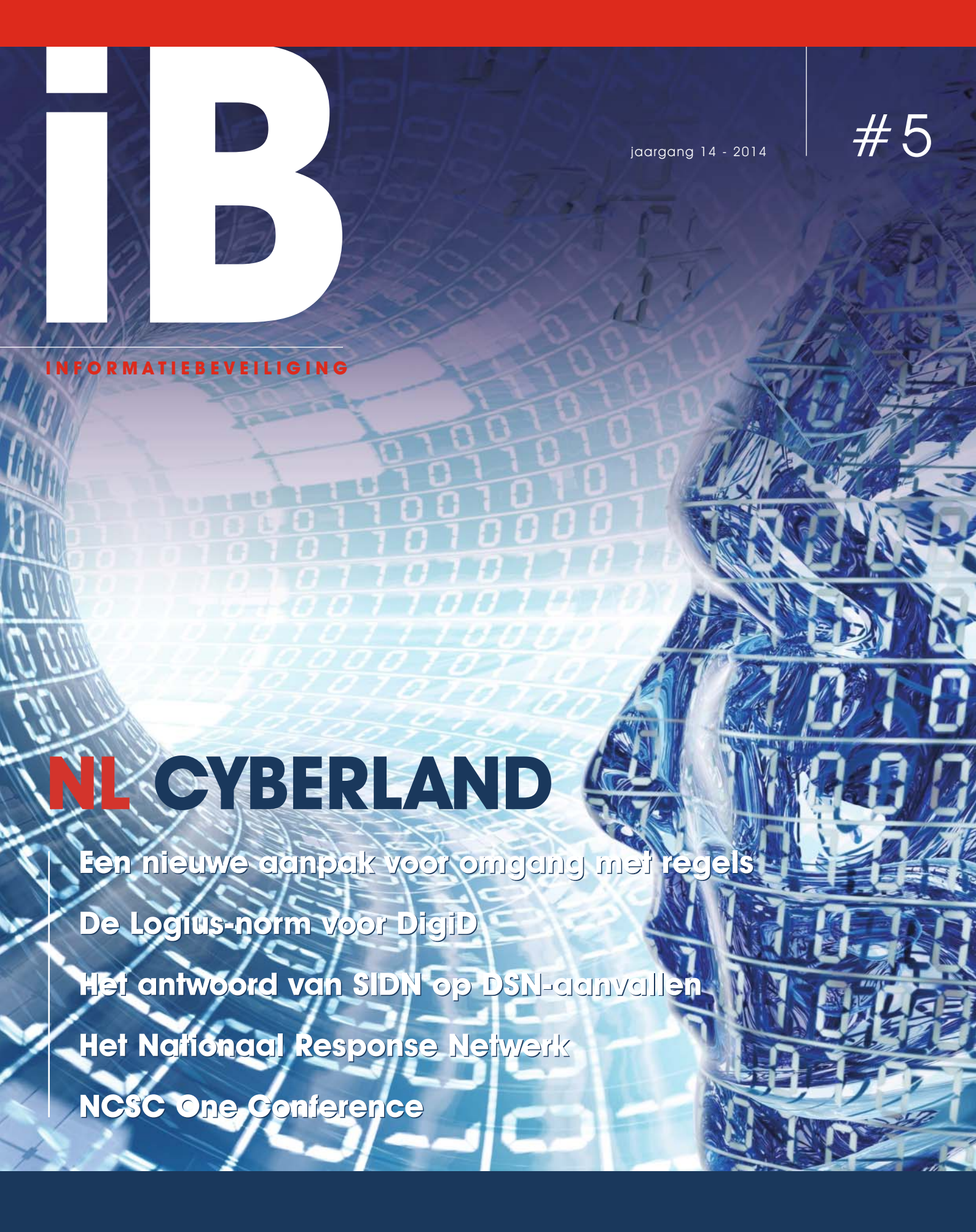
iB
INFORMATIEBEVEILIGING
jaargang 14 - 2014
#5



# NL CYBERLAND

Een nieuwe aanpak voor omgang met regels

De Logius-norm voor DigiD

Het antwoord van SIDN op DSN-aanvallen

Het Nationaal Response Netwerk

NCSC One Conference


# Ethical Hacking: Foundation – Practitioner – Specialist

***De Security Academy heeft voor zowel de beginnende als de gevorderde ethical hacker een heel mooi portfolio aan hacking opleidingen ontwikkeld.***

Bent u nieuw in de wereld van het ethical hacken of wilt u nu weleens zien en ervaren hoe een hacker te werk gaat? Dan is de **Ethical Hacking Foundation** cursus wat voor u. In 2 dagen leert u de basisprincipes van hacking en wordt ingegaan op de meest voorkomende lekken in websites en leert u deze zelfstandig te ontdekken.
Het vervolg is de **Ethical Hacking Practitioner** (niveau CEH) die naadloos aansluit op de Foundation cursus. In drie dagen wordt dieper op de stof ingegaan en wordt het scala aan hacks en aanvalsmethoden uitgebreid.
Voor de echte ethical hacker (vervolg op CEH niveau) hebben wij de **Ethical Hacking Specialist** ontwikkeld. Ook deze opleiding sluit weer naadloos aan op de voorgaande. In deze opleiding leert u niet alleen netwerken en systemen binnen te dringen, maar ook hoe u uw sporen kunt wissen en wordt dieper ingegaan op minder gebruikelijke hacks als Evil Access Points, USB infection en lockpicking.

Alle drie de opleidingen zijn sterk gericht op de praktijk. U gaat met hulp van de docent zelfstandig aan de slag om het geleerde toe te passen op doelwitten in onze Security Academy Course Environment.

**Zie www.securityacademy.nl voor meer informatie.**

## Ethical Hacking Foundation

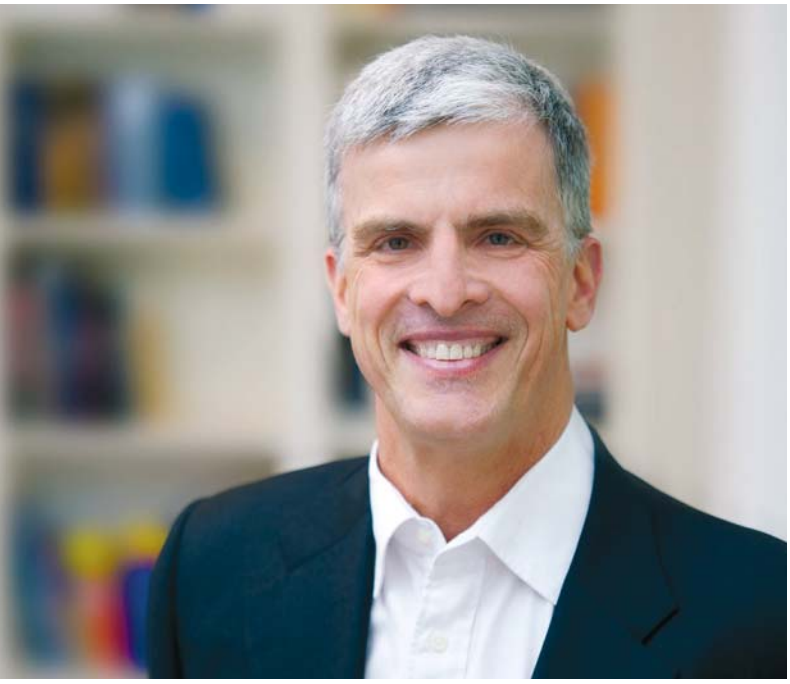
- Startdatum: 2 september
- Duur: 2 dagen
- Lestijden: 9.00 – 16.30
- Locatie: Woerden
- Prijs: € 1.100,- excl. BTW

## Ethical Hacking Practitioner

- Startdatum: 8 september
- Duur: 3 dagen
- Lestijden: 9.00 – 16.30
- Locatie: Woerden
- Prijs: € 1.990,- excl. BTW
- € 100,- korting voor PVIB leden

## Ethical Hacking Specialist

- Startdatum: 1 oktober
- Duur: 5 dagen
- Lestijden: 9.00 – 16.30
- Locatie: Woerden
- Prijs: € 3.250,- excl. BTW
- € 100,- korting voor PVIB leden



# PRIVACY ISSUES

Dat privacy-issues met de komst van web 2.0 danig veranderd zijn, wordt niet betwist. Maar ook web 1.0 heeft een aardige impact gehad op privacy. De eerste browser, de Mosaic browser, werd in januari 1993 uitgebracht. Het WWW Consortium werd in oktober 1994 opgericht. Daarvoor was er wel internet, maar niet als massa-medium.

Neem bijvoorbeeld een groot nieuwsverhaal van twintig jaar geleden, juni 1994: De moord op Nicole Brown en de daaropvolgende rechtszaak tegen O.J. Simpson. Ik heb dit toevallig van redelijk dichtbij meegemaakt. Ik woonde toen nog in California, fietste naar huis en kruiste de I-5 minder dan een half uur nadat OJ in de witte Bronco langs was gekomen. Ik wist door de hoeveelheid helicopters dat er iets heel speciaals aan de hand was, maar er was geen Twitter om even op te zoeken wat er was. De radio en TV waren onze enige nieuwsbronnen voor actuele ontwikkelingen, met de krant voor de 'diepte'-analyse.

Een aantal dagen later werd er op het strand een stille tocht en aansluitende bijeenkomst georganiseerd. Hoe kom je daar achter? Of je hoort het via-via, of via het nieuws. Wil je deelnemen, moet je alert, snel en flexibel zijn. Vandaag de dag is een oproep of Facebook voldoende om een hele menigte op de been te brengen. (Al moet ik eerlijk zijn, de radio-aandacht bij project X was olie op het vuur...)

Een ander aspect: de ouders van Nicole Brown woonden niet zo ver van ons vandaan. Wij winkelden in hetzelfde winkelcentrum. De twee kinderen van Nicole en OJ verbleven bij hen en konden ook daar gezien worden. In de winkels lagen schappen vol met kranten en roddelbladen met de meest schokkende details breed uitgemeten over de voorpagina, in een aandachtsstrijd om de lezer. In 'ons' winkelcentrum lag deze literatuur ook, maar wel weggestopt achter alles-bedekkende planken. De winkeliers konden lokaal zo zorgen voor een black-out voor de kinderen. Stel je eens voor dat je dat vandaag de dag zou willen bereiken op het internet met mobieltjes en sociale media. Ik zou niet weten hoe je dat voor elkaar zou kunnen krijgen.

Het is frappant hoe je door zo'n ingrijpend onderwerp, vastgezet in de tijd, je realiseert hoe snel de privacy-erosie is gegaan.

**Lex Borger**, hoofdredacteur

## In dit nummer

# INFORMATIEBEVEILIGING: HOE GAAN WE OM MET REGELGEVING?

Of je nu een overheidsinstelling of een bank bent, je moet je aan de regels voor privacy-bescherming en informatiebeveiliging houden. Maar hoe doe je dat? Hoe zorg je dat je door de bomen het bos ziet? Cees Zwinkels maakt zich zorgen over de Nederlandse afvinkcultuur en de uitdijende regelgeving. Hij is voorstander van een nieuwe aanpak die meer rekening houdt met de reguliere bedrijfsvoering bij de 'verantwoordelijke' en de 'bewerker'. Daarnaast vraagt hij zich af of de rol van de overheid niet moet veranderen. Blijft ze op ICT-gebied een optelsom van vele fysieke bestuursorganen, ieder met hun eigen optreden? Is de tijd niet aangebroken om de overheid te beschouwen als een multinational met rechten en plichten zoals Google?

De groei van publieke data is explosief. De nieuwe Wet Basisregistratie Personen (wet BRP) moet de beveiliging van de wettelijke persoonsgegevens in goede banen leiden. De ICT-voorschriften uit de oude wet Gemeentelijke Basisadministratie Persoonsgegevens (wet GBA) hebben grotendeels afgedaan. De reden is simpel: regelgevers kunnen de technologische veranderingen niet bijbenen. De nieuwe aanpak is die van open normen en zorgplichten. Artikel 13 van de Wet bescherming bersoonsgegevens (Wbp) is de centrale kapstok voor het beveiligen van persoonsgegevens. Artikel 13 zegt: 'U, verantwoordelijke, zult passende beveiligingsmaatregelen treffen om een passend beveiligingsniveau te waarborgen.' Aanvullend heeft de wetgever het toch niet kunnen laten om in de wet BRP nog een aantal typen beveiligingsmaatregelen op te nemen. Dat kun je lezen in artikel 6 lid 3 Besluit BRP op overheid.nl [1]. Daarnaast zijn in de wet BRP rollen en verantwoordelijkheden van betrokken partijen voor het omgaan met de normen. Centrale spelers zijn het ministerie van BZK, het agentschap BPR en de gemeenten. Zij doen -hopelijk- hun best om gevoelige wettelijke persoonsgegevens adequaat te beschermen. Dat gaat meestal goed, maar zeker niet altijd. Een bekend voorbeeld is inmiddels het SZW-rapport van 2013, waarin gemeenten ruimschoots op de vingers getikt worden voor hoe zij omgaan met informatiebeveiliging en het gebruik van het Suwinet, een systeem waarmee gemeentes onderling uitkeringsgegevens uitwisselen. Daarvoor waarschuwde Zwinkels al in augustus 2012 in het artikel 'Risico's, de persoonsgegevens', in de Automatiseringsgids [2]. Via het Suwinet raadplegen gemeenten persoonsgegevens voor de uitkeringsgerechtigden in onze samenleving uit diverse grote overheidsdatabanken zoals de Belastingdienst, het UWV, de RDW en het Kadaster.

