

**DE COLUMN 2**

Remco Huisman

**HET NIEUWS 3**

Make-over van Madison Gurkha

Vier cent voor gehackte computer

Nog veel bedrijven met DNS-lek

Marnix Aarts **5**

**DE KLANT 4-5**

Uit de verzekeringswereld

**HET INTERVIEW 6**

Ralph Moonen

**DE HACK 7**

Functionele achterdeur...

**HET INZICHT 8-9**

DNS cache poisoning

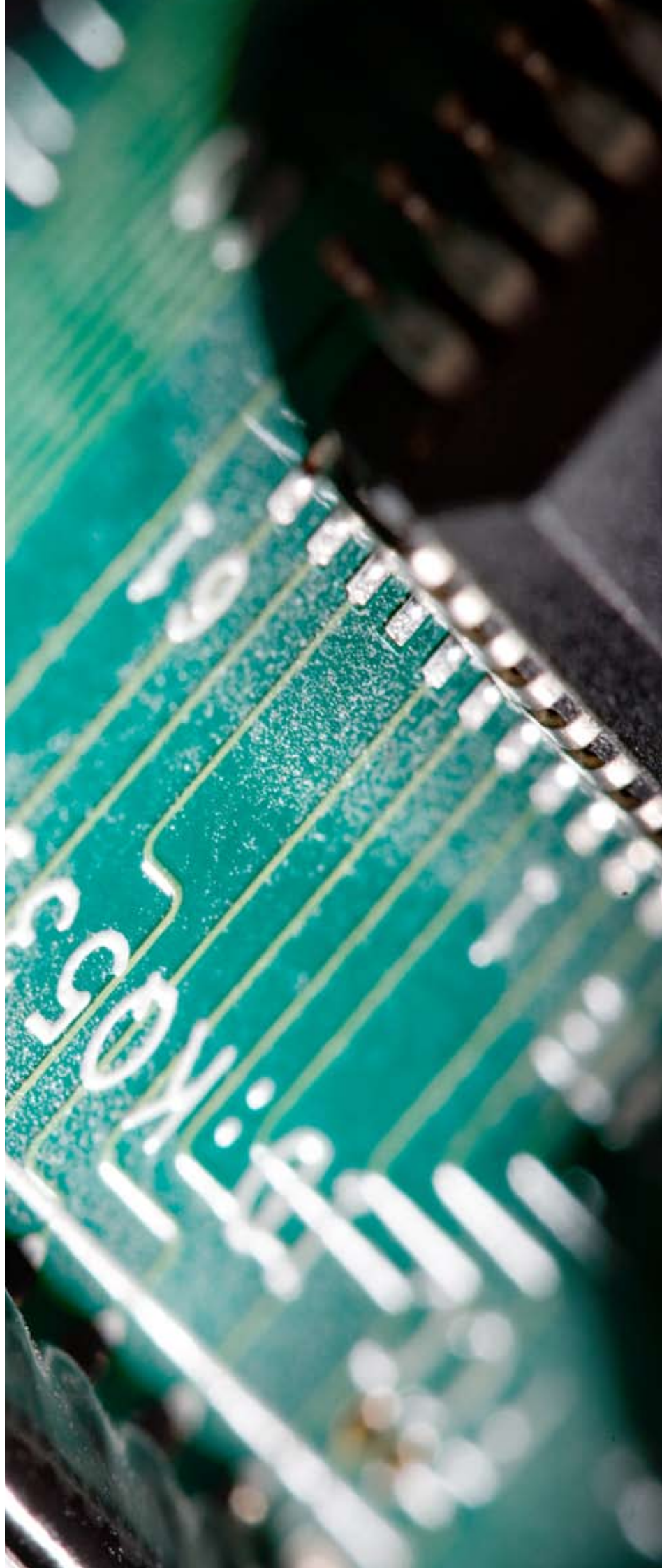
**DE AGENDA 10**

**HET VERSLAG 10-11**

The Last HOPE

**HET COLOFON 11**

.....





## Het nieuwe Madison Gurkha

Voor u ligt de eerste Madison Gurkha Update in een nieuw jasje. Voortaan informeren wij onze klanten en relaties eens per kwartaal over ICT-beveiliging in het algemeen en Madison Gurkha in het bijzonder.

Madison Gurkha bestaat inmiddels ruim acht jaar. In die tijd hebben wij een gerenommeerde naam opgebouwd in de technische ICT-beveiliging. Dagelijks helpen wij met zestien medewerkers organisaties om (technische) ICT-beveiligingsrisico's te identificeren, te verminderen en te voorkomen. Overigens zoeken wij nog steeds collega's, maar dat terzijde.

Om onze huidige en toekomstige medewerkers een passende werkplek te geven, zijn wij eind juni verhuisd. Het klopt dat u hiervan geen adreswijziging heeft gekregen. Wij zijn namelijk verhuisd van enkele kamers op de vijfde verdieping in de Groene Toren naar een halve etage op de 11de etage. Behalve een aanzienlijk beter uitzicht, biedt ons nieuwe onderkomen ook veel meer ruimte en een betere uitstraling.

Over uitstraling gesproken: onze uitingen hebben geen gelijke tred gehouden met onze groei en professionalisering in de laatste jaren. Hoog tijd dus voor het nieuwe uiterlijk van de Madison Gurkha Update. Onze website kon hier uiteraard niet bij achterblijven, dus ook deze heeft een andere vormgeving gekregen. Centraal in onze nieuwe vormgeving staan macrofoto's van computertechniek, want hoewel de menselijke inventiviteit van onze consultants onmisbaar is bij de audits en testen die wij uitvoeren, blijft Madison Gurkha zich richten op technische ICT-beveiliging op projectbasis.

Toch kunnen wij u vanaf heden ook diensten leveren op het gebied van de zachtere kant van informatie-

beveiliging. Het oude merk ITSX – dat wij in 2006 hebben overgenomen – blazen wij samen met Ralph Moonen (KPMG IRM, Ubizen/Verizon) namelijk nieuw leven in. ITSX staat voor Information Technology Security eXperts en dat is precies waar ITSX zich mee bezig houdt. ITSX slaat een brug tussen ervaren en zelfstandige IT Security eXperts en organisaties op zoek naar professionele ondersteuning op het gebied van informatiebeveiliging in de brede zin van het woord.

