iB
INFORMATIEBEVEILIGING
jaargang 16 - 2016
#1

CYBER SECURITY

Meldplicht Datalekken

Risico's en maatregelen Social Login

'Perfect Forward Secrecy' op jouw website

Interview Tammy Moskites

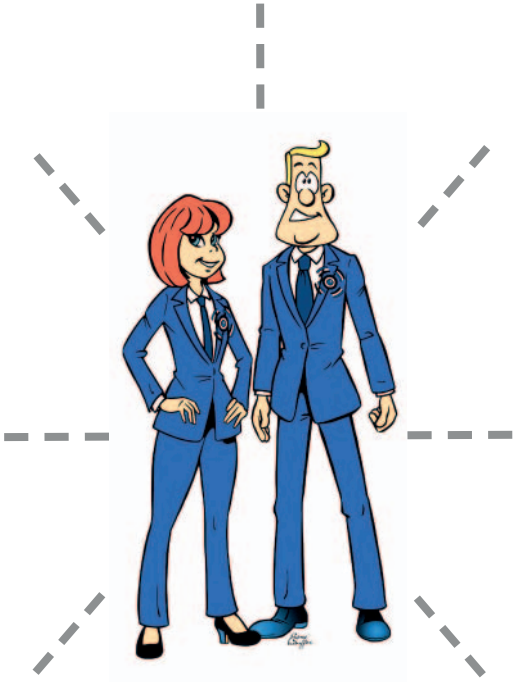
Gezocht: IT security trainees!

"Realiseren van veilige innovatieve IT-infrastructuren."

SecureLink is opgericht in **2003** en heeft **230** enthousiaste SecureLinkers. We hebben **4** vestigingen verdeeld over Nederland en België.

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

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



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

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

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

fd. Gazellen Awards 2011 - 2014

Deloitte. Technology Fast 500

Secure UNIVERSITY

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

Een greep uit onze klanten

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

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

Go Secure!

HET CYBERTIJDPERK

"Cyber - dat is toch verbale opsmuk voor informatiebeveiliging?" hoor ik wel eens. Voor mij zegt 'cyber' meer: we zitten in een nieuw tijdperk, het cybertijdperk, en de informatiebeveiliging die daarbij hoort, vernieuwt mee. Het moet wel.

In 2004 zag de wereld zijn miljardste internetgebruiker. Bedrijven hebben gekozen om meer afhankelijk te zijn van computers en netwerken en minder van mensen. Transacties worden nu technisch afgehandeld. Rond dezelfde tijd zagen we de eerste echt grote internetincidenten. Denk aan MyDoom, Sasser, de TJX hack. Stuk voor stuk veel groter en sneller verspreid dan wat ervoor kwam. Morris, Melissa, Iloveyou waren voorbodes, maar hadden geen slechte bedoelingen en plantten zich niet zo snel voort. Klez en Slammer waren ook voorbodes.

Ik denk dus dat het cybertijdperk zo'n tien jaar geleden begonnen is, misschien iets eerder. De eerste wetten die rekening hielden met een internetsamenleving zijn ook van die tijd: de WBP in 2001 en het Europese Cybercrimeverdrag in 2004. Visionaire stukken, als je terugkijkt. Het publiek begon in die tijd ook te snappen dat er iets aan beveiliging gedaan moest worden, al wisten ze nog niet wat er dan gedaan zou moeten worden. Maar, zoals het gezegde gaat: 'Necessity is the mother of invention', dus we vinden dat snel uit. Encryptie bestaat al vanaf de jaren zeventig, maar het is pas in het cybertijdperk breed beschikbaar en toepasbaar geworden. Er is een revolutie geweest in de techniek voor authenticatie en toegangsbeveiliging. En we hebben tegenwoordig de 'smart'-devices. Iets wat ons online kan authenticeren en dat we ook op waarde schatten, en dus voorzichtig behandelen. De heilige graal van de authenticatie.

Ook de overheden en georganiseerde misdaad worstelden lang hoe ze met het internet moesten omgaan, maar ze zitten nu zo'n jaar of tien in de cyberspionage respectievelijk cybercriminaliteit. Bedrijven investeren als reactie daarop nu ook veel meer in informatiebeveiliging. Het is moeilijk daar betrouwbare cijfers over te vinden, maar ik schat dat die groei wat later opkwam, zo rond 2010.

De laatste 10 jaar waren voor informatiebeveiligers een heel verschil met de jaren ervoor. 25 jaar geleden kenden we al de theorie van beveiliging die we nu toepassen, maar voerden we het nauwelijks uit. We checkten dat de printouts veilig opgeborgen werden... De publicatie van de Code voor Informatiebeveiliging (en de UK tegenhanger BS7799) bracht hier langzaam verandering in. Je wordt nostalgisch als je er aan terugdenkt. Maar de huidige tijd brengt kansen. Volgens een ander spreekwoord: 'May you live in interesting times'. Dat doen we."

Lex Borger, hoofdredacteur

Met dank aan Ben Elsinga, Alan Lechtenberg en Peter Rietveld voor de inspiratie.

In dit nummer

MELDPLICHT DATALEKKEN

Wat wordt er van organisaties verwacht?

Het zal inmiddels niemand ontgaan zijn dat de Wet bescherming persoonsgegevens (Wbp) verandert. Met ingang van 2016 is het toezicht verscherpt en is het verplicht geworden om melding te maken van beveiligingsincidenten. In de volksmond spreken we over de "meldplicht datalekken". Maar wat wordt er nu van organisaties verwacht? Er wordt gedreigd met forse boetes, dus blijkbaar kan men iets "fout" doen in het werken met persoonsgegevens.

De Wbp schrijft "passende" beveiliging voor. De uitdaging is vooral dat de wet niet duidelijk voorschrijft waaraan die beveiliging moet voldoen om passend te zijn. Dit hangt van de interpretatie af en wordt per geval beoordeeld. De Autoriteit Persoonsgegevens (tot 1 januari 2016 College bescherming persoonsgegevens (CBP) geheten), heeft in dit kader twee handreikingen gedaan in de vorm van "beleidsregels". Dit zijn geen ondubbelzinnige uitspraken over passende maatregelen, maar de handreikingen zijn desondanks waardevol. Zoals de Autoriteit zelf stelt [1]:

> Beleidsregels en de bestaande richtsnoeren zijn niet bindend, maar leggen uit hoe het CBP bepaalde artikelen uit de Pbp toepast. Doet het CBP onderzoek naar de verwerking van persoonsgegevens, dan zijn de beleidsregels en de bestaande richtsnoeren daarbij het uitgangspunt.

De Autoriteit heeft meerdere beleidsregels en richtsnoeren gepubliceerd. De twee die relevant zijn om te begrijpen wat verstaan wordt onder passende beveiliging, zijn:

1. **Richtsnoeren beveiliging van persoonsgegevens [2]**
2. **Beleidsregels meldplicht datalekken [3]**

Hoewel de richtsnoeren een duidelijke richting geven, is er nog een vertaalslag nodig naar concrete maatregelen. Die hebben wij samengevat tot een lijst van negen stuks. In twee publicaties in het vakblad IB zetten wij deze lijst van negen maatregelen uiteen. Te beginnen in deze uitgave met maatregel 1 tot en met 5.

1. Beleidskader

Het is aan de organisatie om beleid te ontwikkelen met expliciete maatregelen om de persoonsgegevens te beveiligen. De Autoriteit hanteert de richtlijn dat het beleid is gedocumenteerd en geïmplementeerd in de organisatie. Ook moet dit privacybeleid worden gecommuniceerd naar alle personen in de organisatie en naar relevante externe partijen die betrokken zijn bij het verwerken van persoonsgegevens.
In dit beleid kan bijvoorbeeld invulling gegeven worden aan aspecten als:

- geheimhoudingsplicht m.b.t. de persoonsgegevens (richtsnoeren 2013, p. 24)
- het recht om vergeten te worden, indien gegevens niet meer noodzakelijk opgeslagen hoeven te worden (art. 36 en 40 Wbp)
- Privacy by Design; reeds in de ontwikkelingsfase van producten en diensten rekening houden met privacyvereisten (richtsnoeren 2013, p. 12, paragraaf 1.6)

In de Richtsnoeren beveiliging van persoonsgegevens (2013) staat de plan-do-check-act-cyclus (PDCA) al prominent vermeld. Dit houdt in dat het passend beveiligingsniveau bepaald wordt op basis van een risicoanalyse en de daaruit voortkomende maatregelen. Het is van belang om hiermee te starten om zicht te krijgen op de belangrijkste aandachtsgebieden op het gebied van informatiebeveiliging. Het toepassen van het PDCA-principe voor privacy wordt vaak een "privacybeleidskader" of "privacy governance framework" genoemd.
In het kader van bescherming van persoonsgegevens is het ook belangrijk om een interne toezichthouder te benoemen. De Autoriteit suggereert het aanstellen van een Functionaris Gegevensbescherming (FG), ofwel Data Protection Officer, die intern toezicht houdt op de inrichting en naleving van beveiligingsmaatregelen. Deze FG zal voldoende kennis moeten hebben van de organisatie en de privacywetgeving. De FG dient zich ook te committeren aan een geheimhoudingsplicht. Verder is wettelijk verplicht om de FG controlebevoegdheden te geven, zodat hij onafhankelijk zijn werkzaamheden kan verrichten. Gezien de specifieke rol van een FG geniet deze ontslagbescherming, wat betekent dat hij pas na toestemming van de kantonrechter ontslagen kan worden. In de aankomende Europese Privacy Verordening (EPV) wordt dit vereist voor overheidsdiensten, organisaties met meer dan 250 werknemers en organisaties met als primaire taak het regulier volgen van individuen.

2. Assessments

Privacy Impact Assessment

Een Privacy Impact Assessment (PIA) is een belangrijk hulpmiddel om zelf te controleren of een product of dienst "privacy-proof" is. De NOREA, de beroepsorganisatie van IT-auditors, heeft een standaard-PIA ontwikkeld met als doel om inzicht in risico's te krijgen.
Geadviseerd wordt om de PIA bij het ontwerp van een product of dienst uit te voeren om al de noodzakelijke privacyvereisten mee te nemen. De PIA sluit dus aan op het principe van "Privacy by Design".
Op dit moment is de PIA verplicht voor de rijksoverheid en een handreiking voor overige organisaties die persoonsgegevens verwerken. In de EPV zal de PIA voor elke organisatie verplicht zijn.

Deze tekst is samengesteld door Nandenie Moenielal, Senior Security Consultant en Erik Remmelzwaal, Algemeen Directeur, beide werkzaam bij Nederlands security specialist DearBytes. Vragen of opmerkingen kunt u richten aan nandenie.moenielal@dearbytes.nl of via de website op dearbytes.com/wbp.

Risicoanalyse
Een juist uitgevoerde risicoanalyse past in een privacybeleidskader en geeft de aantoonbare onderbouwing dat technische en procedurele maatregelen zijn getroffen. Het uitvoeren van een gedegen risicoanalyse is een essentieel onderdeel van naleving van de Wbp.

3. Bewerkersovereenkomst met derden

De wet benadrukt de verantwoordelijkheid van de organisatie voor de bescherming van persoonsgegevens, ook wanneer diensten of processen zijn uitbesteed aan derden. Als een organisatie ervoor gekozen heeft om persoonsgegevens in een cloud-applicatie te verwerken, of de website extern te laten hosten, dan is het aan de organisatie om te waarborgen dat de meldplicht datalekken wordt nageleefd.
Het is dus essentieel om heldere afspraken met de bewerker te maken en deze vast te leggen in een zogenaamde 'bewerkersovereenkomst'. Zo kunnen op basis van een risicoanalyse beveiligingsmaatregelen worden bepaald waar de bewerker zich aan moet houden. Ook valt hierbij te denken aan een 'right to audit'-clausule vanuit de verantwoordelijke organisatie, en andere maatregelen om de afspraken met de bewerker te controleren.
Het is belangrijk om ook (keten-)processen in kaart te brengen en de rollen en verantwoordelijkheden in het proces expliciet te benoemen. In de praktijk zal bijvoorbeeld in veel gevallen een datalek bij een bewerker worden geconstateerd. Er moet dan een proces bestaan waarin het datalek onderzocht wordt, besluit tot melding gemaakt wordt en indien nodig de daadwerkelijke melding bij de Autoriteit gedaan wordt. De melding dient uiterlijk op de 2e werkdag na constatering plaats te vinden. De Autoriteit geeft aan dat ook een bewerker melding mag maken in de naam van de verantwoordelijke organisatie.

4. Beveiligingsbewustzijn

De Autoriteit wijst in het kader van beveiligingsbewustzijn vooral op het kenbaar maken van het interne beleid en procedures aan medewerkers. Medewerkers moeten weten wat van hen verwacht wordt, zodat zij daarnaar kunnen handelen. Bij bijscholing moet beveiliging van persoonsgegevens een terugkerend element zijn. Om dit bewustzijn aantoonbaar te maken, kan het zinvol zijn om hierbij gebruik te maken van een eLearning-systeem.