## Categoriseren als 'persoonsgegevens'

Een belangrijk voorbeeld van open data zijn de geo-gegevens op basis van de overheidsregistraties. Deze zijn in beginsel voor iedereen beschikbaar. Denk bijvoorbeeld aan de Waardering Onroerende Zaken -de WOZ-, de BAG, de Basisregistratie Grootschalige Topografie -de BGT- en de nieuwe Wet Basisregistratie Ondergrond; de wet BRO. De uitdaging hier is om per situatie te beoordelen in hoeverre de open data het karakter krijgen van persoonsgegevens, als ze gebruikt worden om profielen van mensen op te bouwen en te onderhouden. De relevantie van het categoriseren van gegevens als persoonsgegevens is dat zij daarmee onder de bescherming van de WBP vallen. Duidelijk mag zijn dat als de datastromen gigantisch groeien, de datakoppelingen ook sterk toenemen. Via de voordeur worden data keurig beveiligd - bijvoorbeeld via de landelijke voorziening basisregistratie personen en de landelijke voorziening handelsregister-, maar via de achterdeur gebruiken overheden en bedrijven regelmatig weinig of niet-beveiligde koppelingen met bestanden binnen de eigen organisaties en daarbuiten. Niemand in Nederland heeft inmiddels nog een compleet beeld van alle datakoppelingen. Als een burger of bedrijf aan de rem wil trekken, moet hij proberen aannemelijk te maken op basis van artikel 8 van de Wet bescherming persoonsgegevens dat de balans tussen het publieke doel van de datakoppeling en de bescherming van de belangen van burgers verstoord is. Een mooi voorbeeld is de uitspraak van de Rechtbank Oost-Brabant op 26 november 2013 over de Belastingdienst versus het bedrijf SMS Parking. De rechter sprak uit dat de Belastingdienst te ruimhartig wilde beschikken over de gegevens van de online parkeerders, de klanten van SMS Parking. SMS Parking protesteerde daartegen. Het achterliggende doel van de Belastingdienst was om de zwartrijders onder leaseautobezitters op te sporen. Zou de Belastingdienst nog in beroep gaan tegen de uitspraak? Ik denk het wel. Daarmee bedoel ik niet dat de overheid zich niet ijverig moet inzetten voor fraudeonderzoek. Integendeel. Waar het om gaat, is dat men zorgvuldig met persoonsgegevens moet omgegaan. Als je bijvoorbeeld een uitkeringenbestand (bestand A) en een bestand van coffeeshophouders (bestand B) met elkaar wilt vergelijken, is het relevant dat de geautoriseerden voor bestand A geen toegang krijgen tot bestand B - en omgekeerd. Dat is ook de opvatting van de wetgever.

## Brussel

Voor mij komt de regelgeving over informatiebeveiliging inmiddels voor bijna 100 procent uit Brussel. De EU-privacyrichtlijn van 1995 wordt opgevolgd door de nieuwe verordening gegevensbescherming. De Kaderrichtlijn van 2009 gaat over hoe om te gaan met elektronische communicatienetwerken en -diensten. Ook de EU-rechters bemoeien zich met de regelgeving. Het Hof van Justitie van de EU haalde op 8 april 2014 een streep door de zogeheten dataretentierichtlijn, een richtlijn die de EU-landen in 2006 oplegde een wet te maken die de telecommaatschappijen en internetproviders verplichtte alle communicatiegegevens via telefoon of internet te bewaren voor minstens zes en maximaal 24 maanden. De verplichtingen tot de bewaring en opslag van verkeers- en locatiegegevens zijn naar de

*Cees Zwinkels is jurist en gecertificeerd public controller en docent en onderzoeker aan de Vrije Universiteit (VU) te Amsterdam, Transnational Legal Studies, Faculteit der Rechtsgeleerdheid. Cees is te bereiken via c.m.m.zwinkels@vu.nl.*

## Wet bescherming persoonsgegevens, wat is het precies?

De Wet bescherming persoonsgegevens (Wbp) beschermt privacy. In de Wbp staat wat er allemaal wel en niet mag met persoonsgegevens. En wat je rechten zijn als je gegevens gebruikt worden. Je hebt bijvoorbeeld het recht op informatie en inzage in je gegevens. En het recht op verzet tegen gebruik van je gegevens. Wat staat er nu precies in artikel 13 van die wet?
'De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.' *Bron: wetten.overheid.nl*

mening van het Hof een te grote inbreuk op ons privéleven. In Nederland staat artikel 13 Wbp centraal. Dit artikel is bijna een één op één vertaling van de EU-privacyrichtlijn en de nieuwe verordening. Omdat artikel 13 Wbp een algemeen geformuleerde zorgplicht is, hebben bedrijven en overheden standaarden voor informatiebeveiliging nodig om te weten welke beveiligings-maatregelen zij moeten treffen. Een bekend voorbeeld is de Code voor Informatiebeveiliging. Diverse sectoren -de zorgsector voorop- hanteren inmiddels specifieke codes.

### Afvinkcultuur

Naar mijn mening is het voor een doorsnee organisatie een zeer zware of zelfs onmogelijke opgave om alle maatregelen uit te voeren zoals die zijn opgenomen in de Code en in de andere standaarden. De vraag van wát geregeld moet worden en de vraag van hóe het geregeld moet worden, zijn opgenomen in dezelfde beveiligingsnormen. Bovendien lopen ze voortdurend door elkaar heen. Deze normen maken managers en gebruikers dus niet echt vrolijk. Er ontstaat een afvinkcultuur: 'Laten we alle voorschriften maar van een 'ja' en hier en daar een 'nee' voorzien.' Dat moet dan maar een keer per jaar gebeuren. Het wachten is op de goedkeuring van de externe accountant. 'De externe toezichthouders, inclusief het CBP, zijn dan tevreden.' Daar komen dan ook nog eens de door de basisregistraties en andere regelgeving verplichte audits bij. En elk incident geeft weer aanleiding tot nieuwe regelgeving. Een voorbeeld is het al een jaar geleden ingediende wetsontwerp meldplicht datalekken, een wijziging van de Wbp. Na zware kritiek heeft de minister recent gas terug moeten nemen. De meldplicht geldt nu alleen nog maar voor inbreuken met ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Daarnaast is de plicht geschrapt om binnen de eigen organisatie alle incidenten te registreren. Kritiek leveren vanaf de zijlijn is natuurlijk altijd gemakkelijk. Maar hoe zou het dan anders kunnen? Bestudering van de rapportages van het College Bescherming Persoonsgegevens leert dat het College de laatste jaren de aandacht richt op de relevante bedrijfsprocessen en ICT-oplossingen. In Zwinkels' publicatie 'Artikel 13 Wbp: Zorgplicht en informatiebeveiliging', in het juninummer van het vakblad Privacy en Informatie lees je hier meer over [3]. Dit artikel geeft een overzicht van bevindingen van het CBP. Mijn constatering is dat het College elk risico én maatregel blijft toetsen aan de voorschriften in de standaarden, uitgaande van de aangetroffen typen risico's. Dat is inderdaad conform de door het College opgestelde richtsnoeren beveiliging persoonsgegeven van 2013.

### Hechte samenwerking

Dit betekent alleen dat de hechte en dynamische samenwerking tussen ICT'ers, controllers en juristen onvoldoende van de grond komen, iets waar ik een groot voorstander van ben. De concerncontroller en/of de directeur Bedrijfsvoering moeten actief informatiebeveiliging aansturen. Dat betekent ruimte voor verbeterteams, toegespitst op privacybescherming en informatiebeveiliging. ICT'ers, controllers en juristen zoeken de zwaarste risico's uit, stellen de betrouwbaarheidseisen op en zorgen voor de uitvoer van de maatregelen, samen met gebruikers. Een voorwaarde is dat de directeur, de controller en de ICT-jurist de ICT-architectuur leren begrijpen. Risico's en maatregelen beïnvloeden de architectuur en de componenten daarbinnen. De architectuur omvat de gegevensstructuren; de databases, de ondersteunende processen, de applicaties en de infrastructuur. Daarnaast is de organisatiecultuur belangrijk voor de ondersteuning van informatiebeveiliging, want bestuur, directie, management, gebruikers en de betrokken supportafdelingen maken óf breken een stevige cultuur voor de veranderingen. Tenslotte is meten weten. Het kiezen voor drie KPI's in het eerste jaar lijkt mij nuttig. In jaar twee kunnen er drie bijkomen. In het derde jaar kunnen de KPI's van jaar één afgesloten worden bij goede meetresultaten. Deze KPI's zijn onderdeel van de afspraken tussen de 'verantwoordelijken' en de 'bewerkers' zoals die genoemd worden in artikel 13 van de Wbp. Verantwoordelijken zijn niet alleen de opdrachtgevers op managementniveau, maar ook steeds vaker de externe ICT-dienstverleners. Zij hebben zoveel kennis van zaken dat zij ook de doelstellingen en de inzet van middelen voor informatiebeveiliging bepalen en moeten erop toezien dat de bewerkers de opgedragen beveiligingsmaatregelen uitvoeren.
De toezichthouders wordt gevraagd zich per casus een beeld te vormen van de opgesomde issues: de verbeterteams (multidisciplinair), de verbeterslagen (risico's, betrouwbaarheidseisen en de maatregelen), de verdeling van rollen en verantwoordelijkheden tussen de belanghebbenden, meten is weten en de cultuur. Daarna kan nog een lichte toetsing plaatsvinden via de voorschriften in de standaarden. Bedrijven en overheden moeten zelf de vrijheid hebben welke technische en

organisatorische maatregelen zij treffen. Overigens zijn de standaarden juridisch nog niet verplicht. De toekomst kan verandering brengen als vanuit een algemene bestuursmaatregel dwingend wordt verwezen naar een specifiek beveiligingsstandaard.

## Een andere overheid

Nevenschikking -waarbij de betrokken overheid ook op verzoek schriftelijk moet communiceren naar de burger- in de algemene Wet bestuursrecht boet snel in aan betekenis. Nieuwe wetten schrijven steeds meer digitale dienstverlening en bedrijfsvoering voor. De ontstane blauwdruk is die van een netwerk van landelijke databases die via sectorale knooppunten nationaal en internationaal gekoppeld worden. De belangrijkste aandachtsgebieden zijn persoonsgegevens, geo-gegevens, zorggegevens, onderwijsgegevens en justitiële gegevens. Daarnaast zijn er publieke partijen die de kwaliteit van de gegevens moeten onderhouden; de bronhouders. Een voorbeeld zijn gemeenten en Kamers van Koophandel die ook nog eens afnemers zijn. De informatiebeveiliging moet zich gaan toespitsen op de landelijke voorzieningen, inclusief de toegang tot de gegevens en de verbindingen tussen de databases. Daarnaast moeten bronhouders de kwaliteit van de aangeleverde gegevens waarborgen. Dat is de vraag naar bijvoorbeeld goede toegangsbeveiliging.

## Eén exploitatiebedrijf

Hoe moet dit groeiende netwerk van landelijke voorzieningen beheerd worden? Naar mijn mening moeten we in ons kleine land de weg inslaan van één exploitatiebedrijf. De landelijke bedrijfsonderdelen zorgen voor het databasemanagement en het beheer van de infrastructuren.  Bronhouders zorgen voor de kwaliteit van de gegevens. Burgers zullen in toenemende mate ageren tegen de dagelijkse profielvorming bij overheden. Denk aan de inmiddels beruchte rechterlijke uitspraak van het Europese Hof van Justitie aan Google van afgelopen 13 mei over het recht om vergeten te worden. En waarom zou er ook geen concurrentie kunnen ontstaan tussen publieke websites, gerelateerd aan de landelijke databases? En hoe moeten we daarmee omgaan? Een voorbeeld is het arrest Gaspedaal versus Autotrack van 15 mei, waarbij het gerechtshof van Den Haag bepaalde dat zoeksite Gaspedaal.nl inbreuk maakt op de database van concurrent Autotrack.nl. Het vonnis heeft vergaande gevolgen voor andere zoeksites want Gaspedaal stelt een database samen van tienduizenden autoadvertenties die van andere sites komen. Stel dat de NV Exploitatiebedrijf Overheidsvoorzieningen Nederland er komt en de invloed van de lokale spelers daarmee kleiner wordt, dan kan de informatiebeveiliging geconcentreerd worden. Is de huidige weg van vele volstrekt verschillende afspraken tussen publieke partijen lokaal, regionaal en landelijk over beveiliging via convenanten en overeenkomsten nog begaanbaar? Niet zo lang meer! Informatiebeveiliging wordt gatenkaas. Praktijk is dat de vele bestuursorganen, van zeer klein tot groot, geen hoge kwaliteit van informatiebeveiliging kunnen leveren.

## Het College bescherming persoonsgegevens in cijfers

**Vragen over toezicht en naleving in 2013, per sector:**

- handel en dienstverlening: 2.103
- overheid: 1.776
- arbeid: 900
- zorg & welzijn: 755
- internet: 315
- andere sector (o.a. cultuur, belangenorganisatie, religieuze instelling): 302
- betrokkene: 289
- telecom: 221
- politie & justitie: 115
- sociale zekerheid: 83
- internationale organisaties: 20
- totaal: 6.879

**Het College wordt het meeste ingeschakeld voor vragen over:**

- identificatie
- gebruik BSN
- direct marketing
- derdenverstrekking
- paspoort
- (heimelijk) volgen van werknemers door cameratoezicht of een personeelsvolgsysteem
- (medisch) dossier
- inzagerecht
- publicatie van persoonsgegevens op internet
- beveiliging van websites
- doorgifte van persoonsgegevens aan 'derde landen': landen buiten de Europese Unie

*Bron: Jaarverslag 2013 CBP*

Links

[1] http://wetten.overheid.nl/BWBR0034306/geldigheidsdatum_11-06-2014#Hoofdstuk1

[2] http://www.automatiseringgids.nl/achtergrond/2012/14/risicosregistreren-pers-oonsgegevens

[3] http://www.uitgeverijparis.nl/tijdschriften/tijdschrift/4/Privacy-Informatie-P-I

# DE DIGITALE WERELD IS GEEN GRENZELOZE DATAGRAAIBAK

Op dit moment speelt in Amerika een Federale rechtszaak die veel te weinig Europese aandacht krijgt. Met steun van de Electronic Frontier Foundation vecht Microsoft een datavordering door de Amerikaanse overheid aan. De data, emails van een Microsoftklant, staan op servers in Ierland. Microsoft en EFF stellen, kortgezegd, dat de Amerikaanse overheid met haar tengels van die emails af moet blijven omdat ze zich in Europa bevinden en ze daar geen jurisdictie heeft.

Microsoft weet zich inmiddels gesteund door Verizon, Apple, Cisco en AT&T. Eerder had een New Yorkse rechtbank het verzoek gehonoreerd op grond van een zeer verstrekkende redenatie over datavorderingen. Zo beargumenteerde die rechter: "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer." Als die lijn navolging zal vinden is data nergens ter wereld meer veilig voor Amerikaanse vorderingen, het enkele verschijnen van data op een scherm is dan voldoende om het in Europa van servers af te laten halen.

EFF en Microsoft proberen met het aanvechten van deze vordering de grenzen weer terug te brengen in de digitale wereld, in ieder geval daar waar het de privacy en vrijheid van burgers betreft. "The Fourth Amendment protects from unreasonable search and seizure. You can't ignore the 'seizure' part just because the property is digital and not physical," zo stellen zij. Dit gevecht zou alleen daarom al meer steun uit het Europese mogen krijgen, het gaat immers ook om onze privacy tegenover datagraaiend Amerika. En ja, natuurlijk is het "good for business" als Microsoft deze zaak wint. Ze zal in ieder geval in Europa op meer klanten mogen rekenen.

Toen de ontwerpverordening voor Privacy van de EU net geïntroduceerd werd, buitelden de Amerikaanse bedrijven nog over elkaar heen om te roepen dat deze voorgestelde strenge privacywetgeving zaken met EU-landen zou frustreren. De ontwerpverordening stelt namelijk dat deze ook geldt voor niet-EU landen die zaken doen op EU-bodem. Diezelfde Amerikaanse bedrijven lijken inmiddels te beseffen dat privacy hen ook business brengt. Sterker nog, zij gebruiken hetzelfde argument nu tegen de Amerikaanse overheid. De arrogante datahonger van de eigen overheid maakt het hen in toenemende mate onmogelijk hier nog vaste cloudvoet op aarde te krijgen.