Uiteraard gaan wij in deze eerste Madison Gurkha Update in de rubriek "Het Interview" uitgebreid in op ITSX door middel van een vraaggesprek met Ralph Moonen. Maar er is meer. In de rubriek "De Klant" laten wij elk kwartaal (anoniem) een van onze klanten aan het woord. Deze keer praten wij met mevrouw A van verzekeraar B. In "De Hack" bespreken wij succesvol uitgevoerde "hacks". Het is uitstekend dat de voordeur een goed slot heeft, maar hoe zit het met de achterdeur? In "Het Inzicht" leggen wij u uit wat de risico's zijn van DNS Cache poisoning. In "De Agenda" en "Het Nieuws" tenslotte, houden wij u op de hoogte over het wel en wee van de ICT-beveiligingswereld en Madison Gurkha in het bijzonder.

Ik wens u veel leesplezier.

**Remco Huisman**  
*Partner, Commercieel directeur*

## Make-over van Madison Gurkha

Al sinds de oprichting in 2000 geniet Madison Gurkha een als maar groeiende positieve naamsbekendheid. Madison Gurkha bedrijft op professionele wijze haar vak en biedt haar klanten oplossingen op maat. Deze toewijding zorgt ervoor dat we blijven excelleren en groeien in onze markt. Deze zorg voor kwaliteit en professionaliteit dragen we uit via ons personeel, maar sinds kort ook via de vernieuwde website en het nieuwe kantoor.

Sinds 1 juli zijn we officieel gevestigd op de 11e etage van de "Groene Toren" in Eindhoven. In plaats van dat

we, zoals op de 5e etage, een aantal kamers bezetten, hebben we nu de beschikking over een complete halve etage. Deze verhuizing heeft dus voor meer ruimte gezorgd voor ons almaar groeiende team en, niet geheel onbelangrijk, het draagt het ook beter bij aan de algehele uitstraling van Madison Gurkha.

Vanwege het groeiende succes en het nieuwe kantoor kon natuurlijk een vernieuwing van onze website niet achterblijven. De nieuwe website is dus nu ook een feit. Er zijn een aantal veranderingen zichtbaar. Zo is er een nieuwe huisstijl geïntroduceerd die beter aansluit op onze visie en is de nieuwe website overzichtelijker. Tevens wordt hij actueel gehouden met alle nodige informatie over onder andere beveiligingsnieuws, publicaties, presentaties en recente seminars, zodat u niets meer hoeft te missen. U kunt de nieuwe website bekijken op [www.madison-gurkha.com](http://www.madison-gurkha.com).



## Minderheid bedrijven heeft DNS-lek gedicht

- SAMENVATTING -

Beveiligingsexperts denken dat slechts een deel van de bedrijven alle benodigde patches heeft doorgevoerd om het DNS-lek af te dekken, dat Dan Kaminsky begin juli bekendmaakte. Daarbij spelen drie factoren een rol: onbekendheid met het probleem, onderschatting van de ernst en een nonchalant patchbeleid. Pieter de Boer, security consultant bij Madison Gurkha: "Microsoft heeft een patch beschikbaar gesteld, maar zijn gebruikers niet aangeschreven; de gebruikers van DNS-server BIND zijn onbekend, omdat het om een open source product gaat. Dat het probleem ernstig is blijkt volgens de Boer alleen al doordat er massaal patches zijn uitgebracht. "Tot nu toe hadden kwaadwillenden alleen via een "brute kracht"-methode kans dat hun aanval lukte. Met de door Kaminsky ontdekte methode is succes gegarandeerd." De Boer stelde dat het patchbeleid in de Nederlandse bedrijven te nonchalant is. "Er kunnen maanden overheen gaan voordat patches worden doorgevoerd. Zoiets kost tijd. Beheerders zijn beducht om wijzigingen aan te brengen in een werkende productie omgeving."

Bron: *Computable* nummer 31/32, 1 augustus 2008

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

## Vier cent voor een gehackte computer

- SAMENVATTING -

Vier cent. Dat is de prijs die internetcriminelen op dit moment betalen voor een gekraakte computer die onderdeel is van een botnet, een netwerk van gekraakte computers. Een 19 jarige Friese hacker werd onlangs aangehouden toen hij een botnet van tienduizenden computers voor 25.000 euro verkocht. Expert Walter Belgers van Madison Gurkha verklaart hoe de Fries aan een koper kwam en of het moeilijk is zelf een botnet te maken.



*Hoe weet ik of mijn computer onderdeel is van een botnet?*

"Soms gaat je computer trager lopen. Of krijg je klachten van iemand die ziet dat vanaf jou computer spam wordt verstuurd. Goede beveiliging helpt, daarmee verminder je de kans op virussen. Via virussen krijgt een hacker toegang tot je computer."

*Wat doet een hacker met een computer als die onderdeel is van een botnet?*

"Ze versturen er spam mee, gooien er sites mee plat of proberen er gegevens mee te ontfutselen. Ik kan eenvoudig zeggen dat drie miljoen computers op zoek moeten gaan naar creditcard gegevens. Weer drie miljoen andere computers kan ik vragen om spam te versturen."

*Moet je heel slim zijn om een botnet te maken?*

"Je hoeft niet superintelligent te zijn om internetcrimineel te worden. Botnets zijn gewoon te koop op internet. Begrijp je Windows, dan is zo'n botnet eenvoudig te bedienen." "... Een botnet bouwen kan eenvoudig zijn. Op internet zijn virussen te koop en codes, de bouwstenen van een botnet."

*Waar vinden die internetcriminelen elkaar?*

"Ik heb eens gezocht en vond via Google snel allerlei plekken waar mensen creditcardgegevens en botnets verhandelen. De prijs voor één botnet is momenteel vier cent. Vaak gaat het om ruilhandel" "... Als je laat zien dat je iets te verhandelen hebt, krijg je al snel toegang tot de chatkanalen waar de professionelere jongens elkaar teffen."

Bron: *Dagblad De Pers*, pagina 3, 6 Augustus 2008





#### In welke branche is uw organisatie actief?

In de verzekeringswereld.

#### Hoeveel mensen houden zich in uw bedrijf bezig met ICT-beveiliging?

Actief een man of dertig, schat ik. Die zijn bezig met het onderzoeken van het beveiligingsniveau en het structureel uitvoeren van activiteiten om geconstateerde beveiligingsrisico's te verminderen of weg te nemen. Het verhogen van de awareness van alle andere medewerkers van het bedrijf, totaal ruim 2000, valt hier ook onder.

