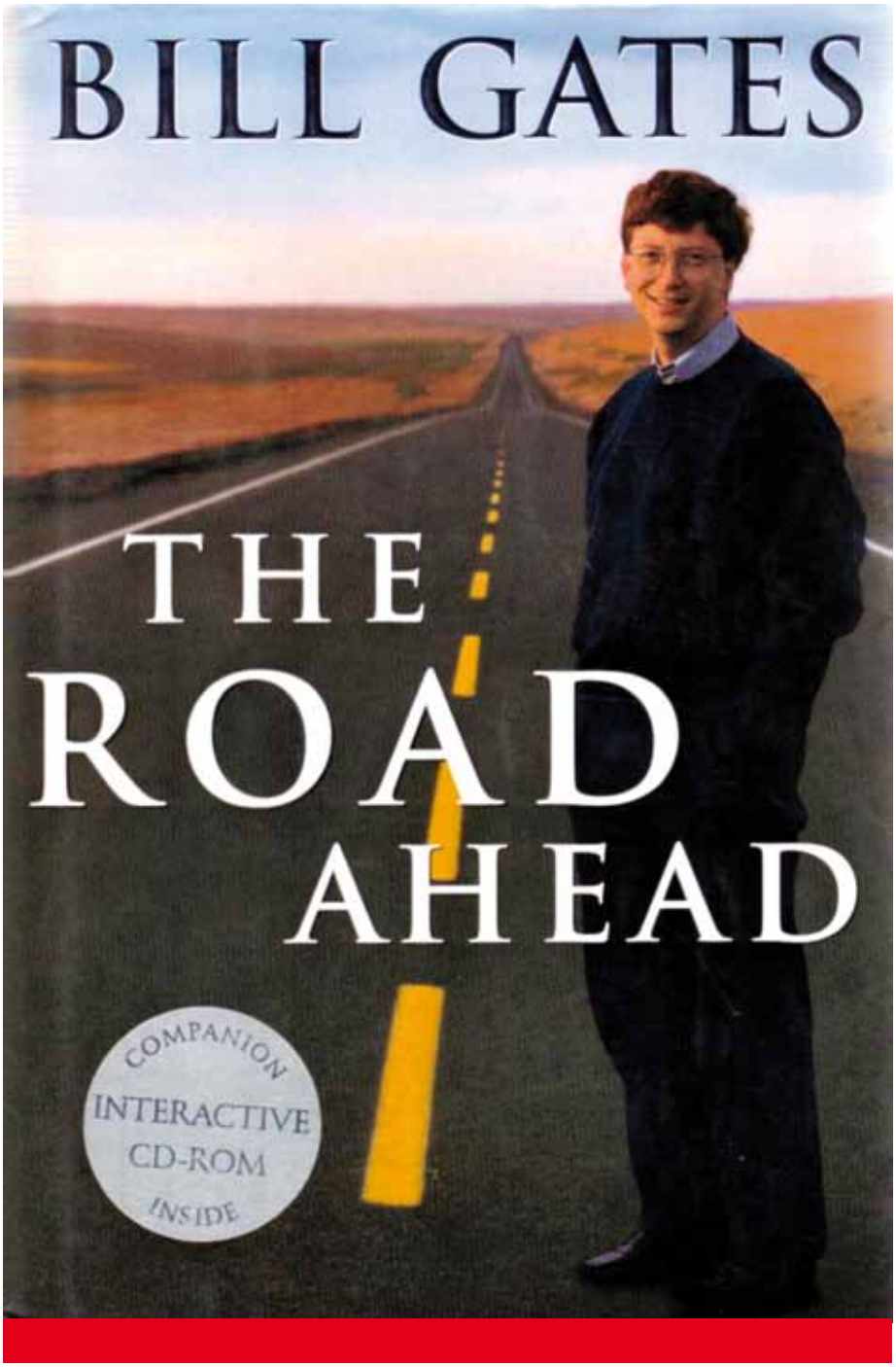
De volgende passage over de alom-aanwezigheid van videocamera's is zeer actueel:

In a world that is increasingly instrumented, we could reach the point where cameras record most of what goes on in public. Video cameras in public places are already relatively commonplace. They perch, often concealed, around banks, airports, automatic-teller machines, hospitals, freeways, Stores, and hotel and office-building lobbies and elevators. The prospect of so many cameras, always watching, might have distressed us fifty years ago, as it did George Orwell. But today they are unremarkable. There are neighborhoods in the United States and Europe where citizens are welcoming these cameras above streets and parking lots. […]

En dan komt eindelijk encryptie ook om de hoek kijken. Eigenlijk verrassend dat het zo laat pas in de conversatie betrokken wordt, omdat de technieken al bekend zijn in die tijd:

At the same time technology is making it easier to create video records, it is also making it possible to keep all your personal documents and messages totally private. Encryption-technology software, which anyone can download from the Internet, can transform a PC into a virtually unbreakable code machine. As the highway is deployed, security services will be applied to all forms of digital information-phone calls, files, databases, you name it. As long as you protect the password, the information stored on your computer can be held under the strongest lock and key that has ever existed. This allows for the greatest degree of information privacy any individual has ever had.

De conclusie laat zien hoe utopisch over cryptografie werd gedacht in die tijd. Inmiddels weten we wel beter, maar dat kan ik Bill wel vergeven. Zelfs Bruce Schneier had die misconceptie in die tijd, dat zette bij pas in 2000 recht in zijn boek "Secrets & Lies". Zo kun je nog eens wat leren over de toekomst uit het verleden. ●



VERSLAG

SECURITY CAFÉ – MOBILE APP SECURITY

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

Vier maal per jaar organiseert Trust in People het Security Café. De editie van 26 februari 2013, werd bij Koetjes & Kalfjes te Zoetermeer georganiseerd. Op LinkedIn hadden de inmiddels 700 leden van de groep wederom voor het onderwerp "Mobile App Security" gestemd. Met de feedback van vorig jaar dat er te weinig diepgang was, heb ik Security Officer Derk Tegeler van Service2Media uitgenodigd om te vertellen over technische details bij de ontwikkeling van o.a. banking apps. Onderstaand volgt een impressie van de discussie.

Bedrijven experimenteren flink met mobile applicaties op zoek naar een toegevoegde waarde. Banking applicaties zijn alom geadopteerd door het grote publiek. Social Media applicaties zijn populair om "anytime, anywhere, anyplace" een foto of een gebeurtenis te kunnen delen. De media brengt graag het laatste nieuws op uw mobiel en voor ontspanning zijn vele games beschikbaar.
Maar er zijn ook bedrijven die via een app contactgegevens van alle vestigingen op een rijtje zetten voor de medewerkers en/of klanten. Maar waar laat je zo'n applicatie ontwikkelen en waar moet het aan voldoen?

Bij het bedrijf waar Derk werkt, worden platform-onafhankelijke apps ontwikkeld. Ontwikkelkosten voor professionele apps zijn al snel enkele tonnen. Dat staat in schril contrast met een hobby app met statische content, die je in de cloud kan laten ontwikkelen door '2 kids in garage' voor zo'n 3000 euro. Professionele ontwikkeling hoort echter niet in de hobbysfeer thuis. Professionele apps worden in een ontwikkelomgeving vervaardigd, waar een uniek ontwerp geïmplementeerd wordt in één raamwerk om vervolgens apps te genereren voor de verschillende mobiele platformen. Dit contrasteert met de zogenaamde 'native' ontwikkelingen waar elk OS een eigen implementatie in specifieke programmeertaal is. Dit is duur en moeilijk te onderhouden.

Apps worden door identificeerbare ontwikkelaars gesigneerd en aangeboden aan de online stores. Deze apps worden door deze stores getoetst op een aantal aspecten als merkenrecht en toelaatbaar beeldgebruik. Je bent hier afhankelijk van een extern beoordelingsproces, wat erg onhandig is als je een belangrijke update wil uitsturen en je op goedkeuring moet wachten van de store. Wat in het beoordelingsproces onderbelicht is, is of

de autorisaties in verhouding staan tot de functionaliteit van de app en welke privacy wetgeving van toepassing is. Onder valse voorwendselen kunnen gebruikers wel een app accepteren, maar op de achtergrond wordt andere informatie gelekt. Omdat apps vaak een beveiligde verbinding opzetten, is het nog niet zo eenvoudig om te zien welke data wordt verstuurd. Je kunt een apparaat aan een draadloos netwerk koppelen om vervolgens via man-in-the-middle techniek een netwerkanalyse uit te voeren. Dit is wel erg duur en niet schaalbaar als je dit per apparaat moet controleren. Wees daarom voorzichtig welke voorwaarden je accepteert, daar het daarna eenvoudig is voor een geaccepteerde applicatie om bedrijfs- & privé data, zoals keylogs, foto's, contacten, e-mail en geluid over het internet versleuteld te versturen, zonder dat je erachter komt. Awareness bij (zakelijke) eindgebruikers moet omhoog als het gaat om BYOD in een gecombineerde omgeving van zakelijk en privé.