Ik zal de zaak in ieder geval met veel belangstelling blijven volgen. Eind juli mogen partijen voor de Federale rechter de zaak bepleiten. Verwachting is echter dat het na uitspraak van de Federale rechter nog niet gedaan is. Beide partijen in het geding slijpen de messen en hebben veel te verliezen. Amerikaanse rechtsgeleerden voorspellen dan ook dat onafhankelijk van wie er zal winnen, de uitspraak op alle mogelijke gronden zal worden aangevochten.

*Mr. Rachel Marbus,*
*@rachelmarbus op Twitter*

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

*Matthijs Koot, senior security consultant bij Madison Gurkha. Geschreven op persoonlijke titel.*

*E-mail: koot@cyberwar.nl / Twitter: @mrkoot / Blog: https://blog.cyberwar.nl*

# DE LOGIUS-NORM VOOR DIGID: PERIKELEN BIJ TECHNISCH TESTEN

Het NCSC publiceerde in januari 2012 een leidraad met beveiligingsrichtlijnen voor webapplicaties. Een selectie van die richtlijnen werd een maand later door Logius verheven tot een beveiligingsnorm waar de ruim 550 organisaties die DigiD-gekoppelde systemen hebben aan moeten voldoen. In dit artikel bespreek ik enkele van de 'zuiver technische' onderdelen uit die norm die zonder een algemeen geaccepteerde interpretatie niet eenduidig toetsbaar zijn.

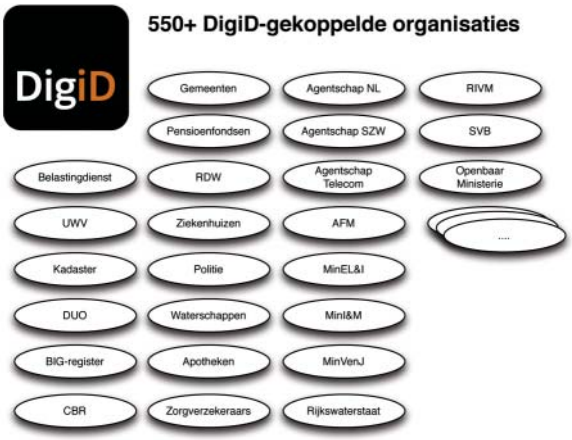
Het valt daardoor te verwachten dat verschillende experts in identieke gevallen tot verschillende oordelen. Bij elk onderdeel geef ik uit de NCSC-leidraad de beschrijving, de doelstelling en de vereiste succescriteria; en vervolgens mijn reflectie en een werkwijze voor toetsing. Later dit jaar wordt een nieuwe versie van de NCSC-leidraad verwacht. Dit artikel, de ingekorte versie, is bedoeld als expositie van de huidige problematiek en als klankbord voor de nieuwe NCSC-leidraad, die nog in ontwikkeling is. Een kopie van de uitgebreide versie van dit artikel is opgestuurd aan het NCSC en Logius.

## Introductie

In januari 2012, in het kielzog van Lektober, publiceerde het NCSC de leidraad "ICT-beveiligingsrichtlijnen voor webapplicaties" [NCSC1]. Het NCSC, Logius en de Rijksauditdienst hebben daaruit een selectie van 28 richtlijnen gemaakt die door Logius is verheven tot de "norm ICT-beveiligingsassessments DigiD" [Logius]. Deze bevat zowel organisatorische als technische richtlijnen en is van toepassing op alle "internet-facing webpagina's, systeemkoppelingen en infrastructuur die met DigiD gekoppeld zijn en betrekking hebben op het proces" [Logius]. (In dit artikel verwijst "norm" naar de Logius-norm en "richtlijn" naar de NCSC-richtlijnen die de bouwstenen zijn van de norm.) Het "ICT-Beveiligingsassessment DigiD" is een jaarlijks terugkerend audittraject dat organisaties met DigiD-gekoppelde systemen in opdracht van Logius dienen uit te (laten) voeren onder verantwoordelijkheid van een RE. In het audittraject kan externe expertise worden ingeschakeld. Een voorbeeld daarvan is een gespecialiseerde technische beveiligingstester. Een externe beveiligingstester verzamelt bewijsmateriaal en kan bij elk van de technische richtlijnen aangeven of de applicatie hieraan voldoet. De RE kan voor diens oordeel steunen op het oordeel en de bewijsvoering van de beveiligingstester. De kernactiviteit van mijn werkgever is technisch beveiligingsonderzoek. We hebben gekeken op welke onderdelen van de DigiD-norm we onze technische kennis kunnen inzetten. (Volledige DigiD-audits voeren we uit in samenwerking met dochtermaatschappij ITSX, maar dat valt buiten de scope van dit artikel.) Na het bestuderen van de richtlijnen kwamen we in 2012 tot de conclusie dat tien van de richtlijnen in de norm niet of nauwelijks afhankelijk zijn van organisatie of beleid: die richtlijnen beschouwen we daarom als 'zuiver

technisch'. Het betreft de B3-richtlijnen (applicatiebeveiliging) en B5-2 (vertrouwelijkheid en onweerlegbaarheid). Bij die richtlijnen gaat het dus niet zozeer om het bestaan van intern beleid en een gehandhaafde praktijk, maar om het actuele technische beveiligingsniveau van de applicatie zelf. Kortom: is de applicatie in praktijk voldoende veilig?

De probleemstelling die ik in dit artikel behandel, is dat de richtlijnen als toetsbaar zijn bedoeld, maar niet alle richtlijnen dat zijn, of in elk geval niet zonder nadere interpretatie. Het valt daarom bij die richtlijnen te verwachten dat verschillende beveiligingstesters in identieke gevallen tot verschillende oordelen komen. Ik betoog dat die NCSC-richtlijnen of de Logius-norm aanpassing behoeven, en dat voor consistente(re) toetsing nader uitgewerkte toetsingscriteria wenselijk zijn. Omwille van leesbaarheid beperk ik me in dit artikel tot de mogelijke (expert)oordelen "voldoet" en "voldoet niet" (niet te verwarren met het oordeel van een RE). In dit artikel kan ik de onduidelijkheid niet volledig wegnemen, maar wel expliciet maken, en deel ik enkele gedachten over de werkwijze bij toetsing.




## Code-inspectie

NOREA heeft eind 2012 een "Handreiking DigiD ICT-beveiligingsassessments voor RE's" gepubliceerd [NOREA]. Uit bijlage 1 blijkt dat de auteurs broncode-inspectie geen noodzakelijk onderdeel vinden om aan de Logius-norm te voldoen: zelfs niet waar het de richtlijn over het gebruik van geparametriseerde SQL-queries betreft (B3-5). Op dat punt ben ik het niet met de auteurs eens, omdat de ervaring leert dat bij broncode-inspectie kwetsbaarheden worden ontdekt die zonder de broncode waarschijnlijk niet zouden worden gevonden. Vooral SQL-injectie die zich in de uithoeken van de applicatie bevindt en/of niet zichtbaar is aan de buitenkant voor tools als Sqlmap; maar ook fouten in authenticatie- of autorisatielogica. Indien de applicatie ook voldoende veilig moet zijn indien geconfronteerd met een misnoegde insider, dan is broncode-inspectie erg belangrijk. (Dat zeg ik uit overtuiging, niet als WC-Eend.) En ja, dat vraagt tijd en eist vaardigheid in broncode-inspectie. Waar het NCSC als succescriterium noemt dat de broncode beschikbaar moet zijn voor onderzoek, citeer ik dat criterium in dit artikel.

## B3-1: invoervalidatie

**Beschrijving:** "De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt."

**Doelstelling:** "Voorkomen [sic] het verlies, wijziging of misbruik van gegevens door onbetrouwbare (malafide) invoer. Voorkom dat de applicatielogica wordt bei?nvloed."

**Vereiste succescriteria:** 1) Beschikken over de broncode van de programmatuur. 2) Validatie vindt plaats op in ieders [sic] geval dynamische onderdelen van de URL, query parameters, form parameters, cookies, HTTP-headers, XML en bestanden. 3) De webapplicatie voert deze validatie uit op basis van: typecontrole (bijvoorbeeld string of integer); lengtecontrole; formaatcontrole (op basis van bijvoorbeeld een reguliere expressie); controle op valide karakters (bijvoorbeeld alleen 'A-Z' en 'a-z'). 4) In het geval de invoer niet voldoet aan één of meerdere van bovenstaande controles, weigert de webapplicatie deze invoer. 5) De webapplicatie filtert de invoer op basis van: malafide sleutelwoorden (bijvoorbeeld 'DROP' of ' rm '); malafide tekens (bijvoorbeeld '" of "'); malafide patronen (bijvoorbeeld '/**/' of '..\..\') (...)"

## Reflectie

De doelstelling "voorkom dat de applicatielogica wordt bei?nvloed" is weinig specifiek. Onder "vereiste succescriteria" staan verschijningsvormen van invoervalidatie, geen succescriteria. Het kan immers niet zo zijn dat een applicatie niet aan richtlijn B3-1 voldoet enkel en alleen omdat niet elke invoer expliciet op lengte wordt gecontroleerd; een goed ingerichte database en goed opgezette foutafhandeling vangt corpulente invoer prima af. En indien een postcodeveld invoer van "<" of ">" niet weigert, maar wel normaliseert, bijvoorbeeld door die tekens te verwijderen of te vervangen door spaties (zie B3-3): dan wordt, strikt genomen, ook niet aan deze richtlijn voldaan. Voor een applicatie die fatsoenlijk omgaat met vreemde tekens, is controle op valide karakters onnodig: het biedt weliswaar een extra beschermingslaag, maar het is geen verstandige minimumeis. Invoervalidatie is een essentieel onderdeel van de beveiliging, maar waar dien je als beveiligingstester, in de context van de Logius-norm, de streep te trekken tussen "voldoet" en "voldoet niet"? Gaat het alleen om afwezigheid van kwetsbaarheden die praktisch en onmiddellijk uitbuitbaar zijn (zoals stored XSS) of om meer dan dat? Ook in het eerste geval blijft de vraag: wanneer is een "voldoet niet" gerechtvaardigd? Het is belangrijk dat verschillende experts in gelijke gevallen (voldoende) gelijk oordelen.

## Mogelijke toetsing

Concreet testen: XSS; LDAP-injectie; XXE, XSL/XML/XPath-injectie; OS/shell-injectie; JSONP-hijacking; Linq-injectie; blacklist/whitelist-evasion; path traversal; XML Signature wrapping, et cetera (n.o.t.k.).

Oordeel "voldoet niet" indien ten minste één gemiddelde of hoge kwetsbaarheid is gevonden die (ook) door invoervalidatie kan worden weggenomen. (n.o.t.k.; voor het bepalen van "laag", "gemiddeld" en "hoog" is een algemeen geaccepteerd beslissingsmodel wenselijk: hiertoe zouden beveiligingstesters het inschalingsmodel kunnen gebruiken dat het NCSC

## Tien 'zuiver technische' richtlijnen

**B3-1:** De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt.
**B3-2:** De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.
**B3-3:** De webapplicatie normaliseert invoerdata voor validatie.
**B3-4:** De webapplicatie codeert dynamische onderdelen in de uitvoer.
**B3-5:** Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.
**B3-6:** De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.
**B3-7:** De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).
**B3-16:** Zet de cookie attributen 'HttpOnly' en 'Secure'
**B5-2:** Maak gebruik van versleutelde (HTTPS) verbindingen.

hanteert voor haar beveiligingsadviezen [NCSC2]. Indien alle beveiligingstesters tijdens DigiD-beveiligingsassessments hetzelfde inschalingsmodel gebruiken, vermindert de kans dat verschillende beveiligingstesters in gelijke situaties verschillend oordelen.)
Oordeel "voldoet niet" indien er structurele gebreken of inconsistenties in de invoervalidatie zijn, ook als er geen sprake is van een onmiddellijk uitbuitbare kwetsbaarheid: denk aan blacklist/whitelist-evasion zonder dat daarmee op dit moment een uitbuitbare kwetsbaarheid kan worden aangetoond; en aan het accepteren van "<" en ">" in een context waar dat niet passend is, ook al worden de tekens netjes gecodeerd in de uitvoer (zie B3-4). Oordeel "voldoet" in alle andere gevallen.

### B3-3: normalisatie

**Beschrijving:** "De webapplicatie normaliseert invoerdata voor validatie".
**Doelstelling:** "Normaliseer alle invoerdata voor deze te valideren om te voorkomen dat filteringmechanismen ongewenste patronen niet herkennen."
**Vereiste succescriteria:** "Beschikken over de broncode van de programmatuur."

### Reflectie

Normalisatie is een optionele voorfase van invoervalidatie (B3-1) en hoort daaronder thuis. Je moet zorgen dat de applicatie bestand is tegen alle soorten invoer, dus ook path traversal-pogingen (die trouwens al zijn afgedekt door B3-7), injectie van NULL-bytes, onverwachte encoding, et cetera. Het enige succescriterium is dat de broncode beschikbaar moet worden gesteld, maar daaruit kan natuurlijk niet automatisch het oordeel "voldoet" volgen. Waar dien je als beveiligingstester de streep te trekken tussen het oordeel "voldoet" en het oordeel "voldoet niet"? De enige manier die ik kan bedenken, blijft vaag: bevat de applicatie een kwetsbaarheid die (gedeeltelijk) aan een gebrek aan normalisatie kan worden toegeschreven? In dat geval zou ook XSS meestal resulteren in een "voldoet niet" op deze richtlijn, omdat de XSS-kwetsbaarheid voorkomen had kunnen worden door normalisatie. Of normalisatie daartoe de beste maatregel is, blijft dan buiten beschouwing.

### Mogelijke toetsing

Concreet testen: zie B3-1.
Oordeel "voldoet niet" indien er ten minste één gemiddelde of hoge kwetsbaarheid is gevonden die (ook) kan worden weggenomen door normalisatie (n.o.t.k.).
Oordeel "voldoet" in andere gevallen.

### B3-6: server-side validatie

**Beschrijving:** "De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde."
**Doelstelling:** "Voorkom dat controles kunnen worden omzeild."
**Vereiste succescriteria:** "1) Beschikken over de broncode van de programmatuur. 2) Voor elke controle die de webapplicatie uitvoert aan de clientzijde, is een equivalent aanwezig aan de serverzijde."

### Reflectie

Om tegen deze richtlijn te toetsen zou je alle client-side controles in kaart moeten brengen en vervolgens toetsen of server-side dezelfde validaties worden uitgevoerd. Aangezien de client reeds als onvertrouwd dient te worden beschouwd, levert deze richtlijn een flinke hoeveelheid overbodig werk op. NOREA interpreteert deze richtlijn terecht als "reeds afgedekt door B3-1, B3-3, B3-4 en B3-5" [NOREA]. Richtlijn B3-6 zou wellicht obsoleet kunnen worden verklaard.

