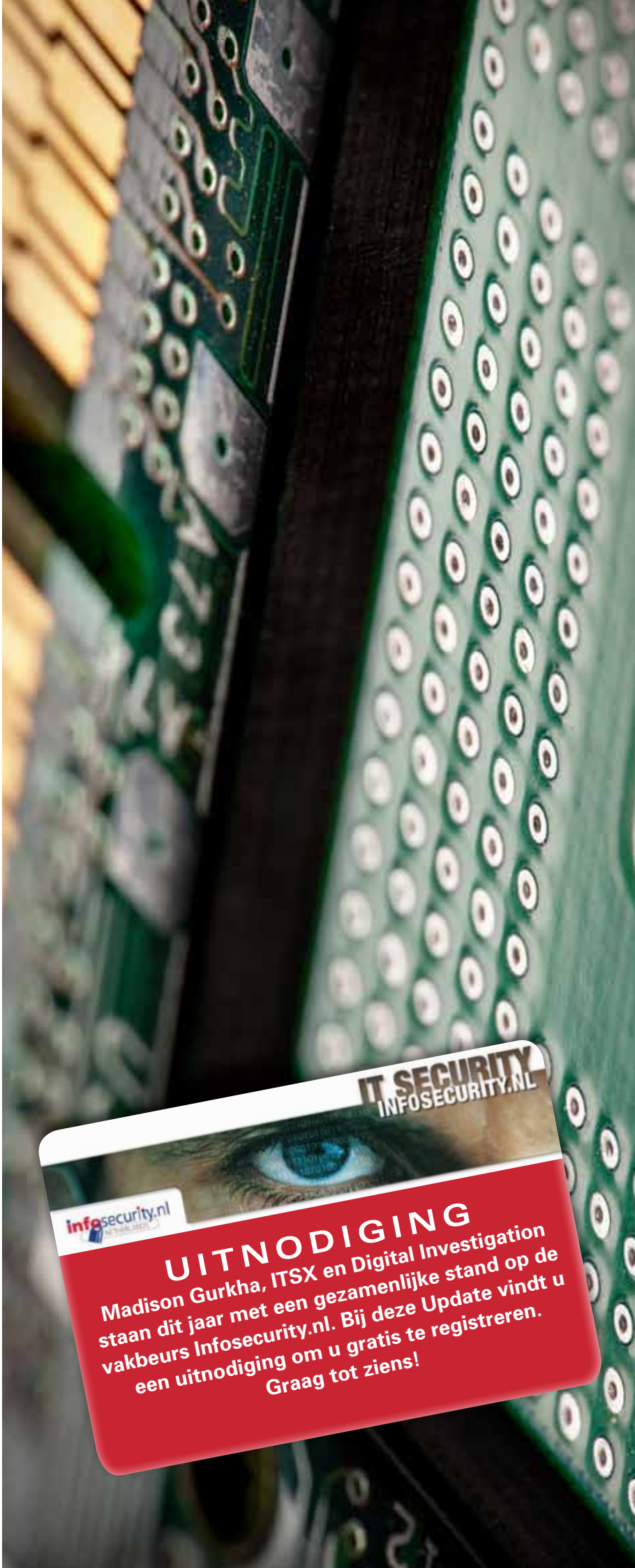
Madison Gurkha

Your Security is Our Business

19 SEPT 2013 UPDATE



In iedere Madison Gurkha Update vindt u een leuke en informatieve column, die de lezer een verfrissende kijk biedt op uiteenlopende onderwerpen rondom IT-beveiliging. Deze keer laten we commercieel directeur Remco Huisman aan het woord.

DE COLUMN

De drukste tijd van het jaar breekt aan

Dat we even hebben mogen genieten van een welverdiende vakantie, komt goed uit. Voor Madison Gurkha breekt namelijk de drukste tijd van het jaar aan. In het laatste kwartaal van het jaar moeten alle auditbeloften die door organisaties zijn gedaan, nog 'even' door ons gerealiseerd worden. Ook de eis van Logius dat er voor het einde van het jaar een DigiD-audit moet zijn uitgevoerd, zal het er voor ons niet rustiger op maken. Ik roep bij deze dan ook iedereen op om tijdig contact met ons op te nemen om onderzoeken in te plannen en voor te bereiden. Madison Gurkha breidt haar capaciteit gestaag uit, maar tot op heden is gebleken dat we hiermee maar net aan de groeiende vraag kunnen voldoen. Onze wervingsinspanning hebben we daarom ook aanzienlijk opgevoerd. Daarnaast hebben we wat aanpassingen in de organisatie gedaan om deze groei op te vangen (zie ook het Nieuws).

In de maand mei van dit jaar werden we opgeschrikt door een aantal DDoS-incidenten op onder andere de financiële sector en de DigiD-voorziening. Het maakte duidelijk dat het internet behoorlijk kwetsbaar is en dat het mogelijk is om cruciale voorzieningen zoals DigiD en telebankieren voor enige tijd onbereikbaar te maken. Het is van belang dat we ons van deze kwetsbaarheid bewust zijn en waar mogelijk maatregelen treffen. Gezien de aard van het internet en de werking van applicaties blijft een zekere kwetsbaarheid voor dit soort aanvallen echter altijd bestaan, maar de gevolgen kunnen desalniettemin wel verminderd worden.

Er zijn ook aanvallen die wel degelijk plaatsvinden, maar die wat minder bekend zijn dan bijvoorbeeld DDoS, SQL-injectie, Cross Site Scripting (XSS) of Cross Site Request Forgery (CSRF). Een van die minder bekende aanvallen beschrijven we in deze Update: 'Session Poisoning'. Op onze website kunt u overigens de 'Explanimations' bekijken over SQL-injectie, XSS en CSRF. We kennen de termen vaak wel, maar wat is het nu precies? Kies een filmpje en binnen drie minuten weet u het!

In mijn vorige column (zie Update 11) schreef ik over de business case voor informatiebeveiliging. Die business case wordt weer makkelijk te onderbouwen als het wetsvoorstel meldplicht datalekken wordt aangenomen. De meldplicht en de bijbehorende boete tot maximaal 450.000 euro zal denk ik wel de nodige awareness opleveren. Het CBP heeft ook richtsnoeren 'Beveiliging van persoonsgegevens' opgesteld die sinds 1 maart dit jaar van kracht zijn. In deze uitgave hebben we een extra artikel opgenomen om een gastschrijver aan het woord te laten. Tom de Wit van Louwers IP|Technology Advocaten zal u meer vertellen over deze richtsnoeren.

Ten slotte nodig ik u graag uit voor de Infosecurity.nl vakbeurs op 30 en 31 oktober in de Jaarbeurs Utrecht. Samen met ITSX en Digital Investigation hebben we een grote stand vlakbij de ingang. U kunt ons bijna niet missen en we verwelkomen u dan ook graag!

Remco Huisman
Commercieel directeur

HET COLOFON

Redactie
Daniël Dragičević
Laurens Houben
Remco Huisman
Matthijs Koot
Maayke van Remmen
Ward Wouts

Vormgeving & productie
Hannie van den Bergh / Studio-HB

Foto cover
Digidaan

Contactgegevens
Madison Gurkha B.V.
Postbus 2216
5600 CE Eindhoven
Nederland

T +31 40 2377990
F +31 40 2371699
E info@madison-gurkha.com

Redactie
redactie@madison-gurkha.com

Bezoekadres
Vestdijk 9
5611 CA Eindhoven
Nederland

Voor een digitale versie van de Madison Gurkha Update kunt u terecht op www.madison-gurkha.com.