#### Wat is uw functie?

Binnen de ICT-divisie geef ik leiding aan een team van professionals, dat verantwoordelijk is voor de informatie-analyse, het functioneel ontwerp en het testen van met name de applicaties voor klantgegevens, commerciële zaken en marketing & communicatie. Onze afdeling is de schakel tussen business en IT. Als teamleider ben ik verantwoordelijk voor de planning van het onderhoud op de systemen en de coördinatie van alle benodigde ICT-activiteiten.

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

Ondernemerschap, communicatieve vaardigheden en plannen & organiseren. En toch een vierde: resultaatgerichtheid.

#### Heeft u hiervoor een specifieke opleiding genoten?

Nee, ik heb Italiaans gestudeerd en een aantal jaren als zelfstandig ondernemer gewerkt. Eind jaren '90 ben ik overgestapt naar de IT. Ik heb diverse technische vakinhoudelijke cursussen gevolgd en een managementtraining.

#### Welke rol speelt IT security in uw functie?

De systemen die wij ontwikkelen en beheren, verwerken

en ontsluiten veel gevoelige informatie. Wij moeten er onder andere voor zorgen dat dit op een veilige manier gebeurt. Al vanaf de informatieanalyse moet je hier rekening mee houden. Hoe eerder een onvolkomenheid wordt ontdekt, hoe lager de kosten om maatregelen te nemen. Wij hebben niet alle benodigde expertise in huis om te bepalen of een applicatie ook daadwerkelijk veilig is. Daarom werken we samen met externe bureaus om audits en penetratietesten uit te voeren.

#### Wat is volgens u het belangrijkste aspect van ICT-beveiliging?

Bewustzijn bij de hele organisatie. Alle medewerkers komen hier in aanraking met gevoelige informatie. Niet iedereen is zich bewust van de risico's op en de consequenties van misbruik van deze informatie.

Om het beveiligingsniveau voldoende hoog te houden, is fysieke beveiliging alleen niet voldoende. Het is noodzakelijk dat medewerkers alert zijn op mogelijke risico's en deze herkennen en melden, zodat de benodigde maatregelen genomen kunnen worden.

#### Hoe is uw belangstelling voor ICT-beveiliging ontstaan?

Eind vorig jaar bleek dat een van onze webapplicaties onvoldoende beveiligd was. Dit was voor ons aanleiding om het totale niveau van beveiliging binnen de organisatie nader te onderzoeken. We hebben onder andere penetratietesten laten uitvoeren op onze applicaties, audits laten doen op onze technische infrastructuur en een onderzoek gedaan naar social engineering. Door de bevindingen die daaruit kwamen, ben ik me bewust geworden van de risico's en heb ik me meer verdiept in de ontwikkelingen op dit gebied.

#### Wat vindt u het leukste aan uw functie?

In de ICT en ook in de branche waarin ik werk, gaan de ontwikkelingen heel snel, en sta ik steeds weer voor nieuwe uitdagingen. Om mijn resultaten te behalen werk ik samen met veel verschillende soorten mensen en onderhoud ik relaties met interne en externe partijen. Een van mijn belangrijkste verantwoordelijkheden is om de randvoorwaarden te scheppen om mijn team optimaal te laten functioneren. Ik heb er echt voldoening van als ik zie dat mijn medewerkers uitgedaagd blijven, zich ontwikkelen en met plezier werken en we tegelijkertijd ook de gestelde doelen halen.

#### Wat is het meest uitdagende probleem geweest waar u mee te maken heeft gehad tijdens de uitvoer van uw functie?

Ik kan niet echt een specifiek probleem bedenken, maar het is elke keer weer een uitdaging om de opdrachten zo te verdelen over mijn team, dat iedere medewerker op de juiste klus zit. Vooral als de prioriteiten veranderen, zoals bijvoorbeeld met het beveiligingsprobleem dat we eind vorig jaar hebben gehad. Toen moesten we aanpassingen in verband met de beveiliging direct realiseren. Dan probeer je alles toch zo te organiseren, dat je de planning van lopende projecten zo min mogelijk verstoort.

#### Op welke manier heeft de opgedane kennis van uw vakgebied invloed op uw dagelijkse leven?

Ook in mijn privéleven maak ik natuurlijk gebruik van digitale gegevensuitwisseling. Ik ben me, zeker na het bezoeken van een van jullie Black Hat Sessions, meer bewust van de wijze waarop mijn pc en mijn gegevens misbruikt kunnen worden.

#### Hoe helpt Madison Gurkha daarbij?

Wij hebben de ervaring en kennis van Madison Gurkha nodig om ons beveiligingsniveau voldoende hoog te houden en ons bewustzijn te vergroten. De beveiligingsrisico's veranderen zeer snel en wij hebben intern geen mogelijkheden om de kennis met betrekking tot de gevaren en de technieken om beveiligingsrisico's vast te stellen, courant te houden. Madison Gurkha heeft veel ervaring en is continu bezig met alle ontwikkelingen op dit gebied.

#### Wat zijn uw ervaringen met Madison Gurkha?

Ten eerste is Madison Gurkha een expert op het gebied van beveiliging. Dat blijkt onder andere uit de mondelinge en schriftelijke adviezen. De rapportages van de audits zijn zeer helder: de bevindingen zijn goed onderbouwd en de adviezen zijn duidelijk en praktisch. Hierdoor kunnen wij direct actie ondernemen, als we ergens een risico constateren.

De medewerkers van Madison Gurkha zijn heel enthousiast bezig met hun vak en weten waar ze het over hebben. Ze zijn heel sterk in het meedenken met de klant en het zich verplaatsen in de behoefte van de klant.

Tenslotte zijn de medewerkers van Madison Gurkha open en vriendelijk en dat vind ik persoonlijk heel prettig in de samenwerking.

