juli 2009 nummer 5

INFORMATIEBEVEILIGING

Vertrouwelijke informatie in het buitenland

AutoNessus: makkelijk herhaald scannen

Black Hat Europe

European Identity Conference 2009

Anonimiteit versus verantwoording

creative commons

PvIB
Platform voor InformatieBeveiliging

ib

Voorwoord/colofon

Beste lezer,

Tijd voor vakantie, dus waar haal je dan de inspiratie vandaan om een voorwoord te schrijven? Geen idee, het is nu even mooi weer en wat doe je dan? Even mijn browser starten en mijn startpagina verschijnt, een rss-aggregator, waarmee ik mijn RSS-jes kan volgen. En dat levert dan meteen inspiratie op. Want waar haal ik normaal alle kennis vandaan? Van internet, blogjes en zo. Er zijn zoveel sites die interessant en relevant zijn, die kun je niet allemaal actief volgen. Vandaar dat ik gebruik maak van een rss-reader. Ik gebruik zelf netvibes.com. Igoogle is ook leuk, maar ja, Google weet al zo veel van mij, ik wil niet alle eieren in één mandje bewaren. In ieder geval is zo'n aggregator erg handig. Zo kan ik van tientallen sites het nieuws volgen. En kan ik op basis van een enkele regel tekst besluiten om de site te bezoeken. Dat gaat veel sneller dan al die sites altijd te bezoeken. Ja, ja, zo hou ik alles in de greep...

Een paar van de sites die ik via rss'jes volg:

- http://www.itsprivacy.nl/, een Nederlandse site over privacy. Geen idee wie erachter zit, maar zo af en toe volg ik een berichtje.
- Natuurlijk ook http://www.security.nl/. Heel veel info, meningen en peilingen. Een aantal vakbroeders neemt actief deel. En de site levert natuurlijk altijd screendumps voor weer een powerpoint over informatiebeveiliging.
- http://cloudsecurity.org/ heb ik in een eerder nummer al opgevoerd, maar verdient weer een nominatie.
- We hebben ook een digitale concurrent: http://www.net-security.org publiceert ook een gratis vakblad. Leuk om eens te vergelijken!
- Je bent als professional natuurlijk geen knip voor je neus waard als je Bruce Schneier op zijn blog http://www.schneier.com/blog/ niet volgt. Nuttig ook als je inktvis op vrijdag leuk vindt.

Mijn 'identity' hobby kan ik botvieren op de volgende sites:

- Paul Madsen: http://connectid.blogspot.com/
- Ash (Ashraf Motiwala) http://identityman.blogspot.com/
- Kim Cameron natuurlijk: http://www.identityblog.com/
- Mike Jones: http://self-issued.info/
- Eve Maler: http://www.xmlgrrl.com/blog
- Jeff Bohren: http://idlogger.wordpress.com/
- Ian Yip: http://blog.ianyip.com/
- En goede kennis Marcus vind je hier: http://www.bloglines.com/blog/Marcus-Lasance

Er zijn nog veel meer interessante sites, maar ja, ik heb niet zoveel ruimte. En ik wil toch nog even mijn blogje melden: http://id-use.blogspot.com/, waar ik wat nadenk over identity 2.0 dingetjes.

Behoefte aan nog meer information overflow: start Twitter en volg gerust @securitystuff, @prabath, @websecuritynews, @ryanaraine, @gcluley (jawel van sophos), @cloudbook, @metadaddy, @remcobakker, @robstwitts, @meneer (dat ben ik).

Veel leesplezier,

André Koot
Hoofdredacteur

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

Redactie
André Koot (hoofdredactie, werkzaam bij Univé-VGZ-IZA-Trias),
e-mail: A.Koot@Unive.nl
Peter Westerling/Monique van Diessen (eindredactie, TOPpers Media bv, Berlicum)

Redactieraad
Tom Bakker (Delta Lloyd)
Mario de Boer (Logica)
Lex Borger (Domus technica)
Lex Dunn (Capgemini)
Rob Greuter (Secode Nederland)
Aart Jochem (GOVCERT.NL)
Renato Kuiper (HP)
Henk Meeuwisse (Sogeti)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving
Van Velzen Grafisch Ontwerp, 's-Hertogenbosch

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

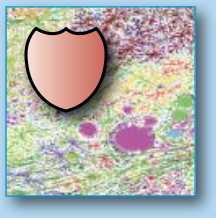
Abonnementen
De abonnementsprijs bedraagt 115 euro per jaar (exclusief BTW), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

Inhoud





AutoNessus: herhaaldelijk scannen realiseert gemak

Auteur: Ing. Frank Breedijk CISSP > Frank Breedijk werkt al ruim drie jaar als Security Engineer voor Schuberg Philis en is bereikbaar via fbreedijk@schubergphilis.com.

Tijdens mijn werk als Security Engineer bij Schuberg Philis maak ik regelmatig gebruik van vulnerability scanners zoals Nessus en OpenVAS. Deze scanners zijn krachtig gereedschap, maar bij lange na niet perfect. Iedere scan levert een rapport op met een groot aantal bevindingen. Iedere bevinding moet (separaat) worden onderzocht om op de juiste waarde te kunnen schatten. Logischerwijs vergt dit een aanzienlijke tijdsinspanning. Vaak worden deze scanners slechts op ad hoc basis ingezet, bijvoorbeeld bij het opleveren van een nieuwe infrastructuur of bij grote veranderingen. De dynamiek van de IT, waar iedere infrastructuur die we beheren regelmatig verandert, maakt het wenselijk scans herhaaldelijk uit te voeren. Deze uitdaging heeft me ertoe aangezet het programma AutoNessus te schrijven, een programma dat het uitvoeren en het verwerken van de resultaten van deze scans vereenvoudigd.

Wat is een vulnerability scanner?
In de voorgaande paragraaf heb ik een aantal keren het woord vulnerability scanner gebruikt, maar… wat is een vulnerability scanner nu eigenlijk?
Een vulnerability scanner is een programma dat als doel heeft kwetsbaarheden in software of infrastructuren geautomatiseerd op te sporen. Nessus en OpenVAS zijn bekende netwerk vulnerability scanners. Deze programma's zijn er dus speciaal op gericht om via het netwerk kwetsbaarheden op te sporen, maar er zijn nog veel meer vulnerability scanners, ieder met zijn eigen doel en insteek (zie kader).

Nessus en OpenVAS werken aan de hand van de volgende procedure:
Stap 1: Stel vast of een IP adres actief is. Hiervoor worden technieken als een ping en een simpele portscan gebruikt;
Stap 2: Probeer vast te stellen welk diensten (services) een IP adres aanbiedt aan het netwerk en welk besturingssysteem aanwezig is;
Stap 3: Bepaal of bekende kwetsbaarheden (mogelijk) aanwezig zijn in de aangeboden services. Dit kan door simpel weg het versienummer van de applicatie te vergelijken met een lijst van bekende kwetsbaarheden, maar ook door eventueel stap 4;
Stap 4: Misbruik een kwetsbaarheid op het systeem om zijn aanwezigheid aan te tonen;
Stap 5: Rapporteer de bevindingen.

Helaas is het zo dat geautomatiseerd vulnerability scanners enkel die kwetsbaarheden vinden waarvoor reeds een test bestaat. Een goede penetration tester zal, geholpen door zijn of haar menselijke creativiteit, meer kwetsbaarheden vinden dan welk geautomatiseerd gereedschap dan ook. Een geautomatiseerde scanner kan en zal dus nooit een compleet beeld geven. Daarnaast is geen enkele test zonder risico. Geen enkele penentration tester of scanner fabrikant zal harde garanties geven dat een test geen enkele invloed zal hebben op de beschikbaarheid van de te testen applicatie of infrastructuur.

Waarom scannen?
Het potentiële risico van een vulnerability scan wordt vaak als argument gebruikt om helemaal niet te scannen. Of er wordt bijvoorbeeld besloten vulnerability scans alleen uit te laten voeren door penetration testers. Hoewel ik de gedachte hierachter begrijp, wil ik iedereen toch aansporen om ook zelf vulnerability scans uit te voeren. En wel om twee redenen: vulnerability scanners zijn vrijelijk beschikbaar voor zowel 'de goeden' als 'de slechten' en het daadwerkelijke risico valt wel mee.

Veel vulnerability scanners zijn open source en/of gratis beschikbaar. Nessus, OpenVAS, NMAP, Nikto en vele anderen zijn voor iedereen te downloaden en dus door iedereen te gebruiken. De informatie die een dergelijke tool geeft over de aanwezige kwetsbaarheden kun je dus feitelijk als publiek beschikbare informatie beschouwen. Het is weliswaar illegaal om zonder toestemming een scan uit te voeren, maar iedereen die wel eens een firewall log gezien heeft, weet dat dit niet betekent dat het niet gebeurt. En als iedereen, goed of slecht, deze informatie kan genereren, kun je het maar beter zelf weten ook.

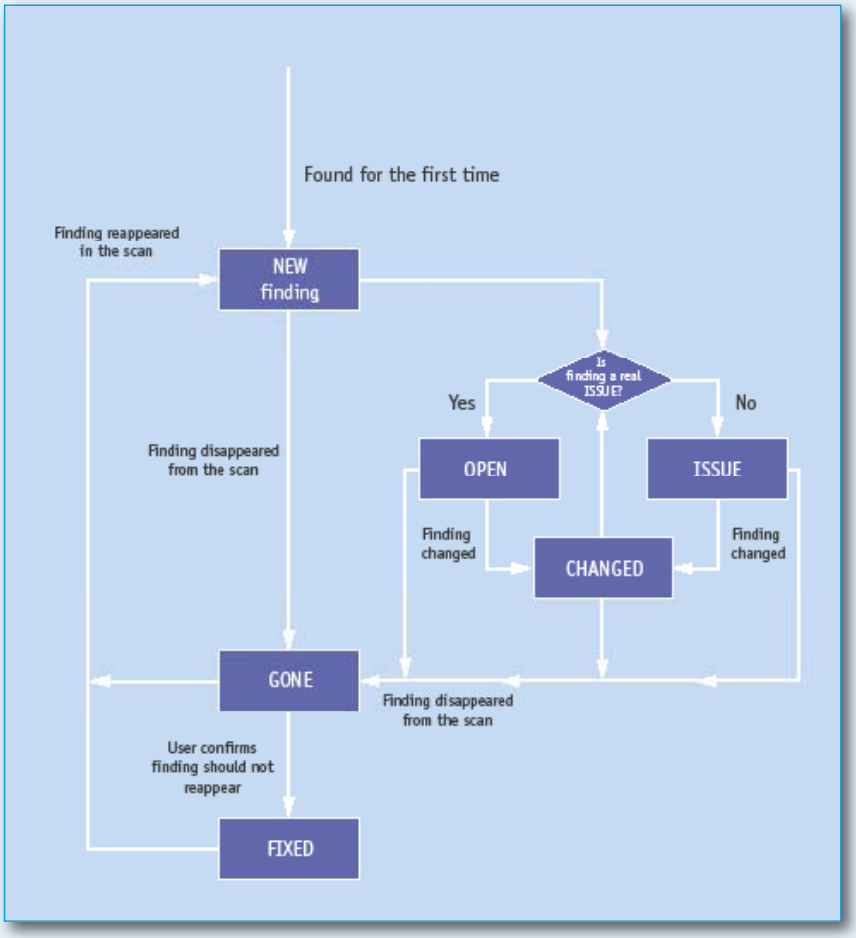
Bij het uitvoeren van een vulnerability scan ontstaat een spanningsveld. Immers, om de drie aspecten van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) te garanderen, moet een actie worden uitgevoerd, waarbij één van deze aspecten, beschikbaarheid, niet honderd procent kan worden gegarandeerd. Dit

risico kan niet worden uitgesloten, maar het is wel te relativeren. Allereerst is de omgeving waarschijnlijk al zonder ons medeweten gescand. Alles wat met het internet verbonden is, wordt immers wel eens gescand. Ten tweede valt het daadwerkelijke risico wel mee. Ik heb in drie jaar redelijk intensief scannen slechts twee maal een infrastructuur tijdelijk verstoort. In beide gevallen was er geen permanente schade en kon de scan met een lagere intensiteit later gewoon worden voortgezet.

Vulnerability scans zijn niet de enige werkzaamheden die verstoringen kunnen veroorzaken, changes zorgen vaak ook voor geplande of ongeplande verstoringen. Door een scan net als een, regelmatig terugkerende, change in te plannen, kan vaak een voor iedereen werkbare situatie geschapen worden.

Dubbel scanner, dubbel werk?

Het controleren van een netwerk op kwetsbaarheden zou geen eenmalige activiteit moeten zijn. Vrijwel iedere IT infrastructuur is aan verandering onderhevig. Zelfs een volledig statische infrastructuur beweegt ten opzicht van zijn omgeving. Iedere dag worden nieuwe kwetsbaarheden gevonden. Een systeem waarin we vandaag geen kwetsbaarheden konden vaststellen, kan met de informatie die we morgen hebben plotseling kwetsbaar blijken te zijn.



Het uitvoeren van een vulnerability scan is relatief eenvoudig. Helaas is het analyseren van de resultaten arbeidsintensief. Om een voorbeeld te geven: ik scan iedere maand een omgeving met 130 IP-adressen. Geen van de IP-adressen biedt normaal gesproken voor de scanner benaderbare diensten aan. Als ik deze infrastructuur met Nessus scan, dan levert dit een rapport van 52 pagina's op met meer dan vierhonderd bevindingen. Het kost mij zeker twee uur om dit volledig door te lezen en zeker vier uur als er ook een formele rapportage nodig is.
Ik vind het erg inefficiënt om elke maand wederom twee uur te investeren om een relatief statische omgeving te scannen, daarom ben ik AutoNessus gaan schrijven.

Wat doet AutoNessus?

AutoNessus is een tool die het mogelijk maakt op gezette tijden automatisch Nessus en OpenVAS scans uit te voeren. Daarnaast reduceert AutoNessus de tijd die nodig is voor het analyseren van twee opeenvolgende scans van dezelfde infrastructuur, door de resultaten van de huidige scan met de eerder beoordeelde resultaten van de voorgaande scan te vergelijken.

Over de auteur

Ing. Frank Breedijk CISSP werkt al ruim drie jaar als Security Engineer voor Schuberg Philis, de leverancier van bedrijfskritische outsourcings diensten met een honderd procent functionele beschikbaarheid. Zijn taken omvatten onder andere het geven security awareness trainingen, vulnerability management, interne security consultancy en het uitvoeren van technische audits. Voor Schuberg Philis werkte hij als security consultant by INS (nu BT), als ICT Security Officer bij InterXion en was hij drie en een half jaar langer manager van het EMEA Security Operation Center voor Unisys Managed Security Services. Naast zijn werk is Frank de auteur van AutoNessus. Frank is bereikbaar via het email adres fbreedijk@schubergphilis.com.

Stel dat een infrastructuur voor het eerst via AutoNessus wordt gescand. Als de vulnerability scanner zijn werk heeft gedaan, worden de resultaten naar AutoNessus gezonden. AutoNessus leest de scanresultaten en slaat ze intern op. Ook het scannerrapport (dat van 52 pagina's) wordt als HTML of XML bestand opgeslagen.