Madison Gurkha **GROEIT** door

Het is de ervaring, kennis en kunde van onze consultants die bepalend is voor de kwaliteit die onontbeerlijk is in ons vakgebied. Met het groeiende aantal medewerkers en de diversiteit aan opdrachten is af en toe verandering nodig. Sinds mei 2013 werken we met twee teams van technische consultants. Elk team heeft een eigen teamleider, die ook de planning en werkvoorbereiding doet voor het team.

Naast het opsplitsen in teams is bovendien per kennisgebied een kennisgroep samengesteld met elk een kenniscoördinator voor het bijhouden en ontwikkelen van Tooling en het zorgdragen voor een optimale kennisoverdracht.

Hiermee kunnen we u te allen tijde de kwaliteit en service blijven bieden die u van ons gewend bent! Daarnaast blijven we onze doelstellingen verwezenlijken om op lange termijn een succesvol bedrijf te zijn, waar het prettig werken is aan uitdagende projecten.

Vacatures

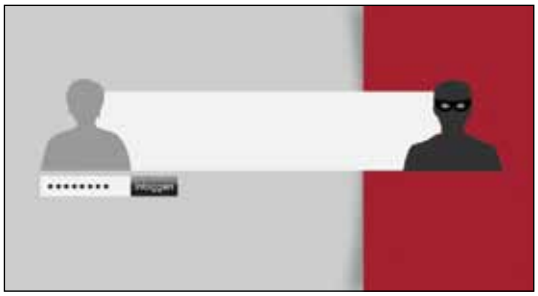
Door de aanhoudende groei zijn we nog steeds opzoek naar:

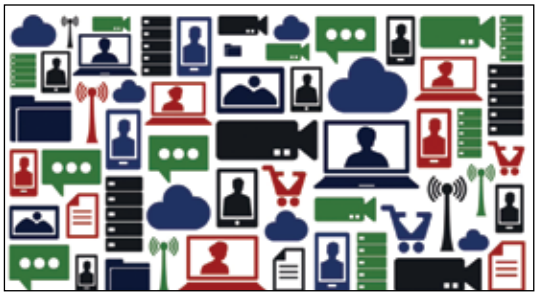
technische security consultants

Kijk voor meer informatie op onze website.
Ben je echt goed en heb je interesse?
Stuur een mail naar hrm@madison-gurkha.com.

Save the Date!

In mei dit jaar vond de elfde editie van de Black Hat Sessions met het thema Cyber Security plaats. Op dit moment zijn wij al weer druk bezig met de samenstelling van een interessant sprekersprogramma voor de twaalfde editie. Het thema blijft nog even een verrassing, maar het belooft wederom een inspirerende, informatieve en bijzonder evenement te worden.
Zorg dat u erbij bent en noteer alvast in uw agenda: **dinsdag 17 juni 2014**, Black Hat Sessions Part XII.





Wilt u weten hoe hackers te werk gaan? Aan de hand van een duidelijke en simpele video?

Ondanks vele voordelen verhoogt digitalisering ook het aantal beveiligingsrisico's. Om u meer inzicht te geven in bepaalde beveiligingsproblemen, heeft Madison Gurkha zogenaamde 'explanimations' laten ontwikkelen. Bekijk via onze website de Madison Gurkha Cyber-Security Series voor een korte en bondige uitleg van de veelvoorkomende IT-beveiligingsproblemen zoals SQL-injectie, XSS en CSRF.

Madison Gurkha interviewt voor iedere editie een gerenommeerd persoon in de ICT-beveiligingswereld om zijn of haar visie te delen. Deze keer een interview met Eileen Monsma van het Team High Tech Crime.

"Nederland is erg populair op cybergebied"

Misdaad heeft tegenwoordig bijna altijd een digitale component of speelt zich zelfs volledig af in het digitale domein. Binnen de politie houdt het Team High Tech Crime zich bezig met het bestrijden van de meer geavanceerde vormen van cybercrime. Eileen Monsma is waarnemend teamleider bij het THTC. Op onze Black Hats Sessions vertelde ze met passie over het werk en de resultaten van het team.

Wat is de primaire taak van het Team High Tech Crime?

"De opsporing van cybercrime is een steeds belangrijker aandachtsgebied voor de nationale politie. Ik bedoel dan die zaken waarbij ICT zowel middel als doel van de dader is. Daarbinnen is het THTC verantwoordelijk voor 'high tech crime': opsporingsonderzoeken die gericht zijn op de meest complexe en innovatieve vormen van cybercrime, die vaak een grote maatschappelijke impact hebben."

Hoe is het team georganiseerd?

"We werken vanuit Driebergen met vier vaste teams, die ieder voor de ene helft bestaan uit mensen met een politie-achtergrond en voor de andere helft uit zij-instromers. Onze digitaal experts hebben vaak één of meerdere ICT-studies gedaan. Die kruisbestuiving werkt heel goed: met elkaar verzinnen we per zaak de beste methode om deze op te lossen, terwijl we de aansluiting op het politiedomein vasthouden. Er zitten ook financieel experts op de teams; die zijn belangrijk omdat veel high tech crime gepaard gaat met ingewikkelde geldstromen."

Wanneer komt het THTC wel en wanneer niet in actie?

"We geven geen preventieadviezen en surveilleren ook niet online. Net als bij andere misdrijven doe je als burger aangifte van cybercrime op het lokale politiebureau. Het is dan wel handig om vooraf te vragen of er een digitaal rechercheur bij aanwezig kan zijn. Wij worden door de regionale eenheden ingeschakeld als er sprake is van high tech crime. Denk aan een botnet dat gegevens steelt, of malware die bankoverschrijvingen manipuleert. We gaan zonodig ter plekke sporen veiligstellen met onze cybertruck en daarna kan ons digitale laboratorium ermee aan de slag. Ook worden we vanuit de maatschappij soms ingeschakeld als er een acute behoefte aan onze expertise is. Dat zijn de zaken die je op het nieuws ziet."

Jullie hebben toch ook veel contact met de buitenwereld?
"Ja, maar je kunt ons als burger niet zomaar bellen. Onze contacten zijn altijd heel gericht en gebaseerd op afspraken. Vanwege een internationaal verdrag kunnen we bijvoorbeeld dag en nacht benaderd worden door politiediensten van andere landen, wanneer zij onze hulp nodig hebben om bewijsmateriaal veilig te stellen of verdachten te traceren. Voor een Amerikaans onderzoek hebben we onlangs een bijdrage geleverd aan de aanhouding van de mensen achter een grote internationale virtuele witwasbank, gewoon hier in Nederland. En we delen gericht kennis over de bestrijding van high tech crime, bijvoorbeeld met organisaties achter de vitale infrastructuur, maar ook via de wetenschap en onze professionele netwerken."

Staat het THTC open voor publiek-private samenwerking? Zo ja, hoe wordt dat in de praktijk gerealiseerd?
"Jazeker! We hebben naast rechercheurs een groep informatie- en beleidsspecialisten. Zij onderhouden veel contacten met publieke en private partijen zoals ook Madison Gurkha. Daar steken we veel energie in, omdat niemand het in dit werkveld alleen kan. Onze specialisten verzamelen ook zelf kennis en doen onderzoek zodat we een breder beeld krijgen waarmee we criminele organisaties kunnen ontmantelen. Daarvoor is er bijvoorbeeld de Electronic Crimes Taskforce, ofwel het bankenteam, dat bij ons is gehuisvest. Hierin werken de grootbanken samen met de politie aan de bestrijding en opsporing van digitale fraude."