5. Toegangsbeveiliging

Fysieke en logische toegangsbeveiliging hebben als doel om toegang tot informatie te reguleren. In overeenstemming met het privacyprincipe van 'dataminimalisatie' is binnen het autorisatiemanagement het principe van 'need-to-know' en 'need-to-use' van toepassing: welke personen hebben toegang tot welke persoonsgegevens? Hier kunnen we onderscheid maken tussen fysieke en logische toegangsbeveiliging.

Fysieke toegangsbeveiliging
Ten eerste moet worden vastgesteld waar, wanneer en door wie met persoonsgegevens wordt gewerkt. Vervolgens zal expliciet moeten worden onderbouwd of dit noodzakelijke processen zijn. De volgende stap is het inrichten van adequate fysieke beveiligingsmaatregelen, die de identiteit van de persoon controleren en vervolgens de juiste rechten toekennen (authenticatie en autorisatie). Denk hierbij aan toegangscontrole voor gebouwen, afgesloten (server)ruimtes, afgesloten (archief)kasten en kluizen. Een ander belangrijk controlepunt is de toegangscontrole voor externe personen (zoals bezoekers, derde partijen), bijvoorbeeld door het hanteren van beveiligingsprotocollen bij binnenkomst van een pand.

Logische toegangsbeveiliging
Ook bij logische toegangsbeveiliging zullen eerst de informatiestromen die persoonsgegevens betreffen in kaart moeten worden gebracht. Beleidsregels moeten worden opgesteld waarin aangegeven is hoe met informatieverspreiding en autorisatie wordt omgegaan. Daarom moet informatie worden geclassificeerd en moeten beveiligingsniveaus daarop aansluiten.
Logische toegangsbeveiliging in het kader van bescherming van persoonsgegevens houdt vooral in dat strikt wordt toegezien op het beheer van toegangsrechten in applicatie- en netwerkomgevingen waarin persoonsgegevens verwerkt worden. Enkele belangrijke beveiligingseisen hierin zijn:

- Het borgen van krachtig gekozen wachtwoorden
- Het scheiden van toegangsbeveiligingsrollen
- Het inrichten van formele autorisatieprocessen bij toegangsverzoeken
- Het periodiek evalueren en beoordelen van autorisaties

6 tot en met 9

Tot zover deze eerste vijf maatregelen voor "passende" beveiliging. In de volgende editie van IB bespreken we maatregel 6 tot en met 9:

6. Security monitoring: Logging, controle en beheer van technische kwetsbaarheden
7. Databescherming: voor controle over data en om te voorkomen dat betrokkenen over het datalek moeten worden geïnformeerd
8. Incidentenbeheer: voor aantoonbaarheid en om te voldoen aan maximale doorlooptijden
9. Controle op (al dan niet technische) naleving: valideren dat maatregelen ook echt werken

Referenties

[1] https://cbpweb.nl/nl/zelf-doen/beleidsregels
[2] https://cbpweb.nl/nl/richtsnoeren-beveiliging-van-persoonsgegevens-2013
[3] https://cbpweb.nl/nl/nieuws/cbp-publiceert-beleidsregels-meldplicht-datalekken

IK LEK, IK MELD, IK FAX

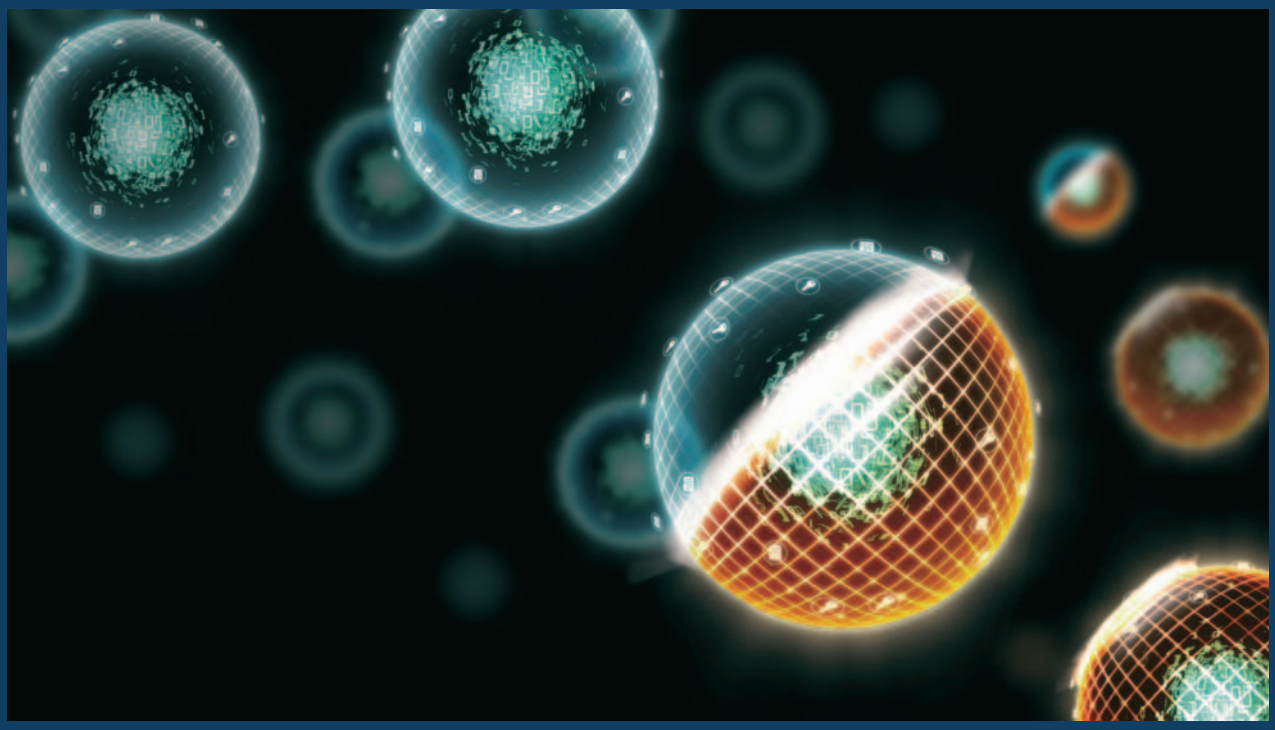
Met een glas champagne in de hand, proostend op 2016, bedenk ik me dat het zover is: de Meldplicht Datalekken. Ergens achter in het hoofd wist ik het al wel op het moment dat ik thuis, vlak voor vertrek naar het oudejaarsfeest, mijn werktelefoon in de tas stopte. "Je weet maar nooit wat er om 00:00 gebeurt". Het feest was waanzinnig, de treinen reden niet (dat doen ze nooit met Oud & Nieuw), kantoorpersoneel was aan het vieren en had hooguit de privételefoon in de hand om te pogen familie en vrienden te appen: het lekte gelukkig niet bij oNS op 1 januari.

Het jaar is amper een paar dagen oud als ik dan eindelijk mag doen waar ik niet naar uitgekeken heb: de eerste melding van een datalek bij de Autoriteit Persoonsgegevens (het is even wennen, maar zo heet het CBP tegenwoordig). U moet zich daar niet al te veel van voorstellen hoor, iemand was zijn GSM verloren en had dat netjes bij de IT-desk gemeld. Desalniettemin, toch spannend zo'n eerste melding. Bij het online meldloket mag ik een hele lijst aan vragen invullen en ik zal het u eerlijk zeggen: daar was ik flink lang mee bezig. Zuchtend worstelde ik me erdoorheen. Wat is ook alweer ons KvK-nummer? En, moet ik bij de technische beveiliging alle details van de versleuteling melden of mag ik volstaan met simpelweg melden dat de door de aanbieder van het toestel voorziene standaardversleuteling gebruikt is? En, als er versleuteling en toegangsbeveiliging op het toestel zit en het alleen gebruikt kan worden door een ander als deze is "schoongeveegd", is er dan nog sprake van "Lezen" bij mogelijk misbruik van de data? Aan het eind gekomen netjes op verzenden gedrukt. En toen gebeurde er niets. Het voelde een beetje als een anticlimax zeg ik u. Afijn, de terugmelding over goede ontvangst alsook het meldnummer zal wel via mijn emailadres binnenkomen, toch? Niets en de dag erna ook niet. Inmiddels was ook al iemand een Railpocket verloren – zo'n scanding van de Hoofdconducteur – en waren er wat simkaarten zoekgeraakt in het magazijn. Die Railpocket bleek uiteindelijk gelukkig teruggevonden. De simkaarten bleven zoek. Weer een paar meldingen en weer niets. Even bellen met de AP. Het meldloket heeft een bug. Een wat? En meldingen komen niet aan. Eh wat? Dus alles met de hand tikken en lekker ouderwets naar de toezichthouder faxen. Ik was inmiddels veel zuchten verder.

Niet gedacht dat ik anno 2016 mijn privacyjaar zou starten met het handmatig intikken van allemaal vragen over een verloren telefoon en wat simkaarten. De meldplicht als middel an sich, daar ben ik nog steeds een groot voorstander van, maar hoe het er nu aan toegaat is volgens mij oprecht niet wat "we" voor ogen hadden toen het eerste wetsvoorstel er lag. Want, laten we wel wezen, ik ben al met al twee werkdagen zoet geweest met wat "mini-meldingen" en ik vrees voor wat nog komen gaat. Dertigduizend medewerkers met allemaal een bedrijfstelefoon en een gedeelte daarvan met Railpockets of andere apparaten. En ja, als die verloren raken, zal ik die allemaal – stuk voor stuk – gaan melden. Er staan immers altijd contactgegevens op…
Oh trouwens nog als laatste toegift: iedereen kan het formulier invullen met een mooie melding. Er is namelijk nergens sprake van authenticatie of identiteitsverificatie bij de online melding.

Proost iedereen! Op een mooi, lekvrij 2016!

Mr. Rachel Marbus
@rachelmarbus op Twitter



HET ONDERSCHEID KUNNEN MAKEN

Een gesprek met Tammy Moskites

Vandaag ontmoeten wij Tammy Moskites, CIO & CISO van Venafi, voor een gesprek in een hotel in Amsterdam. Het eerste dat opvalt is dat zij een bruisende persoonlijkheid is, ze verbergt zich zeker niet achter een gordijn van privacy, zoals sommige van haar collega's. We komen ongevraagd te weten dat ze oma is en met de kleinkinderen naar Disneyworld is geweest. Voor je het weet is het net alsof je haar al veel langer kent.

Ze vertelt dat er fundamentele problemen zijn met de beveiliging van het Internet, waarbij de recente ontwikkelingen binnen de Internet-of-Things de problematieken hieromtrent exponentieel doen toenemen. Dit blijkt uit vrijwel wekelijkse berichten over ontdekte kwetsbaarheden en cyberaanvallen. Tammy is hiervoor in Nederland en spreekt de komende dagen met een aantal grote Nederlandse organisaties die sterk afhankelijk zijn van het Internet.

Gezien haar loopbaan bij Ponemon Institute, Qualys en Venafi, heeft zij diepgaand inzicht in de oorzaken en mogelijke gevolgen van die toenemende incidenten en is bereid om deze met ons te delen.

Tammy heeft sinds de tachtiger jaren een loopbaan binnen de IT. Zij is begonnen "net na het tijdperk van de ponskaarten", en heeft een administratieve achtergrond op actuarieel gebied, waarbij zij voor een verzekeringsmaatschappij kansberekeningsmodellen ontwierp, om sterfte-tabellen te produceren. Een voortuitziende blik, want dit gaf haar de basis om risico-gebaseerd te kunnen leren denken. Deze vaardigheid benut zij nu in haar dagelijkse werkzaamheden.

Voordat Tammy in haar huidige functie stapte, heeft zij onder meer ook bij Home Depot en Time Warner Cable gewerkt. "Dat was niet ten tijde van de hack bij Home Depot", voegt ze er nog snel aan toe. Ze weet dus goed hoe het er in het bedrijfsleven aan toegaat. Nu is zij als CIO/CISO werkzaam bij Venafi, en is negen maanden per jaar op reis. Zij spreekt met CIO's van grote bedrijven over de hele wereld over Risk en Security vraagstukken.

Nep van echt kunnen onderscheiden

Wij vroegen haar wat de grootste zorg is bij bestuurders die zij spreekt. "Niet het onderscheid kunnen maken tussen echt en nep", was haar reactie. "De grootste pijn is het gebrek aan vertrouwen. Men mist de mogelijkheid om goed van slecht te kunnen onderscheiden op het internet. Een eenvoudige illustratie hiervan is dat een gemiddelde gebruiker geen verschil meer kan zien tussen gewone en een geïnfecteerde e-mail, en aangezien 95% van alle security-breaches een van oorsprong menselijk falen betreft, is dit een zeer zorgelijke ontwikkeling." We vragen waar dit falen door wordt veroorzaakt. "De klassieke cartoon 'nobody knows you're a dog' (afbeelding 1) [1] is nog steeds actueel. We weten niet wie of wat iemand is aan de andere kant van het netwerk en we hebben daardoor geen goede basis voor vertrouwen op het internet."

We werpen nog tegen dat er authenticatiesystemen zijn, zoals de TLS-certificaten. "Het certificaatsysteem is op dit moment het beste dat we nu hebben. Een probleem hierbij is dat we niet met zekerheid de status van die certificaten kennen, wat op haar beurt het vertrouwen ondermijnt." Tammy valt stil. Ze weet dat in dit gezelschap het woord 'Diginotar' niet nodig is.