De AutoNessus web interface heeft twee functies. Allereerst staat hij je toe de bevindingen op verschillende manieren te filteren, waardoor er minder tijd nodig is voor de analyse.

Het belangrijkste is echter een status aan de bevindingen te hangen die aangeeft of een bevinding al dan niet een daadwerkelijke kwetsbaarheid is.

Als we nu dezelfde infrastructuur nogmaals scannen, kan deze statusinformatie op een slimme manier gebruikt worden om te bepalen welke bevindingen aandacht nodig hebben:

- Bevindingen die in de vorige scan niet voorkwamen, maar in deze scan wel (bijvoorbeeld omdat een nieuwe host is gevonden);
- Bevindingen waarvan de tekst veranderd is (bijvoorbeeld omdat het versienummer van een webserver is veranderd);
- Bevindingen die in de vorige scan wel voorkwamen, maar in deze scan niet (bijvoorbeeld omdat een kwetsbaarheid is opgelost).

Doordat de hoeveelheid te analyseren informatie afneemt, is er minder tijd nodig voor de analyse. Daarnaast gaat de accuratesse omhoog omdat de repetitiegraad van het werk omlaag gaat. Dat dit het resultaat ten goede komt, moge duidelijk zijn.

Praktijkvoorbeeld: Schuberg Philis

Mijn werkgever Schuberg Philis biedt outsourcing van bedrijfskritische applicaties met een honderd procent functionele beschikbaarheid. We gebruiken AutoNessus nu bijna twee jaar en scannen alle externe IP-adressen van al onze klanten (4000+ adressen) iedere maand. We scannen onder andere een flink aantal online banken, een grote webshop en de publieke website van een grote financiële instelling. Op dit moment staat een kleine

Vulnerability scanners

- Nessus – Network vulnerability scanner - www.nessus.org
- NMap – Network Mapper – www.insecure.org
  De network portscanner
- OpenVAS – Open Source network vulnerability scanner
  www.openvas.org
  Gebaseerd op de laatste opensource Nessus versie
- Nikto – Web server vulnerability scanner
  http://www.cirt.net/code/nikto.shtml
- Arirang – Open Source web server security scanner
  http://monkey.org/~pilot/arirang/
- Acunetix – Web application security scanner
  http://www.acunetix.com/
- GFI Languard – Network vulnerability scanner
  http://www.gfi.com/languard/
- Retine – Network vulnerability scanner
  http://www.eeye.com/html/Products/Retina/index.html
- SAINT – Network security scanner
  http://www.saintcorporation.com/index.html
- Qualys – Software as a Service network vulnerability scanner
  http://www.qualys.com/
- N-Stalker – Web application vulnerability scanner
  http://www.nstalker.com/
- Core Impact – Penetration testing tool
  http://www.coresecurity.com/
- IIS Internet Scanner – Network based application level scanner - http://www.iss.net/
- Microsoft Baseline Security Scanner – Microsoft Security Tool
  http://www.microsoft.com/technet/security/tools/mbsahome.mspx
- Hailstorm – Network vulnerability scanner
  http://www.cenzic.com/products_services/cenzic_hailstorm.php
- WebInspect – Web application vulnerability scanner
  http://www.spidynamics.com/products/webinspect/index.html
- NTO Spider – Web application vulnerability scanner
  http://www.ntobjectives.com/products/ntospider.php
- Grabber – Web application vulnerability scanner
  http://rgaucher.info/beta/grabber/
- Wapiti – Web application vulnerability scanner
  http://wapiti.sourceforge.net/

9000 bevindingen in het systeem. Voor de analyse van de resultaten is slechts ongeveer anderhalf à twee mandagen nodig. Ter illustratie: voor het analyseren van een eerste scan van 255 adressen is minimaal een halve dag nodig.

Conclusie

Wat mij betreft zou iedereen die een IT infrastructuur beheert deze regelmatig met een vulnerability scanner moeten controleren. Indien je verstandig met het geringe risico op downtime omgaat, is er altijd wel een moment te vinden waarop gescand kan worden. AutoNessus is een door mij geschreven open source tool, die de hoeveelheid werk gepaard gaand met het herhaaldelijk scannen van dezelfde infrastructuur kan reduceren en de nauwkeurigheid van de analyse kan verhogen.

Een overzicht van alle bevinding met status CHANGED van plugin 14260 voor een specifieke infrastructuur.

Een overzicht van een enkele bevinding. De status en remark velden kunnen door de gebruiker worden aangepast. Het veld diff geeft het textuele verschil tussen de laatste en de voorgaande scan aan.

Links

- www.autonessus.com
- www.schubergphilis.com
- http://twitter.com/autonessus
- http://www.linkedin.com/in/schanulleke
- www.cupfighter.net

Black Hat Europe 2009

Auteur: Lex Borger, met bijdragen van Ronald van Erven en Ronald Rietveld

Het PvIB sponsort Black Hat in Europa en de locatie is dit jaar weer Amsterdam. Dit geeft de redactie van Informatiebeveiliging een prachtige kans om deze speciale conferentie bij te wonen. Het is en blijft een hele goede ervaring om als beveiliger blootgesteld te worden aan de beste aanvallen die mogelijk zijn. En deze worden gepresenteerd op Black Hat, met een hoog 'show-me' gehalte. Als het even kan, wordt het live getoond.

De kledingcode is duidelijk 'extreme casual' en de sfeer Amerikaans. Een goede tip is het om alle draadloze communicatie op je gadgets uit te schakelen. Je weet maar nooit. Ondanks de getoonde aanval op GSM, durf ik het nog net aan mijn telefoon wel aan te laten staan.

Hierbij een bloemlezing van de bijgewoonde presentaties:

Fun and Games with Mac OSX and the iPhone
Charlie Miller & Vincenzo Iozzo
Charlie en Vincenzo doen een leuke duo-presentatie waarin ze laten zien dat de Mac zeker niet onfeilbaar is in zijn beveiliging. Ze beschrijven een aanval op de Mac in twee stadia.
Voor de eerste stap gebruiken ze het feit dat de programmalader niet deelneemt in de address space layout randomization (ASLR) om een willekeurig programma wat geladen wordt te besmetten. Door de lader in het geheugen aan te passen bijvoorbeeld via een email bijlage kan als volgende stap elke programmacode geïnfecteerd worden.

Verder laten ze nog wat andere zaken zien, zoals een port van de Meterpreter naar de Mac, waarmee redelijk ongemerkt een programmacode in het geheugen uitgevoerd kan worden. Ze geven ook een leuk overzicht van de security architectuur van de iPhone. De iPhone is hier en daar eenvoudiger dan de Mac (geen ASLR), maar gebruikt ook meer geavanceerde geheugenbescherming. Het grappige hierbij is dat het al snel duidelijk werd dat een 'jailbroken' iPhone essentieel onveiliger is dan de gewone iPhone. Nog leuk om te vermelden is dat de iPhone alle applicaties in 'sandboxes' draait, en dat er verschillende typen zijn, zodat eigen iPhone applicaties, zoals Safari en SMS minder restricties hebben dan applicaties uit de iStore.

Bron: William Hook via Flickr

A Cloud Security Ghost Story
Craig Balding
Cloud computing is een nogal vaag begrip. Het is dan ook verhelderend als je een presentatie bijwoont waar het helder uitgelegd wordt door een autoriteit op dit gebied. Het meest verhelderend zijn de kenmerken die hij schetst, die op elke cloud van toepassing zijn: Het is een service model, dus... – as-a-service, het is beschikbaar on-demand, afrekening pay-as-you-go en het is elastisch – het kan dynamisch groeien en krimpen.

'It's only day 1 for Cloud computing', alle bekende security problemen zijn ook van toepassing op cloud computing. Echter; de huidige aanbieders lijken hier nog weinig aandacht voor te hebben gehad en meer te focussen op performance, zoals met een aantal voorbeelden wordt geïllustreerd:

- Er zijn issues (geweest) met 'het opschonen' van vrijgegeven storage.
- Bij AWS is één account en password gekoppeld aan één creditcard. Er is nog geen verdere differentiatie mogelijk in sub-gebruikers met eigen passwords en rechten.
- Een aantal data replicatie fouten. In hoeverre wordt de integriteit gewaarborgd door de cloud?
- Geen transparantie ten aanzien van security controls in de cloud, maar een 'trust us' houding.
- Weinig aandacht voor vulnerability reporting processes (behalve bij MS).

Stripping SSL To Defeat HTTPS in Practice
Moxie Marlinspike
Dit was zonder meer de meest interessante presentatie op Black Hat dit jaar. Moxie voldoet geheel aan het stereotype beeld

van een hacker. Dat zet in ieder geval een goede toon voor de presentatie. Moxie is erg rustig, terughoudend in zijn presentatiestijl, hij laat de wow-factor over aan de inhoud. Hij beschrijft eerst hoe hij jaren geleden een tool sslsniff heeft geschreven, wat gewoonweg een man-in-the-middle aanval uitvoert op een SSL-verbinding door naar beide zijden technisch correcte SSL-verbindingen te leggen. Het enige nadeel is dat naar de client-kant de vertrouwensketen van de certificaten niet helemaal klopt. Hij maakt hierbij gebruik van aspecten die de browsers toen niet controleerden of waar je zo'n vage foutmelding op krijgt, dat je de gebruiker toch kunt overhalen het certificaat te accepteren. Met name het controleren van de basic-contraints van certificaten wordt nog steeds niet goed geïmplementeerd.

Maar nu de recente activiteiten. Browsers zijn beter in het controleren van certificaten (maar nog niet goed) en gebruikers zijn zich meer bewust van de waarschuwingsdialogen. Dus, redeneert Moxie, gaan we SSL helemaal van de connectie afhalen. Veel websites proberen in hun inhoud nu al ons zo te overtuigen van de beveiliging van de pagina, dat de 's' in https:// nauwelijks nog opvalt. Verder zijn er steeds meer sites die de (veilige) 'log in' knop op een gewone webpagina zetten. Als gebruiker moet je maar vertrouwen dat je op een SSL-pagina uitkomt. Is dat niet het geval, dan is je wachtwoord toch al verzonden. Moxie heeft hier ook een applicatie voor geschreven, sslstrip. Hij laat zien wat er is gebeurd toen hij dit draaide op de uitgang van een TOR-server. Hij wist honderden accounts met bijbehorende wachtwoorden te vangen. Veel effectiever dan phishing.

Bron: bpedro via Flickr.com

Het gebruiken van een TOR-server is voor een hacker eigenlijk het equivalent van het bevuilen van je eigen nest. Dat beseft hij zich en dus is hij bezig met een applicatie voor TOR-gebruikers om te testen of de online TOR-nodes zich netjes gedragen op dit punt. Grappige twist.

Op het eind was ik heel blij met mijn beslissing om mijn draadloze communicatie uit te zetten. Moxie toonde acht wachtwoorden op een slide. Hij vertelde hierbij dat hij sslstrip twaalf minuten had aangezet tijdens de ochtendkoffie en in dit publiek van veiligheidsbewuste professionelen het mogelijk was om deze wachtwoorden te verzamelen!

Link:
www.thoughtcrime.org/software/sslstrip/

Hijacking Mobile Data Connections
Roberto Gassira & Roberto Piccirillo
De twee Roberto's presenteerden hun aanval op de smartphone - elke telefoon met een internetfunctie. De basis van hun idee is om de DNS-instellingen van de telefoon te wijzigen naar hun eigen DNS-server. Als dat eenmaal gedaan is, heb je alle internetverkeer op de telefoon volledig overgenomen. Ze spelen dit klaar door een provisioning sms te sturen naar de gebruiker, vooraf gegaan door een gespoofde notificatie van de bijbehorende PIN naar de telefoon. Hun ervaring is dat de eigenaar bijna klakkeloos de pincode accepteert en die vervolgens ook ingeeft als de telefoon provisioned wordt. Alles vanaf dit moment is een grote man-in-the-middle aanval. Deze aanval omvat ook de 'eigen' sites van de mobiele provider, omdat die ook gewoon via DNS lopen.

Wat ze in de praktijk gevonden hebben, is dat in de praktijk mobiele providers geen filtering toepassen op hun sms-verkeer om vreemde provisioning sms-berichten te voorkomen. Op de telefoon zelf is het ook moeilijk, de aanvaller hoeft alleen maar wat spoofing erbij te betrekken om de telefoon van echtheid te overtuigen. Verder merkten ze op dat mobiele providers ook geen filtering toepassen op het 'eigen' internetverkeer om verkeerd DNS-verkeer of onderschepte interne sites te detecteren.

Passports Reloaded Goes Mobile
Jeroen van Beek (dexlab.nl)
In deze presentatie een Nederlands succes: Jeroen van Beek laat zien hoe onveilig de nieuwe generatie paspoorten zijn, doordat de internationale afspraken zo flexibel zijn.

Het Nederlandse paspoort zou goed beveiligd zijn, want het heeft een elektronische handtekening en actieve authenticatie van de RFID-informatie. Al deze elementen staan op de chip van het paspoort in aparte files. De lay-out van dit geheel is gestandaardiseerd in de ICAO-specificaties. Nu willen niet alle landen in de wereld zo volledig meedoen als Nederland, dus veel van de elementen die het paspoort beveiligen zijn optioneel. Nu blijkt dat het ontbreken van informatie gewoon betekent dat dit optionele deel niet aanwezig is. Het is dus mogelijk om een paspoort te klonen, als je maar selectief delen weglaat.

In de basis gebruikt Jeroen een zelf-ontwikkelde kopieerapplicatie/emulator. Hiermee kan hij informatie kopiëren en valideren. Vervolgens toont hij vele paspoort RFID-hacks live. Hij laat door middel van filmpjes ook zien dat het op de scanners van Schiphol en op een gemeentehuis werkt.

Hij gaat nog een stap verder. Behalve kopiëren, kan hij ook zijn eigen paspoort-informatie genereren. Ook hierbij laat hij zien dat het mogelijk is om een geldig paspoort voor Elvis Presley te maken. Hij laat zelfs zien dat het mogelijk is een nieuw land te definiëren en een geldig paspoort uit te geven. Het probleem hier is dat lang niet alle landen de top-certificaten van andere landen cross-signen. Een self-signed certificaat is dus voldoende om een

WWW.HEROTH.NL – WWW.SECURITYACADEMY.NL

SECURITY SERVICES

Heroth is een onafhankelijke dienstverlener die op een betrouwbare en slagvaardige wijze security, compliance en business continuity diensten levert.

Wij kunnen adviseren op de volgende gebieden:
- Definiëren, opstellen en onderhouden van het informatiebeveiligingsbeleid en organisatie
- Periodiek uitvoeren van Risico Analyses
- Implementeren van normen als ISO27001, ISO27002, NEN7510
- Ontwikkelen en uitvoeren van bewustwordingsprogramma's
- Periodiek inzet van een Mystery Guest
- Periodiek uitvoeren van netwerkscans en penetratietesten

SECURITY ACADEMY

Onderdeel van Heroth is de Security Academy. De Security Academy is het opleidingsinstituut in Nederland dat zich specifiek richt op het vakgebied informatiebeveiliging. Zo kunt u aan de Security Academy o.a. de volgende opleidingen volgen:
- Post- HBO Information Security Management Professional
- Post- HBO Information Security Technology Professional
- CISSP

Zie www.securityacademy.nl voor meer informatie.