Het THTC heeft flink aan de weg getimmerd om nieuwe mensen te werven, onder meer met een spannende Cybercrime Challenge. Jullie theatershow was zelfs uitverkocht. Lukt het om genoeg goede mensen te werven?
"Er zal altijd meer criminaliteit zijn dan de politie kan opsporen, maar we zijn goed op weg. Minister Opstelten heeft aan de Tweede Kamer toegezegd dat ons team vanaf 2014 twintig grote zaken per jaar zou moeten kunnen draaien op het gebied van high tech crime. We hebben uitgerekend dat we hiervoor 120 mensen nodig hebben. Dit jaar groeien we boven de 80 teamleden en er komt dus nog een grote wervingsronde aan. Ik was al trots op wat we aan specialisten in huis hebben en ben nu weer positief verrast door het aantal parels dat we deze keer een contract hebben kunnen aanbieden. Mensen die bij ons solliciteren vinden het werk even leuk als belangrijk. Het betaalt ook niet slecht en de secundaire arbeidsvoorwaarden zijn hier prima."

Welke trends ziet het THTC op het gebied van high tech crime?
"Zoals alle software breder toegankelijk is geworden, geldt dit ook voor malware - hierdoor raken de werelden van cybercrime en van de 'oude' georganiseerde misdaad steeds meer vervlochten. Maar ook vormen scriptkiddies een steeds grotere bedreiging, omdat ze niet doorhebben wat hun gegoogelde exploits kunnen aanrichten. Daarom is het nuttig wat een bedrijf als Madison Gurkha doet. We zien wel een toename van criminele dienstverleners: tussenpersonen die een oogje toeknijpen richting klanten die zwaar illegale praktijken uitvoeren. En een voorbeeld dat veel mensen persoonlijk raakt is ransomware. Daarbij wordt je harddisk 'gegijzeld' en moet je geld betalen in de hoop dat je de geblokkeerde gegevens weer terugkrijgt. Wat vervolgens niet gebeurt. Die ransomware wordt steeds bedreigender van aard."

Hoe staat het THTC tegenover het terughacken dat door minister Opstelten is voorgesteld?
"Het klinkt wel stoer, maar juridisch gezien bestaat 'terughacken' niet. Hacken is een strafbaar feit en de politie maakt alleen zulke inbreuken na toestemming van de officier van justitie of de rechter-commissaris. Het definitieve wetsvoorstel is er nog niet, maar het concept dat wij hebben gelezen lijkt te verduidelijken wat we online wel en niet mogen. Dat is nuttig, omdat de ontwikkelingen op digitaal gebied zo snel zijn gegaan. Doordat alles met elkaar verbonden raakt en steeds meer gegevens versleuteld in de cloud hangen, worden onze opsporingsmogelijkheden op scherp gezet. Wij vinden het belangrijk dat er ook vanuit de maatschappij kritisch wordt meegekeken met de definitie van onze bevoegdheden. Je moet je wel afvragen wat je erger vindt: een rechercheteam dat het huis van een verdachte betreedt om een keylogger te plaatsen, of een stukje software dat van afstand wordt geïnstalleerd. Dat binnensluipen mogen we al!"

In je presentatie op de Black Hats Sessions zei je dat Nederland in 2017 onaantrekkelijk moet zijn voor cybercriminelen. Hoe gaat het THTC dat realiseren?
"Dat kunnen we natuurlijk niet alleen. Onder meer het Nationaal Cyber Security Centrum speelt hier een grote rol in, maar ook wat jullie doen is van belang voor de cyberveiligheid. Nederland is erg populair op cybergebied en dat moet vooral zo blijven. Maar dat heeft wel een keerzijde: criminelen die onze infrastructuur misbruiken. Die willen we afschrikken. Het is daarom heel belangrijk dat de politie een goede informatiepositie heeft en daarop snel kan handelen. Momenteel zit een Armeense cybercrimineel dankzij ons een celstraf van 4 jaar uit omdat hij miljoenen verdiende met zijn criminele botnet dat hij via Nederland aanstuurde. Die zien we hier denk ik niet meer terug."

"Ik was al trots op wat we aan specialisten in huis hebben en ben nu weer positief verrast door het aantal parels dat we deze keer een contract hebben kunnen aanbieden."

In de rubriek 'Het Inzicht' stellen wij bepaalde (technische) beveiligingsproblemen aan de orde. Deze keer geeft Matthijs Koot meer inzicht in inlichtingendiensten op internet.

Inlichtingendiensten op internet

In project 'Argo 2', alias 'Symbolon', worden de SIGINT/CYBERINT capaciteiten van de AIVD en de MIVD samengevoegd in een gezamenlijke eenheid. De focus van die eenheid ligt op nationale veiligheid, aldus de Symbolon-directeur tijdens het NCSC-symposium in januari 2013. Iets concreter werd daaronder verstaan: cyberterrorisme (vooralsnog geen reële bedreiging), digitale activiteiten van andere staten, digitale spionage en digitaal extremisme (waaronder 'hacktivisme' werd genoemd). De nieuwe eenheid is een kern van Nederlandse digitale expertise die ook gaat bijdragen aan ontwikkeling van offensieve capaciteit van het Ministerie van Defensie.

De eerste taakstelling van de AIVD in de Wet op de Inlichtingen en Veiligheidsdiensten 2002 (Wiv 2002, art. 6, lid 2a) luidt: "het verrichten van onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat".

DOEL VAN INLICHTINGENDIENST

Je zou kunnen zeggen dat de kernactiviteit van inlichtingendiensten bestaat uit het testen van hypothesen die voortvloeien uit observatie en inlichtingen. Hypothesen over activiteiten die een gevaar vormen voor het voortbestaan van de democratische rechtsorde of voor de staatsveiligheid. Bij het testen van hypothesen bestaan twee soorten fouten: fout-positieven (type I fout) en fout-negatieven (type 2 fout). Een voorbeeld van een fout-positieve is een persoon die onterecht wordt verdacht. Een voorbeeld van een fout-negatieve is wanneer een onbekende, of iemand die bekend is bij de inlichtingendienst maar nergens van wordt verdacht, 'ineens' een aanslag pleegt. Fout-positieven zijn vervelend, fout-negatieven zijn potentieel dodelijk: inlichtingendiensten zijn er daarom primair op geënt fout-negatieven te voorkomen.

TERRORISMEBESTRIJDING

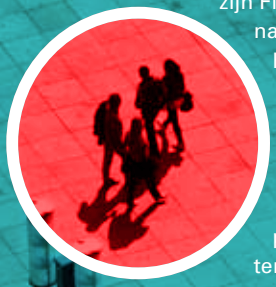
Eén aandachtsgebied van de AIVD is terrorismebestrijding. Bij 'zelfradicalisering' speelt het radicaliseringsproces zich deels of geheel via internet af. Bij vroege signalering van radicalisering kan de AIVD proberen een individu te beïnvloeden voordat deze tot (voorbereidingen tot) een aanslag overgaat. Het is dus niet vreemd dat de aandacht van inlichtingendiensten uitgaat naar mogelijkheden om op internet te observeren: te zien welke berichten door wie op een forum zijn geplaatst, welke informatie iemand raadpleegt en wie met wie contact heeft. In het jaarverslag 2011 schat de dienst dat ongeveer 25.000 jihadisten uit meer dan 100 landen deel uitmaken van de kerngroep van invloedrijke jihadistische webfora. Het voorkomen van fout-negatieven wordt er niet makkelijker op: herken de spelden maar eens in de digitale hooiberg - die zich natuurlijk niet beperkt tot jihadistische webfora.

Een bekend voorbeeld van een fout-positieve hier is een docent wis-, natuur- en scheikunde werd in 2004 door de AIVD verdacht van betrokkenheid bij de verspreiding van massavernietigingswapens, nadat hij per e-mail bij een Britse onderzoeker en vijf Canadese fabrieken informatie zocht over zwaar water – ook woonde hij ooit in dezelfde straat als de Pakistaanse atoomspion Abdul Qadeer Khan. Achteraf bleek de docent te werken aan Cito-examenvragen [1,2].

