iB
INFORMATIEBEVEILIGING
jaargang 14 - 2014
#2

WEERBAARHEID

De sterkte van wachtwoorden en hun tekortkomingen

ISO27001 herzien

COLUMN: het recept voor privacyvriendelijk innoveren

Nationale Cyber Security Strategie 2

Secure Link
Infrastructure Security Solutions

Gezocht!
Security Engineer

SecureLink is sterk groeiende en is daardoor op zoek naar Security Engineers die ons team komen versterken!

Als Security Engineer heb je diepgaande kennis op het gebied van onze security en networking producten. Je wilt met uitdagende technologieën van leidende security vendoren projectmatig werken. De combinatie van enerzijds de security technologie en anderzijds de integratie met de networking technologie is iets waar je jouw energie in kwijt kunt. Je krijgt veel zelfstandigheid om security oplossingen te pre-stagen, implementeren en onderhouden.

Benieuwd? Kijk dan op www.securelink.nl/vacatures

Integrated Networking Security Solutions

SecureLink is een vooraanstaande Benelux georiënteerde security en networking integrator. SecureLink onderscheidt zich door haar geïntegreerde security en networking specialisatie, voorname vendor statussen, managed services en hoge klanttevredenheid.

Go Secure!

SecureLink Nederland B.V. | Trapezium 224 | 3364 DL SLIEDRECHT | T +31 88 1234 200 | info@securelink.nl

PRIVACY WEERBAARHEID

Ik erger me soms aan de discussies over privacy. Privacy gaat niet alleen over het NIET delen van informatie. Een van de belangrijke aspecten van privacy is juist dat ik WEL informatie mag en kan delen. Chester Wisniewski schreef: "Privacy is about controlling what information about you is known and who you want to know it" [1]. Vooral dat tweede deel gaat over weerbaarheid.

Heb ik er moeite mee als Albert Heijn bijhoudt waar ik stilsta in de winkel en wat ik uiteindelijk koop? Nee. Laat AH alsjeblieft zijn winkel afstemmen op mijn koopgedrag. Maar laat mij daarbij verder een nummer zijn en verkoop het niet door aan bijvoorbeeld Unilever. Bewaar het niet voor altijd. En pas goed op de spullen. Denk om Chester. Een variant is het Facebook model: Geef me al je informatie, en ik geef je de mogelijkheid aan te geven hoe het gedeeld moet worden. Dit klinkt heel erg 'Chester', op een punt na: Facebook wil wel ALLES weten. En dan moet je er nog op vertrouwen dat jouw informatie goed beveiligd is. Die garantie krijg je nauwelijks.

Bij de overheid gaat het al verder. Alles wordt gecombineerd middels mijn BSN. Geen opt-in. Niet eens een opt-out. Geen beheersing (control) vanuit mijzelf, het is gewoon de wet, wen er maar aan. Ik ben niet degene die informatie deelt, dat wordt voor mij gedaan. Maar met privacy heeft het niets meer te maken volgens Chester. Steeds meer van mijn belastingaangifte is voor mijn gemak voor mij ingevuld. Ook dit is big data. Het maakt het wel makkelijker, maar het geeft je ook de privacyrillingen.

Nog een stap verder gaat de wereld van on-line adverteren. Door middel van gratis diensten en ingenieuze systemen die mijn zoek- en klikgedrag bijhouden bouwen ze een profiel van mij, wat gebruikt wordt om mij advertenties te tonen waarmee ze denken mij te verlokken. De schaarse beheersingsfuncties die er zijn, zoals het do-not-track HTTP headerveld, zijn afhankelijk van goed gedrag van websites. Er zijn zoveel meer manieren om je, veelal ongemerkt, te volgen dan er manieren zijn om aan te geven dat je dat niet wilt.

Dit alles samen voedt een zee aan privacygevoelige informatie die maar groeit en groeit. Als we het dan over privacy hebben, wil ik niet alleen het recht hebben te mogen beslissen wat er met wie gedeeld wordt, want dan blijf ik zitten met alle risico's van slechte beveiliging bij al die locaties. Er zijn voorbeelden zat van big data breaches: Adobe, Target, TJ Max, Heartland - om er maar een paar te noemen. Mijn informatie mag niet zomaar overal zijn. Ik wil ook weerbaar kunnen zijn en het recht hebben te bepalen dat mijn informatie 'gewist' wordt [2]. Hier moeten we de komende tijd als samenleving maar eens aan werken...

Lex Borger, hoofdredacteur

Links:

[1] http://nakedsecurity.sophos.com/2014/01/28/privacy-is-not-dead-youre-just-doing-it-wrong/

[2] http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2119#

In dit nummer

DE STERKTE VAN WACHTWOORDEN EN HUN TEKORTKOMINGEN

Wachtwoorden kraken is een kunst, geen exacte wetenschap…

In 'Achter het Nieuws' in IB-8 van 2013 kwam de hack bij Adobe aan de orde, waar talloze wachtwoorden van klanten waren buit gemaakt. Ook bij diverse andere hacks werden wachtwoorden ontfutseld. In dit artikel wordt ingegaan op de problematiek rondom het gebruik en de sterkte van wachtwoorden en worden suggesties gegeven voor alternatieven.

Wachtwoord sterkte meter

Een wachtwoord is een geheim, dat geraden kan worden. De sterkte van een wachtwoord is dus afhankelijk van de snelheid waarmee het wachtwoord geraden kan worden. Hackers zijn erop uit om wachtwoorden snel te kunnen achterhalen, omdat een gebruikersnaam/wachtwoord combinatie vaak toegang biedt tot allerlei waardevolle persoonlijke en financiële gegevens en soms zelfs tot iemands online identiteit. De snelheid waarmee een wachtwoord geraden kan worden, hangt af van een variëteit aan psychologische en technische factoren.

Figuur 1 - Voorbeeld (Bron: Google)

Het bepalen van de sterkte van een wachtwoord is een ingewikkeld probleem. Een herkenbaar voorbeeld van de visualisatie van de sterkte van een wachtwoord is een 'wachtwoord sterkte meter', welke vaak getoond wordt bij het aanmaken van een account (zie figuur 1). Die meter laat aan de gebruiker zien hoe sterk het ingevoerde wachtwoord is. Toch hangt de sterkte van een wachtwoord vaak van veel meer factoren af dan een dergelijke meter in ogenschouw neemt.

Nico van Heijningen is afgestudeerd aan de Hogeschool van Rotterdam in de richting van Technische Informatica, waar hij zich in de laatste periode van zijn studie gericht heeft op computerbeveiliging. Tijdens zijn afstuderen bij TNO heeft hij onderzoek gedaan naar de patronen in de wachtwoorden. Het resultaat van zijn afstuderen is een geavanceerde 'wachtwoordsterkte analyse demonstratie', die de opbouw van een wachtwoord analyseert en een uitspraak doet over de sterkte van het wachtwoord. Naast toegepast computerbeveiligingsonderzoek liggen zijn interesses onder andere in de hoek van cryptografie. Nico is bereikbaar via nico.heijningen@gmail.com.

Psychologie en Technologie

Dankzij technologische ontwikkelingen en de daaruit verkregen psychologische inzichten kan beter worden begrepen hoe mensen hun wachtwoorden kiezen, hoe wachtwoorden zijn opgebouwd en wat voor patronen er binnen wachtwoorden bestaan. Deze kennis kan gebruikt worden bij het raden/kraken van iemands wachtwoord.

Het proces werkt als volgt. Regelmatig wordt er een nieuwsbericht gepubliceerd over een bedrijf dat de wachtwoorden van zijn gebruikers heeft gereset omdat hackers toegang hebben gekregen tot de interne netwerken. Meer dan eens wordt de verkregen data door de desbetreffende hackers op het internet gelekt. Laatst was dit het geval bij Adobe en eerder gebeurde hetzelfde onder andere bij LinkedIn [1,2]. Onderdeel van deze gegevens zijn soms de (door het bedrijf) gehashte wachtwoorden van de gebruikers. De hash van een wachtwoord kan worden gezien als de vingerafdruk (zie figuur 2) van een wachtwoord, gegenereerd door een onomkeerbaar algoritme. Het doel van het hashen van de wachtwoorden is dat hackers nu niet direct de wachtwoorden kunnen misbruiken, alleen de hash is bekend en niet het daadwerkelijke (klare tekst) wachtwoord.

Figuur 2 - Visuele weergave (Bron: Wikimedia)

Wanneer het hackers gelukt is om in te breken bij een bedrijf blijkt jammer genoeg vaak dat het door het bedrijf gekozen hashing-algoritme niet van toereikend niveau is. Er worden bijvoorbeeld hashing-algoritmes als MD5 of SHA1 gebruikt, terwijl deze algoritmen niet zijn ontworpen om wachtwoorden mee te hashen. In plaats daarvan zijn ze ontworpen om grote hoeveelheden data snel te kunnen hashen. Dit betekent dat het genereren van een hash erg snel kan worden gedaan; extreem snel zelfs wanneer de parallellisatiekracht van videokaarten (GPUs) wordt ingezet [3] (verderop in het artikel worden geschikte hashing-functies toegelicht). Door met behulp van GPUs extreem snel allerlei verschillende wachtwoorden te hashen en deze te vergelijken met de gelekte hashes, kunnen hackers kijken of het wachtwoord dat ze geprobeerd hebben daar ook daadwerkelijk in voorkomt. Zo kunnen ze alsnog een lijst van gebruikte wachtwoorden genereren.

Patronen in wachtwoorden

Aan de hand van de lijst van gekraakte gebruikerswachtwoorden kunnen bijvoorbeeld de meest gebruikte wachtwoorden berekend worden [4], maar wat interessanter is voor de hackers zijn de veel gebruikte patronen. Oftewel: wat voor patronen gebruiken mensen binnen een wachtwoord? Voorbeelden van een patroon zijn (hier gerangschikt van simpel naar geavanceerd):

- **Welke soorten karakters worden het meest gebruikt in wachtwoorden?**
- **Op welke positie binnen een wachtwoord wordt welk karakter het meest gebruikt?**
- **Wat zijn de overgangskansen tussen de verschillende karakters binnen een wachtwoord?**

Veelvoorkomende patronen

Een voorbeeld van eenvoudig te herkennen doch effectief te misbruiken patronen zijn wachtwoord masks. Een wachtwoord mask is de abstractie van een wachtwoord per karakterset per positie. Waarbij '?l' een kleine letter voorstelt (lowercase) en '?d' een getal (digit). Het wachtwoord 'hond1' wordt weergegeven als '?l?l?l?l?d'. Deze notatie wordt gebruikt bij de GPU wachtwoordkraker Hashcat [5].

?l?l?l?l?l?l	9,87%
?l?l?l?l?l?l?l?l	7,71%
?l?l?l?l?l?l?l	6,76%
?d?d?d?d?d?d	4,4%
?l?l?l?l?l?l?d?d	3,7%
?l?l?l?l?l?l?l?l?l	3,48%
?l?l?l?l?l?d?d	1,72%

Tabel 1 - Veelvoorkomende wachtwoord masks (Bron: TNO)

In tabel 1 [6] vindt u de meest voorkomende wachtwoord masks uit tien verschillende lijsten met wachtwoorden die op internet zijn gelekt (in totaal ongeveer 45 miljoen wachtwoorden). U ziet dat veel van de meest gebruikte patronen erg simpel zijn, bestaande uit alleen kleine letters, alleen getallen of een aantal kleine letters gevolgd door een aantal getallen. Deze patronen leiden tot een extreme reductie in de grote van de zoekruimte en toch kan hiermee gemiddeld bijna 40% van alle wachtwoorden worden gekraakt.

Door dergelijke patronen te ontdekken kunnen de pogingen die gedaan moeten worden om een wachtwoord te raden statistisch geordend worden. Wanneer een poging voldoet aan een patroon dat veel voorkomt in reeds gekraakte wachtwoorden, is die poging waarschijnlijker dan een poging die niet voldoet aan een dergelijk patroon. Door wachtwoorden met een hogere slagingskans eerder in het kraakproces te proberen zijn er minder pogingen nodig om de wachtwoorden te kraken. Zo kunnen er meer wachtwoorden gekraakt worden in kortere tijd. Met deze patronen kunnen ook andere wachtwoorden sneller gekraakt worden [7]. Wanneer een nieuwe lijst met gehashte wachtwoorden wordt gelekt, mogen de wachtwoorden dan wel anders zijn, maar de patronen die mensen gebruiken om een wachtwoord te kiezen zijn veelal hetzelfde.

Figuur 3 - Apple iCloud Keychain (Bron: Apple)

Echter, de patronen die je vindt in de analyse zijn erg afhankelijk van de eisen die gesteld worden aan het wachtwoord oftewel het wachtwoordbeleid. Er worden geheel andere patronen gebruikt wanneer er van een gebruiker geëist wordt dat er een hoofdletter en cijfer in het wachtwoord aanwezig moeten zijn, dan wanneer bijvoorbeeld alle wachtwoorden ingevoerd mogen worden. We merken op dat een wachtwoordbeleid vaak onbedoelde gevolgen heeft. Veel mensen kiezen voor de makkelijkste optie. Wanneer alles wordt toegelaten, kiezen mensen een kort wachtwoord bestaande uit alleen kleine letters. Wanneer er een minimumlengte van acht karakters wordt geëist met zowel een hoofdletter en cijfer, zal het wachtwoord veelal bestaan uit acht karakters met de hoofletter op de eerste positie en het cijfer aan het einde (vaak het cijfer 1). Wanneer een wachtwoord-rotatie-beleid wordt afgedwongen (het wachtwoord dient bijvoorbeeld maandelijks veranderd te worden), plakt men een cijfer aan het einde van het wachtwoord, betreffende het getal van de huidige maand (1 voor januari, 2 voor februari enzovoorts).