**Madison Gurkha voert per jaar tientallen IT security audits uit voor uiteenlopende organisaties: van verzekeraars tot banken, van pensioenfondsen tot de overheid en van technologie bedrijven tot internet winkels. Al onze klanten hebben een ding gemeen: ze nemen IT security uitermate serieus. Zij weten als geen ander hoe belangrijk het is om zorgvuldig met kostbare en vertrouwelijke gegevens om te gaan. Zij laten hun technische IT security risico's daarom dus ook structureel onderzoeken door Madison Gurkha.**

## Marnix

Ik ben Marnix Aarts, 22 jaar oud, en werk sinds 1 juli jl. bij Madison Gurkha. Kort na mijn HBO-opleiding commerciële economie ben ik op zoek gegaan naar een leuke en interessante baan. Deze heb ik gevonden in de vorm van commercieel medewerker bij Madison Gurkha. Ik ben onder andere verantwoordelijk voor de uitwerking van offertes en het courant houden van de website, tevens zit ik in de redactie van Madison Gurkha Update. Mijn eerste twee maanden zitten er nu inmiddels op en ik moet zeggen dat het me erg goed bevalt. A-technisch als ik ben, moest ik de eerste weken wel een beetje wennen aan al die



ICT-lingo, je kunt dan natuurlijk nergens over mee praten. Maar met behulp van enkele boeken, verkregen door collega's, gaat dat helemaal goed komen. Ik heb de afgelopen maanden veel bijgeleerd bij Madison Gurkha waardoor de werkzaamheden steeds interessanter worden.

In mijn vrije tijd sport ik graag en ben ik meerdere malen per week te vinden op het rugbyveld van Rugby Club Eindhoven (RCE). Naast dat ik zelf speel, ben ik sinds een aantal jaar ook actief als jeugdtrainer, wat erg leuk is om te doen.

# Ralph Moonen



**December 2007 tot heden**  
Eigenaar, Moonen Media & Management

**1998 tot heden**  
Spreker op het instituut voor gevorderde management studies (TIAS) in Tilburg

**Maart tot December 2007**  
Hoofd Professional Services bij Verizon Business Security Solutions (Voorheen bekend als Cybertrust)

**1998 - February 2007**  
Manager Security Testing Services, IT-security Consultant en IT-auditor bij KPMG Information Risk Management

**1994 - 1998**  
Publieke omroep VARA

**1989 - 1994**  
AT&T Network Systems (Nu bekend als Lucent)

**Contactgegevens**  
IT Security eXperts BV  
Ralph Moonen  
Annie M.G. Schmidweg 12  
1321 JE Almere  
www.itsx.com  
info@itsx.com  
gsm +31 (0)653251082

## Hoe ben je ertoe gekomen om ITSX (Information Technology Security eXperts) op te zetten?

Ik werd een aantal maanden geleden benaderd door Madison Gurkha met de vraag of ik geïnteresseerd was in het opzetten van een nieuwe onderneming onder een oude naam. Ik was natuurlijk direct geïnteresseerd en na wat initiële gesprekken werd ons duidelijk dat we beiden (Madison Gurkha en Ralph Moonen) de behoefte hadden om diensten te kunnen leveren die wat minder technisch van aard waren dan wat Madison Gurkha doet, maar wel met security management te maken hebben. Aan de andere kant wilden we niet zomaar een nieuwe beveiligingsonderneming opzetten. Ik ben zelf, na bijna tien jaar KPMG en een blauwe maandag bij Verizon Business, sinds 1 januari als "Zelfstandige Zonder Personeel" (ZZP'er) begonnen. Ik heb gemerkt dat er voor ZZP'ers nog een hoop verbeterd kan worden. ITSX zal deze ZZP'ers aan zich binden door het uit handen nemen van de "rompslomp", het bieden van een samenwerkingsplatform en uiteraard het kunnen verzorgen van uitdagende en interessante opdrachten op ICT-beveiligingsgebied bij gerenommeerde bedrijven. Deze bedrijven kunnen voor zelfstandige ICT-beveiligingsspecialisten eindelijk terecht op een betrouwbaar adres: ITSX.

## Waarom samen met Madison Gurkha?

Ik ken de mensen bij Madison Gurkha al lang, zowel zakelijk als persoonlijk en Madison Gurkha heeft natuurlijk een uitstekende reputatie in de markt. De stap om ook samen te gaan werken was dus niet zo heel erg groot. Mijn bekendheid met Madison Gurkha betekent natuurlijk ook dat er van beide kanten een vertrouwen is in elkaars kwaliteiten, vaardigheden en kunnen. Dat zijn kritieke factoren want we staan allemaal voor een onderneming die aan klanten en ZZP'ers de hoogste kwaliteit moet gaan leveren.

## De naam ITSX komt bekend voor...

ITSX is inderdaad een bekende naam. De oprichter van ITSX, Rop Gongrijp, heeft de bedrijfsactiviteiten en de 'brand' overgedaan aan Madison Gurkha, maar daar werd nog geen gebruik van gemaakt. Het oude ITSX zul je ook niet meer herkennen. Zie het als een doorstart met nieuwe doelen.

## Het logo en de site zien er wel anders uit...

Dat klopt, we hebben ervoor gekozen om bij deze doorstart een nieuwe huisstijl te ontwikkelen omdat de activiteiten anders worden. Dat voelt ten

eerste beter, en ten tweede vonden we de oude stijl enigszins gedateerd en niet helemaal aansluiten bij de doelgroepen: het management in grote (overheids)organisaties.

## Hoe onderscheidt ITSX zich van de concurrentie?

Op dit moment bestaan er nog geen organisaties in het ICT-beveiligingsvakgebied die zich richten op interim-management en grotere opdrachten, ingevuld door ZZP'ers. Daarin zijn we sowieso de eerste en onderscheiden we ons door deze innovatie. Daarnaast is het kwaliteitsaspect uiteraard zeer belangrijk. Net zoals Madison Gurkha, heeft ITSX als voornaamste doelen kwaliteit en klanttevredenheid. Dit gaan we bereiken door een strenge selectie van ZZP'ers met wie we gaan samenwerken en het leveren van de 'best-man-for-the-job'. Uiteraard zullen we ons ook onderscheiden door onze ZZP'ers te stimuleren zichzelf te profileren door publicaties, presentaties en onderzoek.

## Hoe verhouden de diensten van Madison Gurkha en ITSX zich tot elkaar?

Het voornaamste verschil zit hem in de focus van ITSX op langdurige opdrachten in de interim-managementsfeer, terwijl Madison Gurkha zich richt op technische, kortlopende opdrachten. Natuurlijk zullen beide bedrijven zich met kwalitatief hoogstaande dienstverlening op ICT-beveiligingsgebied bezighouden, maar de overlap zal zeer beperkt zijn.

