

DE COLUMN 2

Remco Huisman

HET NIEUWS 3

- Madison Gurkha groeit
- Madison Gurkha levert bijzondere bijdrage aan Alpe d'HuZes

HET EVENT 4-5

Black Hat Sessions Part IX,
The Human Factor

HET INZICHT 6

Laurens Houben over persoonsgegevens
als lucratieve handelswaar

HET INTERVIEW 7

Schrijfster en columniste
Karin Spaink over datalekage
van persoonsgegevens

DE HACK 8-9

Karmetasploit, een assessment
voor WiFi-client beveiliging

DE KLANT 10

Uit de zorgsector

HET VERSLAG 11

27ste editie van Chaos Communication
Congress in Berlijn

HET COLOFON 11





Datadiefstal en lekkage Hoezo paranoia?

Toen ik acht jaar geleden partner werd bij Madison Gurkha, leek de digitale wereld een stuk veiliger dan nu. Ja, er waren de nodige virussen en ja er waren hackers actief, maar het leek - in het nazien - allemaal nog tamelijk onschuldig. Over identiteitsdiefstal en verlies van gegevens maakte ik me ook niet zo heel druk in die tijd. Mijn collega's van het eerste uur daarentegen waren daar toen al wel bezorgd over. Ik vond dat toen af en toe redelijk overdreven. Je kunt toch best een kopie van je paspoort opsturen per email? En waarom moet het sofi/BSN-nummer nu perse worden doorgestreept op een kopie van een dergelijk document? Bij het uitvoeren van testen in een productieomgeving waar DigiD's voor nodig zijn, kun je toch ook wel die van je zelf gebruiken?

In het kader van "voortschrijdend inzicht" ben ik er inmiddels ook anders over gaan denken en ben ik in de ogen van vrienden en kennissen (licht) paranoia geworden. De meeste mensen realiseren zich eenvoudig niet in hoeveel bestanden er gegevens over hen zijn opgeslagen. Een paar voorbeelden: de huisarts, het ziekenhuis, de bank, je hypotheekverstrekker, je (zorg)verzekeraar, de gemeente, je internetprovider en niet te vergeten de webshops waar je iets koopt, nog maar niet te spreken over de sociale media zoals Facebook en Hyves, waar veel mensen zichzelf volledig in de etalage zetten. Gaat u zelf maar eens na, in welke bestanden er gegevens over u opgeslagen zijn; het kunnen er zomaar meer dan honderd zijn.

Er zijn niet alleen gegevens die je zelf bewust achterlaat. Gegevens worden ook aangevuld en verrijkt. Veel websites en online advertentiebedrijven maken tegenwoordig gebruik van tracking methodes en zien dus waar u allemaal nog meer naar toe surft. Met de komst van smartphones en RFID- kaarten als de OV-chipkaart wordt het allemaal nog een tikkie enger. Een smartphone met GPS-functie is heel goed te traceren, ook voor niet overheidsdiensten. Deze diensten kunnen trouwens ook heel goed de locatie van gewone GSM's bepalen. Je OV-reisgedrag wordt met de komst van de OV-chipkaart haarfijn vastgelegd. Dan koop je toch een anonieme kaart? Klopt, maar dan moet je die niet met een bankpas betalen... want dan is die kaart ineens niet meer zo anoniem. Je wordt bovendien gefilmd op straat en je kenteken van je auto wordt door camera's geregistreerd en gevolgd. Koppel al deze gegevens eens aan elkaar en je krijgt

een beangstigend beeld. Goed voor scenario's van een hele reeks Hollywood films. U kent er vast wel een paar en nee, het is niet hypothetisch. Datalekage en de gevolgen daarvan zoals identiteitsdiefstal zijn een steeds groter probleem aan het worden. Een hele ondergrondse economie floreert op een jaloesmakende wijze.

Kortom, er is alle reden voor lichte paranoia bij burgers. Organisaties zouden zich veel drukker moeten maken over de opslag van deze persoonlijk gegevens en de beveiliging ervan. Redenen voor Madison Gurkha om de Black Hat Sessions Part IX op 26 april als thema "The Human Factor" mee te geven. Dit seminar gaat over de menselijk aspecten van informatiebeveiliging en dus ook over privacy, datadiefstal en verlies, af luisteren etc. Gelukkig zijn er ook individuen en organisaties die zich richten op de bewaking van die gegevens. Uiteraard spreken zij tijdens de Black Hat Sessions op 26 april. Denk aan Ot van Daalen van Bits of Freedom, maar ook columniste en schrijfster Karin Spaik, die zich al lang inzetten voor het beveiligen van persoonsgegevens en privacy (verder in dit nummer is een uitgebreid interview met Karin Spaik te lezen). Er is die dag veel meer te beleven, maar daarvoor verwijs ik u graag naar de rubriek "Het Event" in deze Update, waar een uitgebreid programma is opgenomen.

Nog even wat anders, nu ik toch uw aandacht heb.

Op 9 juni a.s. ga ik zoveel mogelijk geld bijeen fietsen voor KWF Kankerbestrijding. Hoe? Door zo vaak mogelijk de Alpe d'Huez op te fietsen. Waarom? Ik zie deze nare ziekte heel veel om me heen, vaak redelijk ver weg, soms beangstigend dichtbij. Wilt u mij (het KWF dus) steunen? Dat kan en uw bijdrage is zeer welkom. Zie het nieuwsartikel verder in deze Update. Overigens is het ook mogelijk om als bedrijf, net als Madison Gurkha, shirt-sponsor te worden. Neem dan contact met mij op via 06-52015115. Alvast bedankt!

Ik wens u veel leesplezier en hopelijk tot 26 april bij de Black Hat Sessions.