Om mensen te helpen een sterk wachtwoord te kiezen worden allerlei wachtwoordschema's als advies gegeven. Toch is dit snel een vorm van 'security through obscurity'; wanneer er maar genoeg mensen gebruik maken van een dergelijk schema, kan hier op gefocust worden door hackers. Een noemenswaardig voorbeeld is het gebruik van 'passphrases', oftewel gehele zinnen als een wachtwoord. Er zijn zowel voordelen als nadelen: het is sterker dan een kort wachtwoord bestaande uit een woord met wat cijfers er achter, maar er zijn ook erg veel patronen in te vinden. Denk hierbij bijvoorbeeld aan het aantal woorden dat een gemiddelde gebruiker kent (als parate kennis) en deze daadwerkelijk gebruikt bij het bedenken van een 'passphrase'. Daardoor zijn veel van dit soort schema's toch minder sterk dan men zou verwachten.

Password Analysis and Cracking Toolkit

Een wachtwoordbeleid en 'slimme' wachtwoordschema's introduceren onbedoeld patronen in de opbouw van wachtwoorden. Dit soort patronen kunnen geautomatiseerd ontdekt worden door gebruik te maken van de Password Analysis and Cracking Toolkit (PACK) [8]. Door het hiervoor beschreven proces te herhalen bij verschillende lijsten wachtwoorden met verschillende achtergronden, wordt er steeds meer kennis vergaard over de opbouw van wachtwoorden over de gehele linie (zie [6] voor een dergelijke analyse). Zowel wachtwoorden voor belangrijke sites (bijvoorbeeld: Bitcoin handel sites) als wachtwoorden voor minder belangrijke sites (bijvoorbeeld: online spelletjes sites) worden zo geanalyseerd.

Hulpmiddelen

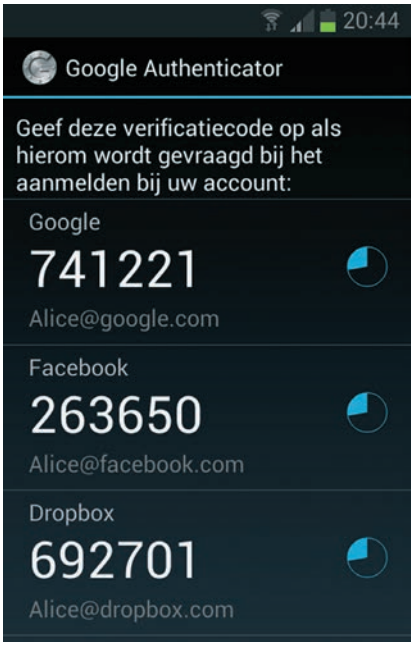
Het is niet verwonderlijk dat er patronen zijn te ontdekken in wachtwoorden, aangezien het menselijk brein niet goed is in het exact herinneren van willekeurige reeksen karakters. In plaats daarvan is het brein beter in het herinneren van structuren en patronen. Zeker wanneer er verwacht wordt dat mensen een aantal verschillende, lange en willekeurige wachtwoorden onthouden, is dit voor veel mensen een brug te ver. Onthoudbare wachtwoorden zijn vaak gemakkelijker te kraken. Terwijl wachtwoorden die lastig te kraken zijn, niet te onthouden zijn. Zeker niet wanneer de hoeveelheid te onthouden wachtwoorden groter wordt. Om toch voor ieder account een ander en sterk wachtwoord te kunnen gebruiken hebben mensen een hulpmiddel nodig.

Hiervoor kan gebruik gemaakt worden van een wachtwoordmanager. Voorbeeld hiervan zijn de Apple iCloud Keychain [9] (zie figuur 3) en KeePass [10]. Dit zijn programma's die voor ieder account een ander, lang en willekeurig wachtwoord genereren. Elk wachtwoord wordt in een wachtwoordenbestand opgeslagen dat op zijn beurt weer beveiligd is met één onthoudbaar wachtwoord. Zo wordt het zwaartepunt verschoven, van online naar offline: wanneer hackers een service hacken, komen ze nu in het bezit van een erg lastig te kraken wachtwoord, dat nergens anders gebruikt wordt en gemakkelijk vervangen kan worden. In plaats van een simpeler te kraken wachtwoord, dat bij verschillende services wordt gebruikt en lastig te vervangen is. Het zwakke punt is nu één wachtwoord geworden waarmee het wachtwoordenbestand beveiligd wordt (ervan uitgaande dat de encryptie van het wachtwoorden-bestand van afdoende niveau is).

Deze werkwijze is niet vrij van kritiek/problemen. Zo dient het wachtwoord waarmee ingelogd wordt op de pc nog steeds zelf onthouden te worden en is de synchronisatie van het wachtwoordenbestand bij gebruik van meerdere apparaten vaak een struikelblok. Het wachtwoordenbestand dient dan toch ergens online te worden opgeslagen (tegenwoordig vaak bij een cloud service als Dropbox of Google Drive). Ook moet hierbij in gedachten worden genomen dat het vaak de al beveiligingsbewuste gebruikers of slachtoffers van een eerdere hack zijn die dit soort methoden überhaupt in overweging nemen.

Toekomst van authenticatie

Wachtwoord gebaseerde authenticatie blijft de dominantste authenticatiemethode in het cyber-domein. Het principe is simpel te implementeren, er zijn weinig kosten mee gemoeid en gebruikers zijn er mee bekend. Hoewel er veel alternatieve authenticatiemethoden beschikbaar zijn, is er nog geen methode breder geïmplementeerd en geaccepteerd dan authenticatie met behulp van wachtwoorden. Mijn verwachting is dan ook dat deze vorm van authenticatie in de nabije toekomst nog altijd een groot percentage van de volledige authenticatiemarkt zal blijven omvatten. Een breed gedragen overgang naar een andere vorm van authenticatie is in mijn ogen dan ook alleen stapsgewijs haalbaar.



Figuur 4 - Google Authenticator

Echter, afhankelijk van de context van de authenticatie zal dit ook niet per definitie wenselijk zijn. De waarde van de informatie waarvoor ingelogd dient te worden, is hierbij een belangrijke factor. Voor minder waardevolle informatie is een lager beveiligingsniveau afdoende, waar bij waardevolle informatie een hoger beveiligingsniveau gerealiseerd zal moeten worden. In de meeste gevallen voldoet wachtwoord gebaseerde authenticatie daarbij nog prima. Bij de gemiddelde gebruikers is de drijfveer voor het gebruik van sterkere wachtwoorden niet groot genoeg. Hierbij blijkt training erg lastig, heeft beveiliging bij veel mensen geen prioriteit en staat gemak hoger in het vaandel. Daarnaast zien we dat het veelal de extreem zwakke wachtwoorden zijn die risico lopen op misbruik. Wanneer er voldaan wordt aan basale minimumeisen is misbruik vaak te voorkomen.

Het grootste gevaar bij het gebruik van wachtwoorden is dan ook niet het gebruik van zwakke wachtwoorden, maar het gevaar van hergebruik, wanneer men een wachtwoord op verschillende plaatsen (her)gebruikt is één zwakke schakel voldoende om toegang te krijgen tot alle verschillende accounts. Wanneer een wachtwoord bij een 'onbelangrijke' dienst gekraakt wordt, kan de gebruikersnaam/wachtwoord combinatie daarna ingezet worden bij een andere dienst die wél belangrijk is. Dit wordt voorkomen door gebruik te maken van een van de eerder genoemde wachtwoordmanagers.

De 'FIDO Alliance' [11] is hierom in het leven geroepen om technische specificaties te definiëren die de afhankelijkheid van wachtwoorden om gebruikers te authenticeren moet verminderen. Hierbij worden ook concepten in beeld genomen die in dit artikel buiten beschouwing zijn gelaten. Deze samenwerking wordt gesteund door gewichtige partners als o.a. Google, Microsoft, Paypal en Mastercard.

Time-based One-time Password Algorithm

Een voorbeeld dat reeds in gebruik is genomen waarbij er zowel een breed draagvlak, de juiste context, als een sterke drijfveer aanwezig waren om over te schakelen naar een sterkere authenticatie methode, is bij de beveiliging van accounts bij grote web-services als die van Google, Facebook en Dropbox. Deze bedrijven hebben het Time-based One-time Password Algorithm (TOTP) [12] geïmplementeerd. Hiermee moet naast het wachtwoord een token worden ingevoerd die elke dertig seconden veranderd. Dit token wordt gegenereerd door een applicatie op een smartphone (zie figuur 4). Door de smartphone als tweede factor te gebruiken in de authenticatie dienen hackers niet alleen kennis te hebben van het wachtwoord, maar ook controle te hebben over de smartphone. Dit maakt een aanval significant moeilijker.

Geschikte wachtwoord hash-functies

Eerder in het artikel is beschreven dat bekende hash-functies als MD5 en SHA1 ongeschikt zijn om te gebruiken als hash-functie om wachtwoorden te hashen. De reden hiervoor is dat de Graphical Processing Units (GPUs) van moderne videokaarten zeer goed geoptimaliseerd zijn om grote hoeveelheden eenvoudige bewerkingen parallel uit te voeren. Hiermee zijn deze hash-functies eenvoudig door middel van brute-force

Concluderend kunnen we zeggen dat het opslaan en verwerken van wachtwoorden voor gebruik als authenticatiemiddel veel meer voeten in de aarde heeft dan men in eerste oogopslag zou denken.

aanvallen te kraken.
Er bestaan al lange tijd hashing-algoritmes die veel beter gewapend zijn tegen de rekenkracht van GPUs. Deze hashing-algoritmes laten zichzelf erg lastig parallelliseerbaar maken door relatief veel geheugen te gebruiken in de berekening. GPUs zijn namelijk veel minder sterk in het parallel berekenen van functies die veel geheugen nodig hebben. Tevens is het mogelijk om het aantal iteraties van het algoritme in te stellen om zo een groter processor gebruik te veroorzaken. Het resultaat hiervan is een adaptief onomkeerbaar hashing-algortime, waardoor de tijdsduur om één hash te berekenen gelijk blijft naarmate de tijd en computerkracht voortschrijden. Voorbeelden van dergelijke wachtwoord-hashing-algoritmes of key derivation functions (KDFs) zijn scrypt (2009) [13] en bcrypt (1999) [14]. Bij scrypt is het mogelijk om zowel de hoeveelheid te gebruiken geheugen als het aantal iteraties in te stellen, terwijl bij het oudere bcrypt alleen het aantal iteraties in te stellen is. Voorlopig zal bcrypt nog afdoende zijn, het geheugengebruik kan dan niet ingesteld worden, maar dit is voor de huidige generatie GPUs te groot om bcrypt goed parallelliseerbaar te maken.
Toch zien we dat de adoptie van dergelijke hashing-algoritmes in de praktijk achter blijft. Het is gissen waarom. De algoritmen zijn slechts een beetje complexer, maar ze zijn vaak minder breed geïmplementeerd dan oude vertrouwde algoritmen als MD5 en er bestaat altijd een gezond wantrouwen bij nieuwe cryptografische algoritmes. De Password Hashing Competition (PHC) [15] probeert vooruitgang te boeken in de ontwikkeling en adoptie van nieuwe state-of-the-art wachtwoord hashing-algoritmes.

Conclusie

Concluderend kunnen we zeggen dat het opslaan en verwerken van wachtwoorden voor gebruik als authenticatiemiddel veel meer voeten in de aarde heeft dan men in eerste oogopslag zou denken. In dit artikel zijn een aantal problemen besproken, maar een aantal andere problemen zijn bewust buiten beschouwing gelaten. Denk hierbij bijvoorbeeld aan: phishing/social engineering, hardware security modules, FPGAs/ASICs en andere authenticatiemethoden, zoals biometrie of grafische wachtwoorden. Voorlopig zitten we nog vast aan wachtwoorden, maar dankzij (industrie brede) initiatieven als FIDO, TOTP en PHC, en mede door de verschuiving naar cloud services, zullen hier hopelijk meer stappen in gemaakt worden dan is gedaan in de afgelopen 35 jaar. Het is schrikbarend om te zien hoeveel informatie uit het paper 'Password Security: A Case History' van Robert Morris en Ken Thompson [16] nog toepasbaar is in de hedendaagse praktijk.

Bronnen

1. http://www.nu.nl/internet/3592664/adobe-reset-29-miljoen-wachtwoorden-hack.html

2. http://www.nu.nl/internet/2828977/linkedin-reset-accounts-lekken-wachtwoorden.html

3. IB Magazine PvIB Nr 5 van 2011 - Iedereen een supercomputer - Sprengers; http://www.pvib.nl/download/?id=17678137

4. http://stricture-group.com/files/adobe-top100.txt

5. http://hashcat.net/oclhashcat/

6. http://publications.tno.nl/publication/100706/ORbsjc/heijningen-2013-stateofart.pdf

7. http://www.youtube.com/watch?v=5i_Im6JntPQ

8. http://thesprawl.org/projects/pack/

9. https://www.apple.com/nl/support/icloud/keychain/

10. http://keepass.info/

11. http://www.fidoalliance.org/

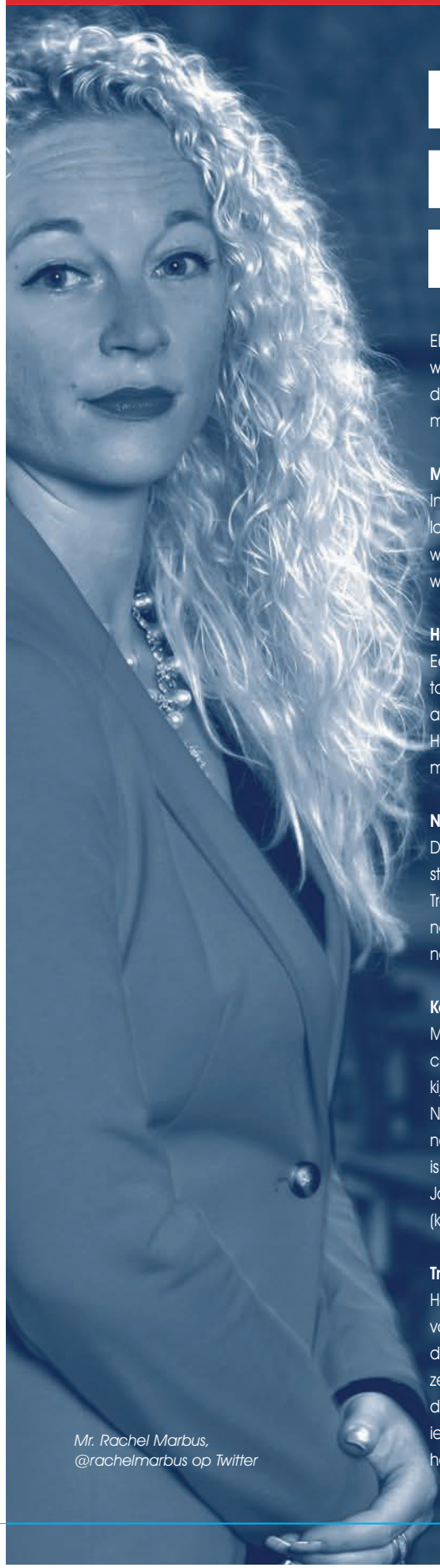
12. https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm

13. https://www.tarsnap.com/scrypt

14. https://www.usenix.org/legacy/events/usenix99/provos/provos_html/node1.html

15. https://password-hashing.net/

16. http://cm.bell-labs.com/who/dmr/passwd.ps



Mr. Rachel Marbus, @rachelmarbus op Twitter

HET RECEPT VOOR PRIVACYVRIENDELIJK INNOVEREN

Elk geslaagd recept begint met een briljant idee. De jonge enthousiaste medewerker die op goede ochtend wakker wordt en weet hoe hij de klant gelukkig gaat maken. De klant, daar gaat het immers om. Dat is degene die het eindresultaat moet gaan eten. Maar, hoe doe je dat nu eigenlijk op een privacyvriendelijke manier? Welnu, hieronder de ingrediënten voor een geslaagd privacyproof innovatierecept.