## Welke expertise kan ik als opdrachtgever inhuren bij ITSX?

De ZZP'ers die voor ons zullen gaan werken hebben allemaal tenminste vijf jaar, maar vaak veel meer, ervaring op het gebied van ICT-beveiliging, audits en security management. Certificeringen vinden wij ook erg belangrijk, denk aan CISSP, CISM, CISA, RE. Dat betekent dat de expertise van deze mensen zowel technisch als organisatorisch en procedureel is. Daarnaast hebben onze ZZP'ers ook in diverse branches veel ervaring, meestal vanuit hun Big-4 (KPMG, Deloitte, PWC en E&Y) achtergrond in finance, industrie en overheid.



**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](mailto:redactie@madison-gurkha.com).**

## Functionele achterdeur blijkt zwakste schakel

Wie kent dit niet: je bent thuis en je wilt nog even inloggen op je werk om het idee dat je in de trein kreeg te versturen naar de overige leden van de projectgroep. Of je wilt je email controleren of er al een antwoord is op de vraag die je aan je afdelingshoofd hebt gesteld. De ICT-afdeling heeft hiervoor de middelen beschikbaar gesteld en ervoor gezorgd dat je op een veilige manier in kunt loggen door gebruik te maken van beveiligde verbindingen en sterke authenticatie-mechanismen. Je gebruikt je ADSL-verbinding eerst om je privé-email te lezen en logt vervolgens in. Helaas, het jou wel bekende login-scherm met bedrijfslogo wil maar niet verschijnen.

Voor jou is het duidelijk: je hebt zelf verbinding met het internet en dus moet het aan de verbinding naar je werk liggen. Je belt het storingsnummer en meldt dit aan de dienstdoende functionaris die eveneens constateert dat er iets aan de hand is. Vervolgens wordt de netwerkbeheerder ingeschakeld voor nader onderzoek. Deze kan via het internet ook geen verbinding meer krijgen, maar beschikt gelukkig over een inbelverbinding. Zo kan hij vanaf het interne bedrijfsnetwerk op onderzoek uitgaan, zonder dat hij naar kantoor hoeft waarbij ook nog eens allerlei personen moeten worden ingeschakeld met betrekking tot alarmcodes. Het euvel was vrij snel gevonden en nadat de VPN-router was gereset, bleek alle connectiviteit hersteld. Gelukkig maar, nu kon iedereen weer inloggen en bleven andere telefoontjes uit.

Het bedrijf in kwestie neemt ICT-beveiliging zeer serieus en doet er zoveel mogelijk aan om het beveiligingsniveau op een hoog peil te brengen en te houden. Hiertoe worden de verschillende middelen ingezet: procedureel, technisch en controlerend. Eén van de middelen is het regelmatig uitvoeren van technische beveiligings-audits. In het kader hiervan werd Madison Gurkha verzocht een beveiligings-audit uit te voeren waarbij de infrastructuur en de services die diensten via het internet aan interne gebruikers alsook aan het grote publiek aanbieden, moesten worden onderzocht.

De infrastructuur bleek op orde te zijn en liet enkel en alleen netwerkverkeer toe voor de diensten die werden aangeboden (volgens het "deny all, except"-principe). Het patch-niveau van de toegankelijke services was bijgewerkt. De webapplicaties konden niet worden misbruikt doordat alle invoer en uitvoer op een adequate wijze werd gefilterd, er geen testbestanden konden worden gevonden etcetera. De beveiliging zat dus goed en gelaagd in elkaar. De VPN-toegang voor de medewerkers liet eveneens weinig ruimte, ook niet in het geval dat we met behulp van geactiveerde tokens ingelogd waren. Ook hier was een gelaagde beveiliging actief.

Uiteindelijk was er nog een laatste item dat getest moest worden: de inbelverbinding. Deze was er alleen voor beheerders zodat men

in geval van calamiteiten via een analog modem de beheeromgeving kon benaderen. Het telefoonnummer was vooraf bekend gemaakt en verwacht werd dat we ook hier weinig zouden kunnen doen. Het tegendeel bleek echter het geval. Nadat we handmatig middels een simpel dial-up programma contact zochten, kregen we na verloop van tijd verbinding. De gebruikelijke banner werd getoond waarin werd aangegeven dat ongeautoriseerde toegang niet geoorloofd was.

Een doelgerichte aanvaller, zal zich door een dergelijke boodschap niet laten weerhouden. Ook zal deze niet het in de banner genoemde telefoonnummer bellen om te melden dat hij/zij "per ongeluk" een verbinding heeft gemaakt. Zeker niet wanneer niet alleen de banner wordt getoond, maar ook de systeem-prompt! Geen prompt die om een gebruikersnaam of wachtwoord vraagt, maar een heuse systeemprompt met daarin de naam van het systeem! Zonder enige vorm van authenticatie was er toegang tot het systeem. Een vraagteken was zeer behulpzaam met het verstrekken van informatie over het systeem alsook de mogelijke commando's. Met behulp van de commando's konden we meer informatie verzamelen over de netwerkinterfaces en de achterliggende netwerken. Vervolgens was het mogelijk om vanaf dit systeem verbinding te maken met andere systemen waaronder routers, switches en andere netwerksystemen.

Voor een aantal van deze systemen was authenticatie vereist. Door gebruik te maken van een aantal "standaard" wachtwoorden was ook deze barrière snel genomen en langzaam maar zeker konden meer en meer systemen worden benaderd. Wat begon als een kleine druppel werd een almaar groter wordende olievlek.

De beheerders werden tijdens de audit op de hoogte gebracht zodat er onmiddellijk tegenmaatregelen konden worden genomen. Deze waren snel geïmplementeerd waarna het een en ander nogmaals getest werd, nu gelukkig zonder resultaat. Vervolgens heeft het bedrijf samen met Madison Gurkha onderzocht hoe het kon dat dit nog niet eerder opgemerkt was. Het antwoord bleek verrassend eenvoudig: voor het gebruik van deze inbelfaciliteit werd gebruik gemaakt van meegeleverde client-software. Hierbij was authenticatie wel nodig. Het gebruik van onze apparatuur en bijbehorende software omzeilde de verplichte authenticatie.

Uiteindelijk heeft dit geresulteerd in verschillende verbeterpunten zoals:

- verplichte authenticatie op alle inkomende verbindingen,
- callback functionaliteit van de inbelverbinding,
- logging van succesvolle en niet succesvolle inlogpogingen,
- aanpassen van alle standaard wachtwoorden op alle systemen.