COMPLIANCY SERVICES

Het aantoonbaar 'in contol' zijn wordt voor organisaties steeds belangrijker. Mede ingegeven door wet- en regelgeving. Denk hierbij aan Sarbanes Oxley, Basel II, code-Tabaksblat en ISO 27001 en ISO 27002. Met de GRC Monitor helpen wij u om 'in control' te komen en te blijven.

De GRC Monitor software ondersteunt u op strategisch en tactisch niveau bij het gehele proces van gapanalyse tot inrichting, verankering, audit, rapportage en beheer van GRC controls en maatregelen.

Onze dienstverlening is speciaal ontwikkeld om het overzicht te houden op de snelle veranderingen van wet- en regelgeving. De zogeheten "compliance" processen worden op een overzichtelijke grafische wijze aan het management gepresenteerd. Hiernaast automatiseert de GRC Monitor veel repeterende controle- en test taken op operationele systemen. U vermindert aantoonbaar de kosten, de complexiteit en de doorlooptijd van compliance en risk management processen.

Heroth B.V. | De Bleek 11| 3447 GV | Woerden | 030-210 60 16 | www.heroth.nl | info@heroth.nl

Bron: jeanbaptisteparis via Flickr.com

paspoort acceptabel te maken!

En als je denkt dat je alles gezien hebt, haalt Jeroen een Nokia NFC telefoon erbij en hij laat zien dat je met de NFC-applicatie ook gewoon een paspoort kunt emuleren. En als klap op de vuurpijl toont hij aan dat je met wireless communicatie gegevens kunt aanbieden aan een paspoortlezer van een paspoort dat helemaal niet ter plekke aanwezig is!

Nu werkt dit alles nog niet echt bij grenspassage omdat er nog steeds een visuele controle van het paspoort plaatsvindt. Maar je ziet op een aantal plaatsen in de EU inmiddels onbemande paspoortleesstations opkomen. Hier zijn dit soort aanvallen theoretisch wel mogelijk succesvol.

Jeroen sloot af met een aantal aanraders voor paspoortbeveiliging. Veel punten op zijn lijst vergen echter wel internationale afspraken en samenwerking bij de naleving daarvan.

Yes It Is Too WiFi, and No It's Not Inherently Secure

Rob Havelt

Deze presentatie gaf een onverwachte draai aan een vergeten draadloze communicatie-techniek - FHSS (frequency hopping spread spectrum). Dit is een techniek uit 1999, maar de basis is gelegd in de Tweede Wereldoorlog. Het heeft wat weg van een simpel BlueTooth-protocol.

Toegangsbeveiliging is op basis van MAC en encryptie is 40-bit WEP. Beiden zijn lang sinds gebroken. Toch vinden veel auditors dat de techniek veilig is, omdat er geen speciale apparatuur meer te krijgen is om deze techniek aan te vallen.
Waar wordt het gebruikt? In bijna elke fabriek of warenhuis met draadloze techniek om bijvoorbeeld barcodes te scannen. Typisch zijn de FHSS-routers direct aangesloten op de bedrijfseigen IP-netwerken. Dus eenmaal gebroken, heeft een aanvaller netwerktoegang.
Rob laat zien hoe je met een software radio-ontvanger door slechts een kanaal af te luisteren binnen minuten het netwerk SSID te pakken hebt. Daarna nog even proberen om de frequency hopping te kunnen volgen. Mac-spoofing en WEP-breken geven we Rob kado. Dat geloven we wel. De laatste stap om daarna actief geldig radioverkeer te genereren, doet hij met BlueTooth-apparatuur.

Tactical Fingerprinting Using Metadata, Hidden Info and Lost Data

Chema Alonso

Een uitgebreide presentatie en demonstraties over het uitlezen van de informatie in de metadata van files. Chema is medeontwikkelaar van een programma genaamd FOCA. Dit programma wordt gebruikt om metadata informatie te verzamelen. Interessant is bijvoorbeeld dat in jpeg-bestanden ook het serienummer van de fotocamera word opgeslagen.

Het uitlezen van metadata word veel door de autoriteiten gebruikt bij het oplossen van misdrijven, maar ook om mogelijk plagiaat bloot te leggen. Zo geeft Chema een voorbeeld van een document dat door Tony Blair gepubliceerd leek te zijn.
Toch bleek dit niet het geval na analyse van de metadata.

Integrating Maltego with Offensive and Defensive Open Source Tools

Roelof Temmingh and Chris Bohme

Roelf en Chris geven een dynamisch demo waar hun tool Maltego toe in staat is: het visualiseren en analyseren van relaties tussen een complexe hoeveelheid informatie.
Van IP- addressen, e-mails, dns-namen, tot resultaten van zoekmachines, met een paar kliks weten de heren fantastische relaties bloot te leggen met hun tool.
De nieuwe versie ondersteunt transforms voor Nmap en Nessus-scan resultaten, waardoor ook systeem services, vulnerabilities en finger printing eenvoudig kan worden betrokken in de analyse. Ook nieuw is de ondersteuning voor SQL database queries, waarmee binnen no time een paar forumgebruikers worden opgespoord, die via/via worden herleid naar hun Hyves-pagina. Als laatst krijgen we nog een 'privé' demo waarbij Maltego via privéscripts is gekoppeld aan een Squid-proxy en on-the-fly sessie cookies gebruikt om de contacten van je Gmail- en Facebook-accounts leeg te trekken voor het betere speur werk.
Helaas is deze optie niet te koop...
In de release die binnenkort uitkomt, kun je zelfs je eigen transforms (input conversie script) creëren en delen met anderen, waardoor de mogelijkheden nog breder worden.

MALTEGO[2]

Links

1 http://www.paterva.com/maltego/
2 http://www.paterva.com/papers/BH-Amsterdam-2009-final.pdf

Auteur: Remco van Mook > Remco van Mook is manager Business Development Europe van Equinix. Hij is bereikbaar via remco@eu.equinix.com.

De beveiliging van IP-routing is een aanfluiting

Ook goedemiddag. De kop liegt er niet om: IP-routing is qua beveiliging een puinhoop en dat het internet het überhaupt nog doet, is een waar wonder. En het is waar: geen enkel IP-routing protocol dat in breed gebruik is, heeft enige vorm van versleuteling of authenticatie. Losse berichten zijn vaak nog makkelijk na te bootsen ook; veel protocollen gebruiken zelfs een broadcast en zijn dus door iedereen te lezen! Maar wat is het probleem hier eigenlijk?

Wat een routing protocol doet is eigenlijk simpel. Apparaten wisselen kennis uit over netwerken waarmee ze verbonden zijn (of waar ze een route voor weten). Intern wordt daar een IGP (Interior Gateway Protocollen) voor gebruikt, zoals RIP, OSPF, IS-IS. Tussen netwerken vooral BGP (Border Gateway Protocol). Niet zomaar alle beschikbare informatie wordt uitgewisseld, voor een externe partij is informatie over interne routes niet relevant. Alle informatie die vergaard wordt door het 'praten' met andere apparaten wordt op één hoop geveegd, de RIB (Routing Information Base). Vervolgens wordt op basis van een aantal (protocol afhankelijke) criteria uit deze grote hoop per route de beste gekozen en opgenomen in de FIB (Forwarding Information Base). Dit is de feitelijke actieve routetabel op basis waarvan IP-pakketten worden doorgestuurd. Elke keer dat er een verandering optreedt in de RIB wordt deze opnieuw doorgerekend en wordt de FIB aangepast.

Criteria die worden gebruikt voor de selectie zijn bijvoorbeeld de bandbreedte van een verbinding, de lokale voorkeur, de lengte van het pad en hoe specifiek een route is. Het voert te ver om hier een uitputtende opsomming te geven, maar het is in elk geval van belang dat een criterium als 'geloofwaardigheid' ontbreekt. Met andere woorden, als het lukt om op wat voor manier dan ook informatie aan de RIB toe te voegen, dan bestaat de kans dat die informatie gebruikt zal gaan worden om IP-pakketten te gaan routeren.

Voor een intern netwerk (en dus een IGP) is een goede netwerkhygiëne voldoende om narigheid te voorkomen. Zolang een routing protocol alleen wordt gebruikt op verbindingen tussen routers (en dus niet zomaar op elke switchpoort voorbij komt) is er weinig aan de hand. Het toevoegen van een key, zoals bij de meeste protocollen kan, is eerder bedoeld om te voorkomen dat onbedoeld verkeerde informatie wordt gebruikt, dan als beveiliging – de key is namelijk onversleuteld in elk pakketje opgenomen.

IP-routing protocollen wisselen informatie in-band uit, dus over dezelfde verbinding als het feitelijke dataverkeer. Op deze manier wordt voorkomen dat IP-routing informatie nog wel aankomt, maar het dataverkeer een zwart gat in verdwijnt. Vervelend genoeg betekent het ook dat het dus mogelijk is om via dat dataverkeer extra IP-routing pakketjes te injecteren, die dan vervolgens door de netwerk-apparatuur behandeld worden als de reguliere routing-informatie. Dat dit niet vaak gebeurt, komt vooral doordat het wat lastiger is om dit te doen dan het klinkt, er moet nogal wat informatie gegokt worden. Voor bijvoorbeeld een BGP-verbinding hebben we het dan over een 16-bit poort-nummer en een 32-bit TCP-sequence nummer, dus in feite 48 bits aan 'versleuteling'. In theorie. In de praktijk

bleek tot een aantal jaren terug het aantal te gokken bits om de verbinding te verstoren eerder rond de zes of zeven te liggen. Met andere woorden, met een keer of dertig gokken was het prijs. Als remedie werd door een flink aantal grotere netwerken het gebruik van MD5 checksums in TCP geëist voor het uitwisselen van IP-routing, een draak van een standaard die elke TCP-header voorziet van een MD5-checksum van de inhoud en een 'shared secret'.

Een ander belangrijk aspect van met name BGP-informatie is dat het transitief is. Tenzij er expliciet wordt gefilterd, wordt door een apparaat eenmaal ontvangen informatie zonder nadenken doorgestuurd naar andere apparaten. Zo kon het dus gebeuren dat door een fout in de configuratie bij Pakistan Telecom de halve wereld niet meer bij YouTube kon komen – of in elk geval dacht dat YouTube in zijn geheel naar Karachi of Lahore was verhuisd. Nu was dit natuurlijk een bijzonder opvallende gebeurtenis die er voor zorgde dat veel netwerkbeheerders over de hele wereld een slechte zondagmiddag hadden. Hetzelfde trucje wordt ook gebruikt voor bijvoorbeeld het versturen van spam.
Er duikt ineens een ongebruikt blok IP-adressen op het internet op dat in korte tijd een grote hoeveelheid spam-mail verstuurt en daarna weer spoorloos verdwijnt.

Hier aangekomen vraag je je af hoe het in vredesnaam mogelijk is dat internet nog werkt, en waarom dit soort dingen kunnen gebeuren. Internet is immers 'serious business'. Er wordt wel degelijk veel gedaan door individuele partijen, echter; niet alle partijen doen even veel. Zo bestaat binnen Europa een redelijk werkend systeem voor het uitwisselen van filterinformatie tussen netwerken (de RIPE routing DB), maar in andere regio's bestaat zo'n systeem of niet, of het is niet in breed gebruik. Daarnaast wordt op vrijwillige basis door een aantal organisaties nog meer lijsten met 'onzin' netwerken bijgehouden, zoals de zogeheten 'bogon' lijst.

Filteren heeft ook zijn nadelen: voor hele grote wereldwijde netwerken is er simpelweg geen beginnen meer aan. Ze bedienen zo veel klanten en hebben zo veel koppelingen met andere netwerken dat de filters domweg niet meer in de apparatuur passen. Daarnaast is het aanpassen van filters niet gestandaardiseerd en niet in real-time. Dat betekent dus dat elk groter netwerk naast zijn routers nog een apart stuk software (vaak zelfgemaakt) heeft draaien dat deze lijst met filters bijhoudt. Met name de lijst van 'onzin' netwerken wordt vaak niet automatisch vernieuwd, wat tot grote problemen leidt bij het in gebruik nemen van nieuwe IP-adressen door een netwerkaanbieder. De kans is groot dat het blok nog wel ergens in de wereld in een filter voorkomt en dat je netwerk dus uit bepaalde delen van de wereld onbereikbaar is - vaak kom je daar pas achter als de klant al aan de telefoon hangt.

Op technisch vlak wordt er wel degelijk voortgang geboekt. Na een lange aanlooptijd lijkt de Internet Engineering Task Force (IETF) het eens te gaan worden over een standaard voor beveiligde BGP. Tegelijkertijd wordt er wereldwijd hard gewerkt aan een PKI voor blokken internetadressen.

Maar op andere vlakken komen we de echte problemen tegen:

1) Netwerken worden betaald om verkeer te transporteren, niet om het niet te transporteren. Met andere woorden, filteren kost dus omzet. Het kan ook geld schelen natuurlijk, maar dat verband is veel minder direct.
2) Niemand is de baas op het internet. Dat betekent dus ook dat er geen centrale autoriteit is die kan bepalen wie wel en wie geen toegang heeft. Er zijn zelfs grote blokken adresruimte waarvan wel bekend is dat ze ooit zijn uitgedeeld, maar niet meer aan wie. Of blokken waar het eigendom na vijftien jaar fusies, splitsingen en overnames niet meer duidelijk toebehoort aan één organisatie. Of wordt betwist.

Je kunt je de vraag stellen of het internet wel tot stand was gekomen in zijn huidige vorm als er wel een centrale autoriteit was en of het wel wenselijk is dat er een manier komt om op internet te bepalen wie wel en geen toegang krijgt. Een dergelijk mechanisme zal kunnen rekenen op lange rijen van juristen en diplomaten die vinden dat Jantje, Miquel, Roshan of Aung San maar vooral van het internet geweerd dienen te worden. En dat lijkt mij een buitengewoon slecht idee.

Ik geef het questafettestokje door aan Marcel Lavalette van CompLions met de stelling: 'De veelheid aan specifieke IT-security certificeringen (ISO27001, SAS70, PCI-DSS, NEN7510) doet afbreuk aan het doel van certificatie'.