### Mogelijke toetsing

Concreet testen: zie B3-1 en B3-5.
Oordeel "voldoet niet" indien bij B3-1, B3-3, B3-4 en/of B3-5 al "voldoet niet" staat. Verwijs naar de betrokken richtlijnen.
Oordeel "voldoet" in alle andere gevallen.

### B5-2: HTTPS

**Beschrijving:** "Maak gebruik van versleutelde (HTTPS) verbindingen."
**Doelstelling:** "Voorkom misbruik van (vertrouwelijke) gegevens die tijdens transport zijn onderschept."
**Vereiste succescriteria:** "1) De inrichting is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp, waarin is vastgelegd welke uitgangspunten gelden voor de toepassing van versleutelde verbindingen (SSL/TLS). 2) Er vindt een redirect plaats van HTTP naar HTTPS op het moment dat een (contact) formulier wordt opgevraagd."

### Reflectie

Deze richtlijn is minder 'zuiver technisch' dan de andere: het eerste succescriterium spreekt immers over vastgestelde documentatie. Maar technisch testen is op twee manieren relevant: ten eerste vanwege de eis dat er een redirect moet plaatsvinden van HTTP naar HTTPS. En ten tweede omdat er in de configuratie van SSL/TLS allerlei technische details zijn die cruciaal zijn voor de werkelijke bescherming die met SSL/TLS wordt geboden.

| NCSC-leidraad: 59 richtlijnen | | selectie uit | Logius-norm: 28 richtlijnen |
|---|---|---|---|
| B0-1 t/m B0-14 | Algemene beveiligingsrichtlijnen | ----------> | B0-5, B0-6, B0-7, B0-8, B0-9, B0-12, B0-13, B0-14 |
| B1-1 t/m B1-6 | Netwerkwerkbeveiliging | ----------> | B1-1, B1-2, B1-3 |
| B2-1 t/m B2-4 | Platformbeveiliging | ----------> | B2-1 |
| B3-1 t/m B3-16 | Applicatiebeveiliging | ----------> | B3-1, B3-2, B3-3, B3-4, B3-5, B3-6, B3-7, B3-15, B3-16 |
| B4-1 en B4-2 | Identiteit en toegangsbeheer | | (geen) |
| B5-1 t/m B5-7 | Vertrouwelijkheid en onweerlegbaarheid | ----------> | B5-1, B5-2, B5-3, B5-4 |
| B6-1 | Beveiligingsintegratie | | (geen) |
| B7-1 t/m B7-9 | Monitoring, auditing en alertering | ----------> | B7-1, B7-8, B7-9 |

In de succescriteria worden geen eisen gesteld aan deze configuratie: zo bezien zou je met NULL-ciphers (SSL/TLS zonder versleuteling) en SSLv2 (een kwetsbare versie van het protocol) een "voldoet" kunnen krijgen, maar dat kan niet de bedoeling zijn. Op dit vlak is het aan de beveiligingstester om te onderzoeken of de opzet van de SSL/TLS-configuratie voldoende veilig is. Ook hier is de vraag: welk criterium hanteer je? Een strenge beveiligingstester zou al "voldoet niet" oordelen indien de SSL/TLS-configuratie geen ciphers ondersteunt die Perfect Forward Secrecy (PFS) bieden. (PFS voorkomt dat uit een in de toekomst gekraakte langetermijnsleutel sessiesleutels kunnen worden afgeleid die in het verleden zijn gebruikt voor versleuteling, en waarmee in het verleden onderschepte versleutelde SSL/TLS-communicatie alsnog kan worden ontsleuteld.) Een minder strenge tester zal wellicht alleen "voldoet niet" oordelen indien er sprake is van hoge risico's zoals Heartbleed.

## Mogelijke toetsing

Concreet testen: HTTP->HTTPS redirect; HSTS; ondersteunde ciphers en protocolversies; certificaat; kwetsbaarheden in de SSL/TLS-software; et cetera.
Oordeel "voldoet niet" indien gevoelige gegevens op ten minste één locatie in de applicatie over onversleuteld HTTP worden verstuurd (wat "gevoelig" is, is aan de beveiligingstester).
Oordeel "voldoet niet" indien er ten minste één gemiddelde of hoge kwetsbaarheid is gevonden in de opzet van SSL/TLS of de gebruikte software.
Oordeel "voldoet" in alle andere gevallen.

## Denken vanuit kwetsbaarheden

Bijna alle XSS-kwetsbaarheden zijn een probleem van uitvoercodering (B3-4). Bijna alle XSS-kwetsbaarheden kunnen daarnaast ook worden opgevat als een probleem van invoervalidatie (B3-1) en/of normalisatie (B3-3). Neem bijvoorbeeld een XSS waarbij de gebruiker "<script>alert(1)</script>" invoert in een postcodeveld. De tekens "<" en ">" zijn nimmer passend in een postcodeveld: dan is er dus sprake van gebrekkige invoervalidatie, omdat er geen melding komt dat "<" en ">" niet zijn toegestaan. Maar ook van gebrekkige normalisatie, omdat "<" en ">" niet automatisch door de applicatie uit de invoer zijn gehaald.
Indien er onduidelijkheid bestaat over hoe het oordeel tot stand dient te komen, is te verwachten dat beveiligingstesters niet immer tot eenzelfde oordeel komen. We zouden met elkaar concrete afspraken kunnen maken: bijvoorbeeld dat XSS altijd resulteert in een "voldoet niet" op B3-4 (richtlijn over uitvoercodering), tenzij er goede gronden zijn om ervan af te wijken (er zijn allerlei verschijningsvormen van XSS). Daarmee is de norm niet verbeterd, maar wordt wel de beoordeling van verschillende experts meer gelijk. Maar goed, het is even afwachten hoe de nieuwe versie van de richtlijnen eruit zullen zien. De richtlijnen B3-1 en B3-3 zijn niet gericht op specifieke kwetsbaarheden, maar op algemene maatregelen waarmee allerlei soorten kwetsbaarheden, waarvan XSS er één is, kunnen worden weggenomen. Andere richtlijnen, bijvoorbeeld B3-5 (richtlijn over geparametriseerde SQL) en B3-7 (richtlijn over dynamische file includes), zijn welbeschouwd verbijzonderingen van B3-1 die horen bij specifieke kwetsbaarheden (SQL-injectie resp. LFI, RFI). Misschien zou de Logius-norm meer van die verbijzonderingen kunnen bevatten waarbij wordt geredeneerd vanuit specifieke kwetsbaarheden in plaats van vanuit algemene maatregelen voor mitigatie. Denk bijvoorbeeld aan: "de applicatie is niet kwetsbaar voor XSS" (want XSS verdient dan weer wel een eigen categorie - iets dat OWASP al jaren heeft). Dat maakt het eenduidiger voor zowel beveiligingstesters als organisaties die aan de norm moeten voldoen. Immers, redenerend vanuit de bescherming van gegevens en functionaliteit, gaat het erom dat er geen XSS-kwetsbaarheid bestaat, niet om de manier waarop XSS is voorkomen---invoervalidatie, normalisatie of uitvoercodering, het is allemaal goed. Bij het redeneren vanuit kwetsbaarheden zou je de norm kunnen aanpakken vanuit het perspectief "voldoet, tenzij", dat de beveiligingstester uitdaagt om het tegendeel te bewijzen.

## Hoe verder?

Moet het beleidseffect van de Logius-norm zijn: de afwezigheid van specifieke kwetsbaarheden? Of een veilig ontwerp dat veilig is uitgeprogrammeerd? Dat laatste is natuurlijk beter, maar daar is de norm in de huidige opzet simpelweg niet voor geschikt. Het certificeringsmodel van het Framework Secure Software dat recent het licht zag is daar waarschijnlijk beter voor geschikt [SSF]. (Disclaimer: de hoofdauteur daarvan is een bevriende oud-collega.) Wat mij betreft zou het beleidseffect van 'zuiver technische' onderdelen in de Logius-norm zich in eerste instantie moeten richten op afwezigheid van technische kwetsbaarheden en op aanwezigheid van specifieke, eenduidig toetsbare technische beveiligingsmaatregelen; eventueel met een gereserveerde catch-all categorie á la B3-1 waar thans onbekende kwetsbaarheden in kunnen worden opgevangen. Indien toch op generieke beveiligingsmaatregelen moet worden getest, zorg dan dat er een algemeen geaccepteerde interpretatie is die de werkwijze bij toetsing voldoende eenduidig maakt.
Betere aansluiting bij OWASP behoort tot de mogelijkheden: OWASP geeft een breed geaccepteerd vocabulaire en is beter hanteerbaar voor

## Kruisreferentie Logius-norm en OWASP top 10 (versie 2013)

| OWASP-CATEGORIE | VOORBEELDEN VAN KWETSBAARHEID | RICHTLIJNEN UIT LOGIUS-NORM |
|---|---|---|
| A1: Injection | SQL-, LDAP-, Xpath-, Linq-injectie | B3-1, B3-3, B3-4, B3-5, B3-6, B3-7 |
| A2: Cross-Site Scripting (XSS) | alle vormen van XSS | B3-1, B3-3, B3-4, B3-6 |
| A3: Broken Authentication and Session Management | geen server-side invalidatie van sessies bij uitloggen; sessie-identifiers niet onvoorspelbaar; session fixation; | B3-2 |
| A4: Insecure Direct Object References | autorisatiefouten | B3-2 |
| A5: Cross-Site Request Forgery (CSRF) | geen Referer-check of geen nonce; indien wel nonce: nonce niet onvoorspelbaar | B3-2 |
| A6: Security Misconfiguration | TRACE-methode ingeschakeld, cookies niet Secure, cookies niet HttpOnly | B3-16, B5-2 |
| A7: Insecure Cryptographic Storage | (buiten scope van dit artikel) | B5-1, B5-3, B5-4 (buiten scope van dit artikel) |
| A8: Failure to Restrict URL Access | autorisatiefouten | B3-2 |
| A9: Insufficient Transport Layer Protection | SSLv2, Heartbleed, onvoldoende sterke ciphers, zwak sleutelmateriaal | B5-2, B3-16 |
| A10: Unvalidated Redirects and Forwards | open redirection | B3-1 |

beveiligingstesters en de ontwikkelaars die de kwetsbaarheden moet oplossen (bijvoorbeeld dankzij specifieke categorieën voor XSS en injectie). Het vermindert het probleem van slechte toetsbaarheid en inconsistentie in oordelen. OWASP kan een gedeelte van de huidige technische richtlijnen goed afdekken, biedt verbreding, en geeft de beveiligingstester een duidelijker kader voor beoordeling, hoewel algemeen geaccepteerde toetscriteria ook dan nodig blijven voor de groepscategorieën (eigenlijk alles behalve A2 en A5). Bovenstaande tabel geeft een kruisreferentie tussen OWASP en de Logius-richtlijnen. Nota bene: OWASP heeft veel uitgebreidere richtlijnen en volwassenheidsbeschrijvingen die wellicht zelfs beter gebruikt kunnen worden, omdat ze al gericht zijn op webapplicaties en een betere dekking bieden dan de Logius-norm en de OWASP top-10. Deze Tabel dient slechts ter illustratie.

### Afsluiting

Met Lektober nog vers in het geheugen, is het goed dat er een beveiligingsnorm is gekomen voor DigiD-gekoppelde systemen. Maar na twee jaar ervaring te hebben opgedaan met het toetsen van de technische normelementen, is duidelijk dat de eerste versie van de norm casu quo de richtlijnen waaruit de norm is opgebouwd aanpassing en nadere concretisering behoeven. De kinderziekten zouden zich wellicht gedeeltelijk kunnen laten verklaren door verhoogde tijdsdruk als gevolg van de politieke spanning die Lektober veroorzaakte. (Ter opfrissing: tientallen gemeenten werden acuut tijdelijk afgesloten van DigiD nadat tijdens Lektober hoge kwetsbaarheden zijn gevonden en volop media-aandacht kregen.) Waarschijnlijk zal de nieuwe versie van de NCSC-richtlijnen, die later dit jaar wordt verwacht, een opmaat zijn naar verbetering. Met dit artikel, waarvan een kopie is opgestuurd aan NCSC en Logius, hoop ik een kleine bijdrage te leveren aan deze ontwikkeling.


### Dankwoord

De auteur dankt Ton van Deursen (Madison Gurkha), Jan Hendrickx (Madison Gurkha) en Maarten Hartsuijker (Classity) voor hun feedback op conceptversies van dit artikel.


### Links


[SSF] Framework Secure Software (SSF, 2014)
https://www.securesoftwarefoundation.org/FrameworkSecureSoftware.html

[Logius] Beveiliging webapplicaties (Logius, 2012)
http://www.logius.nl/producten/toegang/digid/logiusnlbeveiligingsassessments/

[NCSC1] ICT-beveiligingsrichtlijnen voor webapplicaties (NCSC, 2012) https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

[NCSC2] Inschalingsmatrix (NCSC, 2012)
https://www.ncsc.nl/binaries/nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen-toelichting/1/Inschalingsmatrix.pdf

[NOREA] Handreiking ICT-beveiligingsassessments DigiD door RE's (NOREA, 2013)
http://www.norea.nl/Norea/Actueel/Nieuws/Handreiking+DigiD.aspx

Interview: Michiel Henneke, marketing manager SIDN
(Stichting Internet Domeinregistratie Nederland)

# VOORKOM DNS-AANVAL MET .NL CONTROL OF EEN REGISTRY LOCK

De 'kaping' van de domeinnaam van Google in Ierland, Google.ie, was op 9 oktober 2012 groot nieuws. Dit zeker in beveiligingsland. Internetgebruikers in Ierland probeerden toegang te krijgen tot Google.ie, maar ze slaagden hier niet in. De website was namelijk gekaapt. Niet door een aanval tegen de website zelf, maar door een aanval tegen de domeinregistrar van Google.ie.

*Sandra Kagie is freelance tekstschrijver/journalist (website: www.sanscriptproducties.nl; twitter @SanSanscript). Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst & taal. In het verleden is zij als eindredacteur nauw betrokken geweest bij 'Informatiebeveiliging'.*

Hackers wisten toegang te krijgen tot een account van de registrar van Google.ie waardoor ze de DNS-instellingen van de domeinnaam konden wijzigingen. Met als gevolg dat bezoekers van de domeinnaam Google.ie werden doorgestuurd naar een vermeend frauduleus IP-adres in Jakarta (Indonesië).

Een voorbeeld van een DNS-hack die de bewustwording rond dit type aanvallen de afgelopen tijd volgens Michiel Henneke, marketingmanager SIDN in Arnhem -het bedrijf dat de uitgifte en registratie van .nl-domeinnamen verzorgt-, heeft vergroot. Zeker ook omdat het hier Google, een high profile company, betrof.