Bij netwerkbeveiliging gaat het erom dat alle mogelijke ingangen worden bewaakt en afgeschermd. Verder dienen er op verschillende niveaus meerdere technieken te worden gebruikt om indringers te vertragen en te detecteren zodat er tegenmaatregelen kunnen worden getroffen voordat er schade is aangericht. Een kleine opening in de netwerkbeveiliging kan al fataal zijn.





# DNS cache poisoning



**De laatste weken is DNS cache poisoning veel in het beveiligingsnieuws geweest. Dit omdat er een nieuw probleem in DNS is ontdekt, waardoor het plotsklaps mogelijk is om dit veel sneller te doen. Maar wat is het nu eigenlijk en waarom is dit belangrijk?**

## Wat is DNS?

Simpel gezegd is DNS het telefoonboek voor het internet. DNS vertaalt computernamen, zoals `www.madison-gurkha.com`, naar computeradressen (88.159.10.2 in dit geval). Ook vertelt DNS bijvoorbeeld, waar mail voor een bepaald domein heen moet. Aangezien DNS een gedistribueerd systeem is, kunnen DNS-servers (ook wel nameservers genoemd) ook verwijzen naar andere DNS-servers die het antwoord wellicht weten.

Nameservers kunnen drie verschillende antwoorden op vragen geven:

- 1) het antwoord
- 2) het antwoord op de vraag bestaat niet
- 3) ik weet het niet, maar deze nameserver met dit IP-adres kan je verder helpen

## Soorten DNS servers

Er bestaan twee typen DNS servers, autoritatieve en resolving servers. Ook combinaties hiervan komen voor. Wanneer een server uitsluitend autoritatief is, heeft deze geen problemen met cache poisoning omdat dit type geen cache heeft. Resolving servers kunnen echter wel problemen hebben. Een resolving server is een server die gebruikt

wordt om antwoorden te zoeken. Eindsystemen, zoals een desktop systeem, zullen een resolving server de vraag stellen "wat is het IP-adres van `www.madison-gurkha.com`" en de resolving server gaat dan een rijtje DNS-servers op het internet af om het antwoord te vinden. Met het programma 'dnstracer' is dit inzichtelijk te maken.

Hier een deel van de uitvoer:

```
$ dnstracer -4 -s . -c www.madison-gurkha.com.  
Tracing to www.madison-gurkha.com[a] via A.ROOT-SERVERS.NET, maximum of 3 retries  
A.ROOT-SERVERS.NET [.] (198.41.0.4)  
| \_ H.GTLD-SERVERS.NET [com] (192.54.112.30)  
| | \_ ns6.gandi.net [madison-gurkha.com] (217.70.177.40) Got authoritative answer  
| | \_ ns.madison-gurkha.com [madison-gurkha.com] (194.151.35.243) * * *  
| | \_ ns.gvr.org [madison-gurkha.com] (82.95.154.195) Got authoritative answer
```



## Leuk detail

Zodra Dan Kaminsky bekend maakte dat er op dit gebied een probleem bestond, zonder overigens details te noemen, is Pieter de Boer van Madison Gurkha samen met vriend Peter van Dijk hiernaar op zoek gegaan. Dit leverde in de presentatie van diezelfde Dan Kaminsky een vermelding op als "first finder" van het probleem.

Hier valt te zien dat de delen van 'www.madison-gurkha.com.' (van rechts naar links gelezen) opgezocht worden. De nameserver voor '.' (het meest rechter stukje) zegt dat informatie voor 'com' te halen valt bij 'H.GTLD-SERVERS.NET'. Deze vertelt vervolgens dat informatie voor 'madison-gurkha.com' te halen valt bij 'ns6.gandi.net', 'ns.madison-gurkha.com' en 'ns.gvr.org'. Deze laatste drie weten het antwoord voor 'www.madison-gurkha.com.' en verwijzen dus niet meer verder.

Nadat een resolving nameserver een antwoord heeft gevonden zal deze dit antwoord een bepaalde, met het antwoord meegeestuurde, tijd onthouden. Bij een volgende vraag voor www.madison-gurkha.com zal dit onthouden antwoord gegeven worden en zal niet opnieuw een serie nameservers af gezocht worden om het antwoord te vinden. Dit heet caching.

### Wat is DNS Cache poisoning?

DNS Cache poisoning is het vervuilen van de DNS-cache met leugens. Wanneer een aanvaller succesvol een ander (vals) IP-adres voor www.grotebank.com in de resolving DNS van een internet provider kan stoppen, betekent dat dat alle gebruikers van deze internet provider, wanneer ze www.grotebank.com in hun browser intikken, op het vervalste adres uitkomen. Ditzelfde kan ook gebruikt worden om e-mail naar bepaalde domeinen de verkeerde kant op te sturen.

### Hoe werkt DNS cache poisoning?

Om DNS-informatie succesvol te vervuilen is het nodig om op het moment dat een resolving DNS aan een andere DNS server om informatie vraagt, sneller een nep-antwoord te sturen dan de DNS server antwoordt. Vergelijk het met die onaardige collega die wanneer je op kantoor aan iemand een telefoonnummer vraagt snel uit z'n hoofd een opzettelijk verkeerd nummer geeft. Wanneer je vervolgens dat nummer belt kom je er, in het algemeen, snel genoeg achter dat dit het verkeerde nummer was. Maar computers zijn zo slim niet, die blijven gewoon het verkeerde nummer gebruiken, gedurende de hele tijd waarvoor ze verteld is dat dit nummer geldig blijft.

### Waarom zagen we dit in het verleden niet?

Bij DNS-vragen wordt een willekeurig nummer meegestuurd. Dit nummer, dat tussen 0 en 65535 ligt, moet ook in het antwoord worden genoemd, want anders wordt het antwoord genegeerd. Om succesvol een verkeerd antwoord te kunnen geven, dient een aanvaller sneller te antwoorden dan de legitieme nameserver en moet het correcte willekeurige nummer worden meegestuurd. Wanneer de aanvaller namelijk niet èn sneller is, èn het juiste nummertje gebruikt, onthoudt de resolving nameserver het correcte antwoord gedurende de met het antwoord meegeestuurde tijd. Dit is vaak een week en daardoor kan het een aanvaller mogelijk duizenden weken kosten om het vervalste antwoord in de nameserver te krijgen. Niet bepaald 'get rich quick'. Overigens waren in een verder verleden de nummertjes vaak voorspelbaar, waardoor het toen eenvoudiger was om dit uit te voeren.