"Een goed voorbeeld hiervan is de reactie van bedrijven op de Windows-Heartbleed-kwetsbaarheid. Dit speelde inmiddels alweer anderhalf jaar geleden. Iedereen heeft de kwetsbaarheid gepatcht, maar Venify kan zien dat op dit moment zeventig procent van de certificaten die potentieel gekaapt zijn door exploitatie van Heartbleed, uiteindelijk niet vervangen zijn." Wat kan daar de reden van zijn, willen we weten. "De kosten van het vervangen van de certificaten en het arbeidsintensieve proces van vervanging werken blokkerend. Wanneer de betreffende software gepatcht is, vergeet men de rest liever en gokt dat de certificaten niet getroffen zijn. Over verstoring van de continuïteit maken bedrijven zich drukker dan over een mogelijk probleem met een certificaat."

"Dit creëert een schijnveiligheid in plaats van afdoende bescherming. Om dit in kaart te brengen biedt Venify een dienst die het internet scant om deze onbetrouwbare certificaten op te sporen en heeft op basis van deze scans een bak met informatie. Ze vinden hiermee een heleboel probleemcertificaten. En probleemcertificaten kunnen leiden tot een incident. Neem bijvoorbeeld de hack bij JP Morgan Chase, waarbij in 2014 de gegevens van meer dan 80 miljoen identiteiten werden buitgemaakt. Één van de stappen die de hackers gebruikten, was een certificaat misbruiken dat buitgemaakt was met behulp van Heartbleed."

Het is de passie van Tammy om het mogelijk te maken de bekende goede status van vertrouwen ('known good trust') vast te kunnen stellen. Op basis hiervan wordt nu ook reputatie-checking aangeboden. "Reputatie is een fundamenteel onderdeel van vertrouwen."

Edzard Buddingh is interim manager en program manager bij i-to-i. Edzard is te bereiken via e.buddingh@i-to-i.nl.
Lex Borger is hoofdredacteur van dit blad, security consultant bij i-to-i en docent security aan de Hogeschool Utrecht.
Lex is te bereiken via l.borger@i-to-i.nl.

"On the Internet, nobody knows you're a dog."

De grootste zorg is niet het onderscheid kunnen maken tussen echt en nep

ITIL – hoe was dat ook alweer?

"CIO's zijn bang voor het onbekende en veel van de bedreigingen op het internet zijn onbekend. De grootste angst voor CIO's is niet of er een cyber-attack komt, maar wanneer het komt en hoe de schade beperkt kan worden. Maar ze zijn reactief bezig. Ze hebben niet door dat omdat de asset-registratie niet op orde is, je niet goed weet wat je hebt. Dat simpele feit maakt dat je ook niet kan weten wat er potentieel misbruikt is. Het op orde hebben van Configuration Management, inclusief alle geïmplementeerde patches en releases is de absolute noodzaak om het cyber-attack-monster te bestrijden. Zonder deze informatie ben je zo effectief als een blindeman zonder geleidehond en stok. Hierbij is de grootte van de organisatie geen factor, dit geldt voor bedrijven van elk formaat." De eerste actie die Tammy aanpakte toen ze bij Venafi kwam, was dan ook het volledig op orde hebben van Asset Management, Configuration Management en Patch Management. "Alle ICT-infrastructurele componenten zijn nu getagd."

Ze vertelt verder: "We zien dat Incident response vaak wel is ingevoerd, maar dit wordt niet of onvoldoende getest. Test bijvoorbeeld een aantal echte scenario's, zoals het verliezen van een USB-stick en kijk wat de opvolging daarvan is. Oefen op incidentscenario's door menselijk falen. De menselijke factor zit overal. Veelal goede bedoelingen, vaak resulterend in een incident met een slechte afloop."

IT-security-breaches are a business problem!

"De business is verantwoordelijk voor business-IT-alignment. Hun leiders beslissen wat een acceptabel risico is voor de business. De IT-afdeling moet zorgen dat deze leiders genoeg informatie hebben, zodat ze de beslissingen verantwoord kunnen nemen. IT moet een business-partner worden. Dit partnerschap is traditioneel juist een techniekpartnerschap en gaat over de onderliggende IT-architectuur. Dit is natuurlijk ook belangrijk, maar de focus in de afstemming tussen business en IT moet zich verplaatsen van die IT naar de organisatie- en businessbelangen. Dit laatste dient leidend te zijn in het samenstellen van het IT-Security Program. Het draait allemaal om vertrouwen. Maar dan wel business-vertrouwen, niet het technisch vertrouwen in bijvoorbeeld certificaten."

"De juiste aanpak hierbij is een juiste rolverdeling tussen drie partijen:

- De (IT-)security-afdeling maakt de security risico's inzichtelijk voor de business;
- De business bepaalt welke risico's wel en niet acceptabel zijn en kiest maatregelen tegen de onacceptabele risico's;
- Het IT-project implementeert alleen die maatregelen die door de business aangegeven zijn en waarvoor er dus budget beschikbaar gesteld is.

Een belangrijke bron die hierbij geraadpleegd kan worden om actuele en relevantie informatie te verkrijgen over mogelijke

aanvallen is bijvoorbeeld de Verizon DBR, die jaarlijks uitgebracht wordt."

"In een volwassen organisatie staat IT duidelijk in de memorandum of risk van de business en worden ontwikkelingen in een vroeg stadium over en weer besproken en gedeeld met elkaar. Bij de implementatie en uitrol van een risicovol IT-systeem dient zowel de security-manager als business-contactpersoon betrokken te worden om de beheersing van risico's te bespreken en maatregelen af te spreken met de andere twee partijen. Vervolgens kan de security-manager deze afstemming vastleggen en de afspraken te monitoren. De business kan het niet alleen, security kan het niet alleen."

"Omdat, zoals al eerder gezegd de meeste security-breaches zijn een direct gevolg van menselijk handelen is het daarom ook van essentieel belang om cybersecurity-bewustzijn meer te trainen. Het zal niet te voorkomen zijn dat er mensen zijn die klikken op kwaadaardige links, met als gevolg een Cryptolocker-infectie, maar training kan de kans hierop wel aanzienlijk verkleinen. Keep Security fun." raadt Tammy aan. Het is haar lijfspreuk, waarmee ze aan wil geven dat gebruikers en medewerkers er niet op zitten te wachten om de droge theorie die met security gepaard gaat tot zich te nemen, maar wel openstaan om op ludieke wijze te willen leren. "De awareness-sessies die ik organiseer vul ik met cartoons en rare plaatjes die op het netvlies van de medewerkers gebrand blijven staan. Ik deel lolly's uit met een belangrijke boodschap erop, zodat mensen er met elkaar over gaan praten. Dit zorgt dat de boodschap gedeeld wordt. Dit alles maakt de security-beleving meer persoonlijk en zijn de medewerkers beter betrokken waar nodig." Ze schrijft hier ook een blog over [2].

Female Touch

Omdat de ICT-wereld nog voornamelijk door mannen gedomineerd wordt, kon een vraag omtrent de andere inzichten of aanpak van een vrouw in de security niet uitblijven. "Ik maak geen verschil: 'There is no female touch here'. Er is in security geen apart 'vrouwelijk inzicht', het gaat om de personen en wat ze kunnen en doen. Je selecteert mensen omdat ze passen binnen het team en de kennis en vaardigheid van het hele team op het juiste niveau is of wordt gebracht. Gebruik de diversiteit van de mensen. Wij zijn verschillend in ons denken en doen, we hebben andere opvattingen. Hoe meer hoe beter! Zoek naar de juiste aanvulling voor het team. Passende security-kennis en -vaardigheden vormen slechts de helft van de nodige beoordeling. Als er een goede basis is, is de rest aan te leren op het werk. Ergo, selecteer niet op sekse of ras, maar vorm een heterogeen team van goede mensen. 'Bring smart people to the table'."

We vragen naar Tammy's beeld van het internet van vandaag, met alle regeldruk die er op encryptie ligt. Het is haar uitgangspunt dat het internet ontworpen is om informatie over de gehele wereld vrij te kunnen delen. "Hiermee komt privacy onder druk te staan. Het oplossen van deze problemen moet onze focus hebben en houden. Doe het slim, reageer snel en sluit je niet af." We hebben in het afgelopen uur Tammy leren kennen als een vrouw die van haar werk houdt. Zoveel zelfs dat ze het woord 'passie' gebruikt. Ze sluit dan ook af met de woorden "Ik voel me een gezegend mens".

Links

[1] Peter Steiner Cartoon: https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you're_a_dog

[2] Blog "It's all about the basics": https://www.venafi.com/blog/post/it-security-its-all-about-the-basics/

RISICO'S EN MAATREGELEN SOCIAL LOGIN

Gebruik wat je al hebt

Inloggen met een socialmedia-account is een manier om gebruikers laagdrempelig een website te laten gebruiken.

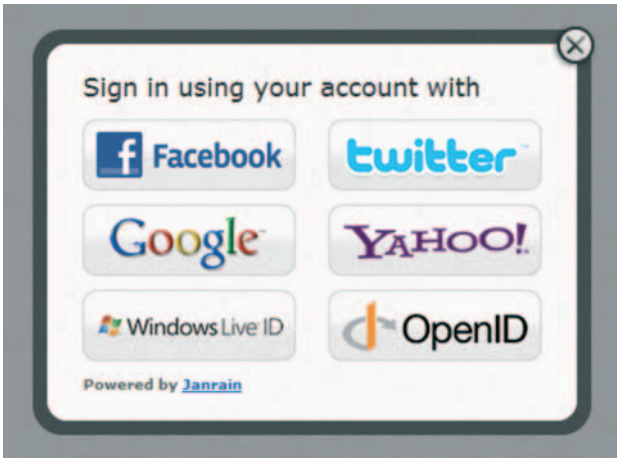
Traditioneel moet je om op een website iets te kunnen doen inloggen met een gebruikersnaam en een wachtwoord. Maar we kennen de knelpunten:

- Elke site een eigen account en een wachtwoord.
- Voor welke site gebruikte je nu welk account en welk wachtwoord?
- Hoe complex moet een wachtwoord zijn?
- Moet je een wachtwoord verversen? Of niet?
- Welk soort wachtwoord is sterk genoeg?
- Wachtwoorden kunnen uitlekken.
- Wachtwoordenbestanden van websites worden gelekt.

Genoeg redenen om eens na te denken over het alternatief van 'social login'. Daarmee maakt iemand om in te loggen op een site gebruik van een account dat hij al heeft. Bovendien hoeft hij dan geen wachtwoord te gebruiken, want met social login maak je gebruik van Single Sign-on. Maar er staat wel iets tegenover. Als eigenaar van een website ben je opeens afhankelijk van de betrouwbaarheid van een externe partij en als consument laat je de derde partij wel iets van je gedrag zien. Het is dus helemaal niet zo vanzelfsprekend om social login mogelijk te maken. Laten we de voor- en nadelen van social login maar eens stuk voor stuk nalopen.

Voordelen

- **Snelle registratie**
  Als je nog niet op een website bent geregistreerd, kun je je snel met een socialmedia-account aanmelden. De website en de identity-provider wisselen relevante profielinformatie uit. Waarschijnlijk moet je alleen wat contactinformatie op de website zelf opgeven, omdat die niet door je IdP wordt geleverd. Je moet wel bij je identity-provider aangeven dat een website de inlog mag gebruiken.



Voorbeeld inlogscherm

- **Snelle inlog**
  Inloggen met een socialmedia-account betekent vaak dat je met een enkele druk op een knop al bent ingelogd. De website en de identity-provider handelen alles onder water af. Het levert daarmee een aanzienlijk hoger gebruiksgemak op dan alweer een inloghandeling op een website.
- **SSO**
  Social login maakt gebruik van moderne protocollen als OAuth, waardoor iemand alleen bij de socialmedia-IdP hoeft in te loggen en vanuit die sessie meteen kan doorklikken. Dus geen wachtwoord meer en een snelle inlog.
- **Geen identiteitenbeheer**
  Websites hoeven zelf geen identiteiten van gebruikers van de website te beheren. Dat is een voordeel, want dergelijke

beheertaken zijn kostbaar en risicovol. De meeste datalekken ontstaan vanuit websites. Gezien de toenemende druk van wet- en regelgeving op het gebied van datalekken is dit een nuttige bonus.

- **Geen wachtwoordenbeheer**
  Als je social login toestaat, dan hebben de gebruikers SSO en hoef je dus zelf geen wachtwoorden te beheren en op te slaan. En wat je niet hebt kun je niet kwijtraken. Met name gezien de toenemende druk van de privacywetgeving is dat een niet te onderschatten voordeel.
- **Wachtwoord reset bij IdP**
  Aangezien mensen via hun IdP inloggen, moeten ze ook bij de IdP hun account en wachtwoord beheren. Dus het 'wachtwoord vergeten' probleem ligt nu bij de IdP.
- **Gratis (of vrijwel gratis) authenticatie**
  Een Identity- en Autheticatiedienst is een dure aangelegenheid. Door dat proces uit te besteden, kan flink worden bespaard op operationele kosten. En soms kan dat dus gewoon gratis.
- **Security**
  De grote IdP's hebben security in de regel goed geregeld, beter dan menig website dat zelf kan doen. Aangezien security ook een kostbare zaak is, levert social login zonder hoge kosten een hoog niveau van betrouwbaarheid op.