Men neme een goede voedingsbodem

Innovatie staat of valt bij de voedingsbodem die het krijgt. Daarom is het zaak om medewerkers de ruimte te laten en te geven nieuwe ideeën uit te werken. Niet elk idee is succesvol, maar de ervaring leert (en de wetenschap beweert) dat briljante geesten eerst vaak moeten falen voordat dit ene geweldige idee geboren wordt. "The best way to have a good idea, is to have a lot of ideas" (Linus Pauling).

Het kiezen van de juiste kok en sous-chef(s)

Een idee kan nog zo briljant zijn, maar als je niet goed van tevoren bekijkt wie betrokken moeten zijn, zal die taart gaan inzakken. De jonge enthousiaste medewerker heeft hulp nodig. En dat is niet alleen financieel van aard. Elk goed nieuw idee wordt sterker als een team van experts om tafel gaat zitten en gaat brainstormen. Het idee vervolmaken tot een succesvol product doe je namelijk samen. En om dat idee privacyproof te maken, zorg je ervoor dat de Privacy Officer vanaf het begin aanschuift.

Niet meteen nee roepen bij ingrediënten die jij niet lekker vindt

Die Privacy Officer moet daar niet gaan zitten als een boe-roepende waakhond. Hij of zij luistert, stimuleert en stelt de juiste vragen. Wat wil je gaan doen? Wat heb je daarvoor nodig? Wat wil je bereiken, wat is je doel? Trek niet meteen een vies gezicht als de jonge enthousiaste medewerker roept dat hij persoonsgegevens nodig heeft omdat hij de klant zo goed mogelijk wil bedienen. Vraag op dat punt wat hij dan eigenlijk precies nodig heeft om de taart te maken.

Kan het een snufje minder?

Mooi. Nu weten we wat er nodig is om de taart te gaan bakken. En juist dan is die Privacy Officer van cruciaal belang. Hij beziet de ingrediënten en weet wat daar uit moet gaan komen. Dit is het punt om te kijken of het ook een snufje minder kan. Stelt u zich voor dat we willen weten of een treincoupe vol of leeg is. Nu kunnen daarvoor camera's opgehangen worden, in een oogopslag valt dan te zien welk compartiment nog lege stoelen heeft zodat die informatie aan reizigers doorgegeven kan worden. Maar als het doel nu juist is om mensen goed over de trein te verdelen, kan dat dan niet ook met andere ingrediënten bereikt worden? Jazeker. Infrarood sensoren kunnen immers prima meten of een stoel rood (warm en dus bezet) of blauw (koud en dus vrij) is. Er hoeven helemaal geen persoonsgegevens verwerkt te worden.

Trial and error: net zo lang bakken tot het goed smaakt

Hoera! We hebben een privacyproof taart! Maar dan zijn we er nog niet. Ervaring leert dat bij het live gaan van een nieuw concept er altijd onverwachte neveneffecten optreden. Er worden meer gegevens verwerkt dan voorspeld, de gewenste resultaten pakken toch anders uit, om iets zinvols over het effect te kunnen zeggen moet data toch langer bewaard worden, etc. etc. Zorg er dus voor dat je een pilotfase inplant en dat je de kok en sous-chef(s) op gezet moment aan tafel zet om te evalueren. Smaakt de taart voor iedereen aan tafel lekker of moeten we nog wat aanpassen? Als alle ingrediënten goed gemixt worden, kan het niet snel meer fout gaan: privacyvriendelijk innoveren is echt niet zo heel moeilijk. Eet smakelijk!

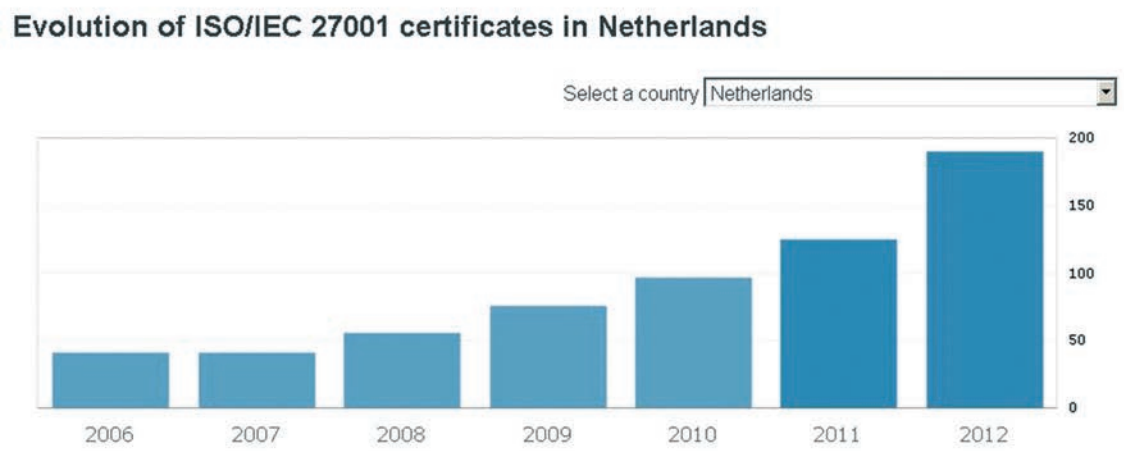
ISO27001 HERZIEN

Op 25 september 2013 is na 8 (!) jaar de langverwachte herziening van de norm ISO27001 verschenen; de eisen gesteld aan de inrichting en het onderhoud van een beheerssysteem voor informatiebeveiliging. In dit artikel wordt ingegaan op het hoe en waarom van de herziening en de veranderingen in de norm.

Na een aanvankelijk langzame start als British Standard 7799 in de jaren negentig van de vorige eeuw, werd in 2000 deel I van die norm onder de naam ISO17799 een wereldstandaard van maatregelen voor informatiebeveiliging. Hoewel in 1998 al deel II, een summiere beschrijving voor het beheersysteem voor informatiebeveiliging (Information Security Management System – ISMS) als BS7799-2 beschikbaar kwam, duurde het nog tot 2005 voordat dit deel als ISO27001 internationale standaard werd. Rond die tijd werd ook ISO17799 hernoemd als ISO27002 en was de norm weer compleet.
De lange periode die het kostte om wereldwijd de beschrijving van het ISMS geaccepteerd te krijgen als ISO norm gaf al aan dat in de wereld op diverse plaatsen anders gedacht wordt over beheer. In Angelsaksische landen, maar ook bijvoorbeeld in Duitsland, wordt meer 'control-based' gedacht; implementeer vooral veel maatregelen dan breng je de risico's omlaag. In grote delen van Europa daarentegen, ook in Nederland, is 'principle-based' beveiliging meer gangbaar; beschrijf vooral doelstellingen, richt beheer in en toets regelmatig en goed of de doelstellingen gehaald worden.
Sinds 1998 is het mogelijk om extern getoetst en gecertificeerd te worden tegen eerst BS7799-2, later tegen ISO27001:2005. Wereldwijd een enorm succes; in Nederland bleef tot ongeveer 2009 het succes beperkt tot enkele tientallen uitgereikte certificaten. Vanaf 2010 is één en ander echter in een stroomversnelling geraakt; wereldwijd zijn nu vele tienduizenden organisaties gecertificeerd en in Nederland waren het er eind 2012 al 200. In 2013 (geschat) is dit aantal verdubbeld (bron: ISO2012 survey).

Afgezien dat uiteraard het succes van de norm reden genoeg is voor het aanpassen van de norm aan veranderingen in het vakgebied is ook binnen de ISO organisatie stilgestaan bij andere toekomstverwachtingen. Daarin speelt mee dat veel organisaties op dit moment de wens hebben hun managementsystemen (zoals voor milieu, kwaliteit, informatiebeveiliging, continuïteit etc.) meer te integreren. Alle normen voor die managementsystemen echter, waren geproduceerd door diverse subcommissies binnen ISO waardoor consistentie ontbrak. In ISO verband is lang gewerkt aan het opnieuw vaststellen van een dwingend voorgeschreven template voor normen voor managementsystemen; gedocumenteerd in Annex SL van het interne ISO handboek. Nu deze template beschikbaar was moeten bij revisie alle nieuwe

Ing. Ernst J. Oud CISA CISSP is ISO27001 Lead Auditor bij BSI Group Nederland. Daarnaast helpt hij grote en kleine organisaties met informatiebeveiligings- en continuïteitsvraagstukken uit zijn eigen praktijk, kineta ICT advies, en geeft hij les aan de VU, bij inSpearIT en bij Security Academy. Hij is te bereiken via info@kineta.nl.



De groei van het aantal certificaten in Nederland t/m 2012

ISO normen aan deze template voldoen. ISO22301 (Business Continuity Management Systems – Requirements) was de eerste norm die aan het nieuwe template voldeed; ISO27001:2013 de tweede.
Als gevolg van de nieuwe template ziet ISO27001:2013 op het eerste gezicht er totaal anders uit dan de voorgaande versie ISO27001:2005. Alle hoofdstukken zijn veranderd; alle tekst is gewijzigd. Geen paragraaf is op zijn plaats blijven staan of gelijk gebleven. Ook opvallend – zeker voor ISO normen die allemaal hierop gestoeld waren – is de niet meer op het eerste oog herkenbare Deming Cycle (Plan/Do/Check/Act). ISO27001:2013 spreekt nu van "Planning", "Operations", "Performance Evaluation" en "Improvement".
Tegelijkertijd met ISO27001:2013 is ook ISO27002:2013, de norm met richtlijnen voor de maatregelen genoemd in Annex A. van ISO27001:2013, verschenen. In de komende tijd zullen alle andere normen in de 27 serie zoals ISO27000 ("Overview and vocabulary") aangepast worden aan ISO27001:2013 en dus ook moeten voldoen aan de nieuwe template Annex SL.
Gezien de grote veranderingen is het zinvol hierbij stil te staan. Aan het eind van dit artikel wordt verwezen naar een uitvoeriger beschrijving, niet in groot detail maar meer op grote lijnen. Na de beschrijving van de belangrijkste wijzigingen voor het ISMS en de maatregelen in Annex A. van de norm, wordt nog stilgestaan bij de gevolgen voor gecertificeerde organisaties.

De belangrijkste wijzigingen voor het ISMS

Beschouwen we nauwkeurig de tekst van ISO27001:2013 dan valt op, zoals hierboven al genoemd, dat de norm volledig anders opgezet is. De Plan/Do/Check/Act stappen van de Deming cycle zijn met enige moeite nog wel te herkennen. Nog steeds is planmatig aan informatiebeveiliging werken (beleid maken, risicoanalyses uitvoeren) en planmatig implementeren (implementatieplan, resources, training etc.) aan de orde. Ook audit en regelmatige management review is uiteraard blijven staan.
Nieuw is echter een meer naar buiten gerichte focus. De inbreng van partijen om de organisatie heen is belangrijker geworden; informatie beveiligen doe je niet voor jezelf maar voor je klanten of om in het algemeen te voldoen aan eisen van derden. Dit is verwoord in een nieuw hoofdstuk: "Context of the organization". Een kort hoofdstuk met relatief weinig eisen maar uitermate belangrijk. In kaart brengen van alle stakeholders van de organisaties en hun eisen, intern maar ook extern, zal binnen organisaties de focus doen veranderen van binnen naar meer buiten gericht. De verkregen informatie van stakeholders is een belangrijke input voor de risicoanalyse.
De voorgaande versie, ISO27001:2005, sprak op veel plaatsen over de verantwoordelijkheden voor het management. Dit riep altijd vragen op bij wat grotere organisaties wie dat dan waren; doe je management review (directiebeoordeling) in de lijn of met de raad van bestuur bijvoorbeeld? En mag informatiebeveiliging door de directie gedelegeerd worden aan de ICT manager? Mag de CISO de management review geheel voorbereiden en alleen nog ter goedkeuring aan de directie aanbieden?
De nieuwe ISO27001:2013 is hier veel duidelijker over; een nieuw hoofdstuk "Leadership" geeft aan welke verantwoordelijkheden en taken het "top management" van de organisatie heeft. De overige taken kunnen dan gedelegeerd worden, maar de in dit nieuwe hoofdstuk genoemde taken niet.
De nieuwe opbouw en de twee genoemde nieuwe hoofdstukken zijn de meest opvallende wijzigingen. Daarnaast zijn de volgende veranderingen van groot belang:

- ISO27001:2005 noemde (bij certificering) een aantal documenten verplicht, zoals de procedure documentatiebeheer en de procedures voor correctieve en preventieve maatregelen. De nieuwe versie schrijft geen enkel document meer dwingend voor. Overal waar een proces beschreven wordt staat nu dat er bewijs moet zijn van een werkend proces in de vorm van 'documented information'. Een voorbeeld: in ISO27001:2005 stond dat er een verslag van de risicoanalyse getoond moet kunnen worden, ISO27001:2013 zegt "The organization shall retain documented information about the information security risk assessment process". Voor een auditor minder gemakkelijk want er is niet meer aan de orde om te toetsen of er simpelweg een verslag van de risicoanalyse is, maar getoetst moet worden of de organisatie voldoende kan aantonen dat er een proces voor risicobeoordeling is. Het proces is belangrijk; de vorm van de output van het proces minder.
- De in ISO27001:2005 genoemde (verplichte) procedure voor preventieve actie is komen te vervallen; preventief met informatiebeveiliging bezig zijn is nu vervat in "Actions to address risks and opportunities" in het planningsproces.
- De tekst is veel compacter geworden; het aantal bladzijden gewijd aan het ISMS is ongeveer gelijk gebleven (9) maar de tekst is abstracter en nog meer "principle-based" geworden.
- De focus van informatiebeveiliging voor ISO27001:2013 is sterk gericht op bescherming van informatie, en niet of minder op bescherming van kapitaalgoederen ("assets"). ISO27001:2005 legde bij de risicoanalyse veel nadruk op dreigingen en kwetsbaarheden verbonden aan assets. Die inventarisatie vergde altijd veel tijd en moeite en leverde niet altijd veel op. ISO27001:2013 legt de nadruk op bescherming van informatie. De risicoanalyse kan zich dus op een hoger niveau afspelen en wordt naar mening van de auteur meer een business impact analyse, waarbij de koppeling tussen risico en maatregel veel meer bij de implementatie gemaakt zal worden en niet tijdens de risicobeoordeling.
- De maatregelen in Annex A. worden niet meer dwingend voorgeschreven. In ISO27001:2005 werd na de risicoanalyse voorgeschreven dat de organisatie voor het reduceren van risico's een keuze moest maken uit de (133) maatregelen in Annex A. In de nieuwe ISO27001:2013 mag de organisatie maatregelen selecteren voor risicoreductie uit elke maatregelenset die zij wenst te gebruiken. Dus bijvoorbeeld het NIST handbook, of het IT Baseline Protection Manual, CobIT of dichter bij huis NEN7510. Wel is verplicht dat de organisatie Annex A. gebruikt als een checklist om na te gaan of er in de gekozen maatregelenset geen omissies zijn.
  Dus als Annex A. nuttige maatregelen noemt die niet in de gekozen maatregelenset aanwezig zijn, moet de organisatie die maatregelen uit Annex A. toevoegen aan de gekozen set. Dit betekent dat de organisatie de auditor dus moet overtuigen dat dit zorgvuldig gebeurd is. Immers; de auditor zal wellicht de gekozen maatregelenset niet kennen; het is dan aan de organisatie om te laten zien hoe die set zich verhoudt tot de eisen in Annex A.

De nieuwe hoofdstukindeling van Annex A. van ISO27001:2013:

A.5 Information security policies
A.6 Organization of information security
A.7 Human resource security
A.8 Asset management
A.9 Access control
A.10 Cryptography
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security
A.14 System acquisition, development and maintenance
A.15 Supplier relationships
A.16 Information security incident management
A.17 Information security aspects of business continuity management
A.18 Compliance

De belangrijkste wijzigingen in Annex A.

Het is een open deur dat informatietechnologie aan verandering onderhevig is. Ontwikkelingen (en de tegen onheil beschermende maatregelen) zoals toenemende (ICT-) automatisering in productieomgevingen (SCADA), bring-your-own-device en "the-internet-of-things" zouden ook hun plaats moeten krijgen in normen voor informatiebeveiliging. In essentie is er echter op het abstracte niveau waarop een wereldstandaard bruikbaar moet zijn voor elke branche, voor grote en kleine organisaties en voor elke mogelijke infrastructuur, niet zoveel veranderd. Op dat niveau houdt informatiebeveiliging zich immers nog steeds bezig met bescherming van beschikbaarheid, integriteit en exclusiviteit. En zijn de maatregelen fysiek, logisch of procedureel van aard. Daarnaast speelt de complexiteit van de genoemde ontwikkelingen in de ICT mee; de ISO organisatie zal dus – of is al gestart – aparte normen voor een aantal van de genoemde deelaspecten van het vakgebied, zoals SCADA beveiliging, ontwikkelen. ISO27001 Annex A. hoeft daarom niet allesomvattend te zijn maar vormt steeds meer slechts een baseline.
In de eerste drafts tijdens de revisie van ISO27001 werd Annex A. steeds uitgebreider. In de uiteindelijke ISO27001:2013 is Annex A. korter en bondiger geworden. Specifieke maatregelen zijn weg en belangrijke nieuwe maatregelen zijn toegevoegd. Het gevolg is drie extra hoofdstukken (nu 14 in plaats van 11) en toch minder maatregelen (nu 114 in plaats van 133).
Verdwenen zijn maatregelen zoals "Controls against mobile code" en "Input data validation" en "Information leakage". Dit waren bij implementatie altijd struikelblokken omdat de daaraan verbonden risico's niet direct duidelijk zijn.
Het hoofdstuk met maatregelen rond toegangsbeveiliging is

Dwingend voorgeschreven template voor normen voor managementsystemen

veel duidelijker geworden; weg is de tegenwoordig kunstmatige scheiding tussen toegang tot netwerk, informatiesysteem en applicatie zoals ISO27001:2005 die kende. Toegang is nu een beheerst proces geworden gebaseerd op de zakelijke eisen tot systemen en applicaties waarin gebruikers de belangrijkste rol hebben.
Van groot belang is de onderkenning dat beveiliging al bij ontwerp en bouw van informatie-systemen meegenomen moet worden. Nieuw zijn dus maatregelen voor informatiebeveiliging in projecten, de nadruk op "secure engineering principles" en beter beschreven maatregelen voor de bescherming van de ontwikkelomgeving.
Nieuw is een hoofdstuk "Supplier relationships" waarin alle maatregelen voor het omgaan met derde partijen opgenomen zijn. Niet onvermeld mag blijven dat het hoofdstuk over "Information security aspects of business continuity management" nu onderscheid maakt tussen continuïteit en beschikbaarheid. Beschikbaarheid borgen door redundantie is hierin nieuw.

Wat heeft het niet gehaald in deze revisie?

Zoals al genoemd zal een ieder die verwacht zaken als SCADA, BYOD e.d. terug te zien in deze nieuwe norm, bedrogen uitkomen. Het ISMS is beter beschreven en meer back-to-basics. De maatregelenset is vernieuwd maar al te grote wijzigingen zijn er niet. Met name had er meer nadruk op herstel van de informatiehuishouding na dataverlies kunnen liggen. De betreffende maatregel heet nog steeds "Information backup", echter backup is slechts een deel van de oplossing van het probleem "altijd kunnen restoren". Ook de verantwoordelijkheden van gebruikers in Annex A. had nog wel meer aandacht kunnen krijgen. Ook is de norm nog steeds meer gericht op ICT beveiliging dan op de bescherming van andere verschijningsvormen van informatie zoals documenten of kennis.

Gevolgen voor gecertificeerde organisaties

Zoals gebruikelijk hebben gecertificeerde organisaties enige tijd om aan deze nieuwe versie van ISO27001 te voldoen; te weten twee jaar. Dus vóór 25 september 2015 moeten alle gecertificeerde organisaties de transitie naar ISO27001:2013 gemaakt hebben om het certificaat te behouden. Tot 25 maart 2014 kunnen certification bodies nog nieuwe certificaten op de oude versie uitreiken. De audit op de transitie naar ISO27001:2013 bij bestaande organisaties zal meegenomen worden in de al geplande jaarlijkse controle-audit of de herhalingsaudit als de organisatie in 2014 of 2015 haar certificaat wenst te verlengen.
De transitie zelf zal voor organisaties betekenen dat ze

aandacht moeten besteden aan de eisen in de nieuwe hoofdstukken "Context of the organization" en "Leadership". Daarnaast zal de organisatie moeten beoordelen of de nieuwe maatregelen uit Annex A. voor haar van belang zijn en dit als zodanig verwoorden in haar Statement of Applicability (Verklaring van Toepasselijkheid). En uiteraard moet de organisatie nagaan daar waar in de nieuwe norm vermeld staat dat er "documented information" moet zijn als bewijs dat een in de norm beschreven proces bestaat of werkt, of deze gedocumenteerde informatie aanwezig is en de auditor (en het topmanagement, niet per definitie in deze volgorde) voldoende zal overtuigen van de effectiviteit van het ISMS. Door het volledig herzien van alle tekst en de herstructurering van de norm is de transitie naar ISO27001:2013 niet te onderschatten. Security managers en auditors, zowel intern als extern, zullen nog moeten wennen aan de veranderingen; de leercurve is zeker niet vlak.

De nieuwe inhoudsopgave van ISO27001:2013 met betrekking tot het ISMS:

4 Context of the organization
- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the information security management system
- 4.4 Information security management system

5 Leadership
- 5.1 Leadership and commitment
- 5.2 Policy
- 5.3 Organizational roles, responsibilities and authorities

6 Planning
- 6.1 Actions to address risks and opportunities
- 6.2 Information security objectives and planning to achieve them

7 Support
- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information

8 Operation
- 8.1 Operational planning and control
- 8.2 Information security risk assessment
- 8.3 Information security risk treatment

9 Performance evaluation
- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal audit
- 9.3 Management review

10 Improvement
- 10.1 Nonconformity and corrective action
- 10.2 Continual improvement

Referenties

- www.iso.org voor aanschaffen van de normen, onder de link naar ISO27001 op de homepage is ook alle informatie over penetratie van de norm in diverse landen en branches te vinden naar aanleiding van de in 2012 gehouden uitgebreide enquête.

- Op www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/ is een zeer uitgebreid overzicht van alle wijzigingen, de transitie etc. te downloaden.
De auteur heeft (in Excel) gedetailleerde overzichten van alle wijzigingen beschikbaar. Op verzoek per email worden deze toegezonden.

OWNED

One of the thorniest issues in information security is the matter of ownership. Who is the owner of the data/information? In SABSA this is especially important because the owner will be the person who makes policy about how that data/information should be protected, against which threats, and for exploiting which opportunities. An owner is a domain authority for all data/information within his/her span of control.

Well that sounds clear and simple, but practical matters make it much less so. One question that arises is: can it be possible for the data, information and knowledge to have different ownerships? Who owns the risk, both opportunity and threat, and can there be a conflict of interest?

For example, a digital photograph is a data set, for which the photographer owns the copyright. However, if the photograph is of a person, then that person is a 'data subject', and EU data protection laws state that data subjects are entitled to data privacy. This issue is brought into sharp focus by so-called 'paparazzi' photographers who take pictures of celebrities without the permission of the subjects. Who owns the image: the photographer or the subject of the photo? If there is more than one person in the photo then the matter becomes even less clear, because one or more of the subjects may have given the photographer permission, whereas other subjects have not. It could even be a malicious plan between the photographer and one or more subjects to compromise the reputation of one or more of the other subjects. So who owns the image now; and who can control its public disclosure?

Now let's make the example even more complex. A family is on holiday and they take many digital photos of places they visit and of family members in various locations. It is common practice to snap a picture of a family member or group standing in a public place outside a famous monument of other visitor attraction. By pure chance, and unknown to the family, one or more pictures include an image of a famous celebrity who just happens to be in the same vicinity at the same time. There are circumstances that make this an embarrassment for the celebrity, because they shouldn't really be there or shouldn't really be with the person next to them. No-one so far has any 'knowledge' of this situation. The data has been captured and information is contained in the data; information about the family, but also information about the celebrity.

Later the photograph is posted on Facebook and seen by a third party who recognises the celebrity. Now there is knowledge based on the information contained in the data set. That knowledge provides an opportunity for those with access to the photograph to blackmail, intimidate or simply ruin the reputation of the celebrity. It also poses a threat to the celebrity who has been misbehaving.

There is a conflict of interest here that is not easy to resolve. Morality is involved for each of the photograph owner, the third party with the knowledge and the celebrity whose misbehaviour has been captured. What about legality? How does copyright law interact with data protection law? Whose interests should prevail? Do the data, the information and the knowledge belong in different domains, subject to different policies, and who should determine those policies?

What this example reveals is that there is potential complexity in 'ownership' that is not easy to resolve. However, SABSA, through the application of Attributes Profiling, provides some analytical tools that will help to bring some simplicity to a complex situation. The attribute 'owned' will need some further decomposition based on sound principles. The question remains, however: what are the basic principles that should be applied in resolving such conflicts? In the days of social media and everyone with a smart photographic device in their pocket or handbag, this is an issue that society as a whole must address.

The Attributer

Op 28 oktober 2013 werd de tweede Nationale Cyber Security Strategie (NCSS 2) uitgebracht, tweeëneenhalf jaar na de eerste. De strategische focus verschuift van publiek-private samenwerking naar publiek-private participatie en strategische samenwerking. De nieuwe strategie beoogt dat Nederland qua volwassenheidsniveau op Cyber Securitygebied van bewust naar bekwaam gaat. Wat zijn de nieuwe doelstellingen en actielijnen van de NCSS 2 en wat betekent dat voor u en uw organisatie?

VERSLAG

NATIONALE CYBER SECURITY STRATEGIE 2

Van bewust naar bekwaam

Nederland internationaal gidsland met onder andere cyberdiplomatie

Bij de start van de campagne Alert Online presenteerde minister Opstelten van Veiligheid en Justitie op 28 oktober jongstleden de tweede Nationale Cyber Security Strategie, de NCSS 2 [1]. Na het uitbrengen van de eerste NCSS tweeëneenhalf jaar geleden zijn grote stappen gezet. Daarentegen is het duidelijk dat de urgentie van aandacht voor en aanpak van Cyber Security alleen maar groter geworden is [2]. Grote incidenten als de DigiNotar-affaire, de KPN hack en de denial-of-service aanvallen op Nederlandse banken, KLM en de overheid hebben dit duidelijk gemaakt.