Internet: anonimiteit versus verantwoording

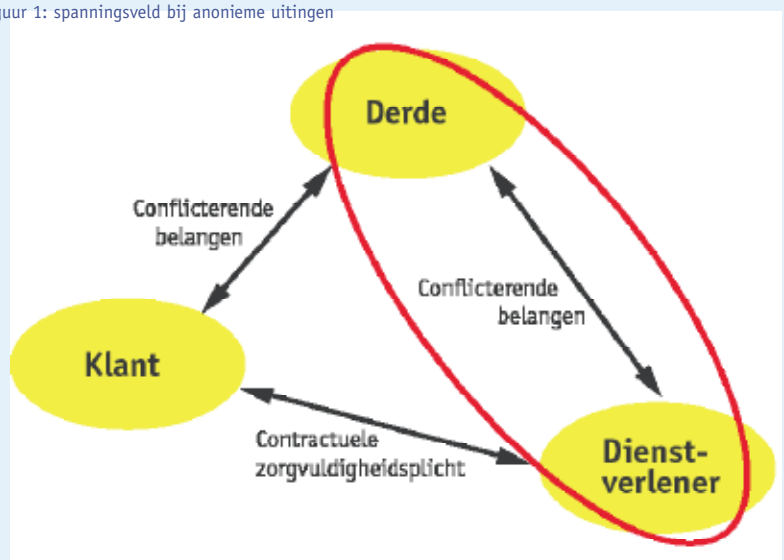
Auteur: ing. Ellen Wesselingh > Ellen Wesselingh is als docent verbonden aan de opleiding Information Security management van de Haagse Hogeschool.

Dienstverleners die diensten aanbieden op internet kunnen te maken krijgen met het gedrag van hun klanten. Internet is een digitale openbare ruimte, waar mensen met hun uitingen of handelen anderen kunnen beschadigen. We denken dan aan uitingen die door derden als beledigend of als laster worden ervaren, of het aanbieden van inhoud die intellectuele eigendomsrechten schendt. De derde wiens belang wordt geschonden, zal willen weten wie de persoon is die dit heeft gedaan en zal dan een beroep doen op de internetdienstverlener om persoonsgegevens van de anonieme eigenaar van de informatie te achterhalen, de NAW (naam, adres, woonplaats) gegevens. De dienstverlener heeft er een zeker belang bij dat zijn klanten (de inhoudsaanbieders) geen onrechtmatige dingen doen via de diensten die hij aanbiedt, maar is niet zelf direct in zijn belang geschaad. Wat moet die dienstverlener dan met een verzoek om hulp bij de aanpak van de inhoudsaanbieder die de rechten van een derde partij schendt?

Het verzoek om verstrekking van persoonsgegevens brengt de internetdienstverlener in een spanningsveld tussen enerzijds het recht op persoonlijke levenssfeer en anderzijds het recht om gevrijwaard te blijven van allerlei onrechtmatige uitingen en criminaliteit. Het eerste verplicht de dienstverlener niet zo maar de gegevens van zijn klanten vrij te geven, het tweede verplicht de dienstverlener om mee te werken door gegevens ter beschikking te stellen. Dit belangenconflict is hieronder weergegeven. De focus in dit artikel ligt op de relatie tussen de derde en de dienstverlener. Tot nu toe werd de strijd om de persoonsgegevens nogal eens via de rechter gestreden (waarover later meer), maar om een aantal redenen is dit een onwenselijke situatie.

Ten eerste is de gang naar de rechter een forse drempel. Het is een zwaar middel om via de rechter gegevens af te moeten dwingen voordat over de inhoud van het conflict gestreden kan worden. Daarnaast wordt de rechterlijke macht door dit soort procedures extra belast. Tenslotte is het een vreemde situatie dat de dienstverlener, die in feite geen partij in het conflict is, zich voor de rechter moet verantwoorden ten behoeve van iemand anders.

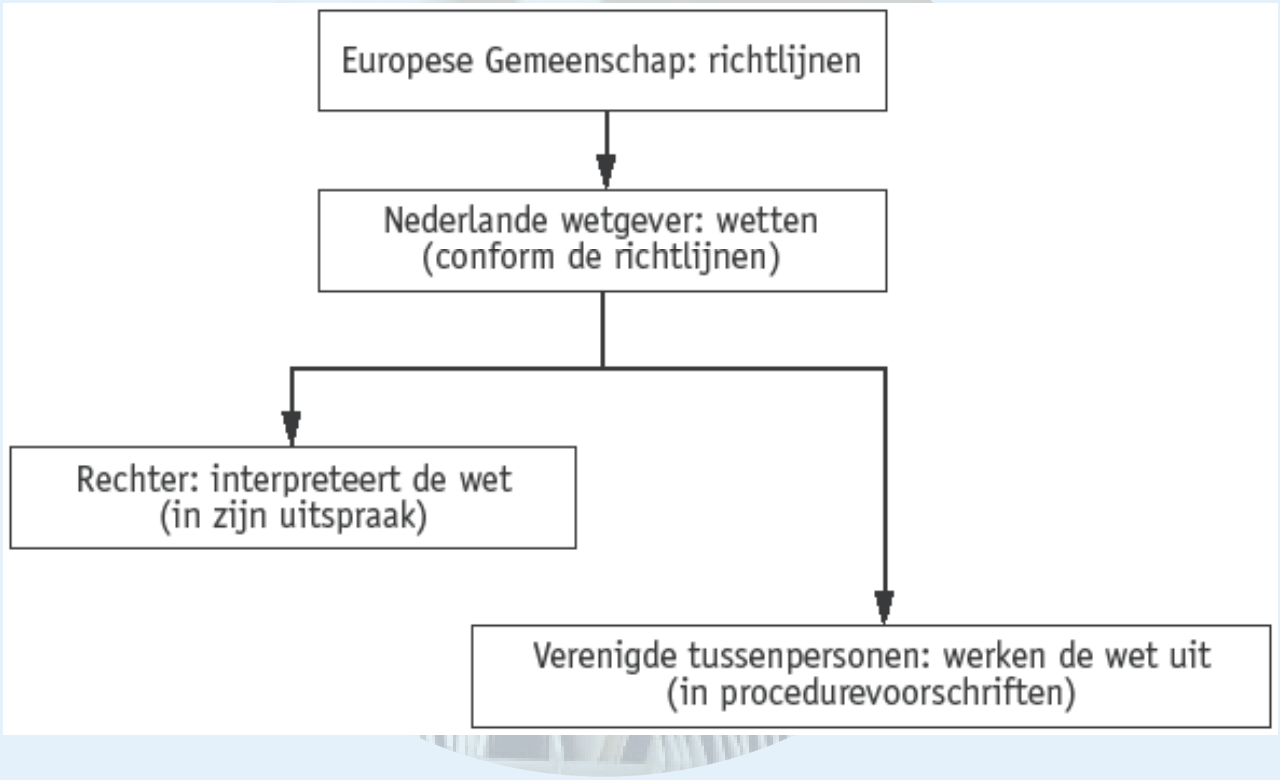
Figuur 1: spanningsveld bij anonieme uitingen



De branche over het verstrekken van identificerende gegevens

De gang naar de rechter is niet ideaal en daarom heeft een aantal partijen het initiatief genomen om tot een andere procedure te komen. In oktober 2008 is de gedragscode Notice-and-Take-Down van kracht geworden. De code beschrijft hoe dienstverleners moeten omgaan met meldingen van onrechtmatig en strafbaar gedrag. De acties die een dienstverlener kan ondernemen zijn bijvoorbeeld het off-line halen van ongewenste inhoud en het verstrekken van persoonsgegevens aan anderen wiens belang is geschaad. Onderschrijving van de code is vrijwillig en betreft internetdienstverleners in Nederland.

De gedragscode geeft vooral de procedurele aspecten aan, er wordt geen indicatie gegeven van wat ongewenste inhoud zou kunnen zijn. Wel wordt gesteld dat er een argument gegeven moet worden voor de beoordeling of er persoonsgegevens moeten worden verstrekt, waarbij dat argument de onmiskenbare onrechtmatigheid en/of strafbaarheid duidelijk maakt. Het is niet altijd juridisch af te dwingen dat de persoonsgegevens van de inhoudsaanbieder worden verstrekt, maar de gedragscode sluit nadrukkelijk aan bij de stappentoets die door het hoogste rechtscollege, de



Figuur 2: wie stelt welke regels vast?

Hoge Raad, is gegeven voor het verstrekken van persoonsgegevens.

De gedragscode maakt onderscheid tussen een onmiskenbaar onrechtmatige inhoud en de situatie dat de dienstverlener niet tot een eenduidig oordeel kan komen. In het eerste geval worden de identificerende gegevens verstrekt, in het tweede geval niet. Als niet tot een eenduidig oordeel te komen is, zal de dienstverlener de inhoudsaanbieder op de hoogte stellen en verzoeken de inhoud te verwijderen. De gedragscode sluit in zoverre aan bij de wet dat deze code voornamelijk gaat over het blokkeren van onrechtmatige inhoud.

Er zit in de code nog een aantal punten dat voor problemen kan zorgen bij verstrekking van persoonsgegevens. De gedragscode gaat uit van onmiskenbare onrechtmatigheid waar de rechter uitgaat van aannemelijke onrechtmatigheid, de gedragscode geeft echter een strengere toets aan. Daarnaast maakt de gedragscode niet helder dat de dienstverlener afzonderlijke afwegingen moet maken voor het blokkeren van de inhoud en het verstrekken van identificerende gegevens. Ook het juridische belangrijke principe van hoor en wederhoor is niet geborgd in de gedragscode. Ten slotte is de code weinig specifiek over de afhandeling van het contact met de inhoudsaanbieder indien deze zich beroept op zijn recht op anonimiteit.

In hoeverre zijn dienstverleners bereid zich aan de gedragscode te conformeren? In maart 2009 deed het bureau ICTRecht een onderzoek naar de toepassing van de code door diverse dienstverleners[1]. Het onderzoek had uitsluitend betrekking op het blokkeren van een mogelijk onrechtmatige inhoud, niet op verstrekking van persoonsgegevens. Het bureau benaderde zeven dienstverleners met het verzoek om vermeend auteursrechtelijk beschermd materiaal te verwijderen. Het verzoek voldeed niet aan de eisen die in de gedragscode worden gehanteerd, niettemin gingen vijf van de zeven dienstverleners over tot verwijdering of blokkering zonder te onderzoeken of de klacht over schending van het auteursrecht daadwerkelijk doel trof. Verder blijken veel dienstverleners geen procedure te hebben of - indien er wel een procedure is - zich er niet aan te houden. Kortom; de resultaten zijn nog niet overtuigend. Maar waarom eigenlijk die gedragscode, waar ook nog eens weinigen zich aan houden?

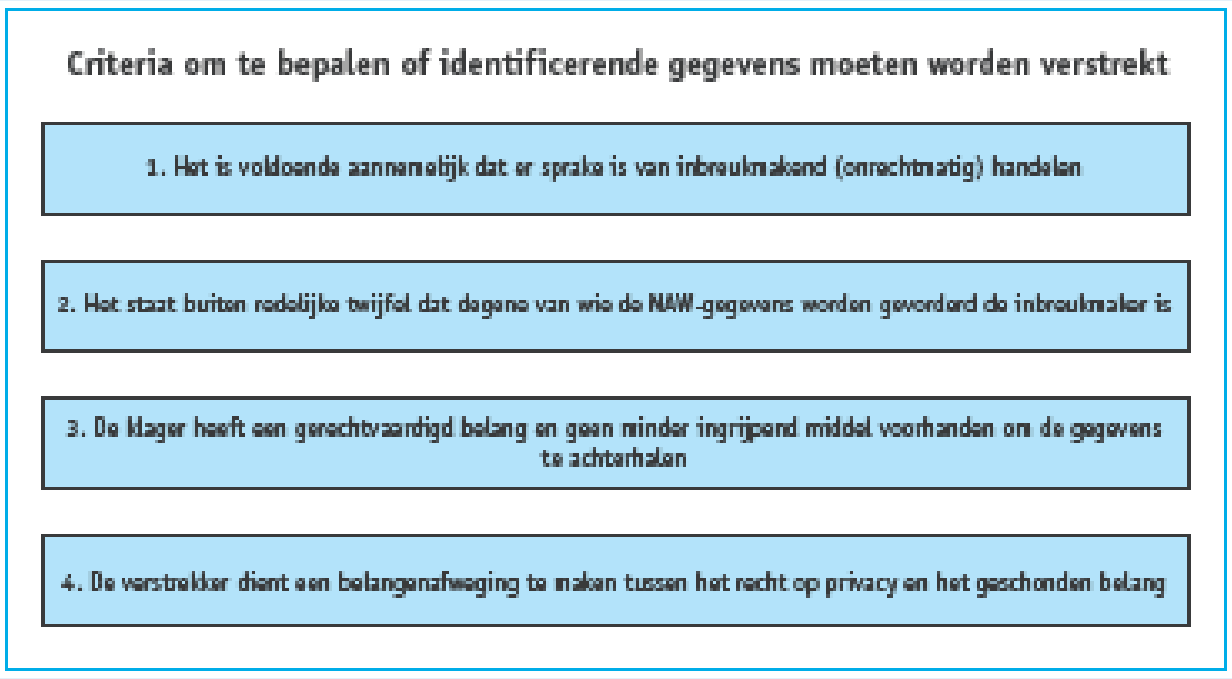
1. Zie ICTRecht, Onderzoeksrapport – Notice & Takedown in Web 2.0: Never Neverland?, 6 maart 2009 <http://ictrecht.nl/notice-takedown-rapport-communitysites-ictrecht-20090306.pdf>

Van Europese richtlijn tot gedragscode
De Europese Gemeenschap heeft al in een vroeg stadium onderkend dat regulering van het Internet een belangrijke voorwaarde is voor het realiseren van de vrije handel in de Europese Unie. Daartoe is een aantal richtlijnen op het gebied van elektronische handel uitgevaardigd, dat in Nederland is uitgewerkt in het recht dat de relaties tussen private (rechts)personen onderling regelt. Vrijwaring van dienstverleners – waarbij de dienstverlener niet aangesproken kan worden voor de schade van derden – is expliciet uitgewerkt (artikel 6:196c BW). Hieronder in schema de verschillende partijen die op dit gebied regels vaststellen.

Als een procedure over (vermeend) onrechtmatig handelen wordt gevoerd voor de rechter, wordt vaak tegelijkertijd geprocedeerd over het blokkeren van de onrechtmatige uitingen én de verstrekking van persoonsgegevens van de onrechtmatig handelende persoon. De aansprakelijkheid van de dienstverlener is voor wat betreft verstrekken van persoonsgegevens niet en het blokkeren van uitingen wél expliciet in de Europese richtlijnen en de nationale wetgeving geregeld. Die onduidelijkheid heeft er toe geleid dat een groot aantal lidstaten van de EU in de nationale wetgeving een algemene verplichting tot verstrekking van die gegevens heeft opgenomen, in zowel strafrechtelijke als civiele zaken. Het Nederlandse artikel 6:196c BW zegt niets over verstrekking van die gegevens, de interpretatie over dit vraagstuk is via de rechter gevormd.

De Europese regelgeving staat verstrekking van persoonsgegevens ook toe in het geval van bescherming van de rechten van derden. De nationale wetgever is niet verplicht om verstrekking van persoonsgegevens als zodanig verplicht te stellen en bij het treffen van maatregelen moet rekening worden gehouden met het recht op privacy. Dit betekent dat de rechter in het geval van schendingen van het auteursrecht in Nederland bij de belangenafweging de betreffende bepaling in de Auteurswet moet meenemen. Daarnaast moet bij de verstrekking van persoonsgegevens rekening worden gehouden met de eisen die de Wet Bescherming Persoonsgegevens (Wbp) stelt[2].