Remco Huisman, Partner, Commercieel directeur

Madison Gurkha *groeit*

In de afgelopen 10 jaar zijn we langzaam maar gestaag blijven groeien; van drie mensen in 2000 tot meer dan twintig medewerkers nu. Ondanks deze groei zijn we nog steeds een klein en flexibel bedrijf dat hoge kwaliteit levert. Om dit in de toekomst te kunnen waarborgen, waren er zo langzamerhand wat aanpassingen in onze organisatiestructuur noodzakelijk. Van sommige van deze veranderingen zult u niets merken, van andere wellicht wel. Eén van de belangrijkste veranderingen is dat de directie de taken anders heeft verdeeld. Dit heeft geleid tot een volgende taakverdeling:

Walter Belgers	Teamleiding
Arjan de Vet	Juridische, Financiële zaken en ICT
Hans Van de Looy	Bidsupport, Quality Assurance, R&D en PR
Guido van Rooij	HRM, Office & Inkoop
Remco Huisman	Sales en Marketing

Het management is uitgebreid met Caroline van de Wiel (Manager Planning en Werkvoorbereiding). De dagelijkse leiding is met dit team goed belegd.



Met de nieuwe taakverdeling kunnen we deze groei opvangen, zonder dat de kwaliteit en flexibiliteit verloren gaat, die u van ons gewend bent. Daarnaast willen we met de nieuwe opzet onze doelstelling blijven verwezenlijken om op lange termijn een succesvol bedrijf te zijn, waar het prettig werken is aan uitdagende projecten.

Alpe d'HuZes

Zes keer naar de top!
Bedwing de Alpe d'Huez voor
de overwinning op kanker

Anderen Faciliteren en Inspireren om Goed, Gelukkig en Gezond te leven met Kanker!

Alpe d'HuZes

9 JUNI 2011

an initiative for
inspire
2live

Steun onze actie! Doe mee, sponsor of meld je aan als vrijwilliger. Kijk voor meer informatie op:
www.opgevenisgeenoptie.nl

Madison Gurkha levert bijzondere bijdrage aan Alpe d'HuZes!

Alpe d'HuZes is het wielerevenement waarbij deelnemers individueel of in teamverband minimaal zes maal op één dag de Alpe d'Huez beklimmen. Niet zomaar, maar om geld op te halen voor het Alpe d'HuZes onderzoeksfonds bij KWF Kankerbestrijding. Alpe d'HuZes is gegrondvest op de absolute overtuiging dat je de grootst mogelijke voldoening bereikt als je je met hart en ziel inzet voor een ander.

Madison Gurkha draagt het evenement en haar doelstellingen een warm hart toe. Vorig jaar hebben wij het team van De Lage Landen gesponsord met een financiële bijdrage. Dit jaar, 9 juni 2011, zet Remco Huisman, Partner, Commercieel directeur, zich persoonlijk in voor het goede doel! In het team De Lage Landen & Friends levert hij op een sportieve manier een bijdrage aan de strijd tegen kanker. "Mijn goal is om minimaal drie keer de Alpe d'Huez te beklimmen en zoveel mogelijk geld in te zamelen". Steun de strijd tegen kanker en doe uw donatie via <http://deelnemers.alpe-dhuzes.nl/acties/remcohuisman/remco-huisman/>.

Dank u wel!

Mist u een nieuws item, of heeft u nog ander opvallend of aanvullend security nieuws? Meld het aan ons door een mail te sturen naar: redactie@madison-gurkha.com. En wie weet staat uw nieuwtje in de volgende Madison Gurkha update!

Black Hat Sessions Part IX, 26 april 2011, De Reehorst Ede

The Human Factor

Privacy, Social Engineering, Social Networks, Awareness, Digital Crime ...

Nadat we vorige jaar de risico's van de "Cloud" hebben onderzocht, gaan we dit jaar in op de rol van en de gevolgen voor de mens van het gebruik van IT. We laten overal waar we komen een digitaal spoor achter. Na het volgen van de bijeenkomst heeft u een beter inzicht in wat u allemaal aan informatie achterlaat en wie daar allemaal de beschikking over heeft (aanvallers, overheden, etc.). Informatie

is waardevol en een geliefd doelwit voor aanvallers. Met het verder aanscherpen van technische beveiliging, wordt de mens de zwakste schakel. Vandaar de focus op uw eigen rol in informatiebeveiliging.

Bestemd voor ú

De bijeenkomst wordt georganiseerd voor beheerders van systemen, netwerken en applicaties, security officers, interne

auditors, het management en andere geïnteresseerden. Dit jaar zullen er geen vendor sessies zijn, waardoor wij ruimte hebben voor 2 parallele tracks, zodat ook niet technische bezoekers een interessant programma kunnen volgen.

Het programma

Het programma start om 9.25 uur en duurt tot 16.30 uur. Aanluitend wordt een bor-

08.30 u **Ontvangst en registratie**

09.25 u **Opening door de dagvoorzitter**
Walter Belgers, Madison Gurkha

09.30 u **Cybercriminaliteit en digitale burgerrechten**
Ot van Daalen, Directeur, Bits of Freedom



De bestrijding van cybercriminaliteit zal de komende jaren een belangrijker thema worden in de politiek. Maar maatregelen om cybercriminaliteit te bestrijden kunnen op gespannen voet staan met het grondrecht op privacy en het grondrecht op communicatievrijheid. Bits of Freedom zal aan de hand van een actueel onderwerp ingaan op de technologische, juridische en maatschappelijke aspecten van deze spanning.

10.20 u **Datalekken**
Karin Spaink, Schrijfster en Columnist



Bedrijven, instellingen en overheidsorganen verzamelen elke dag meer informatie over ons. Die gegevens zijn - zo stellen ze - cruciaal voor hun bedrijfsvoering, voor onze veiligheid en voor ons welbevinden. Het nadenken over een adequate bescherming van die gegevens staat echter nog in de kinderschoenen, met als gevolg dat her en der datalekken ontstaan. Grote verzamelingen gegevens liggen ineens op straat of sijpelen door naar plaatsen waar ze pertinent niet thuishoren. Wat kunnen we doen tegen datalekken? Wat zijn de consequenties ervan? Zou een meldplicht voor zulke lekkages helpen?