De nieuwe nationale strategie gaat uit van de visie dat Nederland samen met haar internationale partners inzet op een veilig digitaal domein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd. Nederland heeft drie ambities die invulling moeten geven aan deze visie: (1) onze samenleving weet op een veilige manier optimaal gebruik te maken van de voordelen en kansen die cyberspace ons biedt, (2) Nederland loopt voorop op het gebied van security-by-design en privacy-by-design en (3) Nederland vormt met internationale partners een vooruitstrevende coalitie voor het beschermen van fundamentele rechten en waarden in het digitale domein, of te wel cyberspace. Voor een dergelijk brede benadering van cyberspace is het nodig om nationaal en internationaal de juiste balans te zoeken tussen veiligheid, vrijheid en de economische voordelen van cyberspace. De eerste Nationale Cyber Security Strategie uit begin 2011 had tot doel om te komen tot bewustwording over het cyberrisico. Deze strategie beoogt een nieuw volwassenheidsniveau qua Cyber Security te bereiken: die van bekwaam. Dat kan natuurlijk alleen in samenwerking met burgers, private partijen en de overheden waarbij kennisontwikkeling en -toepassing, transparantie en (zelf)regulering een grote rol spelen. Van burgers (consumenten) wordt gevraagd om minimaal een basisniveau aan cyberhygiëne te betrachten, een

Auteur: *Eric Luijf is principal consultant Cyber Operations & Critical (Information) Infrastructure Protection bij TNO.*
Eric is bereikbaar via eric.luijf@tno.nl.

eigen verantwoordelijkheid te nemen en een zekere bekwaamheid te ontwikkelen in het veilig gebruik van cybermiddelen en -diensten. Denk aan het gebruik van sterke wachtwoorden en het privé houden daarvan, het regelmatig updaten van de eigen computersystemen en het zorgvuldig beschermen van privégegevens. De overheid verwacht dat private partijen aanspreekbaar zijn op hun verantwoordelijkheid voor veilig cybergebruik. Ze hebben een zorgplicht richting burgers, andere bedrijven en overheden. Van leveranciers wordt verwacht dat zij inzetten op security-by-design en privacy-by-design. Leveranciers, systeemintegratoren en dienstenleveranciers zouden hun producten en diensten veilig 'uit de doos' moeten leveren. Dat betekent bijvoorbeeld dat standaardwachtwoorden uit den boze zijn, dat bij een initiële installatie een sterke beveiligingssituatie wordt afgedwongen en dat dienstenleveranciers zich minimaal houden aan 'good cyber security practices'. De rijksoverheid is van plan dit gedrag sterk te stimuleren.

Doelstellingen

De rijksoverheid faciliteert daarnaast uitwisseling van informatie over dreigingen en actuele incidenten. Ze zet ook de kaders uit voor nationaal beleid en internationale samenwerking. De eigen cyber security capaciteiten van de overheid - het Nationaal Cyber Security Centrum (NCSC), de politie en bij Defensie - worden daarom versterkt. De genoemde visie en ambities vertalen zich in vijf meerjarige doelstellingen:

1. **Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het cyberdomein,**
2. **Nederland pakt cybercriminaliteit aan,**
3. **Nederland investeert in veilige en privacybeschermende ICT-producten en -diensten,**
4. **Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het cyberdomein,**
5. **Nederland beschikt over voldoende cyber securitykennis en -kunde en investeert in ICT-innovatie om onze cyber securitydoelstellingen te behalen.**

Deze vijf doelstellingen zijn uitgewerkt in een actieprogramma 2014-2016 met 37 acties/actielijnen. Nieuw ten opzichte van het vorige actieprogramma is dat de 37 acties zoveel mogelijk SMART (Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden) gemaakt zijn: de acties zijn specifiek, de verantwoordelijke actiehouder(s) zijn aangewezen en er wordt een tijdsverwachting uitgesproken. Ook is aandacht besteedt aan de governance. Jaarlijks zal over de voortgang van het actieplan worden gerapporteerd aan de Tweede Kamer. Ten opzichte van de eerste NCSS wordt hiermee een grote stap vooruit gezet omdat de voortgang of het eventueel achterblijven van de acties op transparante wijze inzichtelijk worden en bijsturing kan plaatsvinden. De acties, die direct van belang zijn voor de lezers van dit blad en hun organisaties, waaronder leveranciers van (beveiligings)producten en -diensten, zijn:

1. **Een nadere aanscherping van welke ICT-afhankelijke systemen, diensten en processen vitaal zijn, een weerbaarheidverhogend programma en publiek-private oefeningen.**
2. **Het verbeteren en ontwikkelen van cyber security standaarden en good practices voor alle organisaties en het ontwikkelen van minimum veiligheidseisen voor vitale ICT-processen.**
3. **Het stimuleren van security-by-design en privacy-by-design doordat de overheid daarvoor eisen gaat opnemen in haar aanbestedingsprojecten.**
4. **Een onderzoek naar een gescheiden, veilig ICT-netwerk voor publieke en private vitale processen.**
5. **Versterking van sectorale toezichthouders door het opnemen van cyber security eisen in de regelgeving.**
6. **Het intake- en registratieproces van aangiften cybercriminaliteit bij de politie wordt versterkt.**
7. **Het instellen van een publiek-private Task Force Cyber Security Onderwijs die zich onder andere gaat richten op certificering van professionals en het verder ontwikkelen van lesmodules.**
8. **De aankondiging van nieuwe tenders 2014-2015 ter waarde van 6 miljoen euro voor cyber securityonderzoek en de mogelijkheid voor het bedrijfsleven van een cyber security 'scientist on the job'.**

Andere actiepunten betreffen onder andere cyberdiplomatie, de versterking van internationale samenwerking en versnelling van de ambities van Defensie op het gebied van cybercapaciteiten. Voor leveranciers van ICT-producten en –diensten en systeemintegratoren biedt de NCSS 2 kansen. Het bewust ontwikkelen en leveren van cyberveilige en privacybeschermende producten en -diensten kan u binnenkort een marktvoorsprong geven. Voor organisaties in vitale sectoren is er daarentegen het risico dat toezichthouders minimum beveiligingseisen gaan verplichten als zelfregulering op het cyber security gebied niet werkt.

Conclusie

Met de nieuwe Nationale Cyber Security Strategie geeft de Nederlandse overheid zowel nationaal als internationaal het signaal af dat de borging van fundamentele rechten en waarden in cyberspace en cyber security hoog op de agenda staan, maar ook dat Nederland de economische kansen die cyberspace biedt wil grijpen.

Dit artikel is eerder verschenen in Beveiliging.

Referenties

[1] Nationale Cyber Security Strategie 2 - van bewust naar bekwaam, Ministerie van Veiligheid en Justitie, oktober 2013. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/10/28/nationale-cyber-security-strategie-2.html

[2] cyber securitybeeld Nederland 3, Ministerie van Veiligheid en Justitie, juli 2013. http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/07/03/Cyber Securitybeeld-nederland.html

VERSLAG

KWALIFICATIESTELSEL VAN INFORMATIEBEVEILIGERS

Vraagt u zich wel eens af welke cursus of opleiding bijdraagt aan de volgende stap in uw ontwikkeling? Kunt u uw werkgever ervan overtuigen dat een bepaalde training of cursus toegevoegde waarde heeft voor de organisatie en dat de investering zich in enkele jaren heeft terugbetaald? Hoe zeker bent u ervan dat de opleiding van uw voorkeur goed aansluit bij uw huidige kennis, competenties en ervaring? Schat u in dat dit bij een eventuele volgende opdrachtgever of werkgever ook begrepen wordt?

Dit artikel is een vervolg op het verslag van de Werkconferentie 'Informatiebeveiligers maken werk van professionalisering' in Informatiebeveiliging nr. 5 (2013). In onderstaand artikel gaan we in op de ontwikkelingen van het project QIS (Qualification of Information Security professionals) dat op initiatief van sponsors in de publieke en de private sector in Nederland is geïnitieerd.

Er komen carrièrepaden voor informatiebeveiligers

We openen dit artikel met vier voorspellingen:

1. **Dankzij een kwalificatiestelsel duurt het niet lang meer voordat de informatiebeveiliger meer duidelijkheid krijgt over het ontwikkelpad van zijn/haar kennis en competenties.**
2. **De komende jaren komt meer duidelijkheid over carrièrepaden binnen organisaties voor informatiebeveiligers.**
3. **Gekwalificeerde informatiebeveiligers hebben binnen Europa vergelijkbare competenties waardoor het voor werkgevers makkelijker wordt het juiste personeel aan te trekken.**
4. **Opleidingsinstituten kunnen hun onderwijs beter afstemmen op behoeften van de markt en werknemers kunnen makkelijker hun kennis en kunde aantonen.**

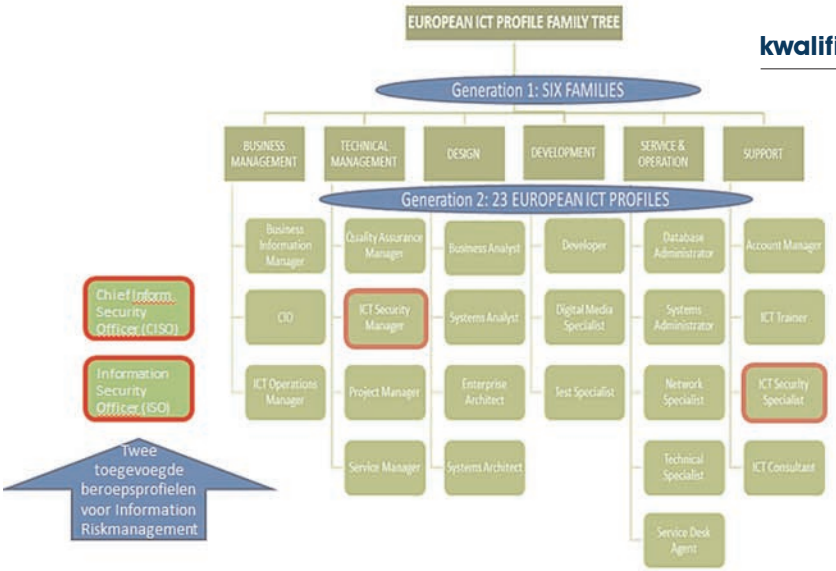
De voorspellingen betreffen zowel de ervaren professional die zich verder wil ontwikkelen, als het jonge talent op de middelbare school die moet gaan kiezen voor een inspirerende en boeiende studie. Waarom we geen harde termijnen opnemen in de voorspellingen laat zich raden: de doorlooptijd van de implementatie van functies en de inpassing in een bestaand functiehuis varieert per organisatie. Bovendien kost het tijd voordat opleidingsinstellingen geschikte curricula hebben ontwikkeld en hun eerste afgestudeerden afleveren. We verwachten wel dat voorspelling 1 eerder zal uitkomen dan voorspelling 3.

De ondertekenaars van het convenant met beide organistoren, Fred van Noord (links achter) en Marcel Spruit (rechts achter).

Er is draagvlak voor een kwalificatiestelsel

We durven deze voorspellingen te doen omdat we zien dat het draagvlak voor een kwalificatiestelsel voor informatiebeveiligers groeit. Belangrijke ontwikkeling hierbij is dat in Nederland het

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



Figuur 1 - European ICT Profile Family Tree

ministerie van Economische Zaken de implementatie van het Europese competentie framework e-CF ondersteunt via het programma Digivaardig & Digiveilig van ECP. Daarnaast stimuleert het CIO Platform Nederland de implementatie van e-CF bij haar leden, ruim 100 grote organisaties.
Op 30 mei 2013 hebben acht CIO's en CISO's (Rabobank, ING, ABN-Amro, AkzoNobel, Equens, Alliander, Eneco en UWV) het convenant [1] ondertekend waarin afspraken gemaakt zijn over kwalificatie voor functies in de informatiebeveiliging op basis van een uniform kwalificatiestelsel. Maar bovenal is in september 2013 de publiek-private samenwerking QIS [2] gestart voor de ontwikkeling van het Nederlandse kwalificatiestelsel.

De vier functies in het vakgebied

Het vakgebied informatiebeveiliging is een breed vakgebied. De beroepsvereniging Platform voor Informatiebeveiliging (PvIB) streeft naar het professionaliseren van de beroepsgroep van informatiebeveiligers en daarbij hoort een overzichtelijke en transparante situatie op het gebied van kwalificatie. Uit vooronderzoek [3] is gebleken dat het wenselijk is om onderscheid te maken tussen de domeinen information risk management (IRM) en ICT security.

Om het kwalificatiestelsel optimaal aan te laten sluiten op de dagelijkse (inter)nationale beroepspraktijk, heeft een PvIB werkgroep vier [4] beroepsprofielen gedefinieerd op basis van het European e-Competence Framework (e-CF). Het e-CF is ontwikkeld door het CEN, het Europese Standaardisatie Comité:

- **Chief Information Security Officer (CISO)**
- **Information Security Officer (ISO)**
- **ICT Security Manager**
- **ICT Security Specialist**

De beroepsprofielen worden beschreven overeenkomstig de structuur van het CEN. Omdat de CISO en ISO niet voorkomen in de CEN documentatie heeft de PvIB werkgroep een voorstel ontwikkeld voor deze twee beroepsprofielen (zie figuur 1). Verder zijn de risk en security aspecten bekeken in relatie tot de e-CF profielen voor de CIO, de Enterprise Architect en de Quality Assurance Manager. Dit heeft geleid tot aanpassingen in de 2.0 profielen van ICT Security Manager en ICT Security Specialist. Die aanpassingen zijn in overweging gegeven aan het CEN. In figuur 1 zijn de CISO en ISO toegevoegd ten opzichte van figuur 1 in CWA 16458 ICT Professional Profiles [5].