Omdat de verantwoordelijke partij de bevoegdheid heeft, maar geen verplichting heeft om gegevens te verstrekken, is er een motiveringsplicht indien wordt besloten de gegevens te verstrekken. De wetgever heeft in de Memorie van Toelichting bij de Wbp aangegeven dat de verstrekker zich daarbij een aantal vragen moet stellen over het belang van de verwerking: Wordt er inbreuk gemaakt op fundamentele rechten, kan het doel ook op een andere wijze worden bereikt en is de verstrekking evenredig aan het beoogde doel? Er dient een belangenafweging te worden gemaakt tussen het recht op anonimiteit en het geschade belang.



Figuur 3: criteria voor verstrekking

In 2005 oordeelde de Hoge Raad dat er ruimte is om de zorgplicht van dienstverleners binnen de nationale wetgeving te regelen. De Hoge Raad stelde ook de criteria vast waaraan getoetst moet worden of verstrekking plaats moet vinden. Het is niet noodzakelijk dat sprake is van onmiskenbaar onrechtmatig handelen, het is voldoende als dit aannemelijk is, degene die de NAW-gegevens opvraagt, moet een reëel belang hebben en er is geen minder ingrijpende mogelijkheid om de gegevens te verkrijgen. Tenslotte moet een belangenafweging worden gemaakt tussen de belangen van de benadeelde, dienstverlener en abonnee. Overigens wil dat niet zeggen een dienstverlener altijd van haar adverteerders moet eisen hun NAW-gegevens te verstrekken, als dit onredelijk bezwarend is kan het achterwege worden gelaten. Latere uitspraken van lagere rechters bevestigen de door de Hoge Raad aangegeven stappentoets uit 2005. Daarmee is de facto het de huidige juridische richtlijn dat aan de volgende zaken wordt getoetst: "Voldoende aannemelijk dat er sprake is van inbreukmakend (onrechtmatig) handelen, het staat buiten redelijke twijfel dat degene van wie de NAW-gegevens worden gevorderd de inbreukmaker is, [klager] heeft een gerechtvaardigd belang en zij heeft geen minder ingrijpend middel voorhanden om de NAW-gegevens te achterhalen. Zij heeft hiertoe verschillende pogingen ondernomen, maar is hierin niet geslaagd. Het is bovendien in lijn met vaste rechtspraak dat [de dienstverlener] de gegevens van haar cliënt aan [klager] moet verschaffen". Hieronder zijn de criteria in een figuur weergegeven.

Hoe nu verder

De gedragscode Notice-and-Take-Down biedt aanknopingspunten om aan de hand van de door de Hoge Raad vastgestelde criteria te komen tot een afweging over het al dan niet verstrekken van identificerende gegevens. Er is echter een discrepantie met uitspraken van de rechter in concrete gevallen, vooral de gebruikte definitie over de onrechtmatigheid van het gedrag en de uitwerking van het 'hoor en wederhoor'-principe kunnen leiden tot conflicten in concrete gevallen[3]. Ook biedt de gedragscode weinig aanknopingspunten voor inhoudelijke beoordeling van het verzoek.

2. Art. 8 sub f Wbp: "De gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert."

3. Artikel 40 lid 1 Wbp geeft de anonieme internetgebruiker de mogelijkheid zich te verzetten tegen verstrekking van zijn NAW-gegevens. Daarvoor moet het die gebruiker wel bekend zijn dat de tussenpersoon deze gegevens wil verstrekken.

Veel dienstverleners zijn (nog) niet bekend met de gedragscode, of passen deze onjuist toe.

Er zijn mij geen uitspraken bekend waarbij de dienstverlener wél wilde overgaan tot verstrekking van identificerende gegevens, en de anonieme inhoudsaanbieder vervolgens via de rechter probeerde zijn anonimiteit af te dwingen. Andersom zijn er uitspraken waarbij de rechter alsnog de dienstverlener dwong de identificerende gegevens te verstrekken nadat verstrekking in eerste instantie was geweigerd. Het lijkt er dus op dat dienstverleners het recht op anonimiteit strikter handhaven dan de rechter. Dit is ook terug te zien in de verschillende definities die worden gehanteerd door de rechter (aannemelijk onrechtmatig gedrag) en in de gedragscode (onmiskenbaar onrechtmatig gedrag).
De verwoording van de code is zodanig dat niet op korte termijn valt te verwachten dat rechter en dienstverlener verzoeken om verstrekking van identificerende gegevens op dezelfde wijze zullen afhandelen.

De ervaringen met zogeheten 'zelfregulering' binnen de branche bieden weinig hoop dat zelfregulering op korte termijn een transparante oplossing is. Het is niet uit te sluiten dat dienstverleners ervaren dat zij zich ondanks de gedragscode 'tussen twee vuren' bevinden. De dienstverlener heeft immers een contract met de klant en niet met de derde wiens belang is geschaad. Daarnaast is niet uit te sluiten dat het bij de dienstverlener aan juridische kennis ontbreekt om een inhoudelijke beoordeling van een aanvraag te kunnen doen. Een ander mogelijk bezwaar is gelegen in de hoeveelheid aanvragen die een dienstverlener te verwerken kan krijgen. De dienstverlener heeft er een zeker belang bij niet op alle verzoeken in te hoeven gaan.

De brancheverenigingen kunnen een rol spelen bij de oplossing van dit probleem. Voor een deel gebeurt dit al: met de Notice-and-Take-Down procedure en Algemene Voorwaarden wil brancheverenigingen ISPConnect als brancheverenigingen een bijdrage aan de professionalisering van de branche leveren [4]. Daarbij kan de ISP of dienstverlener in de algemene voorwaarden een clausule opnemen dat - hoewel de persoonsgegevens in principe alleen gebruikt worden voor uitvoering van de contractuele relatie - persoonsgegevens aan een derde kunnen worden verstrekt, indien deze aannemelijk maakt door het handelen van de abonnee benadeeld te zijn. Dit werkt echter alleen voor dienstverleners die onder Nederlands recht vallen.

Tot slot

In het licht van de constatering dat de code nog weinig door dienstverleners wordt uitgevoerd en de hierboven beschreven spagaat van het 'tussen twee vuren' geraken, moet worden beschouwd of de code in haar huidige vorm de verantwoordelijkheid op de juiste plaats belegt. Ik ben van mening dat dit niet het geval is: uit de onderzoeken tot nu toe blijkt dat een dienstverlener niet goed in staat is om de belangenafweging te maken. Daarbij maakt het niet uit of dit onwil of onwetendheid is. In de praktijk blijkt de dienstverlener bij een klacht te weinig onderzoek te doen en wordt soms te snel en onterecht informatie geblokkeerd.
Bij het verstrekken van NAW-gegevens lijkt te tendens omgekeerd te zijn en moet de rechter er soms aan te pas komen om alsnog de verstrekking te gelasten.

Een veel betere invulling van de op zich juiste intenties van de code is mogelijk. Daarvoor maak ik een uitstapje richting consumentenrecht. Daar is het geaccepteerd dat elke branche een onafhankelijke klachtencommissie inricht.

Deze commissies bieden een laagdrempelige en - door de afstand tot de strijdende partijen - onafhankelijke wijze van klachtafhandeling. Wel is duidelijk dat deze werkwijze moet worden afgedwongen in de regelgeving. De relevante brancheverenigingen kunnen er voor zorgen dat er een onafhankelijk klachtenorgaan komt, dat de aanvragen tot verstrekking van NAW-gegevens behandelt. De branche levert een aantal commissieleden en consumentenorganisaties worden gevraagd een aantal andere onafhankelijke leden aan te melden. In zo'n gezamenlijk klachtenorgaan kan ook de benodigde (juridische) expertise worden geregeld, dat voor de individuele bedrijven moeilijk blijkt te regelen. Een zekere drempel is in te bouwen door een bedrag in rekening te brengen bij de aanvraag. Als de klacht gegrond wordt verklaard, wordt dit bedrag teruggestort.

Noot van de redactie:
Dit artikel is een samenvatting van het referaat van Ellen Wesselingh. Het complete referaat zal op de website van het PvIB bij de digitale versie van dit nummer beschikbaar worden gesteld.

Over de auteur

Ing. Ellen Wesselingh is sinds september 2008 is als docent verbonden aan de opleiding Information Security management van de Haagse Hogeschool. Daarnaast is zij als onderzoeker verbonden aan het lectoraat Informatiebeveiliging van diezelfde instelling. Naast haar werk studeert zij Nederlands recht, dit artikel is een bewerking van haar bachelorscriptie.

Favoriete websites
- http://www.rechtspraak.nl/
- http://www.iusmentis.com/

4. <http://www.ispconnect.nl/nieuwsbericht/2009/03/ispconnect-presenteert-notice-and-take-down-procedure/>

Interview met Amichai Shulman, CTO en oprichter van Imperva

Auteur: Mario de Boer > Mario de Boer is security consultant bij Logica en redacteur van dit blad.
Hij is bereikbaar via mario.de.boer@logica.com

Amichai werkt in de softwarebeveiliging vanaf het begin van de jaren negentig. Zijn eerste voetstappen op dit gebied zette hij bij het Israëlische Ministerie van Defensie. Daarna heeft hij een eigen bedrijf gestart, een adviesbureau in software- en databasebeveiliging. Het bedrijf richtte zich op het uitvoeren van penetratietesten, source code reviews en security design van producten en projecten. Na een aantal jaren is hij samen met een aantal anderen Imperva gestart. Hierbij hebben ze hun kennis op het gebied van softwarebeveiliging omgezet in een aantal producten. In zijn huidige rol van CTO analyseert hij zwakheden van web- en database software en onderzoekt zijn team de verschillende typen bedreigingen en de mogelijkheden om deze te mitigeren. De focus ligt op het bouwen van tools die geen aanpassingen in de applicatiecode zelf vereisen.

Mario: "Waarom is er zoveel interesse in softwarebeveiliging? Komt dit door de risico's of is compliance met bijvoorbeeld de PCI regelgeving de belangrijkste drijfveer?"

Amichai: "Het is een combinatie van redenen. Op korte termijn is compliance de belangrijkste reden, maar op langere termijn gaat het om de dreigingen. Grote organisaties hebben nu veel haast met het voldoen aan PCI-regelgeving. Recente voorbeelden hebben echter aangetoond dat je best PCI-compliant kunt zijn zonder dat je applicaties echt veilig zijn. Op de lange termijn zal het mitigeren van de echte risico's dan ook de belangrijkste reden zijn om iets aan softwarebeveiliging te gaan doen. PCI is een van belangrijkste regelgevingen als drijfveer van softwarebeveiliging over de afgelopen achttien maanden. In de USA zijn er bovendien staten die wetgeving baseren op afgeleiden van de PCI-regelgeving. Wetgeving die het melden van incidenten verplicht stelt, wordt bovendien steeds in steeds meer staten en landen toegepast. Deze meldingsplicht vereist bovendien steeds vaker dat details worden bekendgemaakt van de inbraak. In de komende zes tot twaalf maanden verwachten we bovendien een soort tweede golf van SOx-achtige wet- en regelgeving. De nadruk hierbij zal liggen op meer transparantie van controls die gericht zijn op het tegengaan van misbruik van business processen."

Mario: "Wat is de volwassenheid waarmee organisaties software-beveiliging aanpakken? Zie je een variatie tussen werelddelen of bedrijfstakken?"

Amichai: "Er zijn verschillende volwassenheidsniveaus. Grotere bedrijven in de VS zijn erg volwassen bij het aanpakken van het probleem en bij het reserveren van budget. De noodzaak is voor deze bedrijven duidelijk en de oplossingen worden goed begrepen. Europa loopt hierop een beetje achter, al is PCI-compliancy ook hier een duidelijke drijfveer. Algemeen lijkt het erop dat Europese bedrijven eveneens aandacht besteden aan softwarebeveiliging met als doel compliance, maar ze vullen dit doel in op een manier die past binnen het grotere geheel van security. Azië en Australië lopen achter op zowel de VS als Europa."
"Grotere organisaties kennen de risico's van

softwarebeveiliging en besteden er aandacht aan. Kleinere organisaties hebben nog steeds moeite met het begrijpen van de risico's en het feit dat het daadwerkelijk hun probleem is. Kleinere organisaties denken vaak dat het risico op het hacken van hun organisatie laag is: hackers zullen zich vast richten op grote doelen. We zien echter een indicatie dat bedrijven die deze gedachtegang volgen problemen gaan krijgen. De huidige generatie aanvallers maakt gebruik van massa-aanval tools, tools die grote aantallen mogelijke slachtoffers snel en effectief analyseren, bijvoorbeeld door gebruik te maken van zoekmachines. Hierdoor zullen vooral de kleinere organisaties, die een lager volwassenheidsniveau hebben en mogelijk minder goed zijn voorbereid, juist serieuze problemen krijgen."

Mario: "Wie zou volgens jou het voortouw moeten nemen bij softwarebeveiliging, de security professionals of de ontwikkelaars?"

Amichai: "Ik heb hierover een heel duidelijke mening: de security professionals. Het is de verantwoordelijkheid van de security officer om software veilig te krijgen. Ontwikkelaars moeten tot op een bepaalde hoogte een deel van de inspanning leveren. Het is vrij eenvoudig te meten hoe productief ontwikkelaars zijn en het is dus vrij gemakkelijk om hen op basis daarvan te belonen. Het is echter erg moeilijk te bepalen hoe veilig de software is die ze ontwikkelen. Wanneer je dit niet goed kunt meten, en hen hier niet op kunt afrekenen, waarom zouden ze zich dan druk om maken om de veiligheid van hun code?" "Wanneer we goede metingen hebben voor de veiligheid van software en wanneer we deze metingen kunnen uitvoeren tijdens het ontwikkelproces en wanneer deze metingen gebruikt worden bij de beloning en de evaluatie van het werk van ontwikkelaars, dan kun je een gedeelte van de verantwoordelijkheid naar de ontwikkelaars overbrengen. Tot dat dit gebeurt zul je ontwikkelaars moeten trainen, je moet proberen ze betere en veiligere code te laten schrijven. Maar uiteindelijk is het de security officer die verantwoordelijk moet zijn en dus de tools moet hebben om beveiligingsrisico's in software te mitigeren."

Mario: "Verwacht je dat er nog veel incidenten nodig zijn om organisaties te overtuigen om significant in softwarebeveiliging te investeren?"

Amichai: "Aanvallen op software vormen een nieuw soort economie. We hoeven niet te wachten op aanvallen, het gebeurt al.
Het aantal incidenten groeit, net als de impact van incidenten. Het bereik van aanvallers groeit, ze mikken op meer soorten omgevingen. Incidenten zullen toenemen en iedereen die geen actie onderneemt zal incidenten krijgen.
Vijf of zes jaren geleden werd ook alles aangevallen, maar dat was standaard geautomatiseerd. Nu worden verschillende organisaties op verschillende manieren aangevallen, met verschillende bedoelingen. Wanneer een thuiscomputer je doel is, dan wil je daar bijvoorbeeld een bot op installeren. Wanneer je een kleine webserver aanvalt, dan doe je dat voor een drive-by-download voor het infecteren van meerdere thuiscomputers. En tenslotte, wanneer je grote organisaties aanvalt, dan doe je dat om hun business."