Terug naar de beveiliging van professionele banking apps. Derk vertelt hoe pen-testen zijn uitgevoerd door een onafhankelijk partij. Allereerst is het belangrijk te weten dat apps vaak een thin-client/fat-server structuur kennen en de standaard tools en aanpak voor pentesten van een website niet bruikbaar zijn. Het testen van mobile apps is nog vrij rudimentair en het begint ook gewoon bij input validatie via de user interface. Het gedrag van de applicatie wordt beoordeeld als het naar de achtergrond gaat. Er wordt namelijk een plaatje van je app gemaakt, net voordat deze in de achtergrond opgaat. Dit is niet altijd wenselijk vanuit de optiek van veiligheid. Copy-paste is ook handig, maar hoe wis ik mijn prikbord als ik een wachtwoord heb gekopieerd? Misschien is het veiliger om dit uit te zetten in een bepaalde context. Een bestaande security-netwerk pentest applicatie wordt ingezet om een grondige netwerkanalyse te doen. Ook is het belangrijk om een goede risicoanalyse te doen en maatregelen te nemen om de schade te beperken als er misbruik plaatsvindt.

Er zijn nog weinig voorbeelden van mobile security incidenten in de zakelijke omgeving. Er zijn daarentegen wel veel rapporten over een explosie in malware in mobile space, vooral op Android. Banken hebben wel een bedrag in gedachten na risicoanalyse. Fraude is een feit, geen mythe. Malware kan namelijk eenvoudig in de keten komen, soms zelfs door de fabrikanten zelf geïnstalleerd. Het Carrier-IQ schandaal begon vast met de beste intenties, met name om statistieken over gebruik te vergaren. Iedereen schrok wel toen zelfs onze toetsaanslagen geregistreerd werden. Niemand weet wat er daarna met deze data is gebeurd... ●

Links

Security Cafe: informatie beveiliging community in Nederland
www.trustinpeople.com/security_cafe.php

ACHTER HET NIEUWS

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

MEDIAREACTIES DOOR DE BANKEN OP DDOS AANVALLEN; EEN GEMISTE KANS?

Toen in april Nederlandse banken het doelwit waren van DDoS attacks zijn de landelijke media hier bovenop gesprongen. De teneur van de berichtgeving was dat het toch wel schandalig was dat klanten niet online konden betalen (via IDEAL) of geld overmaken. Internetwinkeliers dreigden zelfs om gederfde inkomsten te claimen bij de betreffende banken. En wat was de teneur van de reactie van de persvoorlichter van de zwaarst getroffen bank: "Ons streven is om altijd 24 uur per dag onze online diensten beschikbaar te hebben". Geen waarschuwing aan de kijkers over de kwetsbaarheid van het digitale betalingsverkeer of een uitleg over de onmogelijkheid om te voorkomen dat mensen of organisaties met kwalijke bedoelingen een aanval doen op het systeem. Goede communicatie is op zo een moment van uiterst belang. Zijn de banken wel voldoende voorbereid op een DDoS aanval? Heeft de bank in dit geval goed gecommuniceerd? Hadden ze bij de bank anders kunnen handelen?

Maarten Hartsuijker

Iedereen die wel eens een load test heeft uitgevoerd weet het: elk systeem heeft een maximum capaciteit. De gemiddelde website zal zo zijn ingericht dat de meeste pieken goed zijn op te vangen. Extreme pieken (we kennen allemaal de voorbeelden van websites die tijdens een vermelding in een tv uitzending tijdelijk lastig bereikbaar zijn) worden vaak buiten beschouwing gelaten. Het is immers kostbaar om standaard berekend te zijn op capaciteitspieken die bijna nooit voorkomen.