11.10 u **Pauze / Informatiemarkt**

11.40 u **Parallele tracks**

11.40 u **Security Awareness**



Hans Van de Looy, Partner en Principal Security Consultant, Madison Gurkha

Tijdens deze lezing wordt aandacht gevraagd voor een moeilijk, ondergewaardeerd, maar uiterst belangrijk onderwerp genaamd beveiligingsbewustzijn. Hopelijk draagt de inhoud bij tot een meer evenwichtige invulling van informatiebeveiliging en nodigt deze uit tot discussie.

Privacy hacking: Dect, RFID & Browser

Ralph Moonen, Directeur, IT Security eXperts



Ralph Moonen zal in een live hacking demo laten zien dat de privacy op een aantal terreinen gevaar loopt. In zijn presentatie/demo zal hij voornamelijk ingaan op security problemen op het gebied van DECT, RFID en in Browsers.

12.30 u **Lunch / Informatiemarkt**

13.30 u **It's all about you**



Andrew MacPherson, Lead Developer, Paterva

Maltego has been featured on the web for some time now as a phenomenal open source intelligence tool. In this talk I want to not only focus on the tool and technology but also on the application of the technology. How much can we really learn from open sources? How much information is really out there and how have this changed in the last few years? Is it really better to have no profile on the net? Also - what happens when



rel georganiseerd. Registratie is mogelijk vanaf 8.30 uur.

Kosten

De kosten voor deelname aan het seminar bedragen € 315,- (excl. BTW) per persoon. Documentatie, lunch en koffie zijn inbegrepen. Speciaal voor alle relaties van Madison Gurkha geldt op dit bedrag een korting van € 35,-. Zo betaalt u dus maar € 280,- (excl. BTW) per persoon. Geef bij uw online-inschrijving aan dat u een relatie bent van Madison Gurkha en de korting wordt verrekend.

THE HUMAN FACTOR mag u niet missen! Meldt u snel aan via het inschrijfformulier op www.blackhatsessions.nl.

a powerful organization has this kind of power - does it really look like in the movies? The talk will also look at ways that you can protect yourself - not just defense, but also detection of information mining.

14.30 u Parallele tracks

14.30 u Social Engineering - Theorie en praktijk

Frans Kollée, Senior Security Consultant en Laurens Houben, Medior Security Consultant, Madison Gurkha
Deze presentatie gaat in op de theorie en een aantal algemene basisaspecten van social engineering, ingegeven en voorzien van voorbeelden uit de praktijk. Het zijn niet de ingewikkelde en tijdrovende voorbereidingen met onbeperkte budgetten die de basis voor de presentatie vormen. Het zijn juist de relatieve eenvoud en natuurlijke improvisaties waarmee de nieuwsgierigheid en hulpvaardigheid van mensen vaak misbruikt kan worden.



15.20 u Pauze / Informatiemarkt

15.40 u Lawful Interception en security

Mark Lastdrager, Directeur, Pine Digital Security
Lawful Interception (LI), ofwel het 'aftappen' van telefonie- en internet verkeer is een belangrijk hulpmiddel voor opsporingsdiensten. Maar er zijn vanzelfsprekend ook risico's verbonden aan de technische mogelijkheid om een kopie van iemands gesprekken of dataverkeer te maken. In de presentatie wordt ingegaan op de wet- en regelgeving rond LI, hierbij zal uitgebreid worden stilgestaan bij de beveiligingsrichtlijnen. Daarnaast zal de techniek rond LI worden beschreven: hoe kom je aan



een kopie van het verkeer, hoe wordt het gekopieerde verkeer naar de overheid gestuurd en hoe kun je voorkomen dat hiervan misbruik wordt gemaakt. Natuurlijk worden er ook voorbeelden genoemd van bekende incidenten waarbij het is misgegaan in het verleden; zaken waar we in Nederland van moeten leren. Als laatste zal Mark een blik op de toekomst werpen: de steeds stijgende bandbreedtes nopen bijvoorbeeld tot nieuwe technische maatregelen om een "information overload" te voorkomen. Daarnaast is er sinds september 2009 daretentie wetgeving, de verwachting is dat opsporingsdiensten hier steeds meer gebruik van gaan maken.

16.30 u Afsluiting door de dagvoorzitter

Walter Belgers, Partner en Principal Security Consultant, Madison Gurkha

16.40 u Borreluur / Informatiemarkt



Lucratieve handelswaar

Meer en meer persoonsgegevens verschijnen maar verdwijnen ook op het internet. Persoonsgegevens zijn lucratieve handelswaar binnen criminele kringen.

"Hoe komen ze aan deze gegevens?" "Wat kunnen criminelen met gestolen persoonsgegevens doen?" en "Wat kan ik doen om mezelf tegen identiteitsfraude beschermen?" zijn veel voorkomende vragen horende bij dit onderwerp.

Hoe komen ze aan deze gegevens?

Het is niet ongebruikelijk dat mensen veel persoonlijke details op sociale netwerken zoals Facebook, LinkedIn en Hyves achterlaten. Denk hierbij aan een e-mailadres, mobiel telefoonnummer, beschrijving over broers, zussen en ouders. Wat gebeurt er met deze gegevens? Wie kan het lezen? Worden ze doorverkocht en zo ja, aan wie eigenlijk? Dit zijn zaken waar vaak niet bij wordt stilgestaan. Vaak komen de gegevens via omwegen terecht bij criminelen. Wanneer logingegevens voor één van de zojuist genoemde applicaties via bijvoorbeeld een "phishing aanval" worden gestolen, is het vaak kinderlijk eenvoudig deze ook voor andere doeleinden te gebruiken. Uit diverse onderzoeken blijkt dat 20 tot 33% van de internetgebruikers één wachtwoord voor alles gebruikt. Criminelen kunnen inloggen in de persoonlijke e-mailbox en vinden daar wellicht een kopie van een paspoort en creditcard, die daar ooit als back-up voor een vakantie is geplaatst. Ook inloggegevens voor andere applicaties op het internet, waar weer andere persoonsgegevens aanwezig zijn, zijn zeer vaak terug te vinden in een mailbox.