Nadelen

- **Identity Provider (IdP) kent het surf- en inloggedrag van de klanten**
  Het belangrijkste nadeel is dat de IdP weet waar iemand inlogt. Er wordt onder water immers een aantal berichten uitgewisseld, waarmee de Identity Provider dus weet bij welke website iemand inlogt. En dat betekent dat het gedrag in het profiel wordt opgeslagen (dit is dus onderdeel van het beruchte profiling). Dit levert een privacyprobleempje op.
- **Betrouwbaarheid van identiteiten**
  Socialmedia-identiteiten zijn lang niet altijd echte identiteiten. Mensen maken om diverse redenen gebruik van schuilnamen en nepprofielen. Een socialmedia-identiteit waarmee wordt ingelogd op een website is dus niet per definitie te vertrouwen.
- **Beschikbaarheid van dienst zonder garantie**
  Als iemand niet kan inloggen, dan kan die persoon geen gebruik maken van de diensten van de website. Het niet kunnen inloggen kan verschillende oorzaken hebben. De IdP kan technisch uit de lucht of niet bereikbaar zijn, of de IdP kan om besloten hebben om de account te blokkeren. Dat zullen we niet weten.
- **Diefstal ID compromitteert alle gekoppelde diensten**
  Als je social ID gecompromitteerd wordt, dan heb je een fors probleem. Alle diensten die dat ID vertrouwen, zijn dan min of meer vogelvrij. Daar is niets aan te doen, behalve om te proberen om het account heel snel te herstellen. Als er al geen fundamentele schade is aangericht.
- **Standaardattributen van IdP**
  Je kunt natuurlijk wel inloggen met een social ID, maar wat je eraan hebt is heel beperkt. Je bent ingelogd, maar verder niets. De waarde wordt hoger als de service provider ook de attributen die een IdP levert kan interpreteren en vertrouwen. Met name dat eerste is lastig. Hoe heten de attributen en welke waarden kunnen ze hebben. Zolang een service provider daar geen chocola van kan maken, is elke moderne vorm van autorisatie (ABAC) zinloos.
- **Geen ID-gegevens bij de service provider, vergt eigen 'CRM'**
  Als een klant zich registreert en inlogt met een social ID, dan heeft een service provider buiten de van de IdP ontvangen gegevens geen informatie over de klant. De service provider moet een eigen CRM-systeem inrichten en hopen dat alle relevante informatie door de klant wordt aangeleverd.
- **Geen Multifactor-authenticatie (MFA) afdwingbaar?**
  Voor sommige processen is het noodzakelijk om Multifactor-authenticatie af te dwingen om meer zekerheid over de betrouwbaarheid van een identiteit te krijgen. Niet elke IdP ondersteunt MFA en bovendien is er nog geen standaard om attributen over MFA uit te wisselen.

Voorbeeld apps via Twitter

André Koot is security consultant, gespecialiseerd op het gebied van digitale identiteiten en autorisatiebeheer. Hij is per e-mail bereikbaar via meneer@tken.net.

- **OAuth-sessie blijft open**
  Als iemand is ingelogd bij een IdP, dan kan vanaf die sessie elke andere Oauth-sessie worden gestart. Single Sign-on is mooi, maar een enorm risico.

"Veel logon credentials" en bron: "Braithwaite Wallets (Raptured)" door papodehomem via Flickr"

Maatregelen

Als we de voordelen op prijs stellen, kunnen we dan de nadelen wegnemen of in ieder geval beperken?

Privacy

Dit fenomeen is niet eenvoudig te beheersen. De rechtszaak van Max Schrems tegen Facebook maakt ook duidelijk dat deze materie door allerhande internationale wetten en regels complexer is dan alleen het feit dat een IdP kan gaan profilen. Er is ook geen eenvoudige oplossing voor. Wel zou overwogen kunnen worden om het profilen door een IdP te compliceren door als een service provider aan een consument de mogelijkheid te bieden om van verschillende social media accounts gebruik te maken. Als een consument onregelmatig switcht van identiteit, krijgt een IdP geen volledig beeld van het inloggedrag.

Betrouwbaarheid

Betrouwbaarheid van identiteiten kan op verschillende manieren worden verbeterd.

1. Te denken valt aan de volgende aspecten: een social media identiteit staat nooit op zich. Een dergelijk account is onderdeel van een sociaal netwerk en staat dus in relatie met andere identiteiten. Door de betrouwbaarheid van de identiteiten samen te beoordelen, kan een soort reputatiewaarde worden bepaald. Op die manier is de betrouwbaarheid van de identiteiten van LinkedIn betrekkelijk hoog in te schatten.
2. De waarde van een social media identiteit kan worden verhoogd door aanvullende verificaties. Die kosten geld, maar leveren een hogere mate van betrouwbaarheid op. Te denken valt aan een betaling voor een product of dienst, een afleverbewijs, of een visuele verificatie door een betrouwbare instantie.

Beschikbaarheid

Als een IdP inloggen niet mogelijk maakt, dan zou er een alternatieve inlogmogelijkheid geboden kunnen worden. Denk aan de oplossing die bij het privacyprobleem werd beschreven: meervoudige identiteiten. Maar technisch gezien kan ook distributie van inlogservers een bijdrage leveren.

Diefstal

Een service provider die zijn diensten heel waardevol vindt, kan een aanvullende authenticatie eisen, bijvoorbeeld in de vorm van een sms of een token met One Time Password (OTP). Nou wordt dat lastig als de smartphone waarop het ID is geactiveerd wordt gestolen. Als vervolgens vanaf die smartphone op een service wordt ingelogd en een sms ter bevestiging van de identiteit wordt opgevraagd, dan levert dat niet veel beveiliging op… Een consument die een smartphone kwijt is, moet in ieder geval zo snel mogelijk het apparaat laten blokkeren. En verder is het zaak om de meest gevoelige diensten niet te ontsluiten met alleen Oauth en om sessies tijdig te blokkeren.

Standaardattributen

Het gebruik maken van attributen is nog lang geen gemeengoed. Dat betekent dat er ook nog geen generieke attribuutstandaarden zijn. En dat hoeft ook niet, zolang er bilaterale afspraken tussen IdP's en service providers gemaakt kunnen worden.

CRM nodig

Ja, natuurlijk heeft elke service provider Customer Relation Management (CRM) nodig. Om producten en diensten te kunnen leveren heb je meer informatie nodig dan een account en e-mailadres. Die aanvullende informatie (adresgegevens, betaalgegevens) moet je hoe dan ook zelf beheren, dus een CRM is helemaal niet zo onlogisch.

Multi Factor Authenticatie

Dit klopt. Er is niet veel aan te doen, behalve gebruik te maken van die providers die het wel snappen en die kennis delen.

Sessie

Dit is natuurlijk niet echt een federatierisico: elke sessie op elke werkplek en elk apparaat lijdt aan hetzelfde euvel. Het enige wat werkt, is om sessies te laten verlopen en om bewustzijn bij de gebruikers te laten ontstaan.

Conclusie

Het lijkt erop dat we veel van de nadelen kunnen wegnemen, of verminderen met passende maatregelen. Het netto risico lijkt dan ook lager dan wat we op voorhand zouden vermoeden. Dat wil niet zeggen dat social login dan ook zomaar in te zetten is. Maar het enkel op grond van het feit dat de grote netwerken het niet zo nauw nemen met privacy negeren van de mogelijkheid is weer het andere uiterste. Gezien de ontwikkelingen op het gebied van privacybescherming, zou het wel eens heet zinvol kunnen zijn om de voors en tegens voor je eigen omgeving nog eens af te wegen.

DATA CENTRIC

It is some years since the Jericho Forum published its 'Commandments' on how to plan for a de-perimeterized future digital business environment. The most recent version 1.2 was published in May 2007. The conclusion of that document included the following words:

"De-perimeterization has happened, is happening, and is inevitable; central protection is decreasing in effectiveness: It will happen in your corporate lifetime. Therefore, you need to plan for it and should have a roadmap of how to get there."

Now in 2016 we see a world where nothing could be a more accurate description of what is now known as 'cyberspace', and the popular buzzword of the time is 'cybersecurity', meaning securing the digital business world against all types of cyber threats. Have we, as an industry, really developed a roadmap of how to deal with pervasive de-perimeterisation? The Attributer thinks not.

We have a tendency to get stuck with our methods of securing systems, with no real innovation to keep up with the innovations on the applications front. The mobile business world of smart phones and tablets, the deep service-oriented supply chains, and the Internet of Things are examples of how technological innovation has surged in terms of applications, but we are still tinkering around with the same old security technologies, trying to make them work in this totally altered world. Not surprisingly it isn't working very well. We still have a system-centric mind-set for securing 'the box' and 'the wire', whatever the box might now look like and despite the fact that in a cloud-based world the idea of a wire with identifiable endpoints is nonsense.

SABSA does have a roadmap for the future, although it has gained little traction so far. In 2010 a SABSA paper published at COSAC was entitled "SABSA Trust, Security and Risk Management in Cloud Computing" in which the basic concepts of data-centric security (as opposed to system-centric security) were set out. In 2012 this was followed by a full day workshop at COSAC called "Securing the IT Spring" in which the concepts of the future of security architecture were presented, including a mixture of system-centricity, data-centricity and people-centricity (anyone, any time, any place), together with the concept of a global network of trust brokerage to provide trusted execution platforms for remote processing in the cloud. These presentations also outlined how these concepts can be implemented using SABSA Business Attributes Profiles to build secure data wrappers called Assurance Policies.

Layered data encryption, data, source and destination authentication, together with key management, are the mechanisms for ensuring that only trusted platforms can be used to execute the applications to transform the data, securing both the mobile data and the transformations that can be performed on it, deep in the digital services supply chain. By layering the cryptography with different keys, different service providers can be used to carry out different operations on the data, before it is returned to the owner. This enables a deep digital supply chain with multiple layered service providers/suppliers. Many people have an impression that when they take a cloud solution it is with a single supplier, but as often as not it is just a portal with multiple services layered behind it. The technology alone is not sufficient to provide a secure solution – a network of trusted brokers and legal contracts is needed to secure the entire supply chain.

The SABSA Business Attributes Profile is the key tool for expressing the Assurance Policies that need to be bound tightly to the data as it travels in cyberspace. Further research and development is being applied to develop an interpretive language that can be used to both write and read these Assurance Policies in the form of metadata wrappers for the data itself. By using a machine-readable language to express the SABSA Business Attributes Profile, automation will be enabled. Only by this type of innovation shall we move on into using technologies that truly support modern cybersecurity.

The Attributer

‘PERFECT FORWARD SECRECY’ OP JOUW WEBSITE

Iedereen die op internet actief is, gebruikt elke dag wel een versleutelde netwerkverbinding (TLS, opvolger van SSL) en daar wil je als gebruiker eigenlijk niets van merken en moet goed beveiligd zijn. Doordat de technieken van afluisteren door geheime diensten zijn blootgelegd, is het aantal van TLS-verbindingen in hoog tempo gestegen en heeft de techniek een aantal verbeterpunten doorgevoerd. Blijkbaar zijn er veel mensen die niet willen dat ze worden afgeluisterd en is de techniek sterk aan het verbeteren.

In dit artikel ga ik dieper in op één specifieke beveiligingsinstelling die op de website zelf geconfigureerd moet worden. Dit noemen we ‘Perfect Forward Secrecy’. Het is tevens één van de belangrijkste configuraties op TLS-niveau om het onderscheppen van encryptiesleutels, waarmee ze de gegevens kunnen afluisteren, tegen te gaan. Deze sleutels worden gebruikt om de gegevens voor derden onleesbaar te maken en zijn cruciaal om de gegevens veilig over internet te versturen.

Wat is Perfect Forward Secrecy?

De sleutels waarmee de verbinding beveiligd is, worden sessiesleutels genoemd. Elke sessie is er een nieuwe sleuteluitwisseling en de sleutels zijn normaal gesproken van de sleutels uit het certificaat of van voorgaande sessiesleutels afgeleid. Met Perfect Forward Security (PFS) zorgt men ervoor dat sessiesleutels altijd geheim blijven, ook als er één van de sessiesleutels gestolen is. Met die gestolen sessiesleutel zijn dan alleen de gegevens van die ene sessie te achterhalen en voorgaande en latere sessies zijn niet met die sleutels leesbaar te maken. Er wordt geen gebruik gemaakt van afgeleide sleutels en elke sessiesleutel is opnieuw gegenereerd.
Met PFS heb je een veiligere verbinding en dat is voor gebruik met kritische bedrijfsgegevens een zeer welkome aanvulling om onderscheppen van gegevens tegen te gaan. Overheden, hackers en criminelen kunnen hierdoor minder eenvoudig de kritische bedrijfsgegevens achterhalen als zij een van de sleutels in bezit krijgen. Als overheden of criminelen bijvoorbeeld de onderschepte versleutelde gegevens voor langere tijd gaan opslaan (zoals inlichtingendiensten waarschijnlijk doen), kunnen ze er in de toekomst nog niet veel mee want de sleutels zijn nooit meer te achterhalen.
Bijna alle PFS-implementaties zijn op het Diffie-Hellman-sleuteluitwisselingsprotocol gebaseerd. Een protocol uit 1977 dat tot op de dag van vandaag nog veilig te noemen is. Mits je de juiste sleutellengtes en hash-algorithmes gebruikt of Elliptic Curve Cryptography (ECC) toepast.
Naast de bekende TLS(https)-versleuteling, wordt PFS ook gebruikt bij VPN (IPSec), SSH (Secure Shell) en OTR (Off-the-Record-chat-protocol). Al is het bij deze protocollen op verschillende manieren ingeregeld.