Als we in ogenschouw nemen dat er in Nederland nooit eerder op deze schaal bedrijven zijn lastig gevallen met distributed denial of service aanvallen, vind ik dat de banken zich er heel redelijk doorheen slaan. Want laten we eerlijk zijn: een aanvaller met een slim aanvalsplan en voldoende aanvalscapaciteit heeft per definitie een flinke voorsprong op de verdediging.

De reactie van de webwinkeliers en klanten is begrijpelijk. Als ik in de supermarkt sta verwacht ik ook dat de kassa werkt. Maar tegelijk vraag ik mij af hoeveel van deze webwinkeliers zelf in staat zouden zijn geweest om met een vergelijkbare aanval om te gaan. En gelukkig zijn we niet volledig van Ideal afhankelijk, maar kan er vaak ook via incasso, Paypal en/of credit card worden betaald.

Tja en die communicatie... Ik had erg veel medelijden met ING Webcare dat alle Twitteraars een identiek "persoonlijk" bericht moest sturen. Maar laten we eerlijk zijn: je doet het als bedrijf niet snel goed. Als je meldt dat je nog niets te melden hebt, ben je te langzaam. Als je iets meldt dat achteraf niet blijkt te kloppen, ben je te snel. En als je iets algemeens bericht, ben je niet specifiek genoeg. Als consumenten en media zijn we er inmiddels aan gewend om overal en met alles live mee te kunnen kijken. Het liefst zien en brengen we vandaag al het nieuws van morgen. Maar misschien is dat in dit soort situaties een beetje teveel gevraagd.

André Koot

Wat niet weet, wat deert.
Het zal wel een enorm dilemma zijn. Vertel ik als bank wel of niet dat er iets fout gaat. Want als ik vertel dat er iets fout gaat, dan betekent dat meteen koersverlies op de beurs en welke graadmeter voor vertrouwen kennen we anders nog in de financiële markt. Als alles gewoon lekker loopt, dan vertrouwt de aandeelhouder mij meer dan als er onrust heerst, maar ooit blijkt dat er iets niet deugt. Dilemma's zat. Levert het al dan niet vertellen meer of minder vertrouwen op dan de andere keuze. Bijkomend probleem is dat een bank niet alleen staat in deze afweging. Ik ben maar een eenvoudige consument, maar ik ben als klant ook partij in dit spel. Ik ben immers de partij die een bank moet vertrouwen. Als de consument de bank niet meer vertrouwt, dan is de waarde van die bank ook opeens verdwenen.
Wat niet weet, wat niet deert, geldt natuurlijk zonder meer. Maar inmiddels weten wij wel beter. En we weten wel meer. En dat betekent dat 'wat niet weet'

opeens wel kan gaan deren. En als ik voor mezelf spreek, dan moet ik zeggen dat het verzwijgen van incidenten mij inmiddels geen vertrouwen meer geeft. Vertrouwen zou voor mij wel gediend zijn met meer transparantie. Dat werkt verschillende kanten op. Ten eerste kan ik 'meeleven' met het slachtoffer van een cyberaanval. Meeleven betekent dan zoiets als dat ik begrip kan opdoen voor het verlaagde serviceniveau. Ten tweede mag ik ervan uitgaan dat de bank in casu mij serieus neemt, als klant en niet als bedreiging.
De financiële sector zal langzamerhand ervaren dat ook de financiële klant mondiger wordt. De medische wereld heeft al een beetje kunnen wennen aan de mondige, internetvaardige patiënt, die eigenlijk sinds dit fenomeen ook klant is gaan heten.
Communiceren is dus randvoorwaardelijk voor het bestaan van vertrouwen.
Maar dan moet er ook wel betrouwbaar gecommuniceerd worden. En daar hebben we de laatste tijd genoeg mee te stellen gehad. Maar wat wil je, als een bank niet goed communiceert, dan vult de maatschappij het verhaal wel aan met alle wild-west verhalen tot gevolg. Als je dan toch communiceert, zorg ervoor dat je de regie zelf in handen houdt. En vertel dus het goede, complete verhaal.
Tijd voor transparantie.