DIGITALE SPIONAGE

Een ander aandachtsgebied van de AIVD is digitale spionage. Het doel van spionage is het verwerven van politieke, militaire, economische en/of wetenschappelijke informatie. Onze kenniseconomie en lidmaatschappen van de EU en NAVO maakt Nederland een interessant doelwit voor spionage.

De commerciële markt voor elektronische spionagemiddelen is recent geschat op 3 tot 5 miljard dollar, met een jaarlijkse groei van 20 procent. Twee van de bekendere producten op deze markt zijn FinFisher van het Duitse Gamma International, en DaVinci Remote Control System van het Italiaanse Hacking Team. Beide zijn 'spionagetrojans'. In 2011 werd bekend dat de kosten voor FinFisher 250.000 euro bedragen voor de basisinfrastructuur, en vervolgens 6.000 euro per afgeluisterd persoon. Wie kopen deze producten? Wie gaan ze ermee afluisteren, met welke bedoeling en met welke



(onvoorziene?) consequenties? Bespioneren FinFisher-klanten elkaar met FinFisher en zo ja, speelt Gamma International klanten dan tegen elkaar uit met uniek maatwerk? In maart publiceerde CitizenLab de resultaten van een wereldwijde speurtocht naar FinFisher-infrastructuur. Daarbij zijn twee FinFisher-servers aangetroffen in IP-adresruimte van Tilaa, een Amsterdamse ISP[3] Wie ze beheert en waarvoor ze worden gebruikt, is niet bekend. FinFisher is ook aangetroffen in Bahrein en Turkmenistan; en van Bahrein staat vast dat de software is ingezet tegen activisten.

De taak van de AIVD is ongewenste inlichtingenactiviteiten te onderkennen en te helpen beëindigen bij overheid, universiteiten en het bedrijfsleven. Dat kan dus ook bestrijding betekenen van FinFisher, DaVinci, en malware van onbekende makelij die tegen Nederlandse belangen worden ingezet. De AIVD waarschuwde in afgelopen jaren ambtenaren (2008), gemeenten (2010) en universiteiten (2010) voor digitale spionage. Sinds 2012 kan iedereen op de AIVD-website gratis de e-learningmodule 'Kwetsbaarheidsanalyse spionage' (KWAS) aanvragen. Die ontvang je op CD, met in de begeleidende tekst de opmerking dat de CD op malware is gecontroleerd.

Bij digitale spionage wordt meestal op enig moment over internet gecommuniceerd tussen de afluisteraar en de afgeluisterde, en dan vaak via onbekende routes. De uitdaging is het herkennen van een patronen. Wanneer een patroon bekend is zou je bij, zeg, de AMS-IX, apparatuur kunnen zetten die die patronen kan herkennen in verkeersgegevens en/of de inhoud. En daar kun je dan meteen patronen in configureren voor observatie van online radicalisering. Technisch zijn daar wel mogelijkheden voor, hoewel versleuteling en cloudcomputing nieuwe uitdagingen geven. Of het juridisch mogelijk is? Nee, de Wiv 2002 staat ongericht tappen niet toe. (Er wordt momenteel gewerkt aan een nieuwe versie van de Wiv, maar bij gebrek aan openbare stukken blijft dat stof voor een toekomstig artikel.) Of het ethisch acceptabel is: misschien, maar democratische controle is noodzakelijk.

WAT NU

De bronnen en methoden van de AIVD moeten natuurlijk zoveel mogelijk geheim blijven, maar het kan niet zo zijn dat alle digitale activiteiten zich onttrekken aan democratische controle. Immers is het beschermen van de democratische rechtsorde nu juist een taak van de AIVD. Die controle moet gaan over noodzakelijkheid en proportionaliteit: zijn er minder ingrijpende middelen dan om digitale spionage en zelfradicalisering tegen te gaan? Is het middel erger dan de kwaal? In Nederland hebben we sinds 2003 de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), die deze controle uitvoert. De toezichtsrapporten van de CTIVD zijn openbaar[4], op incidenteel een geheimgehouden bijlage na. Ik hoop dat de CTIVD de expertise heeft om de juiste kritische vragen te stellen over de digitale activiteiten van de inlichtingendiensten. Het werk van Bits of Freedom is ook hier verschrikkelijk belangrijk (doneer!).

Inlichtingendiensten moeten niet alleen streven naar zo min mogelijk fout-negatieven, maar ook naar zo min mogelijk fout-positieven. Citerend uit het artikel 'Verdenking' van Rob Wijnberg in De Groene Amsterdammer (goed blad!) van week 34[5]: "Het is de hoogste tijd dat de journalistiek, namens de burger, zijn tanden laat zien en de politieke klasse hier zonder enige terughoudendheid en scrupules over ondervraagt. Zonder zwijgrecht. En zonder recht op een spindoctor. Negen uur achter elkaar, desnoods. Verdenkingen genoeg."

1 http://www.nationaleombudsman.nl/rapporten/2006/064
2 http://vorige.nrc.nl/krant/article1700579.ece
3 https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/
4 http://www.ctivd.nl/
5 http://www.groene.nl/2013/34/verdenking

Madison Gurkha, ITSX en Digital Investigation op de vakbeurs Infosecurity.nl

Infosecurity.nl is dé Nederlandse vakbeurs op het gebied van IT security. Spam, phishing, hackers en steeds geavanceerde vormen van cybercrime vormen reële bedreigingen voor het bedrijfsleven. De vakbeurs haakt in op actuele vraagstukken over IT security. Een must voor iedere IT-professional. Madison Gurkha, ITSX en Digital Investigation zijn dit jaar aanwezig met een gezamenlijke beursstand (01.B154) op Infosecurity.nl.

U bent 30 en 31 oktober a.s. van harte welkom op onze stand 01.B154 (u vindt ons meteen vooraan bij de entree). Gedurende deze twee dagen zullen wij u op een interactieve manier kennis laten maken met ons zeer complexe en snel veranderende vakgebied. Madison Gurkha en dochterbedrijf ITSX helpen uw organisatie met kwalitatief hoogwaardige diensten om technische IT-beveiligingsrisico's structureel te identificeren, te verminderen en te voorkomen. En mocht het onverhoopt dan toch misgaan, dan is het toch wel een veilig idee dat u – wanneer dan ook – de specialisten van onze partner Digital Investigation kunt inschakelen. Om ervoor te zorgen dat uw bezoek zeker de moeite waard is, hebben we een interessant programma opgesteld.

Aanval - verdediging demonstratie

Tijdens een boeiende Live Hacking demo zal een aanval, zoals die werkelijk zou kunnen plaatsvinden, van begin tot eind worden gedemonstreerd. Dit gebeurt zowel vanuit het standpunt van de aanvaller als vanuit het standpunt van de beheerder van het aangevallen systeem. Hierdoor kunt u zien welke aanwijzingen kunnen duiden op inbraakpogingen en welke acties uw beheerder kan ondernemen om de inbrekers te detecteren en te stoppen. Op die wijze krijgt u inzicht in de werkwijze van aanvallers en misschien nog belangrijker: hoe hiertegen te beveiligen is. Via onze website zullen wij u binnenkort informeren over de tijden waarop de demonstraties plaatsvinden.

Gratis toegang

Bij deze Update vindt u een uitnodiging waarmee u zich via een persoonlijke code gratis kunt registeren via www.infosecurity.nl. Met één toegangsbadge heeft u bovendien beide dagen toegang tot Storage Expo en het Tooling Event dat gelijktijdig met Infosecurity.nl plaatsvindt.