Welke ciphers zijn nodig

Om PFS op juiste manier in te stellen heb je een aantal mogelijkheden. De basis is om de sessiesleutels niet op RSA- of DSA-basis uit te wisselen maar op Elliptic Curve Cryptography (ECC). Zowel RSA, DSA als ECC zijn cryptografiestandaarden die op basis van asymmetrische sleutels werken. Grote voordeel van ECC zijn de kortere sleutels en hogere beveiliging. De kortere sleutels zijn interessant omdat het aan de serverkant dan minder performance kost om gegevens te versleutelen.
Hiervoor hebben webserver-applicaties de cipher ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) en DHE (Diffie-Hellman Ephemeral) opgenomen. Ephemeral in het protocol zorgt ervoor dat de sleutels alleen bij gebruik bekend zijn en daarna verwijderd worden. Met deze ciphers is PFS goed en veilig in te regelen met als voorwaarde dat je de sleutellengte hoog genoeg instelt. Op het moment van schrijven is 2048 bits hoog genoeg.
Elliptic Curve (o.a. ECDHE) is een relatief nieuw algoritme en gebruikt kortere sleutels dan DHE. Al heeft Elliptic Curve kortere sleutels, het is op dit moment één van de veiligste versleutelalgoritmes.
Ook de volgorde van protocollen kiezen is belangrijk. Er wordt door de cliëntzijde uitgegaan van de volgorde die de server aanbiedt. Zet de meest veilige en snelste protocollen vooraan in de lijst, zodat de cliëntzijde deze als eerste oppakt en daarmee de verbinding maakt. Cliëntapplicaties die niet met de eerste overweg kunnen, zullen een volgende oppakken waardoor ze wel een veilige verbinding maken maar op een iets lager niveau. Zet ECDHE als eerste, DHE als tweede eventueel minder veilige daarna.
Testen die aantonen hoe veilig de webserver uiteindelijk is, kun je op internet uitvoeren. De meeste gebruikte site om dit te achterhalen is http://www.ssllabs.com. Op die site staat tevens de uitleg hoe je moet testen en wat alle gevonden waarden betekenen.

Conclusie

'Perfect Forward Secrecy' is cruciaal om de versleutelde verbindingen veilig te maken. Technisch is het misschien moeizaam en ingewikkeld om versleutelde verbindingen af te luisteren, maar met PFS bouw je een zekerheid in dat het niet meer kan. Wees er wel bewust van dat er browsers zijn die er niet mee om kunnen gaan. Dit zal in de praktijk neerkomen op ongeveer twee tot drie procent van de gebruikers. Er zijn oudere browsers (bijvoorbeeld IE8 op Windows XP) die er niet mee overweg kunnen. Indien je PFS op server-niveau afdwingt, ga je die gebruikers verliezen.

Specifieke Configuraties

Diverse webserver applicaties, zoals Apache en nginx, ondersteunen PFS wel standaard, maar het is niet in de default installatie meegenomen. Hiervoor dien je een aantal aanpassingen door te voeren op de server configuratie zelf. Indien je al een TLS-configuratie hebt draaien is niet de meest ingewikkelde configuratie, maar het heeft wel de nodige impact op de gebruikers.

A. Apache

Voor Apache kun je de volgende SSL-configuratie opnemen. Dit kan voor gehele server (SSL.conf) uitvoeren worden of per website (virtualhost) en staat meestal in de directory \etc\apache2\.

```
SSLProtocol all -SSLv2 -SSLv3
SSLHonorCipherOrder on
SSLCipherSuite "EECDH+ECDSA+AESGCM
EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384
EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384
EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH
EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK
!SRP !DSS !RC4"
```

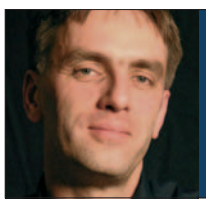
Daarna kun je de webserver opnieuw opstarten en wordt PFS afgedwongen.

B. Nginx

Voor nginx kun je de volgende SSL-configuratie opnemen. De configuratie bestanden (virtual host file) zijn meestal te vinden in de directory /etc/nginx.

```
ssl_protocols TLSv1.2 TLSv1.1 TLSv1;
ssl_prefer_server_ciphers on;
ssl_ciphers "EECDH+ECDSA+AESGCM
EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384
EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384
EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH
EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK
!SRP !DSS !RC4";
```

Daarna kun je de webserver opnieuw opstarten en wordt PFS afgedwongen.



Harld Röling is werkzaam bij de afdeling CISO van een Nederlandse bank en heeft zich vanaf 1999 gespecialiseerd in de technische en organisatorische aspecten van asymmetrisch Key Management en PKI. Daarnaast is Harld vrijwilliger bij Bits of Freedom bij Privacy Cafe's en de Toolbox. Harld is bereikbaar op e-mailadres harld.roling@hroling.nl.

SECURITY-TRAININGEN VIA GROUPON

Te mooi om waar te zijn?

Als security-professional ben ik altijd op zoek naar manieren om mijn kennis uit te breiden. Certificaties zijn een erkend middel in de IT-industrie en dus goed voor je carrière. Echter, de trainingkosten kunnen een niet te verwaarlozen factor zijn als deze niet door de werkgever worden vergoed. Daarom ben ik altijd geïnteresseerd in betaalbare alternatieven, en laatst kwam ik een aanbieding tegen op de Groupon-website: 8 security-certificatie-trainingen voor slechts € 40,- in plaats van normaal € 2541,-.

Te mooi om waar te zijn?

Dit is de link naar de aanbieding: https://www.groupon.nl/deals/career-match-1489. LET OP: als u dit leest kan de aanbieding al verlopen zijn, maar hou dan een oogje in het zeil voor soortgelijke aanbiedingen.

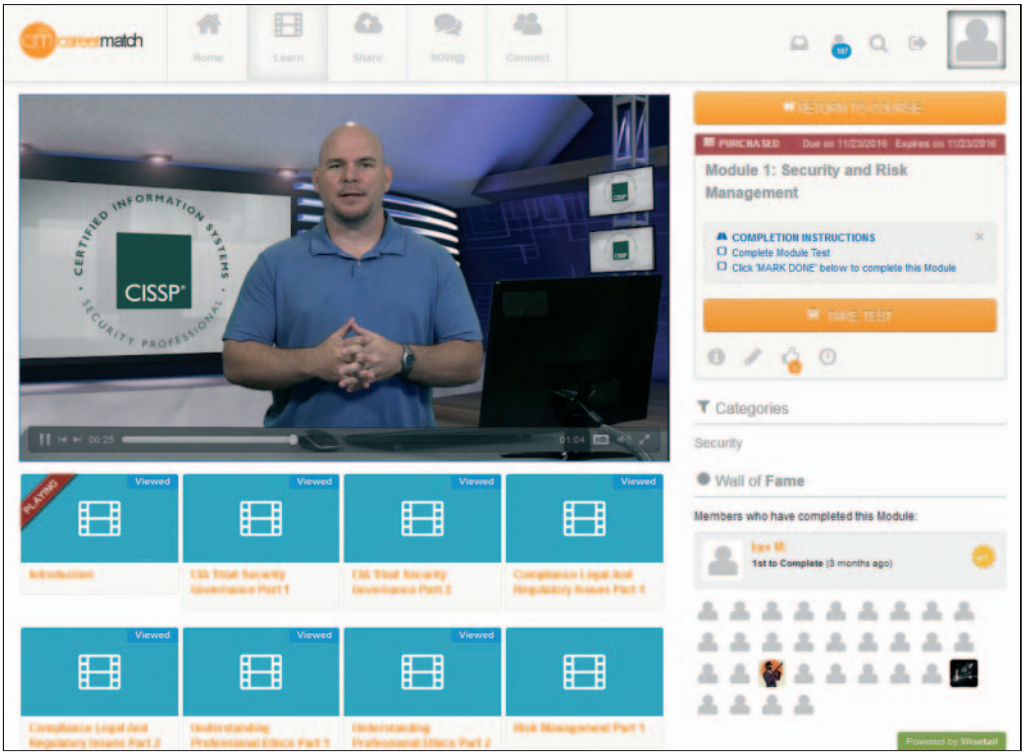
Deze trainingsbundel wordt aangeboden door het Engelse bedrijf Career Match en bevat de volgende (Engelstalige) videotrainingen:

- Certified Information Systems Security Professional (CISSP) (*)
- CompTIA SY0-401 or JK0-018: Security+ (8h27)
- Cisco 640-554: CCNA Security - Implementing Cisco IOS Network Security (7h55)
- Certified Information Systems Auditor (CISA) (12h48)
- Certified Information Security Manager (CISM) (12h38)
- Computer Hacking Forensic Investigator (CHFI) (18h43)
- Certified Ethical Hacker (CEH) (12h28)
- CompTIA CAS-001: Advanced Security Practitioner (CASP) (19h00)

(*): De aangeboden CISSP-training gaat over de nieuwste versie van deze certificatie.

Na aanschaf krijg je toegang tot een webbased portal en kun je beginnen met de training. Voor elke certificatie zijn er een aantal modules, die elk weer een aantal video's bevatten. Je krijgt na aanschaf één jaar toegang tot de portal.

Na het bekijken van alle video's van een module kun je een test doen om je opgedane kennis te toetsen. Na een succesvolle test kan de module worden gemarkeerd als "Done" en kun je verder gaan met de andere modules. Maar je kunt ook modules en video's in willekeurige volgorde doorlopen, waarmee je op één specifiek onderwerp kunt focussen zonder noodzaak eerst voorgaande modules door te lopen.
Per certificatie zijn er andere trainers beschikbaar om je door de stof te leiden, en je alle zaken bij te brengen die je nodig hebt om het betreffende examen met goed gevolg te kunnen afleggen. De verschillende trainers zijn goed gekwalificeerd, hebben zelf een aantal relevante certificeringen en een aantal jaren ervaring in de security-industrie, waardoor het zeker de moeite waard is om naar ze te luisteren. De praktijkvoorbeelden, gebaseerd op hun eigen ervaring, geven



Screenshot portal: CISSP, Module 1 – Security & Risk Management

je waardevolle inzichten hoe theorie en praktijk voor de betreffende certificatie samenhangen.
In aanvulling op de video trainingen zijn er per certificatie nog extra materialen, zoals:

- Flashcards (+/- 50 vragen over belangrijke zaken, uiteraard met antwoorden)
- Test Engine (20 vragen die binnen 20 minuten beantwoord moeten worden)
- Final Test (tussen de 50 en 90 vragen als examentraining, maar pas toegankelijk na het doorlopen van alle modules)
- Toegang tot community forums (Security, CompTIA, Cisco) waar deelnemers actief kunnen discussiëren over certificatieonderwerpen.

Als toegift bevatten de CISSP- en CISA-trainingen ook nog aantekeningen in de vorm van ongeveer 500 slides, die je als "cheat sheets" kunt gebruiken tijdens het leren.

In mijn perceptie zijn deze videotrainingen een aanvulling op de officiële cursusboeken, net zoals de reguliere certificatietrainingen. Ze bieden een goed overzicht van alle termen en concepten die je moet beheersen om het examen met goed gevolg af te kunnen leggen. De inzichten en ervaringen van de trainers helpen je om de moeilijkere zaken goed te begrijpen. Echter zul je naast het volgen van de video's ook nog zelf moeten studeren. Zelf ben ik momenteel met CISSP en CEH bezig, en ik geloof dat het bestuderen van de officiële boeken nodig blijft, niet alleen om het examen te kunnen halen, maar ook om de kennis en "mindset" van de betreffende certificatie goed te begrijpen.

Tot slot: ik heb geen aandelen in Groupon of in Career Match. Middels dit artikel wil ik slechts de lezers wijzen op dit soort mogelijkheden om hun carrière een stap verder te brengen.

Guillaume Dupont is security consultant bij Capgemini. Hij is vooral bezig met Security Information & Event Management (SIEM) en Threat Intelligence. Hij is bereikbaar via guillaume.dupont@capgemini.com.

VERSLAG SECURITY CAFÉ

EEN SERIEUZE STAP

Meldplicht Datalekken

De Meldplicht Datalekken Telecom (autoriteit ACM) en de Meldplicht Datalekken (autoriteit CBP) wordt per 1 januari 2016 centraal geregistreerd bij een nieuwe autoriteit, de Autoriteit Persoonsgegevens (AP). Afgelopen zomer werd door de 1e en 2e Kamer de Wet Meldplicht Datalekken bekrachtigd met de ingangsdatum van 1 januari 2016. Hiermee anticipeert Nederland op de nieuwe EU-privacywetgeving. De Meldplicht Datalekken – als aanvulling op bestaande privacywetgeving – is tweeledig; melding van een datalek bij de AP binnen twee werkdagen ("onverwijld") en melding van een datalek aan gedupeerden.