Ronald van Erven
Ik denk dat we hier een combinatie van communicatie factoren hebben. Hoeveel kan je...nee, moet je als (financiële) instelling doen om internetaanvallen te mitigeren? Wat mag je als klant verwachten van de (financiële) instelling. Het zijn toch mijn gegevens of is toch mijn geld? Wat mag je vandaag de dag als (financiële) instelling van de maatschappij (lees mensen) verwachten qua alertheid op internet?
Techniek is één ding, maar uit een onlangs gehouden poll op security.nl bleek dat de factor mens nog altijd de zwakste schakel is. En daarom moet het algehele bewustzijn/ alertheidsniveau van de maatschappij (lees: de mensen) verder en veel sneller omhoog. De moeilijkheid zal zijn - gemak. Internet gebruik moet niet te lastig of hoogdrempelig worden om te gebruiken, want dan zullen mensen afhaken. En in het zoeken naar die balans tussen werkbaarheid (gemak)- kosten-baten zitten we al enige tijd.

Perceptie Management & Verhogen Alertheid publiek
Mag je inbreken in het huis van iemand anders? Nee. Het gebeurt toch en daarom nemen we maatregelen. Een slot op de deur is een technische maatregel. Een aanvullende maatregel is het verschijnen van de regionale- of wijkpolitieberichten over inbraken en verdere tips waar mensen alert op moeten zijn.
Met internet en alle diensten die over internet lopen, is hetzelfde aan de hand, maar we horen zo weinig over de incidenten en de schade. Pas de laatste paar maanden krijg je dergelijk nieuws door en dan nog als het nieuwswaardig is voor journalisten, vaak is voetballen belangrijker dan het wereldnieuws en worden e-incidenten naar de achtergrond verdrongen.
Het verplicht melden van internet incidenten kan hierbij helpen, naar analogie van de wijkpolitie berichten, maar hoe breng je het onder de aandacht?
De financiële instellingen zijn al een paar jaar bezig met spotjes op TV om het publiek alerter te maken:

- het drie keer kloppen initiatief;
- het phishing initiatief;
- ik verwacht nu meer informatieve filmpjes over DDoS, het weglekken van informatie via apps op je smartphone en ID. diefstal.

Maar financiële instellingen hebben ook een handicap.....

Vertrouwen, Geloofwaardigheid & Reputatie
Het vertrouwen in financiële instellingen is door de crisis laag.
De robuustheid van de diensten over internet blijken niet gegarandeerd.
De combinatie van de 24-uur uptime garantie en 100% veiligheid is niet haalbaar.
Deze garantie is afgegeven in een tijd toen financiële instellingen het gebruik van internetdiensten opdrong aan hun klanten. Met als reden om het betalingsverkeer goedkoop te houden. Nu gebruiken de klanten massaal de dienst, omdat het toch een vorm van gemakt brengt, de kosten stijgen toch en helaas blijken diensten van de (financiële) instelling niet 24-uur gegarandeerd te zijn. Er instellingen die eventueel verlies van geld via internetdiensten of telebankieren niet meer zullen vergoeden, als de klant zelf niet voldoende beveiligingsmaatregelen heeft genomen (zie het 3x kloppen initiatief). Dus zal de klant moeten gaan investeren en moeite moeten doen.....weg gemak.
Mijn inziens zal het nog wel even duren voordat mensen begrip tonen als een internetdienst van een (financiële) instelling weer onderuit ligt door één of andere gebeurtenis op internet.
Financiële instellingen hebben in elk geval de financiële middelen om het publiek bewuster/alerter te maken. Nu komt dit vooral uit de hoek van de banken. Maar als banken, verzekeraars, pensioenfondsen (lees o.a. pensioenregister) de handen ineen slaan en gezamenlijk optrekken om de maatschappij bewuster te maken, moet dit lukken en zal er meer begrip zijn voor internet incidenten. En dit initiatief moet niet door info.security mensen of techies gedraaid worden. Maar door gewone mensen die het in jip-en-janneke taal kunnen vertellen en mensen dit laten ervaren.
Voor de complottheoristen onder ons.... wie zegt dat de (financiële) instelling niet zelf hun internetdiensten onderuit halen om zo het bewustzijn van het publiek omhoog te halen en om zo eventuele kosten van maatregelen uiteindelijk toch door te rekenen aan de klanten. Een soort mysterie guest actie!