Houd onze website in de gaten voor actuele informatie over onze beursdeelname. Hier kunt u zich ook registreren voor uw gratis toegangsbewijs.

30 & 31 oktober 2013

Jaarbeurs Utrecht

Stand 01.B154

Madison Gurkha
Your Security is Our Business

ITSX

DIGITAL Investigation

In elke Madison Gurkha Update vragen wij een klant het spreekwoordelijke hemd van het lijf met betrekking tot zijn of haar relatie met IT-beveiliging.

DEKLANT

9 vragen aan …

… Peter Verhulst, CISO bij de gemeente Rotterdam

1 ***CISO bij de gemeente Rotterdam. Wat betekent dat in de praktijk?***
Als 'Concern Information Security Officer' (CISO) bij de gemeente Rotterdam opereer ik aan de beleid/bestuurlijke kant en werk ik nauw samen met de security manager van onze ICT-organisatie. Belangrijke taken hierbij zijn kaderstelling (beleid, richtlijnen), toetsing, advisering en crisismanagement.

2 ***Wat zijn de belangrijkste kwaliteiten waarover men moet beschikken om deze functie met succes te kunnen uitoefenen?***
Belangrijk is een dienstverlenende houding; dus niet alleen controleren en toetsen maar ook meedenken over praktische oplossingen. Dat vraagt om een flinke dosis sociale vaardigheden. Daarmee vergroot je de acceptatie van beveiligingsmaatregelen en je kunt laten zien dat IB meer is dan 'control'. Het is namelijk ook een 'enabler' voor nieuwe manieren van werken: het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk.

3 ***Hoeveel mensen houden zich in uw organisatie bezig met informatiebeveiliging?***
Dat is moeilijk te zeggen, omdat wij naast een aantal fulltime functies aardig wat medewerkers hebben die een deeltaak vervullen rondom IB. Onze beheerorganisatie heeft bijvoorbeeld per beheerdiscipline een coördinator IB. Binnen elk primair procescluster is een strategisch i-adviseur aangewezen voor coördinatie van IB. We zien wel dat deze functies steeds belangrijker worden. Op termijn zal dat wellicht leiden tot meer fulltime en vooral gespecialiseerde functies.

4 ***Hoe is informatiebeveiliging opgezet in uw organisatie?***
Informatiebeveiliging is opgezet volgens een sturingsmodel voor bedrijfsvoering (governance) met drie rollen: *sturend, vragend* en *uitvoerend*. Binnen elke rol zijn taken en verantwoordelijkheden ten aanzien van IB belegd. Zo opereer ik namens de concern directie in een sturende rol. Onze beheerorganisatie is uitvoerend en richt zich met name op beveiligingstechniek. De 'business' is in een vragende rol onder meer verantwoordelijk voor bedrijfscontinuïteit en sturing op naleving; meer de menselijke kant dus.

Binnen de gemeente Rotterdam is informatiebeveiliging gedefinieerd als cyclisch proces: plan - do – check – act. De komende jaren willen wij ons vooral richten op inbedding van IB in het primaire proces. Dat wil zeggen: informatiebeveiliging maakt steeds meer integraal onderdeel uit van de bedrijfsvoering, zoals dat voor financiële processen (P&C) al grotendeels geldt. Daarmee hebben we de transitie naar risicomanagement ingezet, in feite: het volwassen worden van ons vakgebied.

5 ***Wat zijn in uw organisatie op dit moment de belangrijkste uitdagingen op het gebied van informatiebeveiliging?***
De toename van dreigingen van buitenaf stelt ons doorlopend voor de uitdaging onze beveiligingstechniek te verbeteren. Ik zie echter ook een uitdaging om de IB functie in de organisatie zelf te versterken. De manier waarop we werken is in een paar jaar tijd flink veranderd. We leggen meer verantwoordelijkheid bij medewerkers. Bewust gedrag en sturing daarop is essentieel. Daar ligt een rol voor het lijnmanagement. IB is al lang geen ICT-feestje meer, techniek is maar de helft van het verhaal, zonder goede naleving ben je nog steeds niet in 'control'.

6 ***Op welke wijze maakt uw organisatie gebruik van DigiD?***
Wij hebben één DigiD-aansluiting voor elektronische dienstverlening ('mijn loket' van de gemeente Rotterdam). Achter dit loket zitten tal van producten, zoals vergunningaanvraag of de aanvraag van een GBA-uittreksel.

7 ***Wat zijn op dit moment de belangrijkste uitdagingen omtrent de beveiliging van DigiD?***
Wij proberen zoveel mogelijk dienstverlening aan te bieden middels 'mijn loket' (met gebruik van DigiD). Met name de beveiliging van webapplicaties (die wij zelf ontwikkelen) is van groot belang.

8 ***Welke maatregelen worden genomen om deze risico's onder controle te houden?***
Er wordt ontwikkeld o.b.v. security richtlijnen, zoals de webrichtlijnen van het NCSC. We laten dit regelmatig onafhankelijk testen. Daarnaast bouwen we steeds meer kennis op om zelf op kwetsbaarheden te scannen.

9 ***Wat zijn uw ervaringen met Madison Gurkha?***
Wij hebben het technisch onderzoek in het kader van de DigiD audit laten uitvoeren voor Madison Gurkha. Bij mijn weten was dit de eerste keer dat we zaken hebben gedaan en dat is door beide partijen als positief ervaren. Madison Gurkha heeft een constructieve, no nonsens houding en denkt actief mee over mogelijke oplossingen. Er is voldoende ruimte voor reflectie op onderzoeksbevindingen. Het contact is prettig, de communicatielijnen kort, de documentatie goed verzorgd…kortom, een positieve ervaring.

Dit keer in de rubriek 'De Hack' laat Serge van den Boom, security consultant bij Madison Gurkha, zien hoe relatief makkelijk een sessietoestand is te manipuleren d.m.v. Session Poisoning.

Als je gebruik maakt van een webapplicatie, dan wordt er vaak op de server een toestand ('state') bijgehouden van je sessie. In deze toestand kan informatie worden bijgehouden zoals wie je bent, wat er in je boodschappenwagentje zit, op welke pagina van de zoekresultaten je zit, en welk artikel je hebt geselecteerd. Soms blijkt het mogelijk te zijn om deze sessietoestand te manipuleren, en daarmee de beveiliging te doorbreken.

In de sessietoestand wordt typisch informatie opgeslagen die gedurende meerdere handelingen in de applicatie gebruikt kan worden, en dus niet bij iedere stap opnieuw wordt meegezonden.
Zodra de informatie bekend is, slaat de applicatie deze op in de sessietoestand, en leest deze weer uit wanneer de informatie weer nodig is.
Zo zal 'wie je bent' bij het inloggen in de sessietoestand worden opgeslagen, het 'huidige geselecteerde artikel' bij het aanklikken van de laatste CD van Zanger Rinus, en wordt het boodschappenwagentje bijgewerkt bij ieder paar sokken dat je erin gooit.

Vaak hangen er beveiligingsgerelateerde aannames aan informatie in de sessietoestand. Zo zal er door de gehele applicatie vanuit worden gegaan dat de 'wie ben ik'-informatie na het inloggen niet meer door de gebruiker gewijzigd kan worden.
Op dezelfde manier zal vaak de aanname worden gemaakt dat als je een dossier geselecteerd hebt, er bij de selectie gecontroleerd is dat je toegang mag hebben tot de informatie in dat dossier.
En hier gaat het soms mis en is een 'session-poisoning'-aanval mogelijk. Deze aanval — ook wel bekend onder de naam 'session pollution' — draait om het aanpassen van de informatie in de sessietoestand tegen de gemaakte aannames in.
Als je zo de sessietoestand kunt aanpassen na de controles, kunnen handelingen uitgevoerd worden op gegevens waarvoor de handeling niet is goedgekeurd.