### Waarom is dit nu ineens een groot probleem?

Een onderzoeker (Dan Kaminsky) heeft een nieuwe manier van aanvallen gevonden. Hierbij kan de tijd dat de nameservers de antwoorden onthoudt, omzeild worden. Dit betekent dat een aanvaller simpelweg enkele duizenden vragen aan een nameserver kan stellen in de hoop één van deze vragen als eerste en met het juiste referentienummer te beantwoorden, om zo de cache te vervuilen. 65536 mogelijke getallen zijn er wel veel, maar ook weer niet zo veel dat dit onmogelijk is. Bovendien bepaalt de aanvaller het tijdstip waarop de race om te antwoorden begint en kan de aanvaller in plaats van één antwoord ook bijvoorbeeld honderd antwoorden sturen. Hierdoor wordt de succeskans verhoogd van 1/65536 naar 1/655. In tests is het onderzoekers (en aanvallers) gelukt dit in minder dan 10 seconden uit te voeren. Bij deze nieuwe aanval stelt een aanvaller nieuwe vragen voor hosts binnen het aan te vallen domein aan een recursieve nameserver. Stel, de aanvaller wil de cache entry van www.madison-gurkha.com vervalsen. Dan stelt de aanvaller vragen voor bijvoorbeeld abc.madison-gurkha.com, def.madison-gurkha.com,

com, etc aan de recursieve nameserver. De namen maken niet uit, zolang ze maar niet in de cache zitten. De recursieve nameserver probeert vervolgens een antwoord voor deze hosts te vinden. De aanvaller stuurt antwoorden van het derde type (ik weet het niet, maar deze nameserver met dit IP adres kan je verder helpen) met daarin extra informatie waarin staat "www.madison-gurkha.com met IP adres X.X.X.X kan je verder helpen". De vragende nameserver zal deze extra informatie in de cache opnemen en hierbij eventuele reeds gecachte informatie vervangen. Verder zal deze vervalste informatie bewaard en gebruikt worden gedurende de door de aanvaller opgegeven geldigheidsduur.

### Wat valt er tegen dit probleem te doen?

Eigenlijk maar een ding: DNSSEC in gebruik nemen. DNSSEC staat voor DNS Security Extensions en is specifiek ontworpen om cache poisoning en andere problemen met DNS de wereld uit te helpen. Helaas is dit makkelijker gezegd dan gedaan. Om dit uit te rollen is het namelijk nodig vrijwel alle nameservers op het internet, te beginnen bij de belangrijkste (de root servers, en alle landen en .com, .org, .net servers) aan te passen. Niet iets wat snel gedaan kan worden. Ook moeten registratieprocedures voor domeinen aangepast worden. SIDN, de verantwoordelijke partij voor de .nl servers, heeft hier enige tijd geleden tests mee gedaan maar ze is daarmee een van de weinige partijen die dat überhaupt gedaan heeft. In de tussentijd is het aan te bevelen de software op nameservers aan te passen. Tests wijzen uit dat hierdoor de tijd die nodig is om op de nieuwe manier van cache poisoning toe te passen vergroot wordt; van ongeveer 10 seconden naar ongeveer 10 uur. Geen sluitende oplossing, maar een duidelijke, snel uitrolbare verbetering.

### Kan ik zelf testen of mijn nameserver kwetsbaar is?

Ja, dit is mogelijk door met een browser naar <http://www.doxpara.com> te gaan en daar op de "Check My DNS"-knop te klikken.

Heeft u onderwerpen die u graag een keer terug zou willen zien in deze rubriek? Laat het dan weten aan onze redactie via: [redactie@madison-gurkha.com](mailto:redactie@madison-gurkha.com).



*Veel belangstelling voor lockpicking bij tool.*

# The Last HOPE

**Mensen uit de beveiligingswereld ontmoeten elkaar regelmatig op diverse conferenties ergens ter wereld. Het aantal bijeenkomsten dat aan beveiliging is gerelateerd, is in vergelijking met een aantal jaar geleden sterk gegroeid, wat aangeeft dat de interesse hierin alleen maar is toegenomen.**

Werden "hackerconferenties" heel vroeger beschouwd als een gelegenheid waar criminele subversievelingen bijeenkwamen om in een geheimzinnige sfeer kennis te verspreiden, tegenwoordig zijn er zelfs beveiligingsevenementen die qua publiek variëren van IT-managers tot kunstenaars en van technenuten tot ecologische hippies.

Sinds 1994 organiseert het Amerikaanse hackerstijdschrift "2600 Magazine" de zogenaamde HOPE-conferentie (Hackers On Planet Earth). Vanaf die eerste keer vindt deze traditioneel plaats in het bekende Hotel Pennsylvania in New York. Helaas wordt dit historische hotel met de sloop bedreigd om vervangen te worden door een grote glazen toren waar de financiële wereld zijn intrek kan nemen. Dit zou dan ook de laatste keer zijn dat de HOPE op deze manier wordt gehouden. Om op gepaste wijze afscheid te nemen van deze bijzondere conferentie is de naam dit jaar geheel toepasselijk omgedoopt tot "The Last HOPE".

HOPE is een typische hackerconferentie in de breedste zin van het woord hacken: het creatief gebruik van technologie om hiermee beperkingen te omzeilen. Binnen deze ruime omschrijving valt natuurlijk het omzeilen en doorbreken van computerbeveiliging, maar ook het gebruik van computers en hardware om dingen te bouwen die iedereen doen verbazen. Daarnaast spelen ook politieke en maatschappelijke ontwikkelingen een grote rol op deze conferentie, uiteraard voor zover deze te maken hebben met technologie of beveiliging. Het is dan ook geen wonder dat het publiek sterk varieert qua achtergrond, werkzaamheden en interesses. Het programma is zo samengesteld dat het voor elk van deze doelgroepen wat interessants te bieden heeft.

Vanzelfsprekend is computerbeveiliging in het algemeen een belangrijk onderdeel van het programma. Variërend van social engineering tot aan threat modelling, cryptografie, hardware-analyse en lockpicking. Dit laatste onderdeel werd onder meer verzorgd door de in Nederland opgerichte vereniging Tool (The Open Organisation Of Lockpickers), die sinds kort ook in Amerika actief is. Een van de hoogtepunten was de lezing waarbij nieuwe tools openbaar werden gemaakt voor het kraken van harddiskencryptie door het computergeheugen uit te lezen.