Een app met toegang tot e-mail en telefoongesprekken is een datalek

De nieuwe meldplicht geldt overigens alleen voor bedrijven en niet voor privépersonen. Om iedereen op dezelfde pagina te hebben, moet ook opgemerkt worden dat het huidige Safe Harbour-convenant tussen EU en VS is opgeschort. Alle reden voor professionals om het daar eens over te hebben tijdens een Security Cafébijeenkomst.
Het Security Café 'Meldplicht Datalekken' werd 24 nov 2015 gehouden bij Schuberg Philis als gastheer, panelleden Ralph Moonen (ITSX), Ton van Ginkel (ex CISO T-Mobile) en mr. Sergej Katus (Privacy Management Partners). Aan de hand van 5 praktische cases werd interactief gediscussieerd over de nieuwe wet meldplicht datalekken.

Case 1: Leverancier met datalek van (deels) Nederlandse persoonsgegevens in US

Stel dat uw leverancier c.q. bewerker van data in het buitenland bij u als verantwoordelijke meldt dat er een datalek is met persoonsgegevens. Wat moet je doen? Allereerst moet je vaststellen dat het datalek om persoonsgegevens gaat. Indien dit het geval is, moet je dit datalek binnen 2 werkdagen melden bij de Autoriteit Persoonsgegevens voor zover het gaat om een voldoende ernstige security breach. Vervolgens moet je onderzoeken of er mogelijk nadelige gevolgen zijn voor de gedupeerden. Zo ja, dan heb je een tweede meldplicht naar de gedupeerden. Indien je niet specifiek weet wie de gedupeerden zijn, dan moet je alle mogelijke slachtoffers informeren.
Je blijft verantwoordelijk voor het melden van een datalek, ook al heb je contractueel en juridisch alles dichtgetimmerd met je bewerker, bijvoorbeeld met een bewerkersovereenkomst, assurance rapportage, geheimhoudingsverklaring, dataportabiliteit geregeld en bewaartermijnen vastgesteld.
Welke stappen je doorloopt in een geval van een datalek, heeft een organisatie hopelijk vooraf al uitgedacht en vastgelegd in een draaiboek datalekken en security-incidenten.
Ton van Ginkel: "Op het moment van een datalek moet alles kloppen; zorg vooraf voor een incident management plan."
Sergej Katus: "Let erop dat de wet niet per se tot 'bewerkersovereenkomsten' verplicht. Bewerkerschap ontstaat bijvoorbeeld bij inkoop of uitbesteding of de oprichting van een gezamenlijk dienstenplatform. Wél verplicht de wet vervolgens tot het organiseren van regie en toezicht – met name op het gebied van informatieveiligheid. Daaronder horen ook de afspraken over datalekken."

Case 2: Mobiele telefoon voor zakelijk en privégebruik met apps die met "toestemming" toegang krijgen tot bedrijfsinformatie zoals contacten en e-mails

Met zakelijke apparaten, Bring Your Own Devices (BYOD) en 'choose your own devices' (CYOD), is het corporate beheer van alle apparaten met een MDM-tool niet zo eenvoudig meer. Zakelijk en privégebruik van de meeste mobiele apparaten is in de praktijk niet gescheiden, wat kan leiden tot complicaties. Met BYOD geef je bijvoorbeeld niet zomaar de rechten aan je opdrachtgever om je telefoon te wissen op afstand om je bedrijfse-mail te kunnen lezen. Zo is er ook de wildgroei van dataopslag van zakelijke documenten in privéomgevingen zoals de laptop/iPad thuis, Dropbox, iCloud, Google Drive om nog maar te zwijgen over WeTransfer en Prezi. Kortom, zakelijk en privé lopen in de praktijk op één apparaat door elkaar heen. Zakelijk beleid staat meestal toe om de zakelijke mobiele telefoon en/of e-mail ook beperkt privé te gebruiken. Echter dit is niet zonder risico. E-mail is in de praktijk een waardevolle bron van actuele en vertrouwelijke bedrijfsinformatie. Het geeft inzicht

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

Als wachtwoorden ontsleuteld kunnen worden, dan moeten de gedupeerden geïnformeerd worden

in contactgegevens en contactmomenten met klanten of leveranciers. Het is voor gebruikers ook eenvoudig om een app via de app-store te downloaden en die app alle toestemming geven tot informatie op de telefoon. De leverancier van deze app – die zeker niet voorkomt in de contractenadministratie van het bedrijf – krijgt zo inzicht in alle privé- en bedrijfsgegevens die benaderbaar zijn op dit apparaat. Deze situatie komt in veel gevallen voor, maar zal nog door geen enkel bedrijf gezien worden als een datalek. Mogelijk dat het bestempeld wordt als "geaccepteerd risico." Gedupeerden hebben er nu misschien nog geen weet en/of last van. Toch zie je hier en daar al wat experimenten om zakelijke telefoon schizofreen in te richten om zo scheiding af te dwingen tussen zakelijk en privé om de risico's beheersbaar te maken.
Sergej Katus: "Zelfs als beleid zakelijk en privégebruik van mobiel toestaat, dan is een app met toegang tot e-mail en telefoongesprekken nog steeds een datalek."

Case 3: Onderleverancier met een datalek van persoonsgegevens in de keten

Stel u heeft een leverancier die een website met persoonsgegevens voor u onderhoudt als "bewerker". Bij die leverancier wordt een dagelijkse een back-up gemaakt met een voor u onbekende cloudservice. Nu wordt deze cloudservice "gehackt" met een gebruikersnaam en wachtwoord, waardoor al uw persoonsgegevens op straat komen te liggen doordat de back-up van de website-database wordt gedownload. Hoe komt u hier achter anders dan via een krantenartikel in de Telegraaf? Heeft u een passend beveiligingsniveau geïmplementeerd als verantwoordelijke? Zo niet, dan is de boete voor u onaangenaam hoog, namelijk 810.000 euro of – als dat nog te weinig effect heeft – mogelijk een bedrag tot 10% van de jaaromzet.
Wat moet u doen om dit passend beveiligingsniveau af te dwingen bij de bewerker? Een ISAE 3402 (financieel) of ISO 27001 (algemeen) verklaring van de leveranciers geeft al wat basisgaranties afhankelijk van de scope van het certificaat. Als dit ontbreekt, dient u zelf garanties te definiëren middels een "right to audit". Minimaal stelt u de nieuwe eis om bij nieuwe contracten, contractverlening en/of vernieuwing dat datalekken in de keten binnen twee dagen aan u als verantwoordelijke wordt gemeld.
Sergej Katus: "De verantwoordelijke maakt melding van een datalek bij AP en informeert de gedupeerden als er een redelijke kans is op nadelige gevolgen."

Case 4: Website blijkt na testen een potentieel lek te bevatten, maar persoonsgegevens zijn beperkt tot e-mailadressen en versleutelde wachtwoorden

SQL-injection of Cross Site Scripting zijn onderdeel van de TOP-10 kwetsbaarheden van websites, waardoor hackers onbedoeld gegevens kunnen inzien en/of veranderen. Nu heeft elke website wel toegangsrechten nodig, maar dat is vaak ingericht met een authenticatie service (zoals SAML). Wachtwoorden komen niet meer voor in de applicatie zelf. Echter, er zijn nog vele websites die wachtwoorden onversleuteld opslaan in een database. Beheerders en hackers die deze informatie weten te achterhalen, kunnen hier misbruik van maken. Zo werd in 2012 bekend dat de website van Baby-Dump gehackt was, met gebruikers van KPN die hetzelfde e-mail en wachtwoord hadden gebruikt bij andere onlinediensten. Toegang tot wachtwoorden die mogelijk heeft plaatsgevonden, is volgens AP voldoende om gedupeerden te informeren. Zorg ervoor dat u in ieder geval in kaart heeft welke persoonsgegevens in welke website of applicatie voorkomen.
Ton van Ginkel: "Een gestolen laptop met versleutelde persoonsgegevens is een datalek dat je moet wel melden bij AP, maar je hoeft geen actie te nemen omdat de maatregel "versleuteling" al genomen is."
Ralph Moonen: "Als er een kans bestaat dat versleutelde wachtwoorden toch ontsleuteld kunnen worden, dan moeten de gedupeerden geïnformeerd worden."

Case 5: Datawarehouse met opgebouwd klantprofiel over verschillende kanalen dat zich niet heeft aangemeld bij het CBP

Het correleren van data geeft u nieuwe inzichten waardoor u de klant beter van dienst kunt zijn. Uw bezoek aan websites, uw surfgedrag, uw leeftijd, uw gezinssamenstelling, uw bank, uw adres, uw auto, uw telefoon, uw radio en tv, uw gezondheid, uw hobby's; alles wat we over u weten is straks geld waard. Met de opgebouwde klantprofielen weten ze steeds beter in te schatten wat en wanneer ik wil kopen. Big data heeft de toekomst. Echter, hoe zit dat met de privacy?
Als eerste vraag je toestemming aan je klant om persoonsgegevens te mogen correleren met andere databronnen zodat we u nog beter van dienst kunnen zijn (doelbinding). Met Google heb ik het idee dat als ik een website bezoek of een e-mail van een specifiek bedrijf ontvang, dat ik daarna ook online advertenties zie die gekoppeld zijn aan dit bedrijf. De kans is namelijk groot dat ik daar iets wil kopen. Maar hoelang mag je zo'n klantprofiel bewaren? En wat als ik als klant opvraag wat er over mij is vastgelegd, kan ik als bedrijf die vraag redelijkerwijs aan de klant beantwoorden? Wat gebeurt er als alle data in verkeerde handen valt? Die hackers in diep Rusland kun je niet vragen of ze jouw klantprofiel willen verwijderen of willen stoppen met het verhandelen van illegale data. Zorg ervoor dat uw systemen een Privacy Impact Analyse hebben ondergaan en passende maatregelen zijn geïmplementeerd.
Sergej Katus: "Aanmelden van systemen met persoonsgegevens wordt in komende wetgeving vervangen door een documentatieplicht."

Tot slot

Vergeet natuurlijk niet uw organisatie en uw leveranciers te trainen in het herkennen van een datalek. Want zonder melding van een datalek, gaat dit incident-en-response-proces naar de Autoriteit Persoonsgegevens nooit werken.

Privacy heeft informatiebeveiliging nodig als steunpilaar. Met de Wetgeving Meldplicht Datalekken is dit een onderwerp voor de boardroom geworden en daarmee een katalysator voor informatiebeveiliging, omdat privacy vraagt om passende beveiligingsmaatregelen.

De hoogte van de boete als je niet binnen twee dagen meldt bij de AP is maximaal 500.000 euro. Daar komt nog eens maximaal 500 duizend euro boete bij als je verzaakt om gedupeerden te informeren. Dat is samen één miljoen euro. Mocht vervolgens blijken dat er data was gelekt waarmee de organisatie om andere redenen fundamenteel de privacy schond, komen boetes in beeld van 810.000 euro of tien procent van de (wereldwijde) jaaromzet. Ondertussen lijdt de organisatie waarschijnlijk al grote reputatieschade, waar nog een risico op schadeclaims bij komt. De privacywetgeving geeft iedereen het recht op schadevergoeding.
De AP kan bij kennelijke opzet of ernstige nalatigheid onmiddellijk overgaan tot het uitdelen van een boete. Nalatigheid blijkt uit veruit ondermaats beleid op het gebied van privacy- en informatiebeveiliging of het geheel ontbreken daarvan. Informatiebeveiliging op basis van een standaard als de ISO27000-serie is hét fundament van deugdelijk privacy management en dus compliance. Als bestuurders over de volle breedte van de controls uit de standaard het goed doen (good governance / MVO met data), dan kan de organisatie met vertrouwen rekenschap afleggen als er toch sprake was van een datalek en volgens de regelen der wet keurig bij de AP en betrokkenen melden.

Kortom, met de komst van deze wetgeving wordt een serieuze stap in de goede richting gezet, waarbij privacy en informatiebeveiliging hand in hand verder gaan.

VERSLAG CISO 8

UAV'S EN IOT

Op 9 december sprak één van de genomineerden voor de Joop Bautz Award 2015 met ons over zijn master-thesis. Daarna ging het over de veiligheid van het Internet der dingen (IoT). En behoren die onbemande vliegende dingen eigenlijk ook niet tot het IoT? Het is nuttig om tijdig aandacht te vragen voor veiligheidsaspecten van nieuwe technologieën. Zoals steeds is het ook nu weer de vraag of het al niet te laat is. Loopt het bewustzijn voor risico's bij nieuwe ontwikkelingen ook hier weer achter de praktijk aan en wordt beveiliging pas aangepakt als er ongelukken zijn gebeurd?