De volgende stap valt nu wel te raden.

Wat kunnen criminelen met gestolen persoonsgegevens doen?

Gestolen persoonsgegevens kunnen op diverse manieren worden gebruikt. Creditcardgegevens worden vaak direct gebruikt om online aankopen te doen bij webwinkels, voordat de diefstal wordt opgemerkt en de kaart geblokkeerd wordt. Het is namelijk online niet nodig om de bijbehorende handtekening en/of pincode te overleggen, alleen het creditcardnummer, tenaamstelling en einddatum zijn vereist. Wanneer een

kaart van één van de grotere maatschappijen wordt gebruikt, is ook een card security code noodzakelijk bij een transactie. Al deze gegevens zijn al aanwezig op de creditcard zelf.

In bijna alle gevallen krijg je je geld terug van de creditcardmaatschappij. Maar in dit geval krijgen criminelen dus ook hun online bestelde goederen die ze vervolgens weer kunnen doorverkopen. Het slachtoffer is in de meeste gevallen de online webwinkel, aangezien deze een gestolen creditcard heeft geaccepteerd als betaalmiddel.

Een andere vorm van identiteitsfraude is het onrechtmatig gebruiken van bijvoorbeeld een BSN-nummer in combinatie met andere persoonsgegevens. Denk hierbij aan een ingescande identiteitskaart en bankpas. Met deze combinatie is het bijvoorbeeld mogelijk om online een telefoonabonnement of geldlening aan te vragen, maar ook om goederen zoals groot materieel of apparatuur te huren bij een verhuurmaatschappij. De persoon waar de persoonsgegevens van zijn, krijgt vervolgens de rekening voor het gebruik en het eventueel niet terugbrengen van de producten. Al snel verlopen de vorderingen van de schade via een deurwaardersbedrijf en staat een BKR-registratie als wanbetaler te wachten. De criminelen zijn de lachende derde.

Wat kan ik doen om mezelf tegen identiteitsfraude beschermen?

Let op wat je online deelt. Denk hierbij aan telefoonnummers, e-mailadressen, adresgegevens, geboortedatum maar ook foto's die bijvoorbeeld de locatie van je huis kenbaar maken. Houd altijd in gedachten dat wat op het internet wordt gezet er nooit meer af komt. Denk vooruit en zet wat bijvoorbeeld je (toekomstige) werkgever of je moeder nooit

te weten zou mogen komen, niet op het internet.

Onderzoek hoe je je online gegevens en berichten op bijvoorbeeld Facebook af kunt schermen voor vreemden. Pas de privacyinstellingen zodanig aan dat alleen vrienden in je lijst, deze kunnen bekijken. Wees hierbij ook voorzichtig wie je toevoegt aan je online vriendenlijst en laat niet zomaar iedereen toe. Vrienden hebben immers ook toegang tot deze afgeschermd gegevens. Pas je wachtwoorden aan zodat deze uniek zijn per applicatie. Zo wordt het minder eenvoudig voor criminelen om zodra, een wachtwoord is achterhaald, al je accounts in handen te krijgen. Wees ook alert op mogelijke "phishing aanvallen", via bijvoorbeeld een e-mail waarin wordt gevraagd of je je logingegevens even wilt bevestigen. Geef je gebruikersnaam en wachtwoord nooit weg aan anderen. Vul deze dus ook niet in op een website wanneer daar uit het niets om wordt gevraagd.

Gebruik de tips op de website <http://www.stop-identiteitsfraude.nl/> om jezelf bewuster te maken van de bestaande gevaren en manieren om jezelf hier tegen te beschermen. Op deze websites vindt je ook tips over hoe bedrijven zichzelf beter kunnen beschermen.

Conclusie

Identiteitsfraude is niet iets van de laatste tijd. Het is echter wel omvangrijker en eenvoudiger dan een paar jaar geleden. Iedereen loopt het risico slachtoffer te worden; van een zeven- tot 90-jarige, van bedrijven tot particulieren. Door domme pech of door een domme fout. Een gezond verstand is vaak het beste wapen tegen dit gevaar. Gebruik hem!



Karin Spaink

Kun je in het kort uitleggen wie je bent en waar je je de laatste tijd mee bezig houdt?

Ik schrijf boeken en columns. Ik ben hoofd-redacteur van de boekenserie "The Next Ten Years". In mei vorig jaar is het vijfde deel "Wie is U? Identiteit, privacy & politiek" uitgebracht. Momenteel werk ik ook aan een boek over de geschiedenis van Hack-Tic, XS4all en het ontstaan van het publieke internet in Nederland.

Is informatiebeveiliging een issue voor jou?

Ja, ten eerste omdat allerlei bedrijven en instanties informatie over ons vergaren en opslaan, terwijl we niet precies weten wat er mee gebeurt. Dat is een curieus iets, gezien het vaak om vertrouwelijke informatie gaat. Ten tweede, en dat wordt steeds belangrijker naarmate iedereen steeds makkelijker en grotere databases bijhoudt over alles en iedereen, worden zulke bestanden vaak buitengewoon slecht beveiligd. Dit betekent dat er slordig wordt omgegaan met onze gegevens. Mensen wier gegevens zijn gelekt, lopen het risico dat anderen daarmee aan de haal gaan.

Kun je zeggen in welke mate het aantal databases toeneemt?