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 (Allianz)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
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

LIEVER EEN LEREN BANK

De banken zijn de afgelopen periode weer flink in het nieuws geweest, iedere keer lukt het ze weer om op een negatieve manier in de pers te komen. In eerste instantie wisten ze onze hele economie te ontwrichten met hun ordinaire perverse drang om meer en meer geld te verdienen om de bonus weer eens flink te doen laten groeien.
Momenteel ontwrichten ze de economie weer door onvoldoende beschermings-maatregelen te nemen tegen DDoS aanvallen, of doe ik nu een hele sector te kort?
Mij werd laatst gevraagd wat een DDoS aanval eigenlijk is en ik probeerde dat uit te leggen zonder dat de toehoorder enig verstand van zaken hoeft te hebben.
Stel dat je een geloofwaardig bericht in de krant weet te krijgen dat je aanstaande woensdag 1000 euro per persoon kunt halen op het station in Utrecht en dat er 10 miljoen euro beschikbaar is. Dat is een soort DDoS aanval, aanstaande woensdag zal niemand het station meer kunnen bereiken. Ik ben er zelfs bijna van overtuigd dat de stad ook niet meer te bereiken is. Gezien de reactie die ik krijg, noem ik nog maar een voorbeeld. Stel dat je op Facebook de hele wereld uitnodigt om een feestje te gaan vieren in Haren (Groningen).
De autoriteiten zijn dan op de hoogte en kunnen hun maatregelen nemen om de aanval niet te laten lukken.
Ze zouden bijvoorbeeld de toegangswegen kunnen afsluiten, of een echt feest of andere evenementen organiseren, maar helaas is dat niet gebeurt. Op de donderdag voor de beruchte vrijdag zaten een aantal goedbetaalde ambtenaren met vele potten koffie bij elkaar om de maatregelen te bespreken. In de loop naar die donderdag werd langzamerhand duidelijk dat er misschien toch wel mensen op af zouden komen. De koffie werd gulzig gedronken en de ideeën stroomden over tafel: "We sturen ze terug naar Groningen. Er komen maximaal 100 mensen. We halen de straatnaambordjes weg, dan weten ze niet waar ze heen moeten". Kortom, de temperatuur in de vergaderzaal werd hoger en hoger en het ene na het andere briljante idee werd daar geboren. Tegen de schemer liepen ze allemaal voldaan naar buiten en vertelden ze thuis over hun successen van die dag.
Nog geen 24 uur later sneuvelde de eerste lantaarnpaal en de zes agenten deden hun best om de orde te herstellen. Telefonisch hadden ze geen contact meer door het onvolprezen C2000 communicatiesysteem, dat begint te haperen als er meer dan zes agenten gebruik van maken. ME-busjes kwamen uit alle delen van het land, maar hadden geen idee wat te doen, want ze konden niet met elkaar communiceren. De plaatselijke Albert Heijn werd geplunderd en raakten alle voorraden bier en sigaretten kwijt. De biervoorraad was immens, want in de middag waren de omliggende winkels gevraagd bier te leveren, die avond de omzet geen grenzen zou kennen. Het is duidelijk wat er gebeurde, iedere Noorderling was geschokt, maar burgemeester Bats zag geen aanleiding om op te stappen. Zij hadden er donderdagmiddag immers alles aan gedaan om het niet te laten escaleren. Nee, eerst moest de commissie Cohen nog voor 400.000 euro aan onderzoeken doen om aan te geven dat er fouten waren gemaakt. Burgemeester Bats is inmiddels wel werkloos burger en menig Harenaar heeft daar niet zoveel moeite mee.
Mijn vrouw verteld mij dat ik doorsla en dat ze nu nog niet weet wat een DDoS aanval is. Blijkbaar zijn mijn voorbeelden niet duidelijk genoeg. Ik leg haar uit wat een DDoS aanval is en dat je die gewoon op internet kunt kopen voor een euro of vijf. Kan de ING er iets aan doen? Nee, dit overstijgt ING. Justitie zal de daders moeten opsporen en toegegeven dat is niet eenvoudig! Als ze niet worden gezocht, zullen ze helaas nooit worden gevonden en blijven we vertwijfeld naar het beeldscherm kijken, waarom we niets kunnen betalen. ●

Berry

Foto: cc-by Nathan Meijer

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