## Steeds meer DNS-incidenten

Incidenten als deze waarbij DNS-instellingen via frauduleuze verzoeken op een ongeautoriseerde wijze worden aangepast, komen volgens SIDN incidenteel voor, ook met betrekking tot .nl-domeinnamen, maar de potentiële schade is enorm.

Veel beheerders van domeinnamen bieden de mogelijkheid domeinnamen te beveiligen met een zogenoemd Registry Lock. Een oplossing voor het beveiligen van bijvoorbeeld .com- en .eu-domeinnamen.

Voor het meest gebruikte Nederlandse domein, .nl, heeft SIDN, in lijn met Registry Lock, .nl Control geïntroduceerd. Een dienst waarmee bedrijven en organisaties controle kunnen houden over hun .nl-domeinnaam. Zodat ze zeker weten dat er geen wijzigingen plaats kunnen vinden in hun DNS-instellingen zonder hun expliciete akkoord.

## Bescherming van domeinnamen

.nl Control is na DNSSEC een tweede stap in de bescherming van domeinnamen. Met DNSSEC kunnen bezoekers van een website verifiëren of ze ook daadwerkelijk bij deze website uitkomen en niet omgeleid worden naar een malafide kopie ervan. .nl Control biedt bedrijven een extra mogelijkheid om controle te houden over hun domeinnaam waardoor het risico op ongewenste updates, verhuizing of verwijdering van een domeinnaam volgens Henneke aanzienlijk afneemt.

.nl Control wordt net als andere diensten van SIDN aangeboden via .nl-registrars aan .nl-domeinnaamhouders. Wanneer een bedrijf de extra DNS-bescherming wil, moeten ze dit dan ook via hun registrar (veelal een internetprovider en/of hostingbedrijf) aanvragen bij SIDN. Dit met het daarvoor bestemde inschrijvingsformulier. Na ontvangst van het formulier (inclusief de benodigde bijlagen om aan te tonen dat het verzoek afkomstig is van de houder of een namens de houder bevoegd persoon, meestal een KvK-uittreksel, eventueel een volmacht en altijd een kopie ID-bewijs van de ondertekenaar van het inschrijvingsformulier en, indien van toepassing, het ID van degene die bevoegd wordt voor mutaties) neemt SIDN rechtstreeks contact op met de domeinnaamhouder om te controleren of het verzoek correct is. Pas daarna wordt het verzoek gehonoreerd en krijgt de .nl-domeinnaam de status 'Limited'.

Worden er vervolgens via een registrar verzoeken tot mutaties ingediend voor zo'n 'Limited' domeinnaam dan worden deze handmatig door SIDN beoordeeld. En dus niet geautomatiseerd verwerkt zoals bij mutaties van 'gewone' .nl-domeinnamen gebeurt. In het geval van zo'n handmatige beoordeling wordt naast een telefonisch akkoord van de domeinnaamhouder ook om een schriftelijke bevestiging van de opdracht gevraagd. Een bevestiging die voorzien moet zijn van een handtekening.

"Met .nl Control ligt het accorderen van een wijziging dus volledig bij de domeinnaamhouder", legt Henneke uit. "Zo weet hij zeker dat er geen wijzigingen plaatsvinden met betrekking tot zijn domeinnaam, zonder zijn expliciete akkoord", vat hij de werking in de praktijk van .nl Control samen.

## Welke bedrijven lopen gevaar?

En het zijn volgens Henneke zeker niet alleen 'high profile' bedrijven, zoals Google, die zich bewust moeten zijn van het gevaar van DNS-aanvallen. ".nl Control is speciaal ontwikkeld voor .nl-domeinnaamhouders die de controle over hun domeinnaam willen hebben, zoals bijvoorbeeld banken en (overheids)instellingen, houders van een domeinnaam waar een webshop op draait en eigenaars van nieuwssites", somt hij op. "Bedrijven en organisaties voor wie een downtime van de

**Risico op een DNS-hack is relatief klein, maar de impact kan enorm zijn.**

website van enkele minuten al een enorme strop betekent", licht hij toe.

Maar ook houders van domeinnamen die een bepaalde handelswaarde vertegenwoordigen zouden volgens Henneke .nl Control kunnen overwegen. Net als bedrijven die hun domeinnaam als nameserver gebruiken om verschillende applicaties te ontsluiten. Ook dit type bedrijven moet volgens hem alert zijn.
En ditzelfde geldt voor houders van een domeinnaam waaronder veel meer websites met vaak heel andere namen vallen. Denk aan een website van een thuisbezorgservice die bijvoorbeeld de sites verzorgt voor honderden pizzeria's. Door een wijziging in de DNS-instellingen van de domeinnaam van de thuisbezorgservice worden al die onderliggende sites evenzeer getroffen.

## Impact DNS-hack enorm

Henneke noemt het risico op een DNS-hack in vergelijking met bijvoorbeeld een DDoS-aanval of phishing weliswaar relatief klein, maar de impact ervan kan enorm zijn, zo stelt hij. "Vraag je als bedrijf of organisatie dus af of je in de genoemde categorieën van bedrijven valt. En zo ja, bescherm je domeinnaam dan extra met behulp van .nl Control", adviseert hij.

De kosten hoeven in de ogen van de marketingmanager van SIDN met maximaal enkele honderden euro's per jaar geen drempel te vormen. Ook niet wanneer je als bedrijf of organisatie meerdere domeinnamen middels .nl Control wilt beschermen. Iets dat door SIDN  eenvoudiger is gemaakt. Eén domeinnaamhouder kan .nl Control namelijk sinds kort met één formulier aanvragen voor meerdere websites tegelijk.

Een tip die Henneke bedrijven en organisaties, los van .nl Control, sowieso wil meegeven, is het goed beheren van de domeinnaamportefeuille. "Zorg er altijd voor dat gegevens up-to-date zijn. Weet hoe je portefeuille eruit ziet en wat de contactgegevens voor je domeinnamen zijn. Dit voorkomt problemen op het moment dat je mutaties wilt doorvoeren", geeft hij aan. Zeker bij fusies en overnames of bijvoorbeeld ontbindingen van VOF's is dit volgens hem absoluut iets om goed in de gaten te houden.

## Registrars overstag

Waren registrars van .nl-domeinnamen bij de introductie van .nl Control in 2011 volgens Henneke nog niet zo enthousiast. "Ze zagen de extra bescherming van domeinnamen als een motie van wantrouwen tegen hen", legt hij uit. Inmiddels zien ook de registrars volgens hem het nut van een Registry Lock in.
"Ze plaatsen de bescherming nu zelfs op hun eigen nameservers om zo te voorkomen dat via deze weg de sites van bijvoorbeeld mkb-bedrijven die zij hosten slachtoffer worden van een DNS-hack. Wanneer kwaadwillenden er immers in slagen de DNS van een hostingbedrijf te kapen, is het zomaar mogelijk dat in één keer duizenden domeinnamen naar malware worden doorverwezen", legt hij uit.

In totaal schat de marketingmanager van SIDN in dat er nu enkele honderden houders van een .nl-domeinnaam gebruikmaken van .nl Control. Een heel klein aantal als je weet dat Nederland bijna 5,5 miljoen .nl-domeinnamen telt. Dit heeft volgens hem alles te maken met het feit dat veruit de meeste websites in Nederland niet in het eerder genoemde risicoprofiel vallen.

## Blijven hameren op bewustwording

Wat SIDN wil bereiken, is bewustwording bij bedrijven. "Vraag je als bedrijf dus af wat de potentiële schade voor jouw organisatie is wanneer je te maken zou krijgen met een DNS-hack", benadrukt Henneke. "Is deze schade groot dan is een relatief kleine investering in .nl Control of een Registry Lock wellicht geen overbodige luxe", concludeert hij.
Waarbij hij schade niet alleen wil uitdrukken in financiële schade, maar ook in imagoschade. Word je als bedrijf namelijk slachtoffer van een DNS-hack dan zal dit zeer waarschijnlijk breed uitgemeten worden in de media. Iets waar de meeste bedrijven en organisaties natuurlijk niet op zitten te wachten.

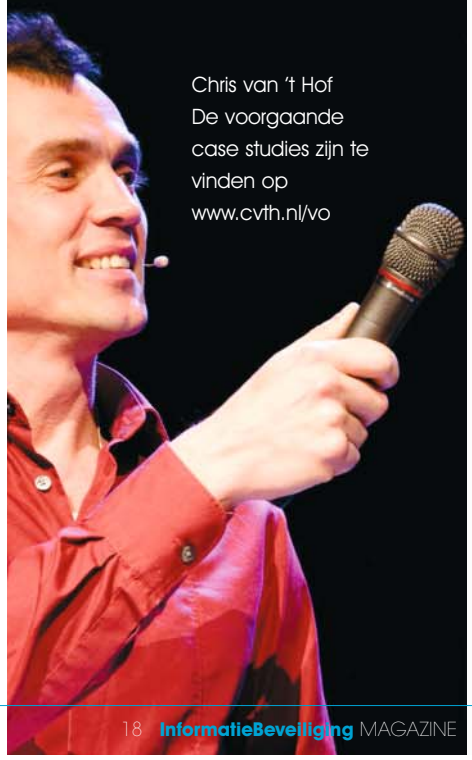
*Meer informatie over .nl Control is te vinden op de website van SIDN, www.sidn.nl. Op de site is ook een informatiebrochure over de dienst te downloaden.*

Verantwoorde onthullingen #8

# AUTORISATIE INFINITAS UITGEVERIJEN MAKKELIJK TE OMZEILEN

## Toen @iliaselmatani een studieboek kocht, kreeg hij er 1643 gratis

**Deze aflevering van Informatiebeveiliging gaat over de beleving van de hacker. Eigenlijk gaat deze column daar altijd wel over, dus deze keer een aspect dat nog onvoldoende belicht is: je moet als verantwoorde hacker vooral heel veel geduld hebben. Zo ook @iliaselmatani die maar liefst een jaar moest wachten totdat een ogenschijnlijk eenvoudige fout in de site van Noordhoff Uitgevers werd gedicht. Waarom? Ze hadden het al zo druk met andere dingen.**



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

Alweer een jaar geleden zag ik op Twitter een uitnodiging voorbijkomen van een zogenaamde #fristileaks. Dat is de jongeren variant van #wiskyleaks, een open informele bijeenkomst waar hackers onder Chatham House rules hun geheimen delen. Oftewel: je mag alles doorvertellen, als je maar niet zegt van wie je het hebt. Buiten dat het altijd wel leuk is jonge hackers te ontmoeten, had ik een doel: minstens een goede case voor mijn onderzoek naar Responsible Disclosure. Ik erheen.

Aan het einde van de avond realiseerde ik me dat ik vooral zelf vanachter een groot glas Triple aan het woord was geweest. Ik weet niet of de verlegen jongens -en een meisje- met hun Fristi's zich hadden vermaakt met de praatgrage onderzoeker, maar ik had gefaald: geen interessante onthulling. Jammer. Onderweg naar de trein komt @iliaselmatani naar me toe. Hij beweert dat hij alle boeken van Noordhoff Uitgevers zomaar kan downloaden. El Matani had dit al eerder willen onthullen via Webwereld, maar die hadden het laten liggen. Of ik wilde bemiddelen tussen hem en de uitgever. Graag.

De volgende dag krijg ik een mail met uitgebreide documentatie. Ilias schrijft dat hij voor zijn studie een online boek had aangeschaft bij Noordhoff. Je logt dan in met een (voucher) code en kan er dan online in bladeren. Pagina's opslaan kan niet. Dat is best lastig als je bijvoorbeeld in de trein wilt lezen. Hij ontdekt echter dat de pagina's steeds geladen worden vanaf een url die eindigt op "page" met een nummer erachter. Als hij nummer handmatig aanpast krijgt hij een foutmelding. Hm, dat zou ook te eenvoudig zijn.

Als hij in de cache van zijn Firefox browser kijkt, ziet hij dat de inhoud van de pagina steeds geladen wordt vanaf een andere url. Als hij hier een van de nummers verandert komt hij wel gewoon uit bij de gevraagde pagina. Maar het boek heeft ook een nummer zo te zien. En als hij dat veranderd…jawel, komt er een ander boek tevoorschijn. Hij heeft zo dus toegang tot alle boeken van deze uitgever. Ilias laat zijn bevinding zien aan @sander2121. Samen schrijven ze een script in Python waarmee de urls automatisch worden aangepast. En ja, het werkt. Maar aan losse pagina's in SWF formaat heb je ook niet zoveel, dus het script zet ze netjes op volgorde achter

elkaar in pdf. En zo zouden ze dus maar liefst 1643 boeken kunnen downloaden.

Wat zou jij doen als je zoiets ontdekt? Ikzelf zou het meteen aan mijn medestudenten doorgeven en zo iedereen trakteren op gratis boeken. @iliaselmatani en @sander2121 niet. Ze willen de slechte beveiliging op een verantwoorde manier melden. Maar hoe zal die uitgever reageren? Zal hij aangifte doen? Ze besluiten het via de media te doen en sturen hun melding op 21 april naar Webwereld. Daar wordt het echter niet opgepakt en daarom komt Ilias nu bij mij.

Best spannend, zo'n uitgever benaderen dat hun site lek is. Er zijn dan wel geen persoonsgegevens gelekt. Je zou zelfs kunnen stellen dat systematisch URL's afgaan niet gezien kan worden als hacken. Maar toch, ze zouden een zaak kunnen starten - alleen al om ons af te schrikken. De uitgever zou immers een flinke reputatieschade kunnen oplopen door deze onthulling. Het miljarden investeringsbedrijf Bridgepoint achter deze uitgever, heeft hoogstwaarschijnlijk een flinke batterij aan advocaten klaar staan om ons het leven zuur te maken – ook als ze geen zaak hebben. Ik begin daarom met een voorzichtig mailtje waarin ik het lek meld en me aanbiedt als bemiddelaar tussen hun en de hacker.

Binnen een dag krijg ik een reactie van Jean Pierre Miani, Technology Officer bij Infinitas Learning. In de CC zie ik nog drie mensen van de technische afdeling. Mooi. Hij zegt de melding zeer serieus te nemen en vraagt met spoed om aanvullende informatie. Even bellen dan maar. Ik vertel Miani over de urls en de boeken. "Oh, dat. Nou, dat is geen hacken toch? Hebben we in april al gehoord en dat is nu gefikst. Is dit nu weer diezelfde jongen?" Dat wil ik natuurlijk niet zeggen. Infinitas kan alle details krijgen, maar eerst moeten ze via een PGP gesigneerde mail beloven niet tot vervolging over te gaan. Miani reageert geërgerd: "Nee, ik ga geen vrijbrief geven."