Ik denk dat de omvang ervan ieders besef te boven gaat. Een paar jaar geleden liep het aantal databases waarin iemand geregistreerd staat al over de honderden. Tegenwoordig hebben instanties vaak de rare neiging om als ze eenmaal contact met je hebben, steeds meer informatie af te dwingen. Een voorbeeld: online een bioscoopkaartje bestellen. Wie aan het loket een kaartje koopt kan dat doen zonder verder enige informatie prijs te geven, maar Belbios eist dat je invult hoe je heet, waar je woont,

hoe oud je bent en of je man of een vrouw bent wanneer je een bestelling wilt plaatsen. Het wordt over het algemeen niet toegelicht waarom dergelijke informatie nodig is. Bovendien is er geen enkele garantie, dat er secuur mee omgegaan wordt.

Wat zijn de belangrijkste oorzaken van datalekage?

Een belangrijke oorzaak van datalekage is dat gegevens op plaatsen worden opgeslagen en gebruikt waar verschillende wet- en regelgeving en gedragsregels gelden. Instanties kunnen bijvoorbeeld zelf secuur omgaan met de informatie die ze verzamelen, maar roepen dan voor de verwerking daarvan de hulp van andere partijen in. Deze partijen zijn lang niet altijd onderhevig aan dezelfde zorgvuldigheidseisen. Neem medische gegevens. Zodra een zorginstantie zulke gegevens door derden laat beheren of verwerken, vallen ze niet meer onder het medisch beroepsgeheim en gelden er veel soepeler beschermingseisen. Dat is toch raar? Een andere oorzaak is dat we niet voldoende zijn geschoold in het zorgvuldig omgaan met data en ons te weinig bewust zijn van de consequenties van slordige omgang ermee.

Hoe kunnen we datalekage volgens jou het beste bestrijden?

Ik begin ondertussen een groot voorstander te worden van het opleggen van een behoorlijke boete op datalekages. Wanneer een bedrijf of overheidsinstantie data lekt, op wat voor een manier dan ook, dan moeten ze daarvoor een stevige boete krijgen. Zodoende leren we misschien dat slordig databeheer

een prijs heeft en misschien helpt het ook om die almaar uitdijende verzameldrift wat in te dammen. Een andere maatregel is dat we systematischer moeten gaan nadenken over "datahygiëne". We hebben in de loop der tijd allerlei dingen geleerd over hygiëne. Je drinkt niet uit een modderpoel, je snijdt groente niet op dezelfde plank waarop rauwe kip heeft gelegen, niemand haalt het in z'n hoofd

om tien mensen met een en dezelfde naald te prikken en we schrikken ons rot wanneer een arts een scalpel gebruikt dat zojuist op de grond is gevallen. Op deze manier moeten we ook een aantal codes gaan ontwikkelen voor het gebruik van data. Er moet een protocol komen van wat wel en niet hoort. Dat gaat niet van zelf. Deels is het een kwestie van mentaliteit, maar er zal ook een regulering moeten komen van zaken die we eigenlijk al als normaal zien. Bovendien gaat het om het aanwennen

van nieuwe gewoontjes en dus absoluut over een stukje opvoeding. Uiteraard moeten we ook gaan denken aan permanente encryptie van gegevens.

Je spreekt de 26e op de BHS. Wat kunnen bezoekers verwachten?

Het thema wat we zojuist hebben besproken: "datalekken". Ik zal tijdens mijn presentatie aan de hand van verschillende voorbeelden mijn standpunten verder toelichten. Ik kan natuurlijk niet te veel prijsgeven nu, anders hoeft men niet meer te komen!

.....
**Kent u iemand die ook graag zijn of haar visie wil delen in een interview (U mag uzelf natuurlijk ook opgeven)?
Neem dan contact op met de redactie door een mail te sturen naar: redactie@madison-gurkha.com.**



Inmiddels is tot het grote publiek doorgedrongen dat WiFi access points kunnen en moeten worden beveiligd zodat onbevoegden hier geen misbruik van kunnen maken. Maar hoe zit het met de beveiliging van de WiFi-clients zelf?

Karmetasploit

Een assessment voor WiFi-client beveiliging

WiFi access points

De afgelopen jaren zijn het aantal WiFi access points in hoog tempo toegenomen. Binnen bedrijven worden WLANS (Wireless-Local Area Network) steeds vaker ingericht, zien we zogenaamde publieke Hotspots overal aanwezig en is het voor de thuisgebruiker de gewoonste zaak van de wereld geworden.

Vooraf bij de thuisgebruiker zien we dat niet alleen het aantal access points is toegenomen, maar dat ook de beveiliging standaard (beter) is ingesteld. Dit laatste is mede dankzij de fabrieksinstellingen van de leveranciers die standaard veiliger zijn

ingesteld. Onbeveiligde access points zijn er nog wel, en zijn steeds vaker voorzien van een SSID (Service

Enkele aantallen

Op het moment dat ik in een standaard woonwijk twee minuten lang signalen bekijk, vind ik 55 access points. Deze zijn onderverdeeld in:

- 32 access points met WPA2
- 14 access points met WPA
- 7 access points met WEP
- 2 open access points waarvan een met "GASTNETWERK VAN ..." in de naam.

Set Identifier - netwerknaam) met als naam "Gasten netwerk van ...", maar het merendeel heeft WPA-beveiliging ingeschakeld. De eenvoudig te kraken WEP-beveiliging kom je overigens nog steeds, zij het in mindere mate, tegen. Zie het kader "Enkele aantallen" voor een illustratief overzicht.

Laten we er voor het gemak van uitgaan dat de WiFi access points goed zijn beveiligd en dat de publieke en/of gasten access points nog steeds aanwezig zijn. Wat betekent dit voor de beveiliging van de gehele keten?

Karmetasploit

Karmetasploit is ontstaan door de toolset KARMA te integreren in het open source pentesting framework Metasploit (zie <http://www.metasploit.com/>). KARMA (<http://www.theta44.org/karma/index.html>) is een set van tools waarmee de beveiliging van WiFi-clients op verschillende lagen getest kan worden. De eerste presentatie van de KARMA toolset werd al gegeven in november 2004.