Mario: "Wat zijn de grootste bedreigingen voor 2009/2010 en wat moeten we doen om voorbereid te zijn?"

Amichai: "Organisaties moeten beginnen met het analyseren van hun softwarerisico's en het maken van een plan om deze risico's te mitigeren. Wat systemen betreft die aan het internet hangen, ben ik uiteraard bevooroordeeld: deze systemen zijn onder constante aanval en vereisen onmiddellijke aandacht. Het aanpakken van de softwarebeveiliging in de code zelf is niet voldoende effectief en organisaties zouden aanschaf van Web Application Firewalls moeten overwegen. Wanneer deze uitgerold

Bron beeld: 'Organic growth' map - jurvetson via Flickr

zijn, kun je terug in de keten de kritieke code en database security aanpakken."
"Belangrijke businessapplicaties binnen grotere organisaties hebben dermate veel gebruikers, zowel intern, als extern, dat deze bijna te zien zijn als externe applicaties. Deze behoeven daardoor net zoveel aandacht als de systemen die direct met het internet verbonden zijn. Eén van de belangrijkste focusgebieden van mijn groep in het afgelopen jaar was het analyseren van grote softwaresystemen zoals SAP en Oracle Business Suite, om specifieke implementaties van onze producten te maken die gebruikt kunnen worden met deze businesssoftware."

Mario: "We kunnen een parallel proberen te trekken tussen netwerk- en software-beveiliging. Een decennium geleden zouden we kijken naar de laatste netwerkbeveiligingstechnologieën en bouwden we architecturen om onze perimeter te beschermen en gingen we naar conferenties voor de laatste netwerk security snufjes. Nu is dit allemaal gemeengoed en bevinden we ons zelfs in de situatie dat de perimeter aan het verdwijnen is. Nu is softwarebeveiliging hot: we gaan naar de conferenties, kopen de laatste tools en ontdekken nieuwe inzichten. Mijn vraag is: wanneer zal softwarebeveiliging gemeengoed zijn? Zullen we dan ook zien dat we niet langer op de veiligheid van software kunnen vertrouwen? En zullen we dan, eindelijk, de oplossing hebben gevonden voor het beveiligen van informatie zelf in plaats van het netwerk of de software waarin deze zich bevindt?"

Amichai:
"Softwarebeveiliging zal inderdaad gemeengoed worden, en dat is goed. We zullen op verschillende niveaus maatregelen moeten nemen. Een firewall bijvoorbeeld kan beslissen dat poort 80 naar een bepaalde machine is toegestaan, maar kan geen beslissing maken op basis van de inhoud. Er zal altijd behoefte blijven aan netwerkfirewalls. Het lijkt erop dat we enkel nog aanvallen zien op applicatieniveau, maar dat komt nou net omdat we netwerkfirewalls hebben. Een Web Application Firewall kan wel naar de inhoud van het verkeer kijken en op basis daarvan beslissen wat wel en niet is toegestaan."
"De aanvaller zal zich altijd richten op het niveau boven de maatregelen die getroffen zijn. Wanneer netwerk en Web Application Firewalls gemeengoed zijn, zullen aanvallers zich richten op het misbruiken van de manier waarop de applicatie werkt om de business aan te vallen. Hier is een voorbeeld, niet origineel van mij, maar het illustreert het wel misbruik van de wijze waarop de applicatiebusiness uitvoert. Er zijn e-trading applicaties die bij registratie een klein bedrag overmaken op je rekening, gewoon om te verifiëren dat alles correct werkt. Wanneer je op een geautomatiseerde wijze miljoenen registraties kunnen uitvoeren, kun je op een snelle manier rijk worden."
"In de toekomst zal er dus behoefte zijn aan een slimmere technologie, die onderscheid kan maken tussen goed en slecht businessgedrag. Denk hierbij aan het detecteren van fraude en aanvallen op de businesslogica. Maar we hebben dan nog steeds netwerk- en Web Application Firewalls nodig, aangezien deze onderscheid kunnen maken tussen goed en kwaad op lagere niveaus."
"We zien meer security aandacht in het software-ontwikkelproces. We zien ook dat er meer en meer tools naar beneden in het ontwikkelproces worden geduwd en niet enkel in productie worden toegepast. Hoewel deze ontwikkeling slechts langzaam vordert, zal dit wel de security van software in het algemeen verbeteren."

European Identity Conference

Auteur: Bavo de Ridder > Bavo de Ridder Solution & Enterprise Architect bij De Ridder Consulting b.v.b.a.
Hij is bereikbaar via bavo.de.ridder@bavoderidder.com

Kuppinger Cole had een interessante agenda in elkaar getimmerd voor de European Identity Conference die van 4 tot 8 mei jl. in München werd gehouden. Vier onderwerpen vormden daarbij de kern: Identity Management, Cloud Computing, GRC (Governance, Risk en Compliance) en ten slotte Role Management. Elke ochtend startte de conferentie met enkele grotere presentaties en key notes. Daarna kon iedereen naar eigen interesse zich aansluiten bij één van de vier tracks, een track voor elk van de onderwerpen hierboven aangehaald.

De sfeer op de European Identity Conference is altijd al zeer gemoedelijk en uitnodigend geweest. Misschien is het de schitterende Beierse omgeving, de historische stad München of de locatie op een eiland in de rivier de Isar, de conferentie voelt al vanaf de eerste dag aan als groep gelijkgestemde deelnemers. Informele gesprekken tussen bezoekers, leveranciers, sprekers of de organisatoren houden je volop bezig tussen de presentaties en workshops.

GRC

De key notes van Martin Kuppinger, één van de stichters en partners van Kuppinger Cole, waren steeds van uitstekende kwaliteit en stonden, zeker op de eerste dag, bol van de voorspellingen. Zo zou GRC het ultieme wapen van Identity & Access Management moeten worden. Ook in eerdere edities van deze conferentie heeft Kuppinger Cole altijd al de nadruk gelegd op governance en compliance als sleutelelementen van een goede IAM-strategie. GRC is voor hen het business perspectief van IAM, provisioning noemen ze het klassieke en vooral technische perspectief.

Forum Deutches Museum in München

Dale Olds (blauw), Kim Cameron (grijs) in een forumdiscussie.

Eigenlijk zie je dat voor een deel al gebeuren in de huidige IAM-projecten. Daar waar enkele jaren geleden de nadruk volledig lag op synchronisatie, provisioning en paswoordbeheer, zie je vandaag meer en meer vragen voor attestation, compliancy controls en een betere aansluiting met risicobeheer. Martin Kuppinger legt daar, terecht, de nadruk op het beheersen van de uitzonderingen of management by risk, zoals hij het noemt. Dat is iets dat vandaag de dag nog niet zo eenvoudig is, omdat risicobeheer vaak verspreid is over verschillende domeinen, zoals compliancy en regelgeving, operationele risico's en IT-risico's. Hier moet volgens Martin een nieuw platform komen dat al deze risicodomeinen als één geheel beheerd.

Identity

Het kernonderwerp van de conferentie, Identity Management, mogen we zeker niet uit het oog verliezen. Tijdens de eerste editie van de conferentie in 2007 was dit onderwerp een bron van inspiratie en motivatie tijdens de presentaties. Alle toen lopende initiatieven, van OpenID over OAuth en Liberty Alliance tot Information Cards waren de hele dag door het gespreksonderwerp. Deze 'grass roots' sfeer was er bijna niet meer deze editie. Van al deze standaarden bleef eigenlijk enkel nog Information Cards over. Dat weerspiegelt niet echt de realiteit daarbuiten. Op het internet is OpenID een stevige speler geworden, ondersteund door onder andere Yahoo, Plaxo, Flickr en nog vele anderen.

Het is duidelijk dat in de visie van Microsoft het gebruik van claims het antwoord is voor alle vraagstukken rond authenticatie en autorisatie. Een standpunt dat af en toe uitgedaagd werd door de aanwezigen, vooral tijdens de panelgesprekken, maar door bijvoorbeeld Kim Cameron van Microsoft steeds vakkundig beantwoord. Niemand op de conferentie twijfelde ook maar een moment aan de kracht en toepasbaarheid van claims. Er was echter wel twijfel over hoe ver je kunt gaan met claims. Kan er naast authenticatie ook autorisatie meedoen?

Microsoft denkt van wel, al geven ze toe nog niet alles op een rijtje te hebben. Anderen durven dit echter tegen te spreken en vrezen dat voor Microsoft nu alles een claim lijkt. Het spreekwoord 'als je enkel een hamer hebt, lijkt alles op een nagel' kwam uit meer dan één hoek.

Role Management

Je kunt geen Identity en Access Management oplossing bedenken of je komt vroeg of laat rollen tegen. Wie heeft er vandaag de dag nog niet gehoord van Role Based Access Control (RBAC) of entitlements? Kuppinger Cole vond dit onderwerp, en terecht, interessant genoeg om er heel wat presentaties aan te wijden. Daarbij werd controverse niet uit de weg gegaan, tijdens meer dan één presentatie kon je de slogan 'RBAC is death' horen. Ondanks het aantal succesvolle customer case studies kon je toch nog veel twijfel horen bij de deelnemers. Bij hun was RBAC niet mogelijk of gaf het te weinig meerwaarde om de investering te verantwoorden.

Een alternatief werd door XACML, eXensible Access Control Markup Language, geboden. Die laat immers een veel fijnere en dynamische vorm van autorisatie toe. Telkens als een toepassing wil weten of een operatie mag worden uitgevoerd, kan die aan de hand van een XACML-bericht vragen of dit wel mag. De XACML-implementatie zal aan de hand van een hele verzameling policies het antwoord berekenen. XACML lijkt echter ook geen magische oplossing te zijn. Op enkele kritische vragen kwam onvoldoende antwoord. Zo is het niet eenvoudig om via XACML te weten te komen wat iemand allemaal mag.

Cloud Computing

De track rond Cloud Computing was een vreemde eend in de bijt op deze conferentie. Het domein van Identity breidt zich natuurlijk uit tot de Cloud, maar in deze conferentie ging Kuppinger Cole toch een eind verder. Heel wat presentaties gingen louter over Cloud Computing zonder een duidelijke relatie met Identity mangement of zelfs GRC. De meeste aanwezigen konden deze onderwerpen echter wel waarderen. Cloud computing is dan ook een actueel topic dat nog iets mythisch heeft. Toch heb ik de indruk dat Kuppinger Cole hier twee vliegen in één klap mee wilde slaan: de agenda wat interessanter maken en een voorbereiding voor hun grotere Cloud-09 conferentie die dit najaar plaatsvindt.

'Fulup ar Foll (Sun): Roles don't fly in the sky'

Daar waar presentaties rond Cloud computing toch raakvlakken hadden met Identity of GRC bleek duidelijk dat het grootste werk zich rond GRC afspeelde.

Identity heeft, dankzij onder andere Liberty Alliance, SAML en Microsoft met hun claims, duidelijk een voorsprong in de Cloud. Al deze elementen lenen zich immers uitstekend voor toepassingen in de Cloud. Voor GRC ziet het plaatje er echter heel wat anders uit. Daar zal Cloud computing vooral voor meer onzekerheid zorgen. Waar we nu eindelijk op weg waren naar een betere beheersing van onze risico's, gooien we al deze voorsprong in één keer overboord door Cloud computing.

Identity Awards

Op de laatste avond van de conferentie werden naar traditie de European Identity

Awards uitgereikt. In verschillende categorieën worden elk jaar de mooiste projecten, de beste innovaties of standaarden in de bloemetjes gezet. Identity management is ook vandaag de dag nog een sterk innoverende tak van IT en informatiebeveiliging. Kuppinger Cole had dan ook veel moeite om in elke categorie maar één winnaar te kiezen in elke categorie. In vele gevallen ging de award voor een categorie dan ook naar meerdere winnaars. De meest uit het oog springende winnaars waren Sun met hun OpenSSO project, in de categorie Best Innovation. Die prijs moesten ze echter delen met Yubico, die met een vernieuwende vorm van eenmalige paswoordgenerators de markt probeert te veroveren, en Microsoft met het Geneva project.

In de categorie van Best new or improved standard werd de eer gedeeld door het Aristotle project, een uitbreiding op het Identity Governance Framework, OAuth, een standaard voor authenticatie tussen systeem in naam van een gebruiker, en de Information Card Foundation voor hun werk rond de standaardisatie van Information Cards.
Een volledige lijst van de winnaars kan je vinden op de website van de conferentie: http://www.id-conf.com.

Bavo (rechts) in gesprek

Exhibition

Wanneer je niet deelneemt aan een presentatie of workshop, is er altijd de uitgebreide exhibition waar zo ongeveer iedereen in de IAM- en GRC-wereld vertegenwoordigd is. Iedereen gaf bijna spontaan dezelfde opmerking: ondanks de economische crisis was de exhibition zeer rijkelijk gevuld. Zelfs nog beter dan de vorige jaren. Je had er uiteraard de klassieke deelnemers zoals HP, Novell, IBM, Oracle en Microsoft. Daarnaast waren er echter ook veel kleinere spelers op de markt zoals Yubico, Axiomatics met een uitmuntend XACML product of Ping Identity, die er al enkele jaren in slagen de markt van federation producten te bepalen.

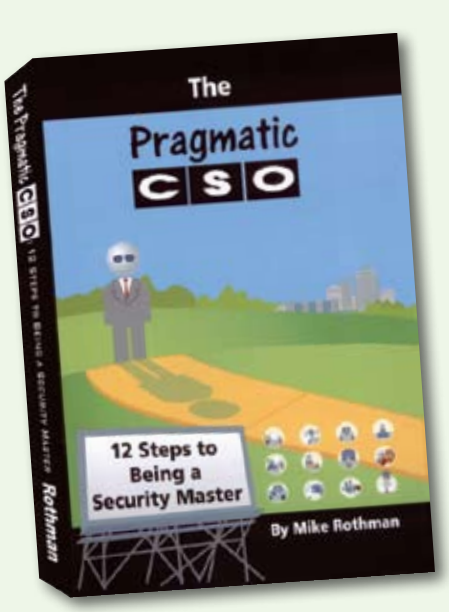
Tot slot

De European Identity Conference was ook dit jaar een uitstekende conferentie voor iedereen die geïnteresseerd is in deze onderwerpen. Het niveau van de deelnemers, zowel de leveranciers, de bezoekers, als de sprekers is elk jaar opnieuw hoog. Deze editie was daar zeker geen uitzondering op. De sfeer tijdens de conferentie nodigt uit tot informele gesprekken. Een Amerikaanse bezoeker aan de conferentie vertrouwde me toe dat dit juist de aantrekkingskracht is: veel gesprekken tussen de presentaties en workshops door, waarbij er geen sprake is van een kloof tussen de deelnemers. Dat in schril contract met de typische Amerikaanse conferenties.

Noteer alvast 4 tot en met 7 mei 2010 in je agenda, dan is het immers verzamelen geblazen in München voor de vierde editie van deze conferentie.