Over kwalificatie en kwalificatiestelsel

Met het grote aanbod van titels en certificaten kan de informatiebeveiliger niet goed meer duidelijk maken welke kennis en vaardigheden hij/zij heeft. Werkgevers kunnen niet zien wanneer zij een goede informatiebeveiliger voor zich hebben, of de betreffende informatiebeveiliger wellicht bijscholing nodig heeft en welke opleiding daar dan voor in aanmerking zou komen. Opleidingsinstellingen hebben daarbij geen referentiekader om investeringen in nieuwe opleidingen te rechtvaardigen.

Een kwalificatie is een formeel resultaat van een beoordelings- en validatieprocedure die wordt verworven wanneer een bevoegde instantie bepaalt dat de leerresultaten die een individu heeft bereikt, aan bepaalde normen voldoen [6]. Het beoordelings- en validatieproces is in het algemeen gebaseerd op toetsing door middel van een examen, of het beoordelen van een portfolio.
De onpartijdigheid en competentie van een kwalificatie instantie zijn niet vanzelfsprekend. Dit moet worden geborgd door een organisatie die toezicht houdt op de kwalificatie instantie. Hierbij zijn belangrijke eisen: onafhankelijkheid, objectiviteit en het ontbreken van commerciële belangen.

Een kwalificatiestelsel beschrijft de kennis en vaardigheden die gekwalificeerde informatiebeveiligers moeten bezitten. Het kwalificatiestelsel heeft drie doelgroepen:

1. **Werkgevers: zij kunnen op basis van eenduidige kwalificaties beter bepalen welke professionals passen op hun informatiebeveiligingsfuncties en hoe de carrièrepaden voor informatiebeveiligers eruit zien.**
2. **Opleidingsinstellingen: zij kunnen de gedefinieerde kwalificaties gebruiken voor het inrichten van opleidingen en bijscholingsprogramma's op het gebied van informatiebeveiliging en het stroomlijnen van de doorstroming tussen aansluitende opleidingen.**
3. **Beroepsbeoefenaren: voor professionals wordt het eenvoudiger om hun kennis en kunde aan te tonen en keuzes te maken voor hun eigen professionele ontwikkeling.**

Wat gaat QIS opleveren?

Het doel van het project QIS is het realiseren van een uniform kwalificatiestelsel voor informatiebeveiligers dat breed wordt gedragen en aansluit op:

- **De dagelijkse beroepspraktijk**
- **Bestaande buitenlandse kwalificatiestelsels op het gebied van informatiebeveiliging**
- **Het Europese e-Competence Framework (e-CF)**

Het stelsel wordt voor Nederland ontwikkeld, maar met de ambitie om deze internationaal te laten adopteren. De eindproducten worden in het Nederlands ontwikkeld en in het Engels vertaald om de afstemming op Europees niveau te optimaliseren.

In een periode van twee jaar moet nog veel werk verzet worden. De vier genoemde beroepsprofielen vormen de basis voor de eindproducten van QIS. Naast de ontwikkeling van de beroeps- en opleidingsprofielen en het opstellen van een kwalificatieschema per beroepsprofiel, worden de gangbare bestaande opleidingen geïnventariseerd zoals ISM (Haagse Hogeschool) en CISSP (ISC2) en vergeleken met de kwalificatieschema's. Om de ontwikkeling van beroepsgerichte opleidingen te stimuleren die bijdragen aan eisen uit de praktijk, worden de opgestelde kwalificatieschema's afgestemd met relevante partijen, te weten kwalificerende instellingen, beroepsorganisaties, werkgevers en opleidingsinstellingen. Verder worden de kwalificatieprocessen gedefinieerd en het kwalificatiestelsel bij een kwalificerende instantie onder beheer gebracht.

Betrekken van de beroepsgroep(en)

Zoals eerder gezegd is informatiebeveiliging een breed vakgebied en heeft ze veel raakvlakken met andere disciplines. Voor de ontwikkeling van het kwalificatiestelsel voor informatiebeveiligers wordt dan ook afgestemd met beroepsgroepen zoals Ngi-NGN, NOREA en ISACA. Dat ondersteunt de samenhang met aanpalende disciplines (ICT, Audit, Business Continuity Management, Compliance) en bevordert de profilering van de beroepsgroep.

Om tot gedragen en kwalitatief goede producten te komen wordt de beroepsgroep op velerlei wijzen betrokken bij de ontwikkeling.

1. In de PvIB werkgroep die de beroepsprofielen heeft ontwikkeld. Werkgroep leden zijn afkomstig van publieke en private organisaties.
2. Professionals met jarenlange ervaring in de CISO rol in verschillende sectoren, hebben geholpen om de CISO rol scherper te krijgen.
3. De leden van de Stuurgroep QIS betrekken de professionals in hun organisaties bij de review. Maar ook willen we graag terugkoppeling van de HRM-afdelingen.
4. Via de leden van de Klankbordgroep benaderen we tientallen organisaties voor input.
5. In maart/april organiseert PvIB een brede consultatie over de beroepsprofielen.

We verwachten dat de eerste publicatie van het concept white paper in maart zal zijn. In april wordt de eerste versie van de beroepsprofielen op basis van e-CF gepubliceerd en dan wordt gestart met de ontwikkeling van de opleidingsprofielen.

Wij houden u de komende tijd op de hoogte van de ontwikkelingen, ook via de PvIB Nieuwsbrief.

Referenties

[1]
Zie het verslag van de Werkconferentie: Informatiebeveiligers maken werk van professionalisering, Informatiebeveiliging nr.5 (2013).

[2]
QIS staat voor Qualification of Information Security professionals. Deelnemers in dit project zijn: Rabobank, ING, ABN-Amro, AkzoNobel, rijksoverheid, Cyber Security Raad, EY, ECP en PvIB. De deelnemers in de klankbordgroep zijn o.a.: VNO-NCW, CIO Platform Nederland, CIP en Alliander.

[3]
Onderzoek naar kwalificatie en certificatie van informatiebeveiligers, rapport VKA/HEC/CPNI, versie 1.0, 2011.

[4]
In het PvIB boek Functies in de informatiebeveiliging zijn ook de functies Business Information Security Architect en Information Security Architect opgenomen. De PvIB-werkgroep spant zich in om competenties van security architecten opgenomen te krijgen in het CEN-beroepsprofiel van de Enterprise Architect en de Systems Architect.

[5]
Ontleend aan CWA 16458 ICT Professional Profiles.

[6]
European Qualifications Framework, Key Terms.

NOMINATIES VOOR ARTIKEL VAN HET JAAR 2013

Van de redactie

Het wordt de zesde keer dat het PvIB een prijs uitlooft voor het artikel van het jaar. Tijdens deze jaarlijks terugkerende activiteit worden drie prijzen uitgereikt, wat de jury de ruime gelegenheid moet geven om gepaste waardering uit te spreken. De eerste prijs zal een waarde hebben 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 goede artikelen die ze ons bezorgen.

De jury is samengesteld uit drie gekozen vertegenwoordigers uit de leden. De redactie heeft een voorselectie gemaakt van twaalf artikelen, de jury zal dus flink aan het werk moeten. De jury kiest uit de voorselectie drie winnaars en onderbouwt haar keuze in een juryrapport. Dit jaar zitten in de jury:

- **Remco Bakker van CQure**
- **Lambrecht Nieuwenhuize van BNG**
- **Renato Kuiper van VKA**

Vaste rubrieken en artikelen van redactieleden dingen niet mee. De criteria die we de jury meegeven zijn ongewijzigd en van oplopend belang. De redactionele begeleiding helpt bij de eerste drie criteria. De laatste twee criteria gaan over de creatieve inbreng van de auteur en zijn dus van speciaal belang. De uitreiking van de prijzen vindt plaats tijdens de ledenvergadering en bijeenkomst op 24 april a.s.

Beoordelingscriteria:

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

Genomineerde artikelen (op chronologische volgorde):

Joosten, R, Van risicomanagement naar succes governance, IB2:4
Demarteau, A., IPv6, niet alleen een langer adres!, IB3:17
Oordt, J.W., Waarborgen continuïteit SaaS-informatiesystemen, IB5:4
Arts, T. & Elsinga, B., Security naar de boardroom, IB5:20
Baaten, D., Met patchen kun je niet winnen, wel verliezen, IB6:4
Biesheuvel, A. & Bekker, G., Europese wetgeving bescherming persoonsgegevens in de schijnwerpers, IB7:8
Elferink, M. & Kortier, M., 'Brede' meldplicht datalekken, preventie en privacy, IB7:13
Vooren, T. van, Agile in informatie- beveiligingsprojecten, IB8:13

Verantwoorde onthullingen #5

Volgende aflevering in verantwoorde onthullingen #6: *"Toen @lilaselmatani een studieboek kocht, kreeg hij er 1600".*

DONGIT EN HET DIGID DEBACLE. ETHISCH HACKEN ALS BUSINESSPLAN

De meeste ethische hackers die ik spreek doen onthullingen vanuit een mengeling van maatschappelijk belang en individuele kick. Maar vaak volgt ook een zakelijk profijt: de hacker heeft zijn kunnen getoond en kan aan de slag als penetratietester. Zo ook Wouter van Dongen. Sinds hij diverse lekken bij gemeentewebsites heeft onthuld, runt hij zijn eigen IT-securitybedrijf aan de Schipholweg in Leiden: DongIT B.V. Daarom aan hem de vraag: is ethisch hacken ook een interessant businessmodel?

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

Wouter studeerde Systems- en Networkengineering, deed daarnaast aan webontwikkeling en werkte bij het NFI en Fox-IT. En zoals zoveel hackers, haalde hij al vanaf zijn puberteit gekke dingen uit met websites. "Het is de drive om zaken te manipuleren, terwijl ik niet altijd wist wat ik aan het doen was," aldus Wouter. Maar, hij heeft het liever niet over zijn jeugdzonden, hij is nu een serieus bedrijf. Die loopbaan begon in 2011 dankzij een kennis die bij een gemeente werkte en net een nieuwe site had. Welke gemeente dan? Dat zegt hij niet. Een van zijn ethische codes is namelijk: noem geen bedrijven of overheidsorganisaties bij naam. "Het gaat mij er niet om mensen of organisaties zwart te maken. Ik wil laten zien dat iedereen fouten maakt en ik vind het belangrijk dat mensen er van leren zodat de digitale veiligheid stap voor stap wordt verbeterd. Dat is mijn doel."

OK, gemeente X had dus een nieuwe site. De kennis was er erg enthousiast over. Totdat Wouter liet zien dat hij binnen een half uur overal bij kon. Hij deed een SQL-

injectie op een zelfgemaakte extensie, kon inloggen bij de backend en kwam zo in allerlei mailsystemen en databases. Hij zag ook dat het Content Management Systeem – waarvan hij de naam ook liever niet noemt - allerlei onveilige default instellingen had: wachtwoorden in platte tekst, geen secure cookies, etc. De gemeente zat toevallig in een gebruikersvereniging van nog veertig gemeenten die hetzelfde systeem gebruikten. De vereniging vroeg Wouter of hij een presentatie over webbeveiliging wilde houden om meer bewustwording te creëren onder de gemeenten.

Dat was een mooie gelegenheid om zijn kunnen te tonen. In overleg met de gebruikersvereniging kreeg Wouter toestemming om praktische voorbeelden bij de aangesloten gemeenten te zoeken voor de presentatie. "Geen saai theoretisch verhaal over beveiliging, maar mensen confronteren, wakker schudden en een oplossing bieden." Wouter schreef een script dat automatisch alle gemeenten testte op de gevonden zwakheden. Hij bracht alle websystemen in kaart, ook verborgen systemen, testsystemen en welke databases, services en versies erop draaiden.

Zo kreeg hij toegang tot de backend van tientallen CMS'en, mailsystemen en honderden databases van raadsinformatiesystemen en gemeentewinkels. En duizenden persoonsgegevens van burgers met wachtwoorden. Bij sommige sites kon hij zelfs DigiD sessies overnemen middels Cross Site Scripting (XSS) en het afvangen van cookies. Dit alles kostte hem nog geen week werk. "Het is best leuk om zo'n script te schrijven, maar waarom doen ze dat niet centraal voor gemeenten, bijvoorbeeld via de VNG?"

Zijn presentatie voor de gemeente was op 29 september. In de aanloop daar naartoe werd hij al diverse keren benaderd door gemeenten die wilden checken of ze genoemd zouden worden. Een leverancier van gemeentelijke systemen en een gemeente stuurden zelfs advocaten op hem af. Hij ging daarom voorzichtig te werk. Hij had veel screenshots van kwetsbaarheden, maar zorgde ervoor dat de namen van gemeenten, systemen en gebruikers niet te lezen waren. En hun wachtwoorden waren natuurlijk ook geblurd.

Het verhaal viel goed. "De sfeer kwam meteen los. Het publiek was geboeid en stelde goede vragen." Wouter liet ook zien welke standaardinstellingen in hun CMS ervoor zorgen dat de wachtwoorden makkelijk te kraken zijn. Hoe hij de DigiD sessies kon onderscheppen, begrepen ze echter niet helemaal. Hij kreeg daarom veel vragen van de gemeentelijke systeembeheerders of hij hun ook even wilde doorlichten. Tevreden ging Wouter naar huis.

Wouter was ondertussen ook benaderd door journalisten, onder andere van Nieuwsuur. De uitzending van 1 oktober begint met onheilspellende muziek. De voice-over zegt: "Wouter van Dongen is veiligheidsexpert en dringt binnen op een gemeentewebsite. Hij gebruikt Cross Site Scripting" [1]. Hij wilde niet zeggen welke gemeente, maar de journalist weet te vertellen dat het gaat om Amsterdam en dat het past in een lange reeks ICT-blunders bij de overheid. Zelfs Diginotar wordt erbij gehaald.

Vervolgens komt journalist Brenno de Winter in beeld: "Het blijkt dat er zoveel privacygevoelige informatie wordt gelekt, dat we elke dag wel kunnen vullen met een voorbeeld. En dat gaan we komende maand ook eens doen." Hij had al eerder contact met Wouter en zijn bevindingen waren een mooie start van Lektober, waarin Webwereld een maand lang elke dag een lek meldde. Lek 1: "Blunder Logius maakt DigiD fraude kinderspel" [2].