Ilias is onaangenaam verrast. "Tsja, hier gaan mijn nekharen van overeind staan. Het is inderdaad geen hacken, eerder ongeautoriseerde toegang. Maar als je dit op Twitter gooit kunnen ze de tent wel sluiten. Dat scriptje heeft me twee uur gekost en zelfs met een gewone verbinding kun je in een nachtje alle boeken downloaden. Kun je je eigen uitgeverij beginnen." Hij begrijpt ook niet hoe de melding al bij ze is gekomen. Ze hebben dit nog met niemand gedeeld, ook niet bij #fristileaks. Vervolgens kijkt hij even op de site van Noordhoff. Nee, het lek is nog niet gedicht. Wat volgt is een langdurige woordenwisseling tussen Ilias en Jean Piere, via mij.

Wanneer we er niet uitkomen besluit ik voor te stellen elkaar dan maar te ontmoeten zonder vrijwaring. Ilias is gelukkig bereid het risico te lopen. Jean Pierre draait bij: "Ik vind dat white hat hackers beloond moeten worden, kan er zelf ook van leren." Op 6 januari sta ik samen met Ilias in het kantoor van Infinitas in Houten. De Technology Officer steekt direct van wal. Security is zijn hoogste prioritiet. Als educatieve uitgever hebben ze vaak aanvallen te verduren van scholieren die vanuit school proberen te hacken en DDoS aanvallen lanceren. Ze verzamelen daarom een minimum aan persoonsgegevens met het idee: als je ze niet hebt, kun je ze ook niet kwijtraken. Het abonnement waarmee je de boeken kunt inzien is dan ook alleen maar een nummer.

Ze hadden dus al in april gehoord van het lek, via een leverancier. Maar om het te dichten moest wel het hele systeem op de schop. En als educatieve uitgever moet alles in juni goed draaien, want dan schaffen scholen de nieuwe uitgaven aan. Je kunt dan niet het hele systeem omgooien. De aanpassing zou worden meegenomen in het groot onderhoud, maar toen werd het druk en verdween het probleem weer naar de achtergrond. Zo spannend is het niet, dat iemand een pagina kan downloaden, vindt de uitgever. En nee, er is daarom geen enkele reden om een rechtszaak tegen ons te beginnen.

Ik opper dat Ilias ook zijn tool aan andere studenten had kunnen geven en er dan veel meer boeken gratis zouden worden gedownload. De auteurs lopen dan hun royalty's mis en zouden die op Infinitas willen verhalen. Volgens Jean Pierre leven niet al hun 6000 auteurs van royalty's, maar ze zouden inderdaad een zaak kunnen starten. "Hoe dan ook", stelt hij trots, "er wordt aan gewerkt en de nieuwe versie wordt binnenkort uitgerold." "Mag Ilias het dan testen?" opper ik enthousiast. Jean Pierre twijfelt: "Eh, nu nog niet, we zijn er nog mee bezig. Geef ons nog en paar weken. Ik zal wat documentatie sturen waar hij naar kan kijken".

De weken worden maanden, zonder bericht van Infinitas. Ilias heeft het inmiddels gehad met de trage uitgever, maar ik wil natuurlijk wel mijn stukje publiceren. Ik wacht daarom maar tot de truc met de urls niet meer werkt, anders zou deze onthulling ook niet erg verantwoord zijn. Het is inmiddels juni en jawel: de geconstrueerde links leiden slechts naar dode pagina's. Blijkbaar is het Jean Pierre toch gelukt. Op de home page staat trots: "Infinitas Learning re-affirms market leadership by launching e-book platform Classmate".

And what's new? De inmiddels 2000 boeken zijn nu eindelijk ook te downloaden - mits je een voucher hebt gekocht natuurlijk - zodat je ze off line kunt lezen. Niet dat @iliaselmatani daar nu nog wat aan heeft, want hij is inmiddels klaar met zijn opleiding. Hij werkt nu als security specialist bij SecureLabs en krijgt, net als de uitgever, eindelijk gewoon betaald voor zijn werk.


# HEARTBLEED EN HET RISICO VAN OPEN SOURCE SOFTWARE!

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

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

## Wat is open source software?

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

## Het ontstaan van Heartbleed

Laten we nu eens kijken hoe Heartbleed is kunnen ontstaan. Er zijn een aantal oorzaken.  OpenSSL is zeer populaire software. Het wordt letterlijk door honderdduizenden organisaties gebruikt. Deze organisaties hebben bij elkaar afgelopen jaar bijna ? 2.000 aan donaties overgemaakt! In totaliteit wel te verstaan. Dit is dus de jaaromzet van OpenSSL. Deze software beveiligt het hele hebben en houden van organisaties en individuen. Inclusief de zwaar bediscussieerde en bevochten privacy.
De eerste oorzaak is hier al uit op te maken. Er was domweg niet voldoende kapitaal een fatsoenlijk product op de markt te zetten en anderzijds is de markt totaal niet geïnteresseerd in een goed product. Als iedere gebruiker ? 1 had gedoneerd waren er vele honderdduizenden of zelfs miljoenen euro's aan kapitaal beschikbaar geweest om een fatsoenlijk product op de markt te zetten. Dit probleem is dus niet alleen de maker(s) aan te rekenen maar ook onszelf. Dit is een uniek probleem. Dit is bijzonder populaire software, je kunt dus niet stellen dat er te weinig interesse is. Het gezegde dat je krijgt waarvoor je betaald, doet hier zeker opgeld.
Dit was echter niet het enige probleem! Een product wordt ontwikkeld door een team. Je hebt ontwerp, bouw en kwaliteitscontrole. Als je naar de sourcecode kijkt van OpenSSL kun je vaststellen dat het een spaghetticode is. Het is zeer moeilijk te lezen, documentatie is niet van een makkelijk begrijpbare soort! Allemaal zaken die het moeilijk onderhoudbaar maken. Er was gewoonweg niet voldoende mankracht. Conclusie is dat de software niet of nauwelijks te onderhouden is. Het lijkt heel veel op software waar voortdurend aan bijgebouwd is, zonder de overtollige delen eruit te halen. Dit lijkt meer op het werkt dus afblijven principe dan professioneel en structureel degelijk werk. Dit is kunnen ontstaan omdat er gewoonweg te weinig mensen in het ontwikkelteam van OpenSSL zitten/zaten. Daardoor is een kleine softwarefout met zeer grote gevolgen twee jaar lang ongemeld gebleven. Onbekend is hoevelen van dit lek op de hoogte waren en er misbruik van hebben gemaakt.
Het dogma ervan uit te gaan dat als het mogelijk is, het ook werkelijkheid is, is een goed dogma. Ga ervan uit dat ook uw organisatie het slachtoffer is van dit lek. Neem maatregelen! In het geval van Heartbleed is het simpel. De eerste stap is de software te controleren en indien nodig te patchen. Tweede stap is de vervanging van alle certificaten. Derde is het gebruik van Hardware Security Modules waarin de certificaten opgeslagen worden. Deze variëren van een smartkaart met cryptochip en kaartlezer tot en met een HSM voor inbouw. Een en ander afhankelijk van de performance die nodig is. De HSM moet wel minimaal voldoen aan Commen Criteria EAL4+ level. Dit is dus een eenvoudige oplossing voor Heartbleed en andere lekken/inbraken die gebruik maken van zachte certificaten (certificaten opgeslagen in software).

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

## Risico's open source software

Laten we eens verder kijken naar de risico's en hoe daar mee om te gaan. Open source software wordt door iedereen gebruikt. Ook de software die nu aangeboden wordt voor gebruik op een smartphone. Wat is er eenvoudiger, je vindt iets leuk of het biedt een oplossing, je betaalt € 2,50, het wordt automatisch geïnstalleerd en je kent wat rechten toe. Plotseling heeft iemand anders toegang tot de smartphone of tablet waarmee op het bedrijfsnetwerk gewerkt wordt. UserID's en wachtwoorden worden uitgelezen en gebruikt. Of nog leuker ze kunnen de microfoon van de telefoon of tablet aanzetten en plotseling zitten ze mee te luisteren met die belangrijke meeting waar gesproken wordt over een overname of een nieuw product. De emails worden gekopieerd! De camera wordt op afstand ingeschakeld en plotseling kunnen ze meekijken.
Het is geen science fiction. Dit is eenvoudig uitvoerbaar. Er zijn SDK's die je gewoon kunt downloaden. Dit zijn compleet uitgeruste SDK's waar je eenvoudig kunt aangeven wat je wilt. Je download de software die je wilt misbruiken, je disassembleert, voegt het samen met de SDK en assembleert de software opnieuw en presto je hebt een besmet softwarepakket die de meeste gebruikers alle rechten geven over hun tablet of smartphone, inclusief de toegang tot de bedrijfsinfrastructuur. Ze hebben immers ook de userID en wachtwoord, dus niemand die het opvalt.
Ik zet de software waar je een klein bedrag voor moet betalen ook in het rijtje van open source software. Het is immens populair omdat het leuk is en gratis of vrijwel gratis. Aansprakelijkheden zijn er niet, want in de voorwaarden staat onder andere dat de software aangeboden wordt "as is" en er geen aansprakelijkheden zijn. Bovendien staat er in de meeste gevallen ook in dat je voor de data die verzameld wordt, goedkeuring geeft en bovendien dat wat verzameld wordt automatisch van "hun" is. Protesteren heeft dus geen zin. Door het downloaden en gebruiken van deze software ben je immers akkoord gegaan met de software en alles wat het doet en draag je de eigendomsrechten van wat de software verzamelt over. Is dus een risico. Kortom, je hebt er TOTAAL geen controle over.
Een tip die ik kan geven is gebruik te maken van een blikken koekjestrommel bij een vergadering. Iedereen doet zijn smartphone in de koekjestrommel en de notebooks en tablets worden volledig uitgeschakeld en ergens anders even opgeslagen, bureau lade of iets dergelijks, als het maar metaal is. Op deze manier is het afluisteren van de meeting langs deze weg in ieder geval uitgesloten. Een lowtech oplossing voor een hightech risico.
Bovenstaande betekent niet dat ik zeg dat je open source software links moet laten liggen. Het betekent alleen dat je voorzichtig moet zijn, maar ja dat moeten we toch altijd?! Als je gebruik maakt van open source software kijk dan eerst naar de juridische consequenties. Kun je iemand aansprakelijk stellen? Als dit het geval is kun je er bijna vanuit gaan dat deze persoon ook zijn best doet goede software te leveren. Wel even aan denken dat dit vaak ook weer gemaximaliseerd is naar een maximum van de aanschafprijs. Dus voor een softwarepakket van € 3,50 kun je een schadeclaim indienen van € 3,50. Wat je dus moet afvragen is welk risico je loopt? Hoeveel is het waard? Is het risico inderdaad € 3,50 dan is er geen probleem. Ik ken echter weinig bedrijfsrisico's die hiermee voldoende gedekt zijn! Daarentegen loopt de kwaadwillende vrijwel geen risico.
Belangrijk is naar de software zelf te kijken. Analyseer de source code alsof de eigen ontwikkelafdeling het gemaakt heeft en haal het door een kwaliteitsmechanisme heen. Pas als alles er goed uitziet, dat wil zeggen de source code is goed leesbaar en goed gedocumenteerd en er zitten geen rare onverklaarbare zaken in of code die niet te verklaren is, dan pas kun je overwegen de software te gebruiken. De reputatie van de leverancier is net zo belangrijk. Kortom, wees voorzichtig. Overigens niet alleen de software is hier belangrijk, ook de compiler die je gebruikt om de sourcecode te compileren kan besmette code meelinken/mee compileren!

## Bescherming

Als de code goed bevonden is, is het belangrijk deze ook te beschermen. De meest eenvoudige is deze software te ondertekenen met een echt certificaat, dat wil zeggen van een erkend CA/trust center bij voorkeur eentje van Nederlandse bodem onder Nederlands recht. Het laatste is belangrijk. Een certificaat verstrekt onder deze voorwaarden geeft de garantie dat alles gaat als voorgeschreven (staat onder scherp toezicht) en juridisch ook afgedekt is/ wettelijk erkend. Dit hoeft niet duur te zijn, hoewel als we bovenstaande goed gelezen hebben, is dit geen issue. Het ondertekenen van software met een certificaat geeft de garantie dat ondertekende software in ieder geval niet gewijzigd is na de ondertekening. Als het wel het geval is, werkt de software niet. Let wel, ik bedoel hier dus niet de waaiboomcertificaten die eenvoudig en tegen lage kosten en minimale identificatie gedaan worden. Oh ja, gebruik een HSM! Als U een HSM gebruikt is Heartbleed geen issue!
Uit bovenstaande zou je kunnen concluderen dat ik wat tegen open source software heb. Dit is echter niet het geval. Het is voor mij software die van een ander businessmodel gebruik maakt. Het moet echter net als vroeger gewoon voldoen aan een aantal kwaliteitskenmerken. Helaas voldoet veel open source software hier niet aan. Helaas ook andere, niet open source software! Mijn advies, wees voorzichtig en kijk goed naar de risico's. Stop het gebruik van software dat niet aan deze voorwaarden voldoet. Last but not least, richt de infrastructuur veilig in, het is niet zo moeilijk en kan zelfs in veel gevallen veel geld besparen. Goede security verlaagd kosten!

# BYOD ENABLED

In this issue we shall look at BYOD with a view to identifying the major risk factors affecting the design of a technical architecture supporting BYOD as a way of working, suing as always the SABSA way of thinking.

The most important thing to consider is the business risk – from both sides of the employer/employee relationship, and from both sides of the risk/reward balance. BYOD presents both opportunities and threats, both to the employer and to the employee who owns the device. The assessment of these risks is something that both parties should undertake independently. BYOD security is a collaborative exercise between the owner of the device and their employer. Each party has some security and risk management requirements. It is a mistake for the employer to assume that they are taking control of the device – they are not – they are sharing its use. Thus the employer may not impose any restrictions on the private use of the device by the owner. That is a policy principle that must be established before any technical architecture can be considered.