Om Karmetasploit te gebruiken dien je over een Linux (FreeBSD 8.x kan ook) systeem te beschikken met een WiFi-adaptor die door de Aircrack-NG suite wordt ondersteund en waarmee pakketten kunnen worden geïnjecteerd. Verder dient het Metasploit framework geïnstalleerd te zijn. Als laatste is een DHCP-server nodig. In plaats van dat je alles zelf installeert, kun je ook gebruik maken van de laatste versie van de Backtrack 4R2 distributie.

Met uitzondering van de "karma.rc"-module is alles al aanwezig.

Het uitgangsprincipe

Karmetasploit gaat uit van het principe dat WiFi-clients de configuratie van de diverse access points waar eerder een associatie mee is geweest, opgeslagen hebben. Dit zijn vaak de beveiligde access points op het werk en thuis, maar ook de onbeveiligde access points in hotels, conferenties en andere ontmoetingsplaatsen. Op basis hiervan kan Karmetasploit de clients misbruiken.

Voor diverse besturingssystemen geldt dat zodra de WiFi-interface wordt geactiveerd (bijvoorbeeld een laptop die uit de slaapstand wordt gehaald), deze op zoek gaat naar de bekende (en dus vertrouwde) access points. Hiervoor zal de WiFi-client één of meerdere probe requests uitzenden. Er zijn besturingssystemen die dit niet meer standaard doen, maar een gebruiker kan dit in de meeste gevallen dan weer eenvoudig activeren. Dit zal dan ook vaak worden gedaan omdat dit een stuk gebruiksgemak geeft.

Dit is nou precies waar het om gaat in het hieronder beschreven aanvalscenario.

Stap 1

Opzetten van een access point

Voor het gebruik van Karmetasploit dient er eerst een access point te worden opgezet dat alle probe requests opvangt en accepteert. Dit kan met "airbase-ng",

een onderdeel van de Aircrack-NG suite. Nadat deze is geactiveerd zal er een nieuw access point beschikbaar zijn. SSID's die door probe requests worden opgevangen, zullen door het access point worden overgenomen. Het access point zal vervolgens al deze SSID's blijven adverteren. Op IP-niveau moet het access point worden voorzien van een IP-nummer. Vervolgens zal een DHCP-server ervoor moeten zorgen dat er IP-adressen en andere instellingen worden uitgedeeld aan de WiFi-clients die om de IP-instellingen vragen.

Stap 2

Activeren van Karmetasploit

Nu alles gereed is, kan Karmetasploit geactiveerd worden door Metasploit op te starten met het "Karma.rc"-script. Het commando `msfconsole -r karma.rc` zorgt ervoor dat alle benodigde modules worden opgestart.

Op dit punt van de aanval hebben we dus een rogue access point dat ieder probe request van een WiFi-client beantwoordt. Verder hebben we diverse services zoals: DNS-, POP3-, IMAP4-, SMTP-, FTP-, SMB- en HTTP geactiveerd. Deze zijn in het Metasploit framework geïntegreerd. Nu is het wachten op een WiFi-client die verbinding zoekt.

Stap 3

Aanval op de client

Zodra er een WiFi-client wordt geassocieerd met het door ons opgezette access point, kan de aanval beginnen. In de praktijk is het zo dat diverse client-programma's zoals mail, webmail en chat, automatisch met de ingestelde servers zal proberen te verbinden. Deze verbindingen worden allemaal door het zojuist opgezette portaal afgehandeld. De DNS-server zal ervoor zorgen dat we zelf de rol overnemen van de eigenlijke server. Hierdoor zal bijvoorbeeld een browser alle cookie-informatie en authenticatie-strings netjes

naar ons versturen. Op deze wijze wordt er al veel vertrouwelijke informatie verzameld.

Maar er is meer. Wat te denken van een browser-versie of een besturingssysteem waarvan diverse kwetsbaarheden bekend zijn en waarvoor er een exploit beschikbaar is? Deze kwetsbaarheden kunnen dan door het Metasploit framework worden uitgebuit om bijvoorbeeld de browser aan te vallen. Dit alles vindt plaats zonder dat de gebruiker hier erg in heeft en omdat hij of zij enkel en alleen de laptop heeft geopend om de familieleden/vriendenkring foto's te laten zien van de laatste vakantie.

Conclusie

Het mag duidelijk zijn dat niet alleen de access points maar zeker ook de WiFi-clients afdoende beveiligd moeten zijn. Iedere WiFi-client die op zijn minst een onbeveiligd netwerk in de preferred network list heeft, is op deze wijze aanvalbaar. Een assessment zou wel eens verrassende resultaten kunnen opleveren, vooral in omgevingen waar gebruikers veelal onderweg zijn en zoveel mogelijk connectiviteit nodig hebben.

Tegenmaatregelen die getroffen kunnen worden zijn bijvoorbeeld:

- Schakel WiFi uit op momenten dat deze niet gebruikt worden en zorg ervoor dat deze niet zelf op zoek gaan naar access points (zie het kader "Verborgen SSID's");
- Zorg ervoor dat alleen beveiligde netwerkverbindingen in de preferred network list worden opgenomen;
- Verwijder tijdelijk gebruikte onbeveiligde netwerkverbindingen in de preferred network list meteen na gebruik;
- Voer regelmatig assessments uit en vergeet daarbij de zogenaamde mobile devices niet;
- Beschouw ieder draadloos netwerk als vijandig. Gebruik alleen versleutelde verbindingen en zorg ervoor dat de

Verborgen SSID's

Vaak wordt gedacht dat het verbergen van de SSID (geen SSID-broadcasting - SSID cloaking) een goede beveiliging is omdat het SSID dan niet zichtbaar is. Maar hoe zit dit met WiFi-clients? Indien een WiFi-client zelf op zoek gaat naar een "verborgen" access point, dan zal deze een probe request versturen met daarin: de SSID. Deze kan dan ook eenvoudig worden opgevangen. Er zijn zelfs WiFi-clients zoals smartphones die altijd op zoek zijn naar "verborgen" access points, ook als de WiFi-scans zijn uitgeschakeld. Concreet betekent dit dat de smartphones te allen tijde iedere minuut het "geheime" SSID zal uitzenden ...

client-software altijd up-to-date is.