Logius is de Dienst Digitale Overheid van Binnenlandse Zaken, oftewel de IT-ers achter DigiD. Die waren uiteraard niet blij met de beschuldiging en namen direct contact op met Wouter. Of hij zijn bevindingen over kwetsbaarheden bij gemeentesites ook daar wilde presenteren. "Als je techneut bent is XSS niet zo moeilijk, maar ik las daar in de implementatierichtlijnen van DigiD niks over. Dus ik had wat tips over HttpOnly cookies, de webserverinstellingen en vulnerabilityscans enzo. Ik was ook wel verbaasd dat ze allemaal druk zaten te schrijven, want wat ik liet zien was toch echt laag hangend fruit."

Als ik Logius mijn stuk toestuur, krijg ik de volgende reactie. "De fout lag bij de webdiensten van de gemeenten en niet bij DigiD. Dit is in een gesprek op 5 oktober bij Logius bevestigd door DongIT. Nadat een burger met zijn DigiD is ingelogd kon door de lekken aan de kant van de gemeenten de opgebouwde sessie van de webdienst met de burger worden overgenomen." Bovendien vinden ze dat Logius niet verantwoordelijk is voor de beveiliging van webdiensten die op DigiD aansluiten. "De dienstaanbieder blijft altijd zelf verantwoordelijk voor de veilige en correcte werking van de systemen die op DigiD aansluiten. De implementatierichtlijn (Checklist Testen) is niet bedoeld als norm voor informatiebeveiliging." Niettemin nam de dienst destijds direct actie: 30 gemeenten die onvoldoende beveiligd bleken, werden afgesloten van DigiD.

De kwestie liep zelfs hoog op in de Tweede Kamer. Kamerleden eisten ingrijpen van de minister van Binnenlandse zaken. Donner en later ook zijn opvolger Spies kwamen met maatregelen. De minister verplichtte de gemeenten een ICT-

24% van alle gedetecteerde gemeentelijke systemen kan mogelijk beïnvloed worden door de kwetsbaarheden met een hoge of kritische impact rating. De verouderde software op deze systemen zou relatief eenvoudig misbruikt kunnen worden door kwaadwillenden.

Beveiligingsassessment DigiD te doen, compleet met een audit en penetratietest per aanwezige DigiD-koppeling. Het Kwaliteits Instituut Nederlandse Gemeenten kreeg opdracht een impactanalyse uit te voeren bij de gemeenten. Samen met de VNG richtte het instituut een Informatiebeveiligingsdienst (IBD) voor gemeenten op, dat per 1 januari 2013 van start ging [3].

Tegen die tijd vindt Wouter het een goed moment om te kijken hoe het ervoor staat bij de gemeenten en hij laat zijn scan over alle gemeentesites gaan. Hij concludeert: "24% van alle gedetecteerde gemeentelijke systemen kan mogelijk beïnvloed worden door de kwetsbaarheden met een hoge of kritische impact rating. De verouderde software op deze systemen zou relatief eenvoudig misbruikt kunnen worden door kwaadwillenden. Het onderzoek toont aan dat de huidige inspanningen om gemeentelijke systemen te beveiligen nog niet afdoende effect hebben gehad" [4]. IBD neemt de melding uiterst serieus, gaat er meteen mee aan de slag, al komen ze naar eigen zeggen tot een iets gematigder conclusie.

Aldus, er is nog veel werk te verrichten bij de gemeenten, maar de bewustwording en zelfs verplichting om meer aan digitale veiligheid te doen is er. Mede dankzij de vrijwillige inzet van DongIT. Maar, is ethisch hacken voor hen nu wel een interessant businessmodel? Eigenlijk niet. Hij werd naar aanleiding van onderzoeken en publiciteit wel vaak benaderd door gemeenten. Dan wilden ze weten of hij ook bij hun lekken hadden gevonden. Vaak wordt er negatief en defensief gereageerd op hun bevindingen. "En dat terwijl de aangetoonde kwetsbaarheden juist behulpzaam zijn bij het verbeteren van de digitale veiligheid van gemeenten en de overheid als geheel." Al met al heeft de hele zaak hem vooral veel tijd gekost, af en toe enkele zorgen opgeleverd, maar ook een leerzame start-up van zijn bedrijf gegeven.

Wouters personeel richt zich nu vooral op bedrijven. Naast veilige webontwikkeling en uitgebreide pentests biedt hij ook gratis scans aan waarvan het rapport en de details achteraf gekocht kunnen worden. En dat loopt goed. Gemeenten zijn weliswaar verplicht security audits te doen, maar die "worden ingepalmd door het sales apparaat van de grotere partijen, die zetten dan voor veel geld een net afgestudeerde HBO'er aan het pentesten", aldus Wouter. Die consultants noemen zich vaak ethisch hacker. Maar zo heel erg ethisch is dit eigenlijk niet, want het gaat toch vooral om het binnenhalen van projecten. Kortom, van echt ethisch hacken word je niet rijk, maar het is wel leerzaam.

Bronnen

Deze tekst is gebaseerd op een interview met Wouter van Dongen 10 oktober 2013 en e-mail correspondentie met Sonja Kok van KING en Michiel Groeneveld van Logius.

Links

[1] http://nieuwsuur.nl/video/277858-kunnen-hackers-de-overheid-helpen.html

[2] http://webwereld.nl/beveiliging/54887-lek1-blunder-logius-maakt-digid-fraude-kinderspel

[3] http://www.ibdgemeenten.nl

[4] https://www.dongit.nl/softwareversies-van-gemeentelijke-websystemen-kaart-gebracht

VERSLAG

EEN BLOEIEND PRIVACY PLATFORM

COMPUTERS PRIVACY & DATA PROTECTION 2014

Het jaarlijkse CPDP congres in Brussel geeft een fantastisch inzicht in het krachtenveld en de achtergronden van het privacydenken in Europa. Het is het speelveld van juristen, politici, privacy waakhonden en consumenten-organisaties. De 7e editie werd gehouden in Brussel op 22, 23 en 24 januari 2014 en stond uiteraard in het teken van de turbulente ontwikkelingen rond de nieuwe Europese privacy regelgeving en de houding van de EU ten opzichte van het NSA PRISM programma.

Voor een visueel ingesteld iemand als ik is het even wennen op de conferentie. De orale cultuur overheerst. Veel woorden, weinig sheets [1, 2]. In 60 panels werden standpunten van verschillende kanten belicht. Dat format blijkt goed te werken voor dit onderwerp. Dit jaar waren er 841 deelnemers, waarvan 343 ook spreker was. Vanuit Nederland werd vooral deelgenomen en bijgedragen door universiteiten en leden van het Europese Parlement, ook Bits of Freedom nam actief deel.

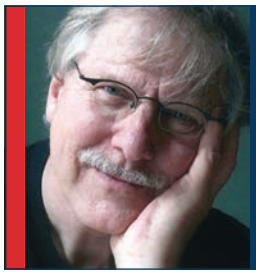
De Europese Commissie en het Europese Parlement hebben een turbulent jaar achter de rug. De conferentie weerspiegelde dit. Zo speelden er de gesprekken met de VS over het afluisteren door de NSA, de Europese parlementaire enquête betreffende Snowden en de behandeling van de nieuwe privacy regelgeving.

Europese privacy regelgeving

In januari 2013 publiceerde de Europese Commissie, voorstellen voor nieuwe regels. Bestaande uit twee onderdelen:

- **General Data Protection Regulation**
  Een Regulation (Nederlands: verordening) die direct verplicht wordt voor alle EU-landen zonder eerst omgezet te worden in nationale wetten. Deze verordening zou dan in de plaats komen voor onze Wet op de Bescherming van Persoonsgegevens.
- **Police and Criminal Justice Directive**
  Een Directive (Nederlands: richtlijn) die in de EU-landen moet worden omgezet in nationale wetten. In ons land komt dat vooral aan de orde bij een herziening van de Wet op de Politie Gegevens.

Opgemerkt zij dat regelgeving voor inlichtingen en veiligheidsdiensten hiermee niet is gedekt. Er is wel een beginnende discussie of de EU hier een rol zou moeten hebben.



Jan Mendrik CISSP is adviseur informatiebeveiliging. De laatste jaren werkte Jan bij het ministerie van VenJ en het ministerie van BZK met bijdragen aan de Baseline Informatiebeveiliging Rijk en met ondersteuning van de invoering daarvan. Jan is momenteel met pensioen, maar nog regelmatig actief op het terrein van informatiebeveiliging. Hij is te bereiken via jmendrik@gmail.com of @jmendrik

Op de conferentie werden twee nieuwe handleidingen van de EU gepresenteerd. Een algemene handleiding bij de huidige privacyregelgeving en een handleiding voor klachtafhandeling voor privacybescherming: "Handbook on European dataprotection law" en "Access to data protection remedies in EU member states". Beide zijn elektronisch beschikbaar op de site van de EU Agency for Fundamental Rights [3].

Verschillende landen willen de verplichtende Europese Regulation niet

De conceptteksten leidden tot meer dan 4000 amendementen die werden behandeld in de LIBE-commissie die bestaat uit zo'n 60 leden van het Europese parlement. Jan Philipp Albrecht was de rapporteur kreeg op de CPDP een prijs voor het monnikenwerk dat hij heeft verricht om de amendementen om te zetten in tekstwijzigingen. Uiteindelijk stemde de LIBE-commissie in oktober 2013 in met de gewijzigde teksten. Groot was echter de teleurstelling toen in december 2013 de Europese raad van ministers het niet eens kon worden. De Regulation en Directive zijn nu in een onderhandelingsfase tussen het Europese parlement (LIBE-commissie), de Europese Commissie en de Europese Raad van Ministers. De hoop is dat er eind 2014 overeenstemming zal zijn bereikt.

In de CPDP conferentie werd meestal gepraat over de Regulation en slechts af en toe over de Directive. Paul Nemitz, van het DG Justice van de Europese Commissie, maakte helder duidelijk dat de onenigheid van de Europese ministers te overkomen moet zijn. Het is een kwestie van politieke wil. Maar daar legde hij wel de vinger op de zere plek. Zo willen het Verenigd Koninkrijk (VK), Denemarken en Zweden die verplichtende Europese Regulation niet. Zij willen veel liever vrijheid houden voor eigen wetgeving.

Veel invalshoeken rond de regelgeving

Prof. Sieber van het Max-Planck-Instituut [4] gaf een heldere analyse over de behandeling van gegevens, afhankelijk van de verschillende doelstellingen. Eén van de aspecten: in Europa vinden we in het algemeen dat gegevens die verzameld worden door inlichtingendiensten strikt gescheiden moeten worden gehouden van de persoonsgegevens die de overheid gebruikt voor opsporing of administratieve taken. Opsporingsdiensten hebben een hoge standaard als het om bewijs gaat, bij inlichtingendiensten is dat minder. In de VS bestaat die scheiding in veel mindere mate dan in de EU. Een zorg is dat de EU het onderling niet altijd eens is. Het VK ziet vaak meer in het Amerikaanse standpunt.

In veel discussies kwam overigens de afwijkende blik van het VK aan de orde. Zo ziet het VK niet het nut van regelgeving voor profiling, en wil zij zich niet achter één Europese wetgeving scharen, terwijl het uitgangspunt is om een Regulation te maken en geen Directive. Het VK wordt door de andere Europese landen ook kritisch bekeken vanwege hun afluisterprogramma dat erg op het Amerikaanse PRISM lijkt.

Achtergronden

In de panels werden veel onderwerpen uitgediept. Bijvoorbeeld het punt van de klachtenbehandeling. Toegang voor gebruikers moet laagdrempelig en gratis zijn. De vraag is daarbij of altijd de nationale Data Privacy Agencies (zoals in Nederland het College Bescherming Persoonsgegevens) het aanspreekpunt moeten zijn. Kan dat misschien beter gecentraliseerd worden of moet er een tussenvorm komen?

Bij de discussies bleek veelvuldig dat principes die in de

Veel betrokkenheid en optimisme over privacy in Europa

Regulation en de Directive zijn beschreven nog niet op alle punten volstrekt eenduidig uitlegbaar zijn. Dat geldt bijvoorbeeld voor de regels rond pseudodata, profiling, mass surveillance, consent, the right to be forgotten en data retention.

Veel specialistische onderwerpen werden in aparte sessies behandeld. Zoals privacy by design, impact assessments (privacy, technology), behandeling van medische gegevens, privacy op de werkplek, automatic numberplate regognition, biometrie, smart metering, plaatsbepaling met mobiele media, privacy en de cloud.

Interessant was een sessie die ging over auditlogs en accountability in the cloud. Het is een lastig gebied. Standaarden ontbreken, de schaalgrootte is een uitdaging, de retention period is verschillend voor verschillende gegevens. Audit logs zijn een belangrijk hulpmiddel voor controles op uitbesteedde diensten (accountability in the cloud). Een mooi Europees programma dat hier waardevol werk levert is het Cloud Accountability Project [5].

Europese houding ten opzichte van PRISM

Het vuurwerk met betrekking tot de NSA afluisterpraktijken en de reactie van de EU was geprogrammeerd voor de laatste middag, als hoogtepunt van de conferentie. Paul Nemitz verwoordde het standpunt van de Europese Commissie: Obama heeft in zijn speech van 17 januari 2014 de opening gegeven voor een begin van vertrouwen. Dat is een basis voor verdere onderhandelingen met de VS. Het is hoopvol dat Obama heeft verklaard dat de bescherming van privacy niet alleen voor Amerikanen moet gelden, maar ook voor buitenlanders. Een in het panel deelnemend lid van de Obama-commissie, Peter Swire, haastte zich om te stellen dat dit voor Amerikaanse begrippen een ongehoord en revolutionair standpunt is. Twijfels waren er ook, want in dezelfde sessie schoot privacy advocate Caspar Bowden m.b.t. de privacy van buitenlanders een aantal gaten in het de teksten van de Obama-commissie. We zijn er dan ook nog niet. Ook een goede safe harbour regeling, die moet garanderen dat Europese data veilig zijn bij Amerikaanse bedrijven, moet nog vorm krijgen. De huidige regeling heeft bewezen niet voldoende te werken.
Viviane Reding stelde zich duidelijk op, op de European Privacy Day, kort na de CPDP:

"A message to our American friends. Data Protection rules should apply irrespective of the nationality of the person concerned. Applying different standards to nationals and non-nationals makes no sense in view of the open nature of the internet" en
"… it is essential these announcements are followed up by legislative action before the summer."