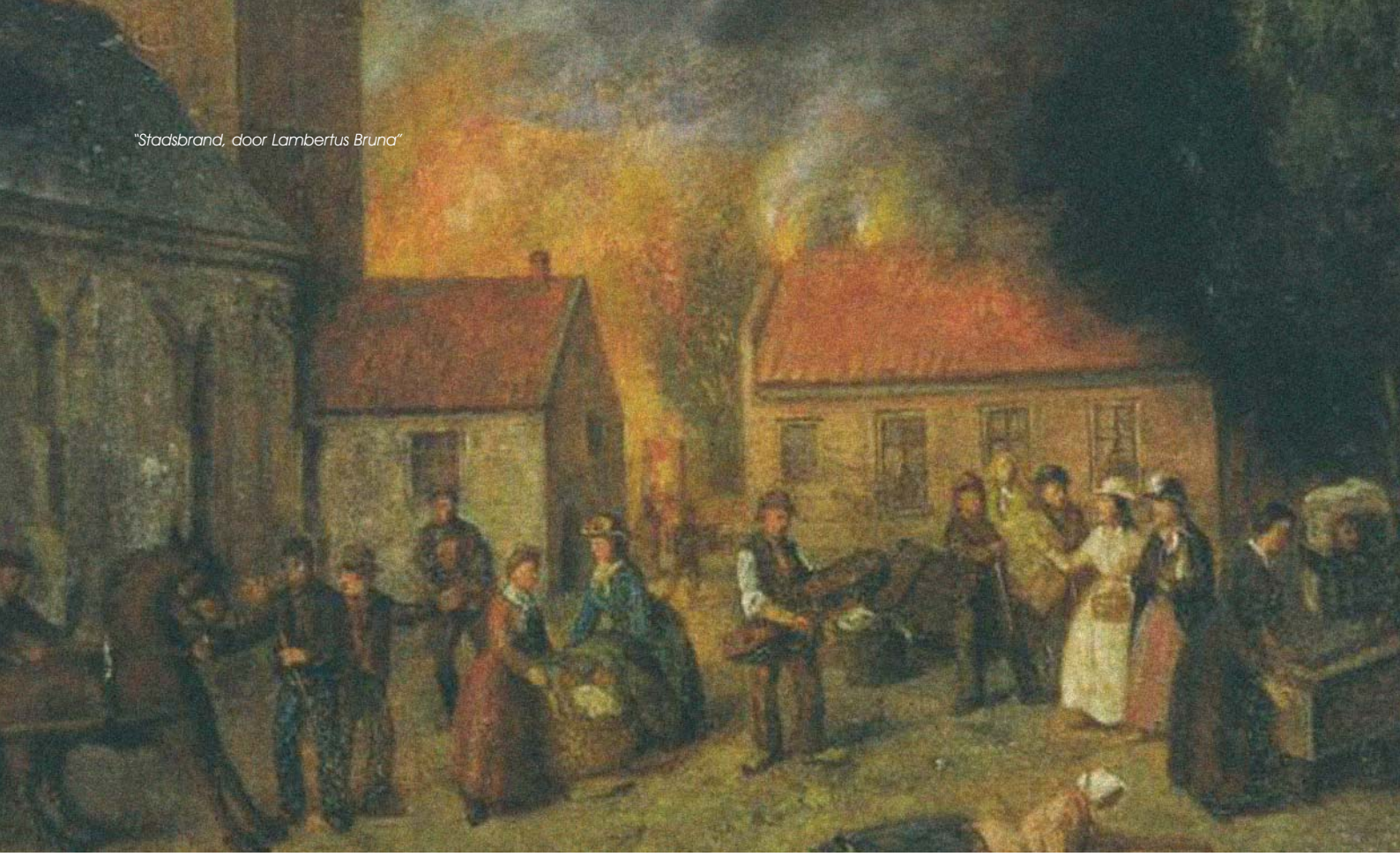
The owner of the device uses it for private, personal applications and data, and should be protected from these being accessed by the corporate centre. At the same time and on the same device, corporate data and applications must be processed without leakage from a corporate domain to the public domain. The user must be free to make decisions as to which applications they will run for personal private use, and must be free of corporate restrictions on what these choices will be, otherwise the device ceases to be 'owned' by the user, and is no longer an 'own device'.

There are also many technical constraints that must be taken into account. Any data stored on the device cannot be differentially secured. Access through the keyboard and other input/output devices must be shared. The operating system on these types of devices does not support multi-user segmentation. Any local data, however it may be presented through various applications, is, at the lowest level, stored as a series of raw files. If you can access one you can access them all. The result of this constraint is that the architecture should not rely on local storage of corporate data. All data should be stored on a central corporate server. That immediately suggests a thin client architecture, in which the client software has minimal functionality, restricted to setting up a VPN connection to the corporate network and allowing thin client agents to be run on the device. A thin client is a virtual presentation only. No actual data processing is done on the client device. Data is transferred to and from the device and all processing and storage is done on the central server.

Malware is a serious technical threat that must be regarded as a major attack vector, especially into the future when malware capability will only increase. Such malware is known to be able to monitor keyboard strokes, take screen-shots and sniff other input/output channels. So, an architecture that allows a corporate application to have direct access to the hardware and operating system will necessarily have a low level of security, since malware can monitor all this activity. That may be avoided by creating a sandbox for the thin client application and by using only keyboard screen images for data entry and randomising the positions of the required mouse clicks on the screen.

In summary, both employee and employer must make risk based decisions about what type of use will be made of BYOD services. If the level of business criticality is very high, then perhaps those specific applications are unsuitable for this approach. However, if a technical architecture along the lines described here can be designed to a sufficient security level, then BYOD has many attractions. SABSA is all about being driven by business risk, and there is no difference here. Being business risk driven will always be the overriding principle for security architecture design.

**The Attributer**



*"Stadsbrand, door Lambertus Bruna"*

# HET NATIONAAL RESPONS NETWERK

## Een virtuele bucket line

Aan het einde van de zomer van 2012 verspreidde het computervirus Dorifel zich razendsnel in Nederland. Criminelen konden op afstand profiteren van verregaande rechten op  besmette computers en bestanden werden onbruikbaar . Als gevolg van het Dorifelvirus stuurden sommige getroffen organisaties medewerkers naar huis. In andere gevallen, zoals bij de gemeente Weert, zetten medewerkers hun werkzaamheden op ouderwetse typemachines voort. De inzet van de typmachine illustreert dat we in de huidige aanpak van cyberincidenten soms terugvallen op techniek uit de jaren zeventig van de vorige eeuw. Dit artikel betoogt dat we voor een adequate respons wellicht nog verder de geschiedenis in moeten duiken, misschien zo ver terug als de Middeleeuwen!

Het Dorifelvirus was een treffend voorbeeld van een digitale olievlek waarbij door onderlinge ketenafhankelijkheden snel en ongecontroleerd uiteenlopende branches en sectoren werden geraakt. In het najaar van 2012 ontstond in Nederland een soortgelijke situatie toen het Pobelka botnet, dat initieel gericht was op het ontvreemden van geld, ook gevoelige gegevens van bouwbedrijven, de chemische industrie en overheidsinstellingen buitmaakte. Ook in 2013 werd Nederland opgeschrikt door digitale keteneffecten toen de initieel op banken gerichte Distributed Denial of Service (DDoS)-aanvallen ver buiten de financiële sector schade aan begonnen te richten. Opvallend is dat bij al deze sector-overschrijdende cybersecurity-incidenten de samenwerking- en coördinatie op het gebied van ICT-respons op ad-hoc basis werd georganiseerd. Getroffen partijen keken vaak niet buiten de eigen sector voor hulp en beschikbare (zowel publieke als private) responscapaciteiten bleken versnipperd belegd. De organisatie van ICT-respons tussen organisaties en sectoren liep hierdoor vertraging op en oplossingen (zoals de inzet van typemachines) werden geïmplementeerd zonder adequate gezamenlijke analyses uit te voeren.

### De NCSC netwerkbenadering

ICT respons is het bestrijden en oplossen van cybersecurity incidenten. Respons bestaat uit:

- Triage: het bepalen van de ernst en urgentie van het incident
- Analyse en oplossing: het analyseren van het incident, hulp bij het onderzoeken en het uitvoeren van oplossingen en het controleren van de uitkomsten
- Opschonen en herstellen: het schonen van de omgeving en het herstellen van de situatie
- Evaluatie: het beoordelen van het proces en de oorzaak van het incident en het nemen van maatregelen om het incident in de toekomst te voorkomen

## Het Nationaal Respons Netwerk

Teneinde het olievlek effect van cybersecurityincidenten een halt toe te roepen en doelmatige respons te organiseren is het samenbrengen en coördineren van beschikbare ICT-responscapaciteiten van groot belang. Om de vereiste samenhang en coördinatie te organiseren is het Nationaal Cyber Security Centrum (NCSC) het Nationaal Respons Netwerk (NRN) gestart. Het Nationaal Respons Netwerk is een formeel samenwerkingsverband tussen het NCSC en ICT - responsorganisaties uit publieke- en private (vitale) sectoren. Het NRN heeft als doel om tijdens grote incidenten vanuit verschillende publieke- en private sectoren capaciteiten te bundelen om de respons op cybersecurity-incidenten te versterken en verdere verspreiding ervan te voorkomen. Het NRN is geen hiërarchische organisatie, maar een organisatie waarbij alle deelnemende ICT-responsorganisaties als gelijkwaardige schakels functioneren om incidenten via reguliere structuren af te handelen. Deelnemende organisaties spreken af elkaar te ondersteunen bij incidenten die zo'n grote impact hebben dat een deelnemer het alleen niet kan opvangen. Als een dergelijk incident impact heeft op de nationale veiligheid, wordt de gebruikelijke nationale crisisstructuur geactiveerd en ondersteunt het NRN hierbinnen de uitvoering van ICT-responsactiviteiten.
Buiten de incidentafhandeling om vervult het NCSC de rol van coalitievormer en begeleider van de samenwerking in het netwerk. In tijden van relatieve rust kunnen organisaties in het NRN actuele dreigingsinformatie, kennis en ervaringen delen om zo de eigen responscapaciteiten te verbeteren. Deelnemers leren van de werkwijze van anderen waardoor best practices gedeeld en communicatiekanalen opgezet worden. Ook wordt in het NRN de ontwikkeling van aanvullende sectorale responscapaciteiten gestimuleerd door het netwerk met nieuwe deelnemende organisaties te versterken en te verbreden. Om deze nieuwe capaciteiten te organiseren stelt het NCSC ervaring, tools en andere middelen beschikbaar (bijvoorbeeld een blauwdruk voor de inrichting van een sectorale Computer Emergency Response Team (CERT)).

## Een virtuele bucket line

Deelname aan het NRN vergroot de slagvaardigheid van organisaties doordat incidentinformatie in het netwerk sneller wordt gedeeld en geëvalueerd en de juiste contactpersonen

*Aart Jochem is Hoofd Monitoring en Respons, Nationaal Coördinator Terrorismebestrijding en Veiligheid; Anouk Vos is Adviseur Cyber Security, Nationaal Coördinator Terrorismebestrijding en Veiligheid. Zij werken bij het NCSC en zijn te bereiken via info@ncsc.nl.*


sneller worden gevonden. Als gevolg is het voor organisaties makkelijker een goed situationeel beeld van incidenten te krijgen waardoor het gecoördineerde handelingsperspectief onder getroffenen, maar ook (nog) niet getroffenen wordt vergroot. Met het NRN wordt zo een virtuele bucket line gecreëerd. Waar ieder huishouden in de Middeleeuwen een blusemmer had en, zodra er brand uitbrak, zich formeerde in een rij van bron naar brand, zijn het in het NRN de responsorganisaties die een rij vormen. De emmers water om een brand te blussen zijn hierbij vervangen door responscapaciteiten om een grootschalig ICT-incident te helpen 'blussen' en verdere verspreiding te voorkomen. Hoewel iedere organisatie in het NRN de primaire verantwoordelijkheid behoudt voor de eigen digitale veiligheid, vergroot de unieke publiek-private samenwerking binnen het NRN de collectieve weerbaarheid van Nederland.

## De netwerkbenadering

Het NRN maakt een deel uit van de netwerkbenadering van het NCSC. De insteek van deze benadering is dat de dienstverlening van het NCSC voor een belangrijk deel zijn meerwaarde ontleent aan de samenwerking tussen publieke en private partijen. De samenwerkingspartners van het NCSC beschikken samen over meer capaciteiten en kennis over dreigingen en risico's dan iedere partner individueel. Hiermee is de business case voor nieuwe strategische coalities om de digitale veiligheid van Nederland te vergroten snel gemaakt. Binnen de netwerkbenadering worden de bestaande publiek-private samenwerkingsverbanden van het NCSC verdiept over drie pijlers. Naast het NRN gaat het hierbij om het Nationaal Detectie Netwerk en het Nationaal Expertise Netwerk.

## De toekomst van een Middeleeuwse benadering

Op 17 april 2014 is het NRN formeel gelanceerd met de ondertekening van samenwerkingsconvenanten met vijf deelnemende partnerorganisaties. Naast het NCSC, gaat het hierbij om de Informatiebeveiligingsdienst (IBD) van het Kwaliteit Instituut Nederlandse Gemeenten (KING) en de Vereniging Nederlandse Gemeenten (VNG), de Belastingdienst, SURFNET en DefCERT. De komende tijd zal het netwerk verder worden uitgebreid, waarbij de nadruk ligt op het organiseren en structureren van sectorale responscapaciteiten van nieuwe partnerorganisaties. De nieuwe deelnemers aan het netwerk dienen daarbij een ruime achterban te vertegenwoordigen, voldoende capaciteiten te hebben en verantwoordelijkheid te dragen voor één of meerdere vitale processen in Nederland. De ambitie is om met deze doorontwikkeling van het NRN op termijn steeds effectievere en innovatievere invullingen te geven aan de gebundelde ICT-responscapaciteiten in Nederland. Zo biedt het NRN de mogelijkheid om een virtual response community te organiseren en kan binnen het netwerk de gezamenlijke ontwikkeling van tools en protocollen worden gestimuleerd.

## Conclusie

De uitbraak van het Dorifelvirus is niet het eerste sector-overstijgende cybersecurity-incident in Nederland, en zal ook zeker niet de laatste zijn. De onderlinge afhankelijkheden in het cyberdomein maken dat digitale brandjes zich snel en via onvoorziene routes verspreiden. Met het NRN worden nieuwe coalities en samenwerkingsverbanden gestimuleerd die ons op deze brandjes voorbereiden, ons in staat stellen informatie uit te wisselen en onze bluscapaciteiten versterken. Het is achteraf natuurlijk onmogelijk te zeggen of het NRN in staat zou zijn geweest om de Dorifelbesmetting in Weert te voorkomen. Echter, met een Middeleeuwse benadering had waarschijnlijk sneller tegen Dorifel opgetreden kunnen worden en waren die typmachines niet nodig geweest!

*Heeft u vragen over het Nationaal Respons Netwerk of wilt u meer informatie? Neem contact op met het NCSC. Telefoon 070-8887555 (tijdens kantooruren) of per e-mail: info@ncsc.nl*

# UNIFORME KWALIFICATIE VAN PROFESSIONALS IN INFORMATIEBEVEILIGING

Op 19 mei jl. is door de beroepsgroep van informatiebeveiligers PvIB, het whitepaper Beroepsprofielen Informatiebeveiliging, een basis voor uniforme kwalificatie van professionals in informatiebeveiliging, gepresenteerd.