Een lekke documentensite

Een voorbeeldje: Op de webapplicatie DeelZooi.nl kunnen gebruikers hun eigen verhalen uploaden. Iedereen kan deze documenten lezen, maar alleen de uploader kan een document verwijderen.
Wanneer de gebruiker aangeeft een document te willen verwijderen, dan controleert de server of dat mag, en zo ja, dan wordt het document in de sessietoestand gemarkeerd als het huidige document. Vervolgens moet de gebruiker op een aparte pagina het verwijderen bevestigen, waarna het huidige document wordt verwijderd.

Om een document te lezen wordt het document ook gemarkeerd als het huidige document, maar wordt er geen controle gedaan, en wordt het document getoond.
Een aanvalsscenario kan er als volgt uitzien: Slachtoffer Alice heeft op DeelZooi.nl haar Twilight-fan-fiction geüpload. Onze aanvaller — die traditioneel Mallory heet — is geen fan van Twilight en voert de volgende stappen uit:
Stap 1: Hij kiest een document van zichzelf (SupermanVsPredator.doc) om te verwijderen, maar bevestigt dit nog niet.
Stap 2: In een apart tabblad in de browser klikt hij op de 'lees'-knop bij het bestand ABloodyMess.doc van Alice.
Stap 3: In het oorspronkelijke tabblad bevestigt hij het verwijderen, zogenaamd van SupermanVsPredator.doc.

In **stap 1** is al gecontroleerd of Mallory het document mag wijzigen, maar in **stap 2** is gewijzigd wat de applicatie als het 'huidige document' beschouwt.
In **stap 3** wordt dan ook in plaats van SupermanVsPredator.doc het nieuw geselecteerde document ABloodyMess.doc verwijderd, tot verdriet van Alice.
(In **stap 4** wordt Mallory gearresteerd wegens computervredebreuk.)
In dit geval zijn er twee aparte handelingen in de applicatie, 'lezen' en 'verwijderen', die beide hetzelfde concept van 'huidige document' uit de sessietoestand gebruiken.

Een manier om deze kwetsbaarheid op te lossen, zou dan ook kunnen zijn om in plaats van 'het huidige document' apart 'huidig document om te verwijderen' en 'huidig document om te lezen' op te slaan.
Maar ook als er maar een enkele handeling in de applicatie is, kan session poisoning mogelijk zijn, zolang deze handeling maar is opgebouwd uit meerdere stappen.
Je kunt dan als je al bij een latere stap bent aangekomen, terug naar een eerdere stap om de sessietoestand aan te passen.

Een lekke goksite
Bijvoorbeeld: Een online gokspelletje bestaat uit drie stappen. In de eerste stap plaats je je inzet. In stap twee draai je aan het wiel. Win je, dan krijg je afhankelijk van het resultaat een bepaald bedrag toegekend, vermenigvuldigd met je inzet. In stap drie kun je dan kiezen om dit bedrag te laten uitbetalen, of om de kans te nemen om je winst te verdubbelen.
Hiervoor wordt in de eerste stap je inzet in de sessietoestand opgeslagen, en wordt deze in de derde stap weer uitgelezen.
Mallory heeft na het hacken van DeelZooi.nl wat geld nodig voor zijn verdediging, en voert de volgende aanval uit: Hij opent de pagina waar je je inzet doet, en dupliceert deze pagina in een tweede tabblad. In het eerste tabblad zet hij steeds één cent in, en speelt het spel, net zolang totdat hij wint. Het spel geeft hem dan (in stap drie) de kans om zijn winst te verdubbelen.
Snoodaard Mallory schakelt echter over naar het tweede tabblad en zet daar (in stap één) € 1337,- in. Vervolgens schakelt hij terug naar het eerste tabblad, dat nog steeds op stap drie staat, en klikt op 'uitbetalen'.

Vanwege de session poisoning wordt zijn winst berekend op basis van die € 1337,-, in plaats van de één cent die hij eigenlijk had ingezet.
Het probleem is hier dat de applicatie toestaat dat de sessietoestand in de eerste stap — het inzetten — opnieuw wordt aangepast, terwijl de informatie uit de volgende stappen — dat de gebruiker net gewonnen heeft — intact wordt gelaten.

Moderne frameworks helpen niet
Moderne frameworks nemen een ontwikkelaar vele beveiligingsaspecten (zoals cross-site-scripting, SQL-injectie en cross-site-request-forgery) grotendeels uit handen. Dit is niet het geval voor session poisoning. We zien dan ook wel dat zelfs wanneer er nagenoeg geen informatie naar de webapplicatie wordt verzonden die een aanvaller kan beïnvloeden, een aanval mogelijk is.
Alles dat een aanvaller hiervoor hoeft te doen is pagina's in een afwijkende volgorde op te vragen.

Deze editie van de Madison Gurkha Update is uitgebreid met een extra rubriek. Hieronder vindt u het ingezonden artikel door gastexpert Tom de Wit van Louwers IP|Technology Advocaten.

GASTEXPERT

Richtsnoeren van kracht

Vanaf 1 maart 2013 zijn de richtsnoeren 'beveiliging van persoonsgegevens' ('richtsnoeren') van het College bescherming persoonsgegevens (CBP) van kracht. Gezien de steeds frequentere melding in de media van datalekken van persoonsgegevens lijkt dat geen overbodige luxe. Met de steeds grotere technologische mogelijkheden voor opslag van persoonsgegevens lijkt het probleem de komende jaren alleen maar toe te nemen. Geen enkele organisatie ontkomt eraan om na te denken over beveiliging.

Met de richtsnoeren wil het CBP invulling geven aan de open normen in de Wet bescherming persoonsgegevens ('Wbp') die gaan over beveiliging. Zo eist artikel 13 Wbp bijvoorbeeld dat bedrijven en overheden die persoonsgegevens verwerken 'passende technische en organisatorische maatregelen' nemen om persoonsgegevens te beveiligen. De richtsnoeren leggen uit hoe het CBP de beveiliging van persoonsgegevens in individuele gevallen beoordeelt en onderzoekt.

Plan-do-check-act

Een centraal uitgangspunt in de richtsnoeren is de zogenaamde Plan-do-check-act. Dit uitgangspunt houdt in dat degenen binnen bedrijven of overheden, die verantwoordelijk zijn voor informatiesystemen nadenken over de manier van beveiliging en dat ook blijven doen gedurende de gehele levensduur van een informatiesysteem. Dit uitgangspunt sluit aan bij de zogenaamde 'privacy by design', dat ook als vereiste is opgenomen in de voorgestelde Verordening gegevensbescherming (zie kader). Plan-do-check-act moet een blijvend en passend beveiligingsniveau binnen organisaties garanderen door:

1 risico's te beoordelen die de persoonsgegevens en de aard van de verwerking met zich meebrengen voor de betrokkenen. Op basis daarvan dient het gewenste beveiligingsniveau te worden bepaald;
2 gebruik te maken van algemeen geaccepteerde beveiligingsstandaarden (zoals NEN en ISO-normen);
3 op regelmatige basis te controleren of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd.

Passende maatregelen

De richtsnoeren benoemen verder twee noodzakelijke randvoorwaarden om passende maatregelen te treffen voor de beveiliging van persoonsgegevens: het treffen van maatregelen op basis van een risico-analyse en het toepassen van beveiligingsstandaarden. In het hoofdstuk 'beveiliging in de praktijk' geeft het CBP aan hoe hij de beveiliging van persoonsgegevens beoordeelt.