De titel die Nils Rodday aan zijn master-thesis (Universiteit Twente) meegaf spreekt al direct aan door de actualiteit van het onderwerp:

Exploring security vulnerabilities of unmanned aerial vehicles

Nils Rodday

Nils Rodday deed verslag over zijn onderzoek naar zwakke kanten van de beveiliging van onbemande luchtvoertuigen oftewel Unmanned Aerial Vehicles. In dat onderzoek beperkte hij zich tot het professionele gebruik ervan, consumenten drones bleven dus buiten beschouwing. Overigens is er een grote verscheidenheid aan UAV's waarbij de mate van intelligentie een van de bepalende factoren is. Nils vertelde over een Europees voorstel voor regels waarbij drie klassen worden onderscheiden. Nederland implementeert een versie die drie klassen kent in de 'open categorie'. Nils uitgangspunt is de gedachte dat van professionele UAV's, gezien hun toepassingsmogelijkheden, verwacht mag worden dat veiligheid een belangrijk thema is. Zijn thesis laat zien dat dit niet het geval is.

Het aanvallen van UAV's kan bijvoorbeeld gebeuren door er met deeltjes op te schieten zodat de communicatie uitvalt en het beheer onmogelijk wordt. Nils heeft voor zijn thesis een poging gedaan het beheer over te nemen van een door een leverancier beschikbaar gestelde UAV. Hij beschreef hoe hij daarbij te werk is gegaan en hoe dat tot een succes leidde. Het lukte hem het beheer over de UAV over te nemen. De leverancier van de UAV werd door Nils keurig voorzien van aanbevelingen om één en ander te verbeteren maar tot een aanpassing van de beveiliging kwam het nog niet. De bekende redenering van de leverancier was dat de klanten weinig bewustzijn vertonen voor de mogelijkheid dat de controle over hun UAV wordt overgenomen door een onbekende derde.

Een discussie over beveiligingsaspecten van IoT

Jan-Jan Lowijs

Jan-Jan Lowijs, privacy- en security-adviseur bij Deloitte Risk Services B.V. nam ons mee naar de wereld van de IoT. Van belang daarbij is het onderscheid tussen sensoren en actuatoren. De eerste soort meet fysieke zaken in de omgeving (beeld, geluid, temperatuur e.d.) en zet die gegevens om in bits. De tweede soort zet bits om in fysieke actie (open-dicht, aan-uit e.d.). Door de mogelijkheden die internet biedt is het nu mogelijk apparaten te voorzien van sensoren en actuatoren en deze te verbinden met sturingsmiddelen op afstand. De kosten van dataopslag zijn inmiddels zo laag dat op grote schaal informatie kan worden opgeslagen. Daarnaast zijn ook de kosten van communicatiechips laag en weten wij via business-analytics wat er allemaal mogelijk is met informatie. Kortom, niets staat het onderling verbinden van apparaten meer in de weg. Er worden dan ook voorspellingen gedaan over enorme mogelijkheden en waardetoevoeging die ons staat te wachten door de toepassing van IoT.

Te verwachten problemen liggen op het gebied van de privacy en de onvoorziene gevolgen van het beschikbaar komen van veel nieuwe data. Gaat een verzekeraar conclusies trekken uit gemeten gedrag van een klant? Of gaat een werkgever gedrag meten? Of wordt een werknemer door de gedachte dat er al automatisch gemeten wordt minder opletten? En dan is er de gebruikte software. Kan een patch worden uitgevoerd als blijkt dat de software een mankement bevat? Ook is er een gevaar van function creep, het verschijnsel dat data wordt verzameld die niet vooraf is afgesproken of wordt gebruikt voor niet vooraf besproken doelen. Kortom, er is een interessante ontwikkeling gaande met nog veel onbeantwoorde vragen.

Discussie

De discussie begon met de belangen. Voor wie moet het gebruik van IoT veilig zijn? De aanleiding was eigenlijk de door Jan-Jan genoemde waterval als metafoor van de levenscyclus van een product. Het inbouwen van veiligheid zou al in de ontwerpfase moeten beginnen. Maar wie heeft dan al belang bij veiligheid? Er dienen nu eenmaal eerst incidenten te zijn alvorens een put wordt gedempt.

Het inbouwen van veiligheid zou al in de ontwerpfase moeten beginnen. Maar wie heeft dan al belang bij veiligheid?

De ervaring van Nils is daarom niet hoopgevend. De leverancier van de door hem 'gekraakte' UAV heeft nog niets gedaan met zijn aanbevelingen. Dat komt in een volgende release aan de orde. Ja, dat hoorden wij al in de jaren 1980 toen Prof. Dr. I.S. Herschberg zijn studenten liet aantonen dat er 'gaten' in de besturingssoftware van IBM zaten. Inmiddels weten wij beter, patchen is tegenwoordig een wekelijks terugkerende actie.

De mate waarin wij wakker liggen van privacyaspecten werd in de discussie door Jan-Jan geïllustreerd met de resultaten van een onderzoek. Slechts 25% is een privacy-fundamentalist, dus iemand die steeds principieel privacy aan de orde stelt als belangrijk thema. 60% daarentegen is een pragmaticus op het gebied van de privacy en laat het van de omstandigheden afhangen of privacy een issue is of niet. De overige 15% is nihilistisch op dit punt en windt zich niet op over privacyaspecten.

Een teer punt in IoT is het feit dat de consument niet kan zien of er in of aan het aangeschafte apparaat een sensor en/of actuator zit. En als dat zo mocht zijn, welke software bestuurt dan de acties daarvan? In de fysieke wereld kunnen wij meestal nog wel vaststellen of een veiligheidsvoorziening aanwezig is of niet. Alhoewel dat bij een airbag bijvoorbeeld ook niet meer is dan het plaatje met de aanduiding ervan.

Er zal dus veel vertrouwen moeten worden gegeven als het IoT de vlucht gaat nemen die ons nu wordt beloofd.

Cees Coumou is sinds medio 2003 gepensioneerd als senior EDP Audit manager bij KPMG. Sindsdien is hij onafhankelijk adviseur en docent aan de IT-Audit Master van de Vrije Universiteit, de opleiding Master of IT auditing van de Universiteit van Amsterdam. Zijn werk op het gebied van organisatieadvisering betrof de laatste decennia met name onderwerpen als risicomanagement, continuïteitsmanagement en informatiebeveiliging. Tussen 2005 en 2012 redigeerde hij voor PvIB 8 boeken over trends in IT-beveiliging op basis van gesprekken met vele verschillende professionals.Hij is bereikbaar via cees.coumou@planet.nl.

NOMINATIES VOOR ARTIKEL VAN HET JAAR 2015

Wederom looft het PvIB dit jaar prijzen uit voor het artikel van het jaar. Er worden drie prijzen uitgereikt, waarbij de eerste prijs een waarde heeft van vijfhonderd euro. De meest belangrijke reden om een prijs uit te reiken aan onze auteurs is om waardering uit te spreken en ze te bedanken voor de interessante artikelen die ze ons bezorgen. Ook willen we zo auteurs een extra zetje geven om toch dat artikel te schrijven waar ze al langer over denken…

Het doet ons als redactie goed wanneer we terugkijken op een jaar waarin er verschillende nieuwe auteurs de stap genomen hebben te schrijven in het lijfblad van het PvIB.

De jury is samengesteld uit drie gekozen vertegenwoordigers uit de leden. De redactie heeft een voorselectie gemaakt van tien artikelen, waarvan er twee in twee delen zijn verschenen. Dit jaar heeft de jury dus weer flink wat leeswerk. De jury kiest uit de genomineerden drie winnaars en onderbouwt hun keuze in een juryrapport. De jury bestaat dit jaar uit de volgende leden:

- **Renato Kuiper van VKA**
- **Ellen Wesselingh van de Haagse Hogeschool**
- **Jurgen van der Vlugt van Maverisk**

Vaste rubrieken en artikelen van redactieleden en juryleden dingen niet mee. Uitreiking van de prijzen vlak voor de aanvang van het programma van de bijeenkomst op 19 april a.s., na de algemene ledenvergadering.

Genomineerde artikelen (op chronologische volgorde):

#	Titel	Pag.	Auteur
IB1	Privacy, ondernemers en providers	4	Niamat, R.
IB1&2	Veiliger met voorkennis (tweedelig)	12&12	Molen, H.J. van der
IB3	Verliefd op onveiligheid	10	Luiijf, E.
IB4	Detectie en risicoclassificatie van typosquatting	4	Broenink, G. en Schotanus, H.
IB4&6	Advanced Business Impact Analysis (tweedelig)	16&10	Janec, M. en Verweij, E.
IB5	CSIRT maturity kit	4	Hamer, M. de en Stikvoort, D.
IB5	Cybersecurity in de boardroom	10	Bobbert, Y.
IB6	Information Security Officer: spelen met invloed	16	Baaten, M.
IB7	Cloud-mythes: Kloppen ze wel?	4	Niamat, R.
IB8	Extreme Weather Events	12	Prins, J.F.

Tom Bakker | Bart van Staveren | Maarten Hartsuijker

Achter Het Nieuws

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

Backdoors in de firewalls van Juniper die er waarschijnlijk al drie jaar zitten. Zou dat een op zichzelf staand incident zijn alleen bij Juniper? Wat zou hier achter kunnen zitten en waar moeten risk-/security-managers nu rekening mee houden? Onze redacteuren geven hun visie.

Bart van Staveren

De speculatie over wie de backdoors bij Juniper gemaakt hebben, is direct gestart. Zowel de NSA als China worden genoemd als kandidaten. Als dit ook inderdaad de auteurs zijn, is de kans groot dat ook andere firewall-leveranciers backdoors in hun software hebben. Het is dus van groot belang om er bij deze leveranciers op aan te dringen ook hun software te controleren op de aanwezigheid van backdoors. Één van de twee backdoors bij Juniper is een in de code opgenomen wachtwoord.
Voor wie weet waar dit in de code zit, is het na de publicatie door Juniper eenvoudig om dit wachtwoord te achterhalen en te gebruiken. Hiermee is er een actueel risico voor alle gebruikers van de Juniper-firewall. De uitgebrachte patches moeten dan ook met voorrang geïnstalleerd worden.
Uit deze case blijkt maar eens weer dat er niet gewenste risico's verbonden zijn aan de wens van overheden toegang te hebben tot versleutelde data zonder dat de eigenaar van die data daarvan op de hoogte is. Misbruik door een echte kwaadwillende wordt wel erg gemakkelijk gemaakt met een in de code opgenomen wachtwoord. De discussie over wat geheime diensten wel en niet mogen zal in 2016 zeker verder gevoerd worden.

Maarten Hartsuijker

Waren het de Amerikanen, de Chinezen, of misschien de Russen? Wie het weet mag het zeggen, maar vermoedelijk kunnen we lang debatteren over welke spionagedienst er achter de Juniper-backdoor zit. Makkelijker is het om lering te trekken uit dit incident. Het benadrukt bijvoorbeeld hoe belangrijk hardening is. Elk bedrijf dat de beheertoegang netjes geïsoleerd heeft in een beheernetwerk is bijvoorbeeld niet kwetsbaar voor dit lek.
Daarnaast laat het incident ook goed zien hoe onverstandig het is om techniek bewust te verzwakken. De toegang tot bewust aangebrachte kwetsbaarheden blijft uiteindelijk niet voorbehouden tot één partij. Ook anderen kunnen de lekken vinden en misbruiken. Dit zagen we bij het genereren van toch-niet-zo-willekeurige nummers die gebruikt worden voor encryptie. En we zien het nu weer bij Juniper. Laten we daarom hopen dat het incident een bijdrage levert aan het vraagstuk over of techbedrijven hun encryptie bewust moeten verzwakken zodat onderschepte datastromen makkelijk toegankelijk blijven. We hebben er wederom een voorbeeld bij van waarom dat geen verstandig idee is.

Tom Bakker

Je vraagt je af welke firewall-leveranciers er naast Juniper nog meer te maken hebben met backdoors. Dat die backdoor-code bij Juniper nu pas ontdekt is na waarschijnlijk drie jaar, is opmerkelijk. Zoals gesuggereerd wordt, is deze code destijds tijdens de ontwikkeling van de software ingebracht. Hoe zit het dan met software testen en het change proces? Je zou verwachten dat een code (peer) review daar onderdeel van is. Één van de twee backdoors was een in de code opgenomen wachtwoord. Een in de code opgenomen wachtwoord zou op moeten vallen, lijkt mij. Er zijn dus nog veel vragen.
Als klant denk je dat je een veilig en betrouwbaar security-product aangeschaft hebt. Moet je dan toch nog extra maatregelen gaan treffen om de werking van dat product te gaan controleren?
Ik weet niet of het in deze casus zou helpen maar je zou denken dat een hacker die binnen is toch verdacht netwerkverkeer veroorzaakt? Die informatie moet toch ergens naar toe. Dus toch ook hier: preventie alleen is niet genoeg, detectie (monitoring) is ook noodzakelijk.