Boekbespreking: The Pragmatic CSO

Auteur: Lex Borger > Lex Borger is Principal Consultant Information Security bij Domus Technica en redacteur van dit blad. Hij is bereikbaar via lex.borger@domustechnica.com.



12 Steps to Being a Security Master, geschreven door Mike Rothman, uitgegeven door Security Incite Publishing (geen ISBN).

Wanneer je een willekeurig hoofdstuk in dit boek 'zo maar' zou gaan lezen, zou je in eerste instantie niet doorhebben dat je een boek over informatiebeveiliging leest. Het heeft meer weg van een 'zelfhulpboek'. Dit komt door de therapiescripts waarmee Mike ieder hoofdstuk begint. Het leest ook redelijk gemakkelijk. Het boek bevat 235 pagina's en is gezet in een redelijk groot lettertype. Een scholier zou er niet van schrikken om dit op zijn boekenlijst te zetten. Het is erg onconventioneel, maar het helpt wel om je in de juiste mindset te brengen om de rest van het verhaal beter te kunnen aannemen. Fans van het tv-programma My Name is Earl zullen zich hier gelijk in kunnen vinden.

Niet alleen de inhoud, ook de publicatie is onconventioneel. Mike geeft dit boek uit in eigen beheer. Het is te koop als traditioneel boek of als PDF-bestand. Hij heeft het ook gestaffeld geprijsd, het is best prijzig als je er eentje koopt, maar koop er meer dan zes en de prijs is bijna gehalveerd. De PDF-bestanden worden door Mike gepersonaliseerd en toegestuurd via email.

Mike heeft dit boek duidelijk gericht op de security officers van deze wereld: de CSO, CISO, security manager of een vergelijkbare functie. Het gaat dan ook over de onderwerpen waar de CSO's van vandaag over het algemeen mee worstelen: hoe krijg ik de juiste aandacht voor mijn programma, hoe krijg en houd ik mijn budget, hoe meet ik dat ik succes heb, hoe vertel ik het anderen. Je zult er niet in vinden hoe je netwerken beveiligt, encryptie toepast of servers hardt. Voor deze doelgroep maakt Mike de titel ook waar. Het is zeker pragmatisch - een twaalf stappenplan om beter te worden in wat je doet.

Het is dus zeker geen boek voor de technisch security specialist, tenzij hij in therapie wil gaan met Mike om een carrièreverandering voor te bereiden. Houd er in dat laatste geval wel rekening mee dat het boek lang niet genoeg informatie bevat om die verandering te kunnen maken, en slechts motiverend kan werken.

Die 'zelfhulp' setting vind je ook terug in de boodschap van het boek. Deze echoot je tussen de regels door tegemoet: je hoeft je niet rot te voelen als CSO omdat je onvoldoende budget hebt en reactief bezig bent. Je moet het vanaf nu wel anders aan gaan pakken en dit boek helpt je daarbij.

Samenvatting

plan - build - run - communicate
move up in the (corporate) world
Mike heeft zich door Deming laten inspireren en beschrijft een twaalf stappenplan rondom security management: plan - build - run - communicate. En kennelijk weet hij ook iets van voetballen, de twaalf stappen zijn niet evenwichtig verdeeld als vier keer drie, maar hij heeft er een drie-drie-vier-twee opstelling van gemaakt. 'Run' krijgt dus de meeste aandacht.

Is het nu allemaal echt zo eenvoudig als Mike het in zijn boek laat lijken? Nee, de echte wereld is veel complexer dan de therapeutische wereld uit het boek. Informatiebeveiliging blijft een vak waar je toch een dosis inhoudelijke kennis nodig hebt en moet kunnen toepassen. Kennelijk vindt Mike dat hier al genoeg aandacht aan geschonken wordt middels bijvoorbeeld certificaties, zoals CISSP, CISA en CISM. Hij noemt de ISO 27001 norm en CobiT. Voor iemand die een betere security manager wil worden (en dat willen we toch allemaal?) en die een duwtje in de rug wil hebben, is het een leuk boek om in die context te gebruiken. In ieder geval heb je geen excuus meer als je budget weer ingekrompen wordt...

Inhoudsopgave

Grenzen aan cryptogebruik

Werken met vertrouwelijke informatie in het buitenland

Auteur: Edwin van Buuren > Edwin van Buuren is adviseur ICT- en informatiebeveiliging bij GOVCERT.NL, het Computer Emergency Response Team (CERT) van en voor de Nederlandse overheid. Hij is via e-mail te bereiken op info@govcert.nl.

De samenwerkingspartners van overheid en bedrijfsleven bevinden zich in toenemende mate in het buitenland. Bij reizen naar het buitenland wordt ten behoeve van deze samenwerking vaak digitale informatie meegenomen die soms een vertrouwelijk karakter heeft. Om deze vertrouwelijke bedrijfs- of persoonsinformatie, die zich op laptops, USB-sticks, PDA's of andere informatiedragers kan bevinden, te beveiligen wordt in veel gevallen cryptografie toegepast.

Wat niet iedereen zich realiseert, is dat in veel landen beperkende wet- en regelgeving geldt voor het bezit of gebruik van cryptografische middelen. Hierdoor is het niet altijd toegestaan cryptografie te gebruiken in een land of cryptografische producten er mee naartoe te nemen. Daarnaast behouden sommige landen zich het recht voor om inzage te eisen in uw met cryptografie beschermde informatie. In dit artikel wordt aangegeven waaraan u moet denken als u met cryptografische middelen en/of versleutelde bestanden van en naar het buitenland wilt reizen.

Cryptografie is overal

Het gebruik van cryptografie is wijdverspreid. Meestal weten we wel dat we cryptografische middelen gebruiken, maar soms gebruiken we deze zonder dat we dat direct beseffen. Denk hierbij aan:

- Het versleutelen van bestanden of volledige informatiedragers (USB-stick, hard-disk).
- Afscherming van de toegang tot informatie of een informatiedrager (computer, PDA, etc.) met bijvoorbeeld een wachtwoord.
- Websurfen via een beveiligde verbinding (https).
- Het opzetten en gebruiken van een beveiligde VPN-verbinding (bijvoorbeeld om vanaf thuis of elders een beveiligde verbinding met kantoor te maken).
- Het versturen van beveiligde e-mail.
- Het zetten van een digitale handtekening.

Enkele producten die cryptografie gebruiken zijn:

- Webbrowsers, zoals MS Explorer, Mozilla Firefox, Opera en Safari.
- Producten voor bestands- of disk-encryptie, zoals TrueCrypt en Safeguard.
- Producten voor het zetten van digitale handtekeningen of beveiligd mailen. Voorbeelden zijn Pretty Good Privacy (PGP) en daarvan afgeleide producten, zoals GPG of andere technieken voor e-mailbeveiliging, zoals S/MIME.
- VPN-client software, zoals standaard opgenomen in besturingssystemen Windows XP/Vista of Mac OS X, maar ook speciale producten van bijvoorbeeld Cisco.

Kortom; cryptografie komt vaker voor dan menigeen denkt.

Met welke wet- en regelgeving kunt u te maken krijgen?

De beperkende wet- en regelgeving die landen opleggen voor het bezit en de toepassing van cryptografie zijn op hoofdlijnen in drie categorieën in te delen:

De belangrijkste feiten op een rijtje

- Vertrouwelijke informatie wordt steeds vaker beschermd met cryptografische technieken.
- Rond het gebruik van en reizen met cryptografie bestaat in diverse landen beperkende regelgeving.
- Het is niet altijd toegestaan cryptografie te gebruiken in een land of cryptografische producten er mee naartoe te nemen.
- Buitenlandse autoriteiten kunnen verzoeken om toegang tot of ontsleuteling van informatie op laptops of andere mobiele informatiedragers.
- Door toegang te geven aan derden, kunt u de controle over de verspreiding van uw vertrouwelijke informatie verliezen.
- Bedenk vooraf welke informatie u wilt meenemen en hoe u deze wilt en mag beschermen.

1. *Beperking aan het gebruik van cryptografische producten*

Een aantal landen kent beperkingen op het gebruik van cryptografie. In combinatie hiermee bestaan meestal ook importbeperkingen om te voorkomen dat inwoners alsnog de beschikking krijgen over verboden cryptografie. Deze beperkingen komen veelal voort uit de behoefte van overheden aan inzicht in communicatiestromen ten behoeve van opsporing en inlichtingen.

Enkele bekende voorbeelden van landen die beperkingen hanteren:

- Frankrijk kent beperkingen voor gebruik van cryptografie door security service providers, zoals trusted third parties (ttp's). In het verleden kende Frankrijk meer beperkingen, maar deze zijn in recente jaren opgeheven.
- Polen heeft een importbeperking, maar standaard cryptografische software voor privé en zakelijk gebruik die voldoet aan de eisen uit de General software note[1] van de Wassenaar Controls (zie ook kader verderop) valt hier niet onder.
- India heeft beperkingen op cryptografie geïmplementeerd in hardware, maar niet in software.
- Zuid-Afrika heeft geen beperkingen voor privé of zakelijk gebruik, maar wel beperkingen voor security service providers.
- Voor onder andere China en de voormalige Sovjet-republieken geldt dat eigenlijk alle vormen van cryptografie verboden zijn, tenzij de autoriteiten expliciet toestemming hebben gegeven voor het gebruik ervan.

2. *Wetgeving inzake het verlenen van toegang tot informatie(dragers)*

In een aantal gevallen kunnen overheden verzoeken om toegang tot uw informatie (drager) of het afgeven van wachtwoorden of sleutels, teneinde uw informatie(dragers) te inspecteren. Dit vindt meestal plaats in de volgende twee gevallen:

Bij het passeren van een landsgrens

Vergelijk dit met het openen van uw koffer, zodat deze door douanepersoneel doorzocht kan worden op ongeoorloofde goederen. Meestal wil men alleen maar vaststellen dat uw laptop daadwerkelijk een laptop is (en geen explosief bijvoorbeeld) en incidenteel ook of u geen ongeoorloofde informatie vervoert. Om meer duidelijkheid te verschaffen, heeft bijvoorbeeld de douane van de USA hun richtlijnen voor grensinspecties van informatiedragers publiekelijk beschikbaar gesteld aangevuld met een toelichting[2].
Ook de Nederlandse douane heeft (steeksproefsgewijs) controles uitgevoerd, zoals onder andere uit de gegevens van een WOB verzoek is gebleken[3]. Het resultaat van deze circa duizend doorzoekingen heeft echter zeer weinig opgeleverd. De vraag is dus reëel of te verwachten valt dat men hier mee zal doorgaan.

In het kader van een (strafrechtelijk) onderzoek

Door politie-, justitie- en veiligheidsdiensten kan in het kader van een (strafrechtelijk) onderzoek gevraagd worden om toegang tot informatiedragers of wachtwoord-afgifte. Het is goed om te beseffen dat in een aantal landen uw medewerking verplicht is. Zelfs het 'verschoningsrecht' (niet hoeven meewerken aan uw eigen veroordeling) is niet altijd van toepassing. Als u weigert de ontcijfersleutel af te geven, kunt u bijvoorbeeld in Groot-Brittannië maximaal twee jaar gevangenisstraf krijgen.
Landen die een ontsleutelplicht kennen zijn bijvoorbeeld Nederland, België, Frankrijk, Groot-Brittannië, Australië en India.
De USA kent geen ontsleutelplicht binnen het land, maar hanteert zoals aangegeven wel strenge grenscontroles.

3. *Exportbeperkingen omdat cryptografische middelen ook militair bruikbaar zijn*

Bepaalde geavanceerde cryptografische technieken zijn door veel landen benoemd als 'dual-use good', oftewel ook militair bruikbaar, en kennen daarom beperkende exportvoorwaarden. Deze voorwaarden staan bekend als de Wassenaar Controls en worden door een zeer groot aantal landen gehanteerd. Daarnaast is er ook soortgelijke EU-regelgeving op dit vlak (zie Council Regulation (EC) No 2432/2001).
De EU-regelgeving staat vrij verkeer tussen de EU-lidstaten bijna volledig toe en hanteert alleen beperkingen voor zeer geavanceerde cryptografie en cryptoanalyse middelen. Ook de Wassenaar Controls gelden alleen voor de geavanceer-

De belangrijkste delen uit de Wassenaar Controls

- Geen exportbeperkingen voor: symmetrische cryptografie met een maximale sleutellengte van 56 bits, alle asymmetrische cryptografie met een maximale sleutellengte van 512 bits en alle overige cryptografie (inclusief elliptische curves) tot 112 bits sleutellengte.
- Het exporteren van producten die encryptie gebruiken om intellectueel eigendom te beschermen, is beperkt toegestaan.
- Voor export van overige cryptografie is een vergunning nog steeds noodzakelijk.
- Voor cryptografische producten of algoritmes die vrij beschikbaar zijn in het publieke domein gelden geen beperkingen.
- De beperkingen gelden voor de algoritmes of software die dergelijke algoritmes bevat.

Voor meer informatie over de Wassenaar Controls zie www.wassenaar.org.

1. http://www.wassenaar.org/controllists/2008/
2. http://www.eff.org/files/filenode/alc/071608_cbp_policy.pdf
3. http://www.bigwobber.nl/wp-content/uploads/2009/04/defensie.pdf

dere vormen van cryptografie. Het gebruik en meenemen van standaard en vrij verkrijgbare producten bedoeld voor persoonlijk of zakelijk gebruik valt hier niet onder.

Welke aandachtspunten en risico's betekent dit voor u?
De beschreven wet- en regelgeving ten aanzien van het gebruik van cryptografie brengt risico's met zich mee voor u als reiziger en voor uw organisatie. Zo kunt u in sommige landen in overtreding zijn als u cryptografische producten gebruikt of bij u hebt.

Verder kan het verplicht toegang verlenen tot uw informatie(drager) of afgifte van uw wachtwoord leiden tot inbreuk de vertrouwelijkheid van gegevens. Wees daarom bij het afgeven van (informatie) dragers bijvoorbeeld bedacht op (industriële) spionage. Vanuit die invalshoek moet u alert zijn op het maken van kopieën van uw informatie, zoals door de AIVD wordt vermoed en ook is beschreven in een brochure over (bedrijfs)spionagerisico's[4].

Op internet zijn ook verhalen te vinden over bij grenscontroles in beslag genomen laptops die pas na lange tijd (één jaar) zijn teruggegeven aan de eigenaar. Met de hier genoemde risico's moet u rekening houden, maar het is niet de algemene indruk dat het hier standaard handelingen betreft.

Besef dat als u toegang geeft u de controle over de verspreiding van uw vertrouwelijke informatie kunt verliezen. Dit kan grote gevolgen hebben voor de toekomstige beveiliging van u of uw organisatie. Wanneer u een encryptiesleutel afgeeft (in plaats van te ontcijferen en alleen het ontcijferde bestand te geven) ontstaat het risico dat ook andere bestanden die met diezelfde sleutel zijn te ontcijferen, toegankelijk kunnen worden. En dat alles wat u in de toekomst met die sleutel wilt beschermen ook toegankelijk kan zijn. Geeft u uw sleutel af die voor het zetten van een elektronische handtekening wordt gebruikt, dan kunnen anderen hiermee in uw naam berichten ondertekenen. Heeft u toch een encryptiesleutel moeten afgeven? Licht dan uw organisatie hierover in, zodat deze maatregelen kan treffen. Denk bijvoorbeeld aan het intrekken van sleutels of het opnieuw versleutelen van informatie met andere sleutels.