In de huidige informatiemaatschappij wordt het steeds belangrijker dat iedere organisatie zorgvuldig omgaat met informatie. Organisaties moeten steeds meer informatie beschermen tegen een steeds complexer dreigingenbeeld. De dagelijkse stroom aan incidenten op het gebied van cyber security maakt de behoefte duidelijk aan goed opgeleide en ervaren informatiebeveiligers. In de afgelopen jaren is op het gebied van kwalificatie van informatiebeveiligers een chaotische situatie ontstaan met onderling moeilijk vergelijkbare certificaten en titels. Daardoor kunnen werkgevers niet zien wanneer zij een goed opgeleide en ervaren informatiebeveiliger voor zich hebben en informatiebeveiligers kunnen met hun titels en de bijbehorende certificaten niet duidelijk maken welke kennis en ervaring zij hebben.

Het whitepaper Beroepsprofielen Informatiebeveiliging beschrijft welke beroepen binnen het vakgebied informatiebeveiliging voorkomen, wat deze beroepen inhouden en welke competenties (kennis, vaardigheden en houding) daarvoor nodig zijn. Dit maakt uniforme kwalificering mogelijk van professionals in de informatiebeveiliging. Het publiek-private programma QIS (Qualification of Information Security) werkt aan transparante kwalificaties in de informatiebeveiliging. Het doel van QIS is het realiseren van een uniform kwalificatiestelsel voor informatiebeveiligers dat breed wordt gedragen en aansluit op de beschreven beroepsprofielen en het Europees e-Competence Framework (e-CF). Het is de basis voor het opleiden van jong talent en bestaande professionals in het complexe en grensoverschrijdende vakgebied informatiebeveiliging.

Het programma QIS is in september 2013 gestart. De deelnemende organisaties zijn: Rabobank, ING, ABN AMRO, AkzoNobel, Rijksoverheid, Cyber Security Raad, EY, ECP (Digivaardig & Digiveilig) en PvIB.

Het whitepaper is te downloaden van de website van PvIB (pvib.nl) of www.pvib.nl/nieuws/17696378/16-05-2014/Whitepaper-Beroepsprofielen-Informatiebeveiliging

PvIB Platform voor InformatieBeveiliging

ECP Platform voor de InformatieSamenleving

**Over ECP**

ECP is een onafhankelijk platform waar overheid, bedrijfsleven en maatschappelijke organisaties kennis uitwisselen en samenwerken om de kansen die de informatiesamenleving biedt te benutten en bedreigingen weg te nemen. Diverse projecten, onderzoeken en debatten verbinden partijen en zetten de maatschappelijke betekenis van ICT op de agenda van politiek, overheid en bedrijfsleven. Zo realiseert het platform doorbraken en creëert het de juiste randvoorwaarden.
**Meer informatie: www.ecp.nl**

DIGIvaardig & DIGIveilig

**Over Digivaardig & Digiveilig**

Digivaardig & Digiveilig is een samenwerkingsverband tussen bedrijfsleven, overheid en maatschappelijke organisaties om de digitale vaardigheid van de Nederlandse (beroeps)bevolking te vergroten en tevens om het vertrouwen in ICT en internet te bevorderen door het vergroten van de digitale veiligheid. Het programma wordt gesteund door het ministerie van Economische Zaken, de Europese Commissie en diverse bedrijven (KPN, UPC, NVB, IBM, SIDN, CA-ICT en Ziggo). Het programma wordt uitgevoerd door ECP, Platform voor de Informatiesamenleving.
**Meer informatie: www.digivaardigdigiveilig.nl**

# 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

# NEDERLAND KAN SPIJKERS MET KOPPEN SLAAN IN HET CYBERDOMEIN

Op de afgelopen NCSC One Conference zei minister Opstelten onder andere: "Nederland mag volgend jaar de vierde editie organiseren van de prestigieuze Internationale Cyberconferentie – met deelname van tientallen ministers en bijna 2000 afgevaardigden van publieke en private organisaties en instellingen uit zo'n 100 landen. Daar hopen we spijkers met koppen te kunnen slaan en internationaal opnieuw verdergaande stappen te kunnen zetten op weg naar een veilig en weerbaar cyberdomein. Vergelijkbaar met een slim en goedwerkend stelsel van dijken, dammen, sluizen en andere geavanceerde waterbouwkundige werken, dat de burgers bescherming biedt – maar dan in het digitale domein. Zodanig, dat hackers, cybercriminelen en andere kwaadwillenden geen kans krijgen om cruciale informatie te bemachtigen, onze vitale diensten en systemen aan te vallen, of zelfs plat te leggen!"

Wat vindt de redactie? Hoe komt het dat specifiek Nederland spijkers met koppen slaan? Komt dat door onze ervaring met watermanagement? Of speelt er iets anders?


Lex Dunn


Ronald van Erven


Rachel Marbus


André Koot

## Lex Dunn

Nederland is bij uitstek het land van de waterbouwkundige werken, en daar zijn we in de wijde wereld om bekend. Nederland is ook het land van vele internationale organisaties, zoals het International Criminal Court, het Vredespaleis, het Joegoslavië tribunaal. Nederland is ook het land van ambitieuze plannen en op het gebied van cyber weerbaarheid is dat niet anders. In de afgelopen paar jaar hebben we al twee versies van onze Nationale Cyber Security Strategie zien verschijnen (meer dan vele andere landen), we hebben de oprichting van het Nationaal Cyber Security Centrum gezien, en er zijn vele conferenties over het onderwerp cyber security geweest. Maar in mijn ogen de belangrijkste factor waardoor dit allemaal daadwerkelijk kan slagen, is de publiek private samenwerking, tegenwoordig publiek private participatie, waarin overheid, onderwijs en onderzoek en de private partijen steeds beter samenwerken. En van huis uit zijn Nederlanders gezegend met een mentaliteit van "niet kletsen, maar poetsen", naast een goed gevoel voor internationale contacten. Dat dit succesvol is, bewijzen de verschillende verhalen van de recente NCSC One Conference, met name van de vrienden van het Team High Tech Crime. Hun strategie om de (potentiële) cybercriminelen te laten merken dat ze gevolgd worden, en dat ze ook opgepakt kunnen worden, lijkt vruchten af te werpen. Daarom denk ik dat we als Nederland niet alleen in staat zijn om volgend jaar een spetterende Internationale Cyber Conferentie neer te zetten (we hebben ervaring met de Nuclear Security Summit), maar dat we ook daadwerkelijk stappen kunnen maken in de bestrijding van de cyber malheur.

## Ronald van Erven

Nederland kan spijkers met koppen slaan in het cyberdomein - dit komt omdat Nederland het centrum is voor vrede, veiligheid en gerechtigheid. Denk maar aan het Internationaal Gerechtshof, het Navo Cyber Security Centrum en Interpol die in Nederland gevestigd zijn. Maar Nederland was in 2013 ook het topland voor cybercriminaliteit [1], [2] en [3] en een waar walhalla voor identiteitsdieven [4]. Er is hier misschien ook voor beide partijen, de good guys en de bad guys, veel te leren. Of loopt Nederland juist voorop in de bestrijding van deze criminaliteit, omdat deze artikelen voor 1 januari 2014 waren. Hierdoor heeft Nederland veel ervaring op dit gebied. Misschien geldt hier wel...met boeven vang je boeven. Voor de BV Nederland is deze conferentie een goede zaak en ik hoop deze prestigieuze Internationale Cyberconferentie te mogen bezoeken.

## Rachel Marbus

Ach, het was een aardige beeldspraak, edoch vertelde slechts de helft van het verhaal. De andere zijde van de medaille liet de minister onbesproken. Jazeker heeft een klein land als Nederland een aantal mooie digitale speurwerkjes laten zien bij het vangen van cyberboeven. De aldaar uitgeteste methodes wil de minister nu dan wettelijk gaan verankeren. Dat moet dan in de derde versie van de wet op de Computercriminaliteit terecht gaan komen. Zo is daarbij het heftig bedebatteerde terughacken alsook het decryptiebevel. Beide opsporingsmethodes dringen sterk in op de grondrechten van burgers. Daar heb ik de minister dan geen gewag over horen maken. Graag had ik een sterker debat over niet alleen de grenzen aan cybercrime door het opleggen van mooie en wellicht ook heel terechte dijken, maar een daarbij gepaard gaand debat over de grenzen aan de binnendringing in de grondrechten die dat met zich meebrengt.

## André Koot

Ik kan wel weer helemaal los gaan op het cyberthema. Ik vind het namelijk maar niks. Alsof we alle computer- en internetgerelateerde incidenten onder één noemer kunnen vangen. Niets daarvan. Maar ja, het bekt wel lekker, dat gecyber. Het zou beter zijn als onze minister en ons NCSC zich zouden richten op specifieke dreigingen en risico's. Of cyberspionage, of cyberoorlog, of datalekken, of verantwoordelijkheden ten aanzien van informatiebeveiliging, of veilige infrastructuur, of ICS, of scada of… noem maar op. Dat huidige gecyber zegt niets meer. Als twee mensen over cyber praten kan de ene het hebben over phishing scams en de ander over DDoS-aanvallen, ze zullen elkaar niet begrijpen en dus elkaar gewoon maar gewoon gelijk geven. Als we dat volgend jaar in Nederland op in een wereldconferentie gaan doen, dan kan ik nu al de eindresolutie voorspellen. Daar zal in staan dat we met meer energie gezamenlijk de problemen moeten aanpakken.

**Links:**

**[1] http://nos.nl/video/469976-nederland-topland-voor-cybercriminaliteit.html**

**[2] http://nos.nl/audio/470090-kamer-bezorgd-over-cybercriminaliteit.html**

**[3] http://www.techzine.nl/nieuws/27097/nederlander-geliefd-bij-hackers-en-cybercriminelen.html**

**[4] https://www.security.nl/posting/373368/Kabinet%3A+Nederlanders+niet+alert+op+identiteitsfraude**

## COLOFON

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

PvIB
Platform voor InformatieBeveiliging

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

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

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

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

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

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

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


ISSN 1569-1063

# SLIMME HACKERS OF DOMME GEBRUIKERS?

Mijn kleinzoon vroeg laatst aan mij of ik een hacker was. Een wonderlijke vraag want ik had geen idee dat dit een vraag was die in de derde groep van de lagere school leefde. Ik vertelde mijn kleinzoon dat ik geen hacker kon zijn omdat ik geen baard heb, geen lang haar heb en geen cola drink, met dat antwoord was hij gelukkig tevreden. Toen hij weg was begon ik zelf na te denken over zijn vraag en vroeg mij af of mijn antwoord wel correct was. Wellicht begonnen de eerste hackers zó, maar uiteraard is dat niet het huidige beeld. Toen ik mijn eerste pogingen deed om met mijn modempje via wardialing binnen te komen bij bedrijven had ik zeker geen baard en mijn pogingen waren dermate amateuristisch dat ik mezelf geen hacker noemde.

De hedendaagse hacker is veelal iemand die zeer goed weet hoe de technologie in elkaar zit en vaak slimmer is dan de ontwikkelaars die de beveiliging hebben ontworpen. Of ze maken gebruik van de laksheid van de gebruiker die bijvoorbeeld het standaard wachtwoord van de door zijn provider verstrekte modem niet aanpast, of van de gebruiker die een phishing mail niet herkend en zijn inloggegevens inspreekt op een antwoordapparaat. Op zich is dit te verklaren en is het de eindgebruiker niet kwalijk te nemen dat de methodes van de hacker niet worden doorzien. Campagneboodschappen over laptop computers die dichtgeklapt moeten worden en telefoons die neergelegd moeten worden zullen weinig effect sorteren, want de misleidingen van hackers worden slimmer en slimmer.

Wat ik wel bijzonder kwalijk vind, zijn de bedrijven die laks zijn in de beveiliging. Ze laten back-upservers openstaan, werkstations van medewerkers updaten ze niet en daardoor zijn ze vatbaar voor aanvallen van buitenaf.  Bedrijven die gebruik blijven maken van internetbrowsers waarvan bekend is dat ze onveilig zijn, die op besturingssystemen werken die uit gefaseerd zijn en niet meer ondersteund worden. Bedrijven die accounts en wachtwoorden van hun klanten lekken, niet voorzichtig zijn met creditcardgegevens. Bedrijven die alleen zaken willen doen als je jouw gegevens bij hen achterlaat. Mag ik verwachten dat zo'n bedrijf er alles aan zal doen om mijn gegevens te beschermen? Ik geef er niet eens antwoord op.

Een hacker is dus iemand die gebruik maakt van dit soort methoden. Als ik de voordeur van mijn huis open laat staan dan weet ik toch dat ik een risico loop? Als ik geen virusscanner op mijn Windows PC plaats dan weet ik toch dat ik een risico loop? Als ik geen pincode activeer op mijn telefoon dan weet ik toch dat iemand daar misbruik van kan maken als ik hem verlies? Als ik in mijn auto stap en wegrijdt zonder mijn gordel om te doen, weet ik dat ik een risico loop. Mijn auto maakt het me trouwens wel heel moeilijk om dit vol te houden, tenzij je van zeer irritante piepjes en knipperende lampen houdt. De fabrikant houdt rekening met jouw gemakzucht en wil niet dat een koper van zijn product door nalatigheid zichzelf ernstig verwondt.

Je zou het in kunnen bouwen in pc's. Laat ze je het werken beletten tenzij je jouw oude browser update en andere nodige beveiligingsmaatregelen neemt. Nee, dit gaan we niet doen, want dit vindt de gebruiker niet fijn. Nee, die vindt het fijn om zijn betaalgegevens kwijt te raken, of geen controle meer te hebben over zijn bankrekening. Zolang pc's, smartphones en tablets, apparaten blijven waarover je denkt 'controle' te hebben maar waarbinnen, buiten jouw eigen zicht, allerlei onzichtbare zaken gebeuren, zullen er risico's blijven. Zoals een journalist tijdens de Olympische spelen in Sotsji zei: "Tijdens een kop koffie werd mijn telefoon 25 keer aangevallen door criminelen". Ik hoop voor hem dat er geen 26 aanvallers waren.

**Berry**

Wist u dat:

# Hackers 210 dagen onopgemerkt blijven*


*Bronvermelding: Michelle Fox. Tuesday. 10 Jun 2014.
http://www.cnbc.com/id/101747867

## Praat eens met CRYPSYS Data Security

**Als value-add distributeur heeft CRYPSYS de afgelopen jaren veel organisaties geadviseerd. Met 25 jaar ervaring zit security in ons DNA.**

**Secure computing is onze "way of life"**
Met zorg selecteren wij onze partners om de juiste oplossing te kunnen bieden voor iedere omgeving. Hierbij kijken wij niet alleen naar de functionaliteit, maar zeker ook naar innovativiteit, continuïteit en betrouwbaarheid.

Dankzij deze ervaring beschikt CRYPSYS over alle expertise op het gebied van security om succesvol samen te werken met haar resellers. Met als resultaat een tevreden eindklant.

**CRYPSYS oplossingen zijn fexibel**

CRYPSYS secure computing

CRYPSYS secure computing 25 years

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

CRYPSYS is officieel distributeur van: Sophos, SMS Passcode, Norman, Adyton, Lumension en Nessus