Maak gebruik van een VPN in geval van bijvoorbeeld een kantoortoepassing.

Een laatste kanttekening: Indien er twee dezelfde SSID's in de buurt zijn, dan zal over het algemeen het access point met het sterkste signaal door de WiFi-client worden gekozen. Met behulp van spoofing is het mogelijk om een WiFi-client opnieuw te laten zoeken naar access points. Tegenwoordig zijn er USB WiFi adapters te krijgen waarbij 2000mW geen uitzondering is. Het gebruik is in Nederland overigens verboden.

Zie ook:

http://www.wifihw.nl/wireless/Regelgeving_Wifi.htm

http://wetten.overheid.nl/BWBR0023553/Bijlage8/tekst_bevat_100%2Bmw/geldigheidsdatum_27-02-2011



In welke branche is uw organisatie actief?

Onze organisatie is actief binnen de zorg, onderwijs en onderzoek.

Hoeveel mensen houden zich in uw organisatie bezig met informatiebeveiliging?

Informatiebeveiliging is een integraal onderdeel van het lijnmanagement en een persoonlijke verantwoordelijkheid van de medewerkers. Dit houdt in dat de gehele organisatie (vaak onbewust) bezig is met informatiebeveiliging. Daarnaast zijn er binnen de organisatie verschillende functionarissen die op onderdelen (Beleid, Fysiek, ICT, Incidentafhandeling, Naleving, etc.) van informatiebeveiliging inhoudelijk betrokken zijn. De (Information) Security Officer houdt zich fulltime bezig met informatiebeveiliging.

Wat is uw functie?

Mijn functie is Senior Security Officer. Ik ben fulltime bezig met informatiebeveiliging in de breedste zin van het woord. Dit houdt in dat ik betrokken ben bij alle verschillende facetten van informatievoorziening (digitaal en fysiek) binnen onze organisatie.

Wat zijn de drie belangrijkste kwaliteiten waarover men moet beschikken om deze functie met succes te kunnen uitoefenen?

Buiten kaders denken

Naast inhoudelijke deskundigheid op het gebied van informatiebeveiliging is het belangrijk om de samenhang tussen informatiebeveiliging en andere gebieden zoals patiëntveiligheid, kwaliteit en risicomanagement te kunnen onderkennen, zodat informatiebeveiliging kan worden geïntegreerd.

Ervaring leert dat vakinhoudelijke specialisten vaak duidelijk weten welke kant ze op willen, maar om dit te bereiken moet je mensen "meenemen". Daarom zijn 'het goed kunnen communiceren met verschillende doelgroepen' en 'geduld om collega's mee te nemen', belangrijke persoonlijke eigenschappen.

In de zorg komt het veel voor dat de fysieke toegang tot de organisatie voor vreemden volledig open is. Wat betekent dit voor de informatiebeveiliging?

Vanuit informatiebeveiligingsperspectief is dit inderdaad een uitdaging. Buiten kaders denken en aansluiten bij de bedrijfsprocessen is dan ook vereist maar niet altijd eenvoudig. Wel is de ervaring dat de medewerkers binnen het bedrijfsproces zelf een aardig goed beeld hebben welke richting het op moet.

Wat betekent het invoeren van de NEN7510-norm, over informatiebeveiliging in de zorg, voor uw organisatie?

De NEN7510 is een beheersmaatregelen-norm. Met andere woorden: er worden voorstellen gedaan vanuit "best practice" maar het geeft geen inzicht in risico's.

Onze organisatie heeft daarom niet tot doel om de NEN7510-norm volledig te implementeren, maar de balans te zoeken tussen (ingeschatte) risico's enerzijds en maatregelen vanuit de NEN7510-norm, kosten & werkbaarheid anderzijds. Hierdoor ontstaat er een passende (voldoende mate van) beveiliging en worden investeringen op een verantwoorde wijze gedaan. De nadruk ligt dan ook op het informatiebeveiligingsproces. Vanuit de procesbenadering wordt informatiebeveiliging geborgd en is er blijvende aandacht voor de samenhang tussen, en de kwaliteit van, de benodigde (beheers)maatregelen.

Welke maatregelen worden genomen om deze risico's onder controle te houden?

Het gaat niet zozeer om de individuele maatregelen, maar het kader waarbinnen de maatregelen zijn genomen. Voor onze organisatie is dat kader:

- Informatiebeveiliging is gericht, vanuit het belang voor interne afdelingen (onderzoek, onderwijs en zorg), op beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
- Informatiebeveiliging is geïntegreerd binnen het "Kwaliteitskader" en "Plan en Control cyclus" van de organisatie en daarmee aantoonbaar.
- Informatiebeveiliging werkt door in cultuur en gedrag binnen de organisatie.

Hoe helpt Madison Gurkha met het onder controle houden van deze risico's?

Er wordt op het gebied van informatiebeveiliging periodiek gebruik gemaakt van "Interne Kwaliteit Audit", "Certificerende Visitatie" en / of "Technische Audit".

Technische audits zijn gericht op de inrichting en werking van technische omgevingen. Het geeft de organisatie inzicht of de daadwerkelijke inrichting (technische gezien) overeenkomt met de gestelde eisen en of er mogelijk extra of veranderende risico's zijn ontstaan. Technische audits worden door (in- of externe) specialisten uitgevoerd. Madison Gurkha heeft in het afgelopen jaar dergelijke audits in opdracht van ons uitgevoerd.