In de eerste plaats moet de verantwoordelijke vaststellen aan welke betrouwbaarheidseisen het informatiesysteem moet voldoen (waaronder begrepen: beschikbaarheid, integriteit en vertrouwelijkheid). Voor het vaststellen van het passende beveiligingsniveau moet de verantwoordelijke een vertaalslag maken van de risico's voor de betrokkenen (de mensen van wie de gegevens worden opgeslagen) naar deze betrouwbaarheidseisen.
Er is sprake van een hoog risico bij bijzondere persoonsgegevens (gezondheid, ras of sexuele geaardheid), gegevens over de financële situatie of gegevens die betrekking hebben op mensen uit kwetsbare groepen. Daarnaast kunnen ook bepaalde typen verwerkingen risico's met zich brengen. Bijvoorbeeld als het gaat om de hoeveelheid verwerkte persoonsgegevens per persoon en de doelen waarvoor de persoonsgegevens worden verwerkt.

In de tweede plaats moet de verantwoordelijke na het vaststellen van de betrouwbaarheidseisen passende beveiligingsmaatregelen nemen die waarborgen dat aan de betrouwbaarheidseisen wordt voldaan. In de richtsnoeren zijn een aantal concrete maatregelen opgenomen die in veel situaties nodig zijn:

- Een door de directie goedgekeurd beleidsdocument voor de informatiebeveiliging;
- Toewijzing van verantwoordelijkheden voor informatiebeveiliging binnen de organisatie;
- Een beveiligingsbewustzijn binnen de gehele organisatie;
- Toegangsbeveiliging, fysieke beveiliging en beveiliging van apparatuur;
- Correcte verwerking van beveiligingsmaatregelen in toepassingssystemen;
- Beheer van technische kwetsbaarheden in software en incidentenbeheer;
- Afhandeling van datalekken en beveiligingsincidenten volgens een eventuele wettelijke meldplicht;
- Continuïteitsbeheer (waaronder preventieve maatregelen en herstelmaatregelen).

"Het is goed dat het CBP handvaten geeft waarmee organisaties kunnen nagaan of de verwerking van de persoonsgegevens in de organisatie goed is beveiligd"

Naast de concreet genoemde beveiligingsmaatregelen wil het CBP dat ook geheimhouding binnen de organisatie goed geregeld wordt. Er moet een beleid zijn voor geheimhouding van persoonsgegevens en de verplichting tot geheimhouding moet vastgelegd worden in geheimhoudingsovereenkomsten. Verder moet Privacy Enhancing Technology toegepast worden.

In de derde plaats verlangt het CBP van de verantwoordelijke dat hij controleert of maatregelen ingevoerd zijn en worden nageleefd binnen de organisatie. Daarbovenop moet de verantwoordelijke nagaan of de organisatie door het treffen van deze maatregelen aan de eerder genoemde betrouwbaarheidseisen voldoet. Dat houdt concreet in dat er op regelmatige tijden controle (het CBP noemt werkplekcontroles en beveiligingsassessments als voorbeelden) moet plaatsvinden en dat de verantwoordelijke corrigerend optreedt als beveiligingsmaatregelen niet worden nageleefd (of niet meer actueel zijn als gevolg van veranderingen in de organisatie of informatiesystemen).

Verwerking door een bewerker

Het CBP besteedt aparte aan de beveiliging van verwerking van persoonsgegevens door een bewerker (bijvoorbeeld als onderdeel van een clouddienst). Ook hier verlangt het CBP dat de verantwoordelijke een risico-analyse uitvoert met betrekking tot de meest gangbare dreigingen en kwetsbaarheden die samenhangen met de uitbesteding van de verwerking van persoonsgegevens aan een bewerker en de mogelijke gevolgen daarvan voor de betrokkenen.

In de richtsnoeren noemt het CBP een aantal aandachtspunten voor de risico-analyse die de verantwoordelijke moet maken voordat de gegevens worden uitbesteed. Het CBP noemt in dat kader de beveiligingsmaatregelen van de persoonsgegevens door de bewerker en de beveiliging van de dienstverlening. Een ander aandachtspunt is de mate van transparantie door de bewerker over de beveiliging en over opgetreden beveiligingsincidenten. Continuïteit van de dienstverlening en de mogelijkheden tot portabiliteit van de verwerkte persoonsgegevens zijn voor het CBP eveneens van belang. Als laatste aandachtspunten noemt het CBP de eventuele inschakeling van subbewerkers en de verwerking van persoonsgegevens door de bewerker buiten de Europese Unie.

De Wbp verplicht de verantwoordelijke om er voor te zorgen dat de bewerker goede technische en organisatorische beveiligingsmaatregelen treft voor de bescherming van de persoonsgegevens die bij hem in de cloud zijn geplaatst. De verantwoordelijke moet aan de hand van de risico-analyse vaststellen welke beveiligingsmaatregelen de bewerker dient te nemen. Deze beveiligingsmaatregelen moeten in een (bewerkers)overeenkomst vastgelegd worden. Het CBP geeft in de richtsnoeren aan welke onderwerpen zij in het kader van de beveiliging beoordeelt als het gaat om de bewerkersovereenkomst:

- Een omschrijving van de dienst(en) die de bewerker verleent en de persoonsgegevens die de bewerker daarbij verwerkt;
- De betrouwbaarheidseisen die op de verwerking van toepassing zijn;
- Afspraken over de technische en organisatorische beveiligingsmaatregelen waarmee de bewerker invulling geeft aan de betrouwbaarheidseisen;
- Afspraken over de inhoud en de frequentie van rapportages die de bewerker aan de verantwoordelijke oplevert over de beveiliging alsmede over beveiligingsincidenten en datalekken;
- Afspraken over het al dan niet toestaan van verwerking door subbewerkers;
- Afspraken over de landen waar persoonsgegevens mogen worden verwerkt;
- Voorwaarden voor de heronderhandeling of de beëindiging van de bewerkersovereenkomst.

Conclusie

Het is goed dat het CBP handvaten geeft waarmee organisaties kunnen nagaan of de verwerking van de persoonsgegevens in de organisatie goed is beveiligd. De methode van de Plan-do-check-act kan inzichtelijk maken welke risico's er bij de verwerking van persoonsgegevens bestaan en welke maatregelen genomen moeten worden om de risico's te beheersen. De nieuwe richtsnoeren zijn een aanleiding voor organisaties om na te denken over het beveiligingsbeleid van persoonsgegevens in de organisatie. Dat is iets waar het op dit moment vaak aan ontbreekt.

Ook de bestaande bewerkersovereenkomsten zullen aan de hand van de richtsnoeren tegen het licht moeten worden gehouden. Wanneer er nog geen afspraken zijn gemaakt over de beveiliging van persoonsgegevens met bewerkers, moet de verantwoordelijke alsnog zo snel mogelijk voor een bewerkersovereenkomst zorgen.

De richtsnoeren zullen in de praktijk van de handhaving van het CBP een belangrijke rol gaan spelen. Zeker ook met het oog op de inwerkintreding van de voorgestelde Verordening Gegevensverwerking die het mogelijk maakt voor het CBP om hoge boetes op te leggen.

Verordening Gegevensbescherming: voorstel tot wijziging van de huidige richtlijn die de verwerking van persoonsgegevens reguleert. Naar verwachting zal deze Verordening in de loop van 2014 in werking treden.

Deze keer doet Jordy Kersten verslag van het hackerfestival OHM2013: Observe. Hack. Make. dat afgelopen augustus plaatsvond.

Elke vier jaar wordt Nederland vier dagen lang omgetoverd tot hacker-hoofdstad van Europa, en dit jaar was het weer zover. In de eerste week van augustus heeft OHM2013 plaatsgevonden. Binnen de hackerscene werd al maanden over niets anders gepraat.