In het geheel waren er lovende woorden voor de resultaten van de Obama-commissie. De commissie heeft, ook in de ogen van Europeanen, 46 goede en relevante voorstellen gedaan waarvan 2/3 direct wordt ingevoerd.

Tot slot

De conferentie liet een beeld achter van veel betrokkenheid en uiteindelijk ook optimisme over privacy in Europa. De bevlogenheid van vertegenwoordigers van de Europese Commissie, zoals Paul Nemitz en op de European Privacy Day ook Viviane Reding was aanstekelijk. Graag wat meer daarvan bij onze eigen Nederlandse politici!

De CPDP in 2015 is van 21 tot 23 januari [6].

Referenties

[1]
De sheets, voor zover aanwezig, verschijnen op: http://www.cpdpconferences.org

[2]
Gestreamde lezingen: http://www.youtube.com/user/CPDPConferences

[3]
European Union Agency for Fundamental Rights: http://fra.europa.eu/en

[4]
Prof. Sieber van het Max-Planck-Institut: http://www.mpicc.de/ww/en/pub/home/sieber.htm

[5]
Cloud Accountability Project: http://www.a4cloud.eu

[6]
CPDP2015: http://www.cpdpconferences.org/Callforpanels.html, op Twitter: #EUdataP; #CPDP2014; #CPDP2015

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

BEWAARPLICHT TELECOMDATA NOG WEL VAN DEZE TIJD?

De advocaat-generaal van het Europese Hof van Justitie zegt dat het in strijd is met grondrechten. Door cruciale mankementen in de wetgeving, zoals het ontbreken van privacywaarborgen kan er geen sprake zijn van legitimiteit stelt hij. Burgerrechten-organisaties laten al jaren van zich horen: de effectiviteit wordt niet onderzocht en de noodzaak is nimmer aangetoond. En als klap op de vuurpijl toonde Brenno onlangs aan hoe makkelijk het is om middels spoofing de data te manipuleren. Is de bewaarplicht telecomdata eigenlijk nog wel van deze tijd?

Rachel Marbus

U verwacht nu natuurlijk, van mij als burgerrechten-fundamentalist, een vlammend betoog tegen de bewaarplicht telecomdata. Dat krijgt u niet. Niet omdat ik er niet tegen ben hoor, maar vooral omdat ik vind dat we het eens ergens anders over moeten hebben.

Als wij veiligheid en de strijd tegen terrorisme nu echt zo belangrijk vinden, waarom beginnen we dan niet eens bij het begin? Geef mij minstens één (liever meer) goed, onafhankelijk wetenschappelijk onderzoek naar het werkelijk verhogen van de veiligheid van burgers. Welke middelen dragen nu echt daaraan bij? En laten wij dan, met de uitkomsten daarvan in de hand, bekijken wat we in de praktijk kunnen doen. Laten wij dan ook gaan wegen. En dan bedoel ik echt wegen, niet middels valse "u wilt toch allemaal een veiligere wereld?" retoriek of "de overheid is de facto een enorme schender van burgerrechten" statements. De uitkomsten, de middelen en methodes tegenover de grondrechten van burgers. Dat in een publiek debat waar de vraag "in wat voor soort maatschappij willen wij leven?" voorop moet staan. Laten wij dat transparant en onbevooroordeeld doen zonder ons te verschuilen achter de veilige linie van ofwel Staatsveiligheid ofwel Burgerrechten.


Lex Borger


Maarten Hartsuijker


Rachel Marbus


André Koot

Maarten Hartsuijker

Mijn oma wist het al: wie wat bewaart die heeft wat. Maar als spiedende ogen ons continue in de gaten houden, vinden we dan nog steeds dat dit gezegde op gaat? Ik denk dat niemand zal ontkennen dat er uit de steeds verder groeiende berg met data een hoop informatie te halen valt. Dat het kan helpen om de kans op terrorisme te verkleinen, misdaden op te lossen en fraude tegen te gaan. Ik zou zelfs nog wel zo ver willen gaan te beweren dat de meeste ambtenaren met de allerbeste intenties aan het datagraaien geslagen zijn. Gewoon, omdat het kan en omdat het, gevoed door slimme IT-marketeers, de beste manier lijkt om het overheidsapparaat nog effectiever te maken. Je zou het een dataverslaving kunnen noemen. We hebben er steeds meer van nodig om aan een niet te verzadigen behoefte te voldoen. Maar wat is eigenlijk de kwaliteit van al deze gegevens? En wat is het effect van datamisbruik op de kwaliteit van onze samenleving?

Iedereen die wel eens een intrusion detection systeem op zijn netwerk heeft geplaatst of zijn systeemlogs in debugging modus heeft geplaatst weet het: bij grote hoeveelheden data komen onvermijdelijk ook false positives en false negatives kijken. Niet elk alarm is een incident. En het is erg makkelijk (en soms verleidelijk) om aan een bepaalde set met gebeurtenissen de verkeerde conclusie te verbinden (zo: case closed).

De wijze waarop telefoniegegevens worden opgeslagen toont maar weer eens pijnlijk aan hoe onbetrouwbaar logberichten kunnen zijn. Terwijl al jaren bekend is dat Caller-ID's gespoofd kunnen worden werd er in de wijze van loggen van telefoniegegevens geen rekening met de integriteit van de bron gehouden. Toch werden deze logs door de rechters als bewijsmateriaal geaccepteerd. Hopelijk leiden dit soort incidenten ertoe dat er weer eens goed wordt gekeken naar het nut van onze verzameldrift en de onweerlegbaarheid en feitelijke bruikbaarheid van onze dataverzamelingen.

Lex Borger

Bewaarplicht is een maatregel. En wat ik altijd stel bij een maatregel is dat we ons bewust moeten zijn van drie zaken: (1) wat is het risico dat hiermee afgedekt wordt; (2) wat introduceren we met de maatregel aan extra werk, problemen, aandachtspunten; en (3) is de maatregel in balans met het risico, qua effectiviteit en efficiëntie.

Basaal kom ik tot een risico-omschrijving dat er in onze samenleving criminele en terroristische activiteiten uitgevoerd worden. De maatregel geeft nogal wat extra werk dat voor rekening komt van de telecomproviders en waar een risico bij geïntroduceerd wordt dat gevoelige informatie 'op straat' komt te liggen.

Is de maatregel dan in balans? Die vraag is eigenlijk alleen te beantwoorden met inzicht in hoeveel criminaliteit en terrorisme voorkomen of opgelost is (mede) met behulp van de bewaarde informatie. Hier is heel weinig informatie of zelfs discussie over te vinden. Dit past in het beeld van een overheid met een honger naar big data. Gegeven het feit dat informatie technologisch te vergaren is, kiezen we er snel voor om het dan ook te eisen. Laten we die balans nou eens meenemen in de evaluatie. Dan komen we volgens mij snel tot een heel ander evenwicht.

André Koot

Nee, natuurlijk hebben we niets tegen het bestrijden van terrorisme. En natuurlijk zijn we bereid om mee te werken om ons land veilig te houden. Maar of bewaarplicht nou het antwoord is op de vraag hoe we terrorisme moeten bestrijden? Voor mij is het simpel, het antwoord is nee. Heel erg nee.

De belangrijkste reden is dat er echt wel eens een terrorist of, laten we het ruimer zien, een pedofiel gepakt is. Echter nog niet dankzij de bewaarplicht. Dat zou ook heel vreemd zijn, want waar zou je op moeten zoeken? Welk communicatiegedrag onderscheidt een terrorist van andere mensen? Als jij terrorist was, zou je dan uitsluitend met je eigen vaste pc op cyberspace rondhangen? Bellen met je eigen abonnement? Natuurlijk niet, je zou gebruik maken van tor-achtige netwerken, van prepaid mobieltjes, van eigen fora en je zou vooral heel mobiel zijn. En ook al moet een provider alles vastleggen, het profilen van zo'n doelwit zal dan niet werken.

Het zal dus niet werken voor de doelgroep die je op het oog hebt. Maar ik maak thuis wel altijd van dezelfde kanalen gebruik, dus mijn gedrag ligt wel aardig vast in die databases. En volgens mij was ik geen doelwit, maar mij kunnen ze wel profilen. Beetje raar. Zou de stelling dan omgedraaid moeten worden? Mensen die niet te profilen zijn, zijn potentiële terroristen en pedofielen? Lijkt me ook niet waarschijnlijk. Nee, laat dan maar niets vastleggen. Wat er niet is, kan ook niet misbruikt worden.

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 Ideas to Interconnect) e-mail: hr@pvib.nl
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

REDACTIERAAD
Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn (Capgemini)
Ronald van Erven (Timeos Pensioendiensten)
Maarten Hartsuijker (ANWB)
André Koot (Strict)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)
Martijn Veken (SNS REAAL)

ADVERTENTIE ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
(Motivation Office Support)
T (033) 247 34 00
ibmagazine@pvib.nl

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

UITGEVER
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
e-mail: secretariaat@pvib.nl
website: www.pvib.nl

ABONNEMENTEN 2014
De abonnementsprijs in 2014 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

WINKELEN WORDT ENG

Mijn telefoon is van het merk met het afgekloven fruit: Hiervan spreekt mij, behalve een subliem fototoestel, beeldtelefoon en MP3 speler, met name de mogelijkheid van GPS heel erg aan. Waar je ook bent, de telefoon geeft het aan. Zoek op Funda naar de huizen die te koop zijn en je krijgt een opsomming van het aanbod in de buurt van jouw telefoon. Ik ga niet alle geweldige toepassingen beschrijven die ik kan gebruiken, maar eens kijken wat anderen kunnen doen met mijn locatie.
Zoals ik wellicht eerder heb aangegeven ben ik niet de enige in mijn gezin die een telefoon bezit. Mijn kinderen en mijn vrouw hebben ook zo'n smartphone. Een geweldig gezicht om acht van die apparaten naast elkaar te zien liggen. Nog leuker is het om de apparaten met elkaar te laten samenwerken. We installeren allemaal de gratis app "Zoek je vrienden" en voegen elkaar toe als vriend. Bij het openen van de app wordt de GPS geactiveerd van het toestel van je vrienden en worden geplot op een landkaart. Op die manier kun je inzien wat de locatie is van de telefoon, waarbij je aanneemt dat de eigenaar hem in de zak heeft. Geweldig, mijn vrouw kan nu op basis van mijn positie besluiten of de aardappelen aan de kook kunnen of niet.
Ook winkels vinden dit geweldig en willen mijn locatie gebruiken om de verkopen iets op te stuwen. Dit wordt niet gedaan met GPS. Kortgeleden werd bekend dat grote bedrijven als Jumbo en Dixons nu al in onze broekzakken loeren om het Wi-Fi of Bluetooth signaal uit te lezen. Zij kunnen dan het MAC-adres (de netwerkidentificatie van de telefoon) van de telefoon lezen en kunnen dan zien of die telefoon al eerder in de winkel is geweest. Ook kunnen ze zien dat ik blijkbaar weer geen keus wist te maken over welk wasmiddel in mijn winkelwagentje gestopt moest worden. Inmiddels heeft het College Bescherming Persoonsgegevens (CBP) aangegeven dat het MAC-adres als een persoonsgegeven wordt gezien en dat het gebruik van dit gegeven als ongewenst moet worden beschouwd. En dan begin ik de draad kwijt te raken. Natuurlijk is het niet netjes om zomaar een signaal af te tappen en te gebruiken voor doeleinden waarvoor ik mijn telefoon niet heb aangeschaft. Natuurlijk moet je ervoor zorgen dat er geen misbruik gemaakt wordt van gegevens die louter en alleen om technische redenen gekoppeld zijn aan een signaal dat de telefoon uitzendt. Maar ik maak me niet druk over het feit dat de Dixons een MAC-adres leest, zonder dat ze weten dat het mijn MAC-adres is. Hoe kan de Dixons de koppeling maken tussen het MAC-adres van mijn telefoon en mijzelf? Het wordt anders als ze naast mijn MAC-adres ook nog telefoonnummers, contactgegevens of mijn SMS-inbox lezen.
Maken we ons nu druk om niets? Of misschien moet ik zeggen: maakt het CPB zich druk over het feit dat de Jumbo nu weet dat mijn telefoon wel erg veel aandacht heeft voor het hondenvoer omdat hij net als vorige week alweer vijf minuten loopt te draaien om de zakken Frolic?
Ik maak me daar persoonlijk beslist niet druk om en vind het ook geen probleem dat winkels mijn koopgedrag willen analyseren. Ik kan ze natuurlijk plagen door tijdelijk bij de Jumbo even het toestel van mijn vrouw om te ruilen voor mijn toestel. Hierdoor worden alle analyses van hen in de war geschopt, want mijn vrouw winkelt anders dan ik.
U zult denken, wordt Berry gematigder? Nee hoor, ik vind de volgende keer wel een onderwerp waar ik me wel heel erg druk over maak.

Berry

Overheid &ict

www.overheid-en-ict.nl

9 en 10 april 2014
Jaarbeurs Utrecht

de brug tussen automatisering en business binnen de overheid

GESPONSORD DOOR:

Decos Information Solutions

Helpt gemeenteambtenaren Gemeente.nu

DE SLIMSTE DAGEN VOOR DE OVERHEID

Overheid & GEO

DECENTRALISATIE CONGRES

Overheid &ict

- SERIOUS AMBTENAAR
- DOOR GEMEENTEN VOOR GEMEENTEN
- REURING CAFÉ
- YOUNG POTENTIAL PROGRAMME

VRAAG NU GRATIS UW TOEGANGSBADGE AAN VIA OVERHEID-EN-ICT.NL

vnu exhibitions europe