Artikelen

[A]	Baaten, M.	Information Security Officer: spelen met invloed	IB6:16
[V]	Bakker, T. e.a.	Sfeerimpressie ONE Conference	IB3:24
[V]	Beerten, A.	Black Hat Sessions: Donkere tinten en lichtpuntjes	IB5:20
[I]	Belder, M.	Vingerafdrukken tegen fraude	IB5:23
[A]	Bobbert, Y	Cybersecurity in de boardroom	IB5:10
[A]	Bobbert, Y.	Op zoek naar een duizendpoot	IB3:14
[O]	Borger, L	Boekbespreking: Elementary, My Dear Watson!	IB7:25
[A]	Broenink, G. e.a.	Detectie en risicoclassificatie van typosquatting	IB4:4
[A]	Child, M. e.a.	Return of the Cybermen.... Or perhaps they never really left!	IB7:12
[A]	Coenen, J.	Logging - Niet Dat, maar Wat en Hoe - deel 1	IB2:10
[A]	Coenen, J.	Logging - niet Dat, maar Wat en Hoe - deel 2	IB4:10
[V]	Coumou, C.	CISO 3: Criteria voor information assurance	IB3:22
[V]	Coumou, C.	CISO 5: Ethics and big data	IB5:30
[V]	Coumou, C.	CISO 6: Een discussie over SOC-SIEM	IB8:26
[I]	Craandijk, C	RedSocks: We zijn geen roepende in de woestijn meer	IB3:4
[I]	Craandijk, C.	Digidentity: 'Je moet in je product blijven geloven'	IB5:16
[A]	Damming, R.	Meldplicht datalekken	IB8:18
[V]	Dunn, L.	Studierapport, Algemene beheersing van IT-diensten	IB3:18
[V]	Dunn, L. e.a.	Sfeerimpressie ONE Conference	IB3:24
[O]	Dunn,L	Boekbespreking: Helpende Hackers en De Rode Hack	IB6:20
[A]	Dusink, M. e.a.	Scheiding tussen werk en daad	IB6:4
[V]	Erven, R. van	Boekbespreking: Hoe veilig is mijn 'aandeel'?	IB4:26
[A]	Eygendaal, R.	Near Field Communication rukt op...	IB2:21
[A]	Eygendaal, R.	ISO 21827 steeds belangrijker bij software ontwikkeling	IB7:22
[V]	Garskamp, R.	IDnext-event	IB5:26
[A]	Gittens, M.	Requirements Dependency Analysis	IB3:8
[A]	Gittens, Ma. e.a.	Modelling Threat Scenarios - deel 1	IB6:22
[A]	Gittens, Ma. e.a.	Modelling Threat Scenarios - deel 2	IB7:18
[A]	Gittens, Mi. e.a.	Modelling Threat Scenarios - deel 1	IB6:22
[A]	Gittens, Mi. e.a.	Modelling Threat Scenarios - deel 2	IB7:18
[A]	Gittens,M.	Treating risk prospectively	IB1:7
[A]	Hamer, M. de e.a.	CSIRT maturity kit	IB5:4
[A]	Hanekamp, W. e.a.	Scheiding tussen werk en daad	IB6:4
[A]	Hartsuijker, M.	KeePass: een einde aan wachtwoordergernissen	IB2:24
[V]	Hartsuijker, M.	Capture the flag competitie	IB8:24
[A]	Janec, M. e.a.	Advanced Business Impact Analysis - deel 1	IB4:16
[A]	Janec, M. e.a.	Advanced Business Impact Analysis - deel 2	IB6:10
[I]	Kagie, S.	Voorzitters in gesprek: Gegrepen door de factor mens	IB7:8
[I]	Kagie, S.	iWelcome: Welkom in de wereld van cloud IAM	IB8:8
[V]	Kanbier, G.	Security Café: Het internet is stuk	IB1:20
[V]	Kanbier, G.	Security Café: Privacy	IB4:22
[V]	Knoblock, M.	OWASP Appsec EU 2015	IB3:21
[O]	Koek, M.	Uitdaging voor gemeenten zit niet in "geblunder"	IB6:15
[A]	Kramer, J	ISO 27001 in het MKB	IB2:4
[V]	Kuiper, R.	Artikel van het jaar 2014: Hier word ik nou blij van	IB3:26
[A]	Luijf, E.	Van Kunst naar Kunde	IB2:18
[A]	Luijf, E.	Verliefd op onveiligheid	IB3:10
[A]	Marbus, R.	Na de veilige haven	IB8:4
[O]	Mars, G.	Boekbespreking: Foundations of Information Security	IB6:28
[A]	May, N. e.a.	Return of the Cybermen.... Or perhaps they never really left!	IB7:12
[A]	Molen, H.J. van der	Veiliger met voorkennis - deel 1	IB1:12

[A] Artikel
[V] Verslag
[I] Interview
[O] Opinie

Jaaroverzicht 2015

[A]	Molen, H.J. van der	Veiliger met voorkennis - deel 2	IB2:12
[A]	Niamat, R.	Cloud-mythes: Kloppen ze wel?	IB7:4
[A]	Niamat,R.	Privacy, ondernemers en providers	IB1:4
[A]	Prins, J.F.	Extreme Weather Events	IB8:12
[A]	Schotanus, H. e.a.	Detectie en risicoclassificatie van typosquatting	IB4:4
[A]	Stikvoort, D. e.a.	CSIRT maturity kit	IB5:4
[A]	Verweij, E. e.a.	Advanced Business Impact Analysis - deel 1	IB4:16
[A]	Verweij, E. e.a.	Advanced Business Impact Analysis - deel 2	IB6:10

Thema's

IB1 Privacy, ondernemers en providers
IB2 Dreigingen en kwetsbaarheden
IB8 Unsafe Harbour

Achter het nieuws

Helpen dwangsommen? - IB1:26
Superfish - IB2:28
Ransomware - IB3:28
In-flight 'entertainment' - IB4:28
Vluchten geannuleerd door cyberaanval - IB5:32
Black Hat en Def Con 2015 - IB6:32
Ligt de fout bij Apple... of bij de ontwikkelaars? - IB7:28
Is er toekomst voor de Safe Harbour-afspraak? - IB8:28

Column Attributer

Forensics Ready - IB1:23
Procesess Controlled - IB2:17
Time-Trusted - IB4:24
Business Context Aligned - IB5:15
Private IB6:25
Pollution Controlled - IB7:21
Cyber Secured - IB8:25

Column Berry

Hardleers - IB1:31
Winkelen, zolang het nog kan - IB2:31
Ze doen het nog hartstikke goed - IB3:31
Lekker onhandig, dat internet - IB4:31
Elk kwartaal een nieuwe soap - IB5:35
Drive-by-hacking - IB6:35
Mag ik uw creditcardnummer? - IB7:31
Autoleed - IB8:31

Column Privacy

Gluren bij de buren - IB1:17
Ome Ivo - IB2:7
Hacking Barbie - IB3:19
Pecunia non olet? - IB4:9
De blunderende gemeente - IB5:9
Burgerlijke ongehoorzaamheid en privacyprotest - IB6:14
Voldoen aan de wet is niet meer voldoende - IB7:11
Het is aan ons - IB8:23

Verantwoorde Onthullingen

Trots op onze digitale polderoplossingen - IB1:24

Redactie

Big Brother Awards - IB1:18
Nominaties Artikel van het Jaar - IB1:19
Jaaroverzicht 2014 - IB1:28
Publicatie: Helpende Hackers - IB2:30
IT-audit-autoriteit Gert van der Pijl - IB3:20
Artikel van het Jaar 2014: Prijsuitreiking - IB4:25
NCSC gebruikt SIVA-raamwerk in nieuwe richtlijn - IB6:31
Lawrence D. Eicher prijs voor subcommissie SC27 - IB7:26
Slimme auto's brengen zorgen en kansen - IB7:27

Voorwoord

Dat gebeurt toch niet echt - IB1:3
Innoveren is aanvallen - IB2:3
Modellen en controlelijsten - IB3:3
De Starbucks hack die geen hack was - IB4:3
De crypto van LastPass - IB5:3
Governance, risk, compliance - IB6:3
Georganiseerde misdaad - IB7:3
De zwakste schakel - IB8:3

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

REDACTIE
Lex Borger (hoofdredacteur, werkzaam bij i-to-i)
e-mail: hr@pvib.nl
MOS bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn (Capgemini)
Maarten Hartsuijker (Classity)
Rachel Marbus (NS)
Bart van Staveren

ADVERTENTIE-ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
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 2016
De abonnementsprijs in 2016 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

INTEGER KAPITAAL

Vlak voor de jaarwisseling kregen de 10.000 medewerkers van V&D een vervelende boodschap: V&D is failliet. De oprichters Vroom en Dreesman waren de grote vernieuwers in de Nederlandse consumentenmarkt. Dat verhaal komt nu tot een einde. Nadat de heren V&D hun bedrijf hadden gerund, hebben ze hun aandeel verkocht. Om een lang verhaal kort te maken: uiteindelijk heeft een Amerikaans bedrijf, Sun Capital, V&D in eigendom gekregen. Sun Capital is een investeringsfonds dat zijn klanten een hoog rendement belooft. Hoe hoger het rendement, hoe tevredener de klanten zijn en hoe meer investeerders er op afkomen.

Van de buitenkant ziet Sun Capital er goed uit, in de bedrijfsmissie komen mooie begrippen voor als transparantie, openheid en integriteit. Tja, dan moet het wel goed zitten natuurlijk. Als je een beetje gaat zoeken op internet dan kom je erachter dat Sun Capital eigenaar is geweest van modeketen Mervyns in de Verenigde Staten. Iemand die een paar jaar geleden nog daar is geweest moet dat weten, want ze hadden 175 vestigingen en dat is veel. Momenteel bestaat Mervyns niet meer, ze zijn failliet. Ze zijn failliet gegaan doordat de eigenaar te veel kapitaal uit het bedrijf heeft gehaald.

Dat gebeurde ook bij V&D. Een aantal jaren geleden werden door de toenmalige eigenaar alle panden van V&D verkocht en weer teruggehuurd. De opbrengst was ongeveer 1,3 miljard euro. Dat geld is natuurlijk naar de toenmalige eigenaar gegaan en V&D had vanaf dat moment de huurlast. Sun Capital kreeg V&D in handen en constateerde dat deze huurlast ten koste van de winst ging. Dat vindt Sun Capital niet plezierig, want daarmee wordt hun investering minder aantrekkelijk voor toekomstige kopers. Dus wordt de noodklok geluid en worden de vakbonden gevraagd de salarissen flink te laten krimpen. De vakbonden geven geen krimp en dus worden de eigenaren van de panden gevraagd de huren te verlagen. De eigenaren van de panden gaan deels overstag.

Uiteindelijk wordt het Sun Capital te gortig en besluit zij, tegen eerdere afspraken in, geen investeringen meer te doen in V&D. Dat is lastig voor V&D, want daarmee kunnen ze de bestellingen niet meer betalen en worden de leveringen aan V&D opgeschort. Ze worden failliet verklaard en de boedel wordt nu uitverkocht. Zoals bij zoveel faillissementen wordt de medewerker van V&D de dupe. Of ze verliezen hun werk, of ze mogen in dienst treden bij de eventuele doorstart tegen nieuwe contracten, die niet beter zullen zijn. Leveranciers van V&D zullen voor grote kosten komen te staan en ook daar zullen bedrijven omvallen.

En Sun Capital? Die gaan op zoek naar nieuwe bedrijven, want ze hebben nog geld staan op hun spaarrekening. Hoe komt Sun Capital aan dat geld? Ze hebben het gekregen van onder andere Nederlandse pensioenfondsen. Die investeren geld, heel veel geld, bij Sun Capital. Deze pensioenfondsen, onder andere ABP en Zorg en Welzijn, zouden zich op hun achterhoofd moeten krabben of ze dit wel willen.

Ik zou Sun Capital willen aanraden de bedrijfsmissie nog eens kritisch te bekijken. Ik heb zelf een heel andere gedachte bij integriteit.

Berry

Masterclass Security & Business Alignment 2.0

Door Security Academy & Universiteit Nyenrode

Start 7 maart 2016

De Security Academy, Universiteit Nyenrode en AutomatiseringGids organiseren voor de tweede maal de masterclass Securtity & Business Alignment.

De masterclass is bestemd voor het hoger management, directieleden, CxO's, business managers en overige geïnteresseerden, die niet zozeer in depth willen en hoeven te gaan op security vlak, maar wel hun verantwoordelijkheid willen en kunnen nemen in het belang van de continuïteit van hun organisatie.

In de Masterclass wordt ingegaan op vragen als:

- Hoe faciliteer ik als algemeen manager dit totale beveiligingsproces optimaal?
- Hoe voorkom ik dat het botst met mijn business belangen?
- Hoe pak ik Business Continuity Management (BCM) aan in mijn organisatie?
- Wat is de relatie tussen privacy en security?
- En als het dan fout gaat, is dan mijn crisismanagement wel goed op orde? Hoe weet ik dat zeker?

Investering

De investering voor deelname aan de collegereeks van 6 colleges bedraagt € 1.795,- per persoon (excl. BTW).

Programma

Het programma is concreet en helder opgezet en behandelt in zes modules:

- High level view op Cyber Security & Business alignment
- Informatiebeveiliging organiseren en succesvol besturen
- Business Continuity Management: waarde creëren waarde behouden
- 'When the shit hits the fan!' Crisismanagement op corporate niveau
- Compliance, regulations and legal: de voetangels en klemmen van de komende Europese Privacyverordering
- Het perspectief van de hacker

Organisatie

Security Academy, AutomatiseringGids en Nyenrode Business Universiteit presenteren samen deze masterclass en wordt uitgevoerd door docenten van de Security Academy.

Voor meer informatie kijk op:
http://www.executiveeducation.nl/security

BEL ONS +31(0)348-408061

WWW.SECURITYACADEMY.NL
INFO@SECURITYACADEMY.NL