Aangezien dit de eerste keer zou worden dat ik dit evenement zou bijwonen vroeg ik mezelf af wat er zo speciaal is aan dit specifieke evenement. Nu zijn de meeste conferenties buiten de inhoud om redelijk hetzelfde. Denk hierbij aan een toplocatie, luxe lunch, en van alle gemakken voorzien. Dit evenement bleek anders. De beste omschrijving voor dit evenement is eigenlijk een vierdaags festival. Hier komen alle nerds, geeks en liefhebbers van computers, techniek, LEDs, drones, retro gaming etc. bij elkaar om te doen waar zij van houden: hacken. Als ik achteraf OHM2013 in een woord zou moeten samenvatten: uniek. Echter, een dergelijk evenement verdient een beschrijving van meer dan slechts een woord.

Villages

Zoals voorgaande jaren wordt er op een groot evenemententerrein in Nederland vier dagen lang in festivalstijl gekampeerd. Het unieke aan dit evenement is dat het community based is. Als bezoeker ben je automatisch vrijwilliger. Dit geeft naast de voldoening in het participeren van het opzetten van een dergelijk evenement ook de mogelijkheid om input te leveren om een beter evenement neer te kunnen zetten. Het terrein is verdeeld in verschillende kampen waar bezoekers de gelegenheid hebben om hun tent op te zetten. Hierdoor hebben bezoekers de mogelijkheid om groepen te vormen en samen een zogenaamde village te kunnen opzetten. Dit gebeurt vaak op basis van al bestaande communities zoals bijvoorbeeld hackerspaces. Deze villages bestonden vooral uit een grote gezamelijke tent die gebruikt wordt als uitvalbasis of om gezamelijke projecten uit te voeren. Het terrein was verder voorzien van de benodigde basisvoorzieningen zoals WCs, douches en (draadloos) internet. Ook aan verlichting is gedacht in de vorm van meer dan vijftig lantaarnpalen met LED verlichting, die elk afzonderlijk aangestuurd konden worden. Dit resulteerde 's nachts in prachtige kleurwisselingen en patronen waarmee het complete terrein verlicht werd. Verder waren er verschillende grote tenten en kampen gebouwd die gebruikt worden voor verschillende activiteiten. Deze activiteiten bestaan voornamelijk uit presentaties, discussies, workshops en trainingen.

> Hier komen alle nerds, geeks en liefhebbers van computers, techniek, LEDs, drones, retro gaming etc. bij elkaar om te doen waar zij van houden: hacken

Tips en trucks
De onderwerpen van de presentaties liepen uiteen van tips en trucks die de ontwikkeling van exploits en payloads kunnen versnellen tot best practices voor het bouwen van een drone. Verder werden er naast de presentaties ook nog open toegankelijke discussies gehouden over verschillende uiteenlopende onderwerpen. Denk hierbij aan onderwerpen zoals PRISM, maar ook netneutraliteit, privacy en het fenomeen 'klokkenluiden'. Naast presentaties en discussies werden er ook workshops en trainingen gegeven. Ook hier liepen de onderwerpen uiteen van soldeerworkshops tot foodhacking, waarbij met dezelfde ingredienten totaal verschillende gerechten gemaakt werden. Naast de presentaties, discussies, workshops en trainingen waren er tal van andere activiteiten aanwezig. Zo kon er in de rainbow village retro computerspelletjes gespeeld worden op oude consoles, arcadekasten en flipperkasten en was het mogelijk om bijvoorbeeld een zelf ontworpen ring te printen met een 3D printer. Er was zelfs een kinderhoek met verschillende activiteiten ingericht waar deze konden spelen en knutselen. Ook hier werden workshops gegeven zoals ballonvouwen waarbij kinderen hun eigen ballonfiguur bestaande uit verschillende dieren konden maken.

Optimaliseren flipboards
Het meest interessante was misschien wel dat er in de verschillende villages verspreid over het gehele terrein iedereen bezig is met hun eigen hackprojecten. Hier worden dingen gehackt onder de ogen van de bezoekers. Het leuke hiervan is dat wanneer er interesse getoond wordt er altijd tijd genomen wordt om uit te leggen wat ze aan het doen zijn. Zo was bijvoorbeeld een Deense hackerspace bezig met het optimaliseren van de aansturing van zogenaamde flipboards. Deze werden vroeger in bussen gebruikt om informatie op te tonen. Het doel was om deze sneller te laten opereren, waardoor het mogelijk wordt om bewegend beeld weer te geven. Verder had een Franse hackerspace 's nachts een wedstrijd tetris spelen op oscilloscopen georganiseerd. Naast de villages waren er ook verschillende sponsoren aanwezig die activiteiten aanboden. Hierbij was bijvoorbeeld ook de overheid present, waarbij het NFI workshops mobiele telefoons uitlezen gaf.

De veelzijdigheid van onderwerpen en activiteiten maakt dit een zeer laagdrempelig en toegankelijk festival dat niet alleen voor hackers leuk is, maar ook voor mensen met algemene interesses in techniek. Daarbij komen ook de hardcore technici en specialisten aan hun trekken door het grote verschil in het aanwezige kennisniveau. Ik kan dan ook iedereen die ook maar enige interesse heeft in techniek ten zeerste aanraden om een bezoek te brengen aan dit unieke hackerfestival. Tot over vier jaar!

In de Madison Gurkha Update presenteren wij een lijst met interessante bijeenkomsten die de komende tijd zullen plaatsvinden.

26 en 29 september 2013
EuroBSDcon 2013
Hilton Conference Centre in St. Julians, Malta
http://2013.eurobsdcon.org/
EuroBSDcon is een unieke gelegenheid om meer te leren over de krachtige BSD-systemen die we dagelijks gebruiken en om in contact te komen en ervaringen uit te wisselen met andere ontwikkelaars uit de hele wereld. Als organisatie steunt Madison Gurkha de doelstellingen van EuroBSDcon en sponsort dit project dan ook van harte.

30 en 31 oktober 2013
Vakbeurs Infosecurity.nl
Jaarbeurs Utrecht
http://www.infosecurity.nl/nl-NL/Bezoeker.aspx
Op 30 en 31 oktober 2013 kunt u terecht in de jaarbeurs Utrecht voor dé Nederlandse vakbeurs op het gebied van IT security. Op de beurs worden de nieuwste producten, oplossingen en diensten binnen de IT-securitybranche gepresenteerd: de ontmoetingsplek voor iedere IT-professional. Wij verwelkomen u graag op onze stand vlakbij de ingang (01.B154). Bezoek aan Infosecurity.nl is na aanmelding gratis. Met één toegangsbadge heeft u bovendien beide beursdagen gratis toegang tot Storage Expo en het Tooling Event.

28 en 29 november 2013
BeNeLux OWASP Day 2013
Amsterdam
https://www.owasp.org/index.php/BeNeLux_OWASP_Day_2013
Het Open Web Application Project (OWASP) is een project gericht op de beveiliging van open-source applicaties. Op 28 en 29 november 2013 vindt in Amsterdam de BeNeLux OWASP Day 2013 plaats. Twee dagen zullen in het teken staan van interessante cursussen en lezingen met betrekking tot de OWASP Top 10.

Madison Gurkha

Safe?

Goede IT-beveiliging is niet zo eenvoudig als vaak wordt beweerd. Bovendien blijkt keer op keer dat deze beveiliging van strategisch belang is voor organisaties. Alle IT-beveiligingsrisico's moeten op een acceptabel niveau worden gebracht en gehouden. Professionele en gespecialiseerde hulp is hierbij onmisbaar. Kies voor kwaliteit. Kies voor de specialisten van Madison Gurkha.

tel: +31(0)40 237 79 90 - www.madison-gurkha.com - info@madison-gurkha.com