Wat zijn uw ervaringen met Madison Gurkha?

Onze organisatie ervaart de samenwerking met Madison Gurkha positief. Dit geldt vanaf het moment van de offerteaanvraag tot en met de uitvoering en rapportage. Technisch gezien zit er veel deskundigheid bij Madison Gurkha. Daarnaast verloopt de omgang met de individuele medewerker van Madison Gurkha professioneel en plezierig.



foto's: maitman23, Mich Altman

Het jaarlijkse congres van de CCC, de Duitse Chaos Computer Club, is één van de oudste hacker-bijeenkomsten die nog steeds gehouden wordt. Afgelopen december vond de 27e editie plaats in Berlijn in het congrescentrum. Het thema was: "We Come in Peace".

Eigenlijk is de conferentie al jaren te groot voor het congrescentrum, maar dat mag de pret niet drukken. De zalen mogen dan wel ruim voor aanvang van de populaire praatjes vol zijn (je komt dan echt niet meer binnen), voor de meeste bezoekers (waaronder ik) is dat niet zo'n ramp. Veel interessante zaken spelen zich namelijk af buiten de zalen. In het congrescentrum zijn zaaltjes ingericht waar mensen met allerlei technologische snufjes spelen. Je kunt er ook zelf leren solderen of lockpicken. Allerlei hackerspaces zijn vertegenwoordigd. En veel sociale contacten worden aangehaald in de binnenstad.

Berlijn is wat dat betreft een schot in de roos: een prachtige stad met veel nachtleven, waar het voor hackers goed toeven is, ondanks de kou dit jaar (tot -14 graden overdag).

De CCC-conferenties zijn van oudsher de plek waar opzienbarende beveiligingsvondsten voor het eerst wereldkundig gemaakt worden. Dit keer was de media-aandacht iets minder dan eerdere jaren, toen het GSM-netwerk en RFID-kaarten gekraakt werden. Persoonlijk vond ik de lezing van Karsten Nohl en Sylvain Munaut het meest

aanspreken. Hier werd namelijk voor het eerst een GSM-gesprek live opgevangen uit de ether en gekraakt. Eerder had ik dat al wel zien gebeuren met SMS-berichten, maar spraak is een stuk moeilijker te decoderen, omdat het signaal op steeds wisselende frequenties wordt uitgezonden. Door een oude GSM van 10 euro te herprogrammeren, kon men er een af luisterapparaat van maken en na korte tijd werden de stemmen van Karsten en Sylvain die uit de computer kwamen overstemd door een luid applaus. Maar ook zij kwamen in vrede, en maakten de fijne kneepjes niet bekend om misbruik te voorkomen. Ook kwamen ze met oplossingen voor de telecomindustrie.

Alle praatjes zijn opgenomen en beschikbaar op het internet. Zie hiervoor de site https://events.ccc.de/congress/2010/wiki/Conference_Recordings/. Voor diegene die het sociale aspect belangrijk vinden: van 10 t/m 14 augustus is er weer het vierjaarlijkse CCC Communication Camp nabij Berlijn.

HET COLOFON

Redactie

Tim Hemel
Laurens Houben
Remco Huisman
Frans Kollée
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. Aan zowel de fysieke als de digitale uitgave kunnen geen rechten worden ontleend.

26 APRIL 2011 - DE REEHORST IN EDE
BLACK HAT SESSIONS PART IX

THE HUMAN FACTOR

PRIVACY, SOCIAL ENGINEERING, SOCIAL NETWORKS, AWARENESS, DIGITAL CRIME

SPREKERS ZIJN:

OT VAN DAALEN > KARIN SPAINK > HANS VAN DE LOOY > ANDREW MACPHERSON > RALPH MOONEN
> FRANS KOLLÉE > LAURENS HOUBEN > MARK LASTDRAGER. DAGVOORZITTER: WALTER BELGERS.



Ot van Daalen Karin Spaink Hans Van de Looy Ralph Moonen Frans Kollée Laurens Houben Mark Lastdrager Walter Belgers



Deze negende editie van de welbekende Black Hat Sessions wordt georganiseerd door Array Seminars en Madison Gurkha en staat volledig in het teken van de menselijke aspecten op het gebied van informatiebeveiliging: "The Human Factor".

Nadat we vorig jaar de risico's van de "Cloud" hebben onderzocht, gaan we dit jaar in op de rol van en de gevolgen voor de mens van het gebruik van IT. Dit jaar zullen er geen vendorsessies zijn, waardoor wij ruimte hebben voor 2 parallelle tracks. Zo kunnen ook niet-technische bezoekers een interessant programma volgen. Er zal deze editie volop aandacht zijn voor onderwerpen als privacy, social engineering, risico's van het gebruik van sociale netwerken, identiteitsdiefstal en fraude, digitale criminaliteit, etc.

We laten overal waar we komen een digitaal spoor achter. Na het volgen van de bijeenkomst heeft u een beter inzicht in wat u allemaal aan informatie achterlaat en wie daar allemaal de beschikking over heeft (aanvallers, overheden, etc.). Informatie is waardevol en een geliefd doelwit voor aanvallers. Met het verder aanscherpen van technische beveiliging, wordt de mens de zwakste schakel. Vandaar de focus op uw eigen rol in informatiebeveiliging.

DATUM
26 APRIL 2011

LOCATIE
DE REEHORST IN EDE

TIJD
09.30 TOT 17.00 UUR

INFORMATIE EN REGISTRATIE
WWW.BLACKHATSESSIONS.NL

BESTEMD VOOR U
De bijeenkomst wordt georganiseerd voor beheerders van systemen, netwerken en applicaties, security officers, interne auditors, het management en andere geïnteresseerden.

Deze Black Hat Sessions wordt georganiseerd door:

Array SEMINARS

INFOSECURITY

Madison
Gurkha
Your Security is Our Business