Wanneer u met autoriteiten in aanraking komt die toegang wensen tot uw informatiedragers, is het onverstandig om

4. https://www.aivd.nl/contents/pages/96114/spionagerisicosbijreizennaarhetbuitenland.pdf

Werken met vertrouwelijke informatie in het buitenland

te ontkennen dat u gebruik maakt van cryptografie of te proberen dit te verbergen. Zodra alleen al het vermoeden bestaat dat u het gebruik van cryptografie probeert te verbergen of dit ontkent, kunnen de gevolgen fors zijn: inbeslagname van de informatiedrager, gedwongen afgifte van de encryptiesleutel(s) onder dreiging van zware straf en/of plaatsing op een zwarte lijst waardoor toegang tot dat land in de toekomst onmogelijk wordt.

Adviezen voor de omgang met vertrouwelijke informatie in het buitenland

De geschetste risico's maken duidelijk dat u bij reizen naar en in het buitenland in een situatie kunt terechtkomen waarbij u toegang tot uw informatie(dragers) moet verlenen. Om in dit kader zo goed mogelijk om te gaan met vertrouwelijke informatie zijn hierna enkele adviezen opgenomen.

Om te beginnen wordt geadviseerd de bescherming van uw informatie zodanig in te richten dat u altijd medewerking kunt verlenen indien de autoriteiten toegang tot uw informatiedrager/laptop willen. Verplaats als organisatie het risico niet naar de individuele medewerker door te proberen gebruik van cryptografie te verbergen.
Stel uzelf en/of de organisatie vooraf de volgende vragen wanneer u naar het buitenland reist:

1. Heeft de informatie die u meeneemt (of op uw bestemming krijgt) een vertrouwelijk karakter?
2. Zijn er (wettelijke) verplichtingen tot bescherming van de informatie, bijvoorbeeld in het kader van de Wet Bescherming Persoonsgegevens (WBP)?
3. Bestaat er in het land van bestemming een kans op verzoek tot inzage?

Moet u één (of meer) van deze vragen bevestigend beantwoorden, overweeg dan het volgende:

- Gebruik altijd een schone 'reislaptop'. Dat wil zeggen dat u een laptop/informatiedrager gebruikt die geen vertrouwelijke informatie bevat of ooit heeft bevat (tenzij de informatie echt gewist is, zie kader Volledig verwijderen).
- Gaat u een vestiging van uw eigen bedrijf/organisatie bezoeken? Ga dan na of u de informatie beveiligd via het bedrijfsnetwerk kunt versturen (zowel vanuit Nederland naar het buitenland en eventueel ook weer de omgekeerde weg) en bij aankomst op uw laptop/informatiedrager kunt zetten.
  Een alternatief is op de plaats van bestemming een beveiligde verbinding (bijvoorbeeld een VPN) met het bedrijfsnetwerk te maken en de vertrouwelijke informatie naar uw laptop/informatiedrager te kopiëren, zodat u deze op uw bestemming kunt gebruiken/bewerken.
- Schoon uw informatiedragers voorafgaand aan de terugreis. Dat wil zeggen dat u de vertrouwelijke informatie op uw laptop of andere informatiedrager weer op een veilige wijze naar uw eigen organisatie stuurt (zoals beschreven onder het vorige punt). Verwijder vervolgens alle vertrouwelijke informatie van uw laptop/informatiedrager (zie kader Volledig verwijderen). Zorg er tijdens de reis wel voor dat uw laptop daadwerkelijk uit staat! In de stand-by mode kan er nog belangrijke informatie in het geheugen achterblijven. Vergeet ook de informatie op uw PDA, Blackberry, mobiele telefoon en/of de daarbij behorende geheugenkaart niet.

Volledig verwijderen

Hoewel veel mensen anders vermoeden, zijn verwijderde bestanden of geformatteerde schijven bijna altijd te herstellen, soms met behulp van extra hulpmiddelen. Dit betekent dat informatie achteraf toch te lezen is. Wilt u er zeker van zijn dat de informatie definitief verwijderd wordt, dan wordt geadviseerd gebruik te maken van speciale tools zoals PGP-shredder of Eraser. Deze tools overschrijven de oude data meermalen waardoor deze (bijna) niet meer terug te lezen is, zelfs niet met specialistische hulpmiddelen. Bedenk wel dat op deze manier wissen erg veel tijd kan kosten (met de huidige capaciteit van harde schijven tot wel een halve dag). Om de verwijdertijd te verkorten, kunt u alleen de bestanden verwijderen die vertrouwelijke informatie bevatten. Het risico is dan wel dat u bestanden over het hoofd ziet. Verdere instructies voor het schonen van media vindt u onder andere in publicaties van NIST (www.nist.org).

Tot slot

Wet- en regelgeving is overal aan verandering onderhevig. In combinatie met het grote aantal landen en het feit dat het zeer lastig is om juridisch taalgebruik exact te interpreteren kan dit artikel alleen op hoofdlijnen de problematiek beschrijven en niet in detail ingaan op specifieke situaties. Er wordt aangeraden om voor specifiek situaties altijd juridisch advies in te winnen.
Voor een goed startpunt met een wereldwijd overzicht van landen die beperkende wet- en regelgeving hebben, wordt verwezen naar de 'crypto law survey' door Bert-Jaap Koops, Universiteit van Tilburg. Zie http://rechten.uvt.nl/koops/cryptolaw.

Dit artikel is gebaseerd op een eerder door GOVCERT.NL gepubliceerd Factsheet. Het Factsheet is te downloaden via http://www.govcert.nl/render.html?it=146. Het is in een Nederlandse als ook in een Engelstalige versie beschikbaar.

De Spaanse zon

De neus van mijn auto staat in zuidelijke richting. Mijn vrouw installeert zich naast me en probeert de thermoskan met verse koffie klem te zetten, zodat niet bij iedere bocht corrigerend werk moet worden verricht. Ze vraagt me of het koffiezetapparaat is uitgezet en ik vraag haar of we de paspoorten bij ons hebben. U raadt het al: we zijn op weg naar onze vakantiebestemming naar het verre zuiden van Europa.

Terwijl ik de eerste kilometers onder de banden laat doorrollen, zie ik de paspoorten liggen. Een wonderlijk document is het wel. Onmiskenbaar een paspoort, onmiddellijk te herkennen. Eigenlijk verwonderlijk dat iedere douaneambtenaar gelooft dat jij daadwerkelijk degene bent die in het document beschreven staat, alleen maar omdat de burgemeester van mijn gemeente het document ter beschikking heeft gesteld (nou ja wat heet, ruim zestig euro kost zo'n document tegenwoordig). Die douaneambtenaar kent die burgemeester niet, heeft waarschijnlijk zelfs nog nooit van hem gehoord, en toch gelooft hij het document.

Wachtend in de file denk ik terug aan gisteravond, toen ik de laatste informatie voor de komende periode van internet afhaalde. Ook mijn webmail nog even opgehaald en toevallig dacht ik toen dat ik eigenlijk niet heel slim bezig ben, want alle toegangscodes op verschillende websites zijn voor mijzelf identiek. Overal waar ik moet inloggen, gebruik ik als gebruikersnaam Berry en een wachtwoord dat ik hier niet kan noemen. Stel nu dat iemand weet welke gebruikersnaam ik gebruik en hij zou ook nog toevallig achter mijn wachtwoord komen, dan zou hij toch heel makkelijk mijn identiteit kunnen overnemen. Cd's en dvd's bestellen bij mijn favoriete winkel, kleding aanschaffen en ik kan dan achteraf proberen aan te tonen dat ik de producten niet besteld heb, omdat ik in de auto zat.

Ik draai de airco nog wat hoger omdat ik het warm krijg van deze gedachte. Overal een nieuw ID aanvragen kost tijd en is lastig. Zou mijn burgemeester geen rol kunnen spelen in mijn identiteit op internet? Het zou toch wel heel handig zijn als ik mijn paspoort omhoog houd en daarmee toegang krijg tot mijn data. Het is en blijft ook het kip en ei-verhaal; als je begint met het spelen van burgemeester zul je eerst het vertrouwen moeten krijgen van diegene die de persoonlijke data ter beschikking moet stellen en jou als burgermeester erkent. Vervolgens moeten websites jou ook nog als burgemeester erkennen en onvoorwaardelijk geloven dat het paspoort ook daadwerkelijk jouw paspoort is. En het zou toch mooi zijn als ik honderd procent zeker weet dat de bezoekers van mijn zakelijke website ook degenen zijn die ze zeggen dat ze zijn.

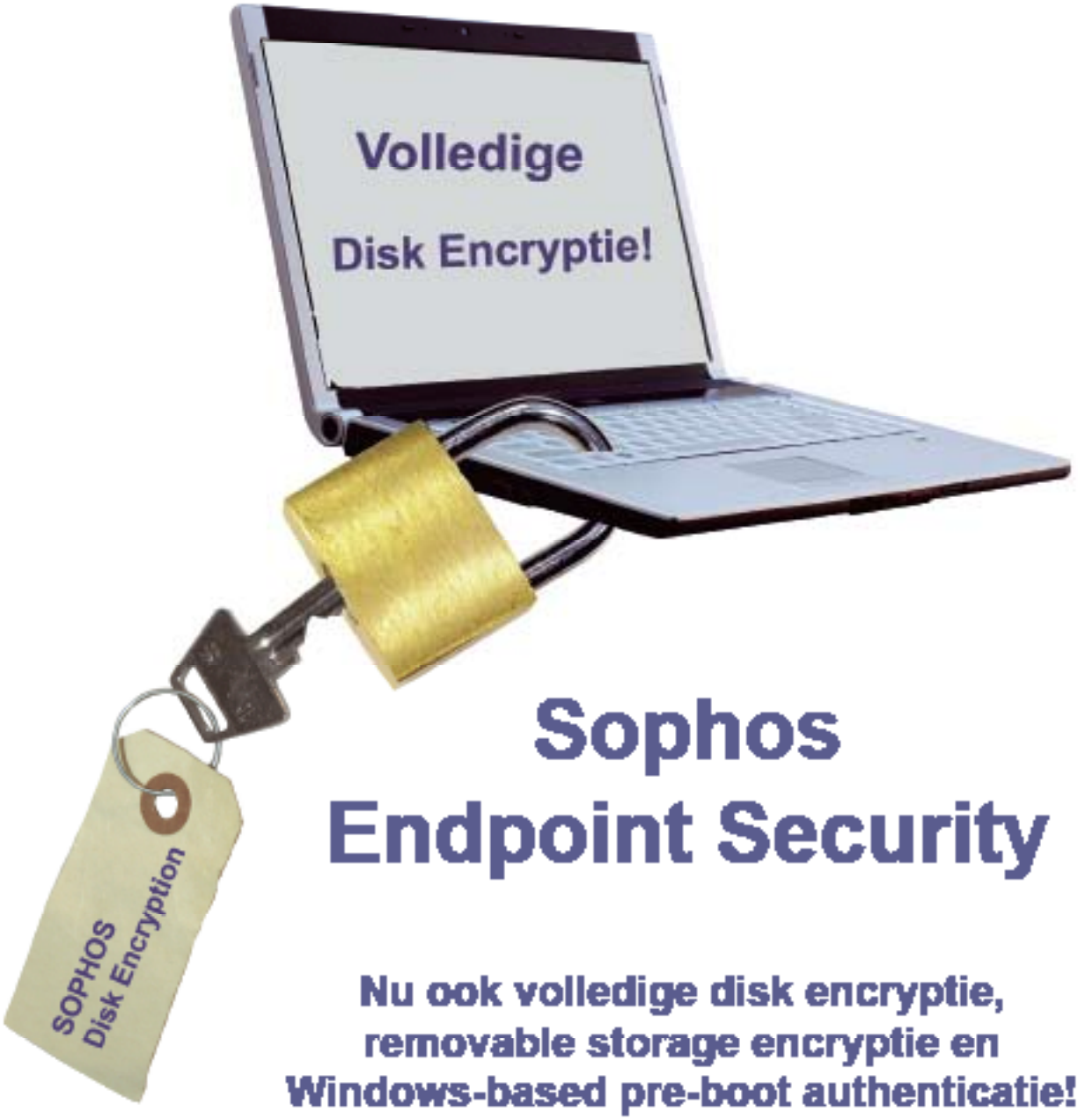
Ik mijmer wat door over de door mij ontdekte impasse en ik heb inmiddels al heel wat kilometers gemaakt. De eindbestemming is in zicht en de kleurige rood/gele vlaggen bij de ingang van onze camping wapperen in de warme bries van de zee. Ik stop voor de poort van de camping en mijn vrouw en ik melden ons bij de receptie. We lopen naar binnen met ons paspoort stevig in de hand. We worden vriendelijk aangesproken door een Spaanse dame die ons van harte welkom heet (tenminste, dat heb ik ervan begrepen) in die mooie Spaanse taal. Na de nodige pijlen op een plattegrond van het terrein weet ik inmiddels waar we de komende drie weken zullen vertoeven. Tot slot verzoekt de dame ons één van de paspoorten in te leveren als borg. Inmiddels ben ik overgegaan op het Engels en verzoek de mevrouw mij uit te leggen waarom ze dat wil achterhouden. Mijn vrouw kijkt mij niet heel vriendelijk aan, want zij heeft deze discussie al vaker aangehoord en ze weet dat ik binnen een paar minuten zal overgaan op het Nederlands omdat ik zelfs in het Engels mijn gevoelens niet meer kan uitdrukken.

Voordat het zover is, krijg ik een knietje tegen mijn bovenbeen en onder invloed van de vele autokilometers, de verzengende hitte en mijn ernstige behoefte aan een biertje geef ik mijn verzet op. Ik geef het paspoort van mijn vrouw af en we lopen terug naar de auto. Mijn burgemeester vindt het vast niet goed dat het paspoort nu in een Spaanse kluis ligt omdat ze bang zijn dat ik de camping zonder betalen zal verlaten. Tja, blijkbaar is het document wel zo belangrijk dat ik ga betalen in ruil voor een ongestoorde terugreis van mijn vrouw (en daardoor ook van mij). Ik besluit om er verder niet bij stil te staan en ons te richten op de komende periode.
'A cuernos, compañeros', oftewel tot horens kameraden.

Saludar,
Berry

NIEUW!

SOPHOS
secured.



Sophos Endpoint Security

Nu ook volledige disk encryptie, removable storage encryptie en Windows-based pre-boot authenticatie!

Kijk voor meer informatie op www.crypsys.nl of bel (0183) 62 44 44.

CRYPSYS Data Security B.V. – Benelux Distributeur van Sophos
Edisonweg 4 – 4207 HG Gorinchem – Postbus 542 4200 AM Gorinchem
T (0183) 62 44 44 – F (0183) 62 28 48 – E sales@crypsys.nl

CRYPSYS
data security