Een van de meest populaire onderwerpen op deze HOPE was de strenge controle die, met name in de Amerikaanse strijd tegen de terroristische dreiging, wordt uitgevoerd. Van onderzoek van laptops van passagiers tot de Bagcam: een in een reistas ingebouwde camera, die filmt wat er met bagage gebeurt nadat

deze is ingecheckt; allen leverden boeiend discussieonderwerpen. Hierbij kwam bijvoorbeeld naar voren dat is gebleken dat de controle op bagage niet zo strikt nageleefd wordt als het jaarlijkse overheidsbudget hiervoor doet vermoeden, en dat ook de bagage niet altijd even zachtzinnig werd behandeld. En dat leverde dan weer voldoende stof op voor een volgende discussie.

Ook stemcomputers zijn in Amerika onderwerp van gesprek en hoewel er in Nederland al veel kritiek bestaat op deze manier van stemmen, blijken de stemcomputers aldaar een heel stuk hackbaarder dan hier. U begrijpt, wederom voer voor een interessante dialoog onder hackers.



*Historisch hotel met de sloop bedreigd.*

Op deze HOPE-conferentie konden ook de handen uit de mouwen worden gestoken in een zogenaamde Hacker Space. Binnen de hackergemeenschap heeft zich in de loop der jaren een subcultuur ontwikkeld die zich bezig houdt met de bouw van kunstwerken op basis van elektronica en het programmeren van robots met microcontrollers. Veel van de ontwikkelingen op dit gebied vinden hun basis in deze "clubhuizen" waar hackers



*Echte phreakers nemen hun eigen telefooncel mee.*

hun hobby beoefenen. Geïnspireerd door het succes hiervan bij de Duitse Chaos Computer Club, zijn nu ook in Amerika en Canada dergelijke ruimtes aan het ontstaan en natuurlijk mocht een echte Hacker Space niet ontbreken bij de HOPE-conferentie. Het concept is zelfs zover doorgevoerd dat speciaal de in Duitsland bij hackers zeer geliefde frisdrank "Club Mate" is geïmporteerd! Dit tot grote tevredenheid van de vele Europese bezoekers. Om het de deelnemers nog meer naar de zin te maken was er bovendien een ruimte ingericht waar men vanaf ligbedden via videoprojectors de lezingen kon volgen.

Ondertussen zal het u duidelijk zijn dat de hackercultuur een eigen geschiedenis aan het schrijven is en ook hieraan werd de nodige aandacht besteed. De geschiedenis van het phreaken (het hacken van het telefoonsysteem) werd uitgebreid belicht in een aantal presentaties en ook bijvoorbeeld Kevin Mitnick, ("the world's most dangerous hacker" in the eyes of the government and mass media, imprisoned for over five years, and now a successful computer security consultant") vertelde zijn verhaal.

De driedaagse conferentie werd afgesloten met een aantal minuten stilte, om deze allerlaatste HOPE te herdenken. Maar de hackers zouden hun reputatie geen eer aandoen als ook deze beperking niet omzeild werd: er werd bekend gemaakt dat de sloopplannen voor het hotel definitief zijn uitgesteld, zodat in 2010 een volgende conferentie met de toepasselijke naam 'The Next HOPE' kan plaatsvinden.

Als u op de hoogte wilt blijven van de laatste ontwikkelingen in de ICT-beveiligingswereld dan zijn beurzen en conferenties de ideale gelegenheid om uw kennis te verrijken en om contacten op te doen. Iedere Madison Gurkha Update presenteren wij in de agenda een lijst met interessante bijeenkomsten die de komende tijd zullen plaatsvinden.

11 t/m 12 september

**Sec-T, Stockholm**

<http://www.sec-t.org/>

Een nieuwe beveiligingsconferentie in Zweden, met een veelbelovend programma. Exotische onderwerpen zoals de beveiliging van Websphere MQ, SAP pentesting, online crime en OpenVMS beveiliging komen aan bod.

vraagt om een multidisciplinaire aanpak. Immers, alleen met een integrale inzet vanuit verschillende disciplines zal Informatiebeveiliging en de inrichting hiervan voldoende en optimaal zijn ingericht. Vandaar dat vertegenwoordigers met verschillende kijk op beveiliging zich hier aan u presenteren.

22 t/m 24 oktober

**Hack.lu, Luxemburg**

<http://hack.lu/>

In een aantal jaar is deze conferentie in Luxemburg uitgegroeid van een kleinschalige conferentie naar een evenement waar de technische professionals elkaar ontmoeten, met als doel het bouwen van bruggen tussen de verschillende spelers in de beveiligingswereld.

27 t/m 30 december

**25C3, Berlijn**

<http://events.ccc.de/congress/2008/>

Het Chaos Communication Congress is een vierdaagse conferentie die jaarlijks georganiseerd wordt door de Chaos Computer Club (CCC). Deze vindt plaats in Berlijn, Duitsland. De Chaos Computer Club stimuleert en bevordert creatieve en onorthodoxe interactie tussen technologie en maatschappij zoals dit past in de hackertraditie. De onderwerpen zijn divers en verdeeld in de volgende zes aandachtsgebieden: Hacking, Making, Science, Society, Culture en Community.

12 t/m 13 november

**Infosecurity, Utrecht**

<http://www.infosecurity.nl/>

Op deze dagen is het in de Jaarbeurs te Utrecht weer tijd voor de Infosecurity beurs. Informatiebeveiliging

**Redactie**

Marnix Aarts  
Tim Hemel  
Remco Huisman  
Frans Kollée  
Caroline van de Wiel  
Ward Wouts

**Vormgeving**

Hannie van den Bergh  
[www.studio-HB.nl](http://www.studio-HB.nl)

**Contactgegevens**

Madison Gurkha B.V. T +31 40 2377990  
Postbus 2216 F +31 40 2371699  
5600 CE Eindhoven E [info@madison-gurkha.com](mailto:info@madison-gurkha.com)  
Nederland redactie@madison-gurkha.com

**Bezoekadres**

Vestdijk 9  
5611 CA Eindhoven  
Nederland

# 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.

**Your Security is Our Business**

tel: +31(0)40 237 79 90 - [www.madison-gurkha.com](http://www.madison-gurkha.com) - [info@madison-gurkha.com](mailto:info@madison-gurkha.com)