4

Madison Gurkha
Your Security is Our Business

ZOMER 2009

UPDATE

WWW.MADISON-GURKHA.COM

In iedere Madison Gurkha Update vindt u een leuke en informatieve column, die de lezer een verfrissende kijk biedt op uiteenlopende onderwerpen rondom ICT-beveiliging. Deze keer vertelt Arjan de Vet over "Juridisch Verantwoord Hacken".

Juridisch Verantwoord Hacken

In de vorige Update kon u op deze plaats al lezen over Ethisch Hacken. Daarin werd al aangestipt dat 'hacken' strafbaar is, vandaar dat we in deze column eens dieper ingaan op het juridisch verantwoord hacken. Hierbij wordt het hopelijk duidelijk waarom we als Madison Gurkha niet, zonder eerst een aantal schriftelijke formaliteiten geregeld te hebben, voor u als klant aan de slag kunnen.

Omdat wij als klein bedrijf zelf geen diepgaande juridische expertise in huis hebben, zijn we onlangs met onze verzekeraars en een jurist om tafel gaan zitten om onze algemene voorwaarden, contracten en vrijwaringen up-to-date te krijgen.

De mogelijke strafbaarheid van onze dienstverlening voor wat betreft security audits is geregeld in de Wet Computercriminaliteit, zie http://www.iusmentis.com/beveiliging/hacken/computercriminaliteit/ voor een uitgebreide beschouwing. Deze uit 1993 stammende wet is per 1 september 2006 aangepast zodat voor 'Computervredebreuk' (artikelen 138a en 138b Wetboek van Strafrecht) het niet meer noodzakelijk is om een beveiliging te doorbreken, elk 'opzettelijk' en 'wederrechtelijk' binnendringen in computersystemen is dus strafbaar.

Het moge duidelijk zijn dat als Madison Gurkha een security audit uitvoert, we opzettelijk proberen binnen te dringen in een computersysteem; daar worden we tenslotte voor ingehuurd. Het is daarom belangrijk dat Madison Gurkha expliciete toestemming krijgt voor het uitvoeren van security audits; in dat geval zijn we namelijk niet meer 'wederrechtelijk' bezig om een computersysteem binnen te dringen. Daarmee vervalt de mogelijkheid om Madison Gurkha strafrechtelijk voor 'hacken' te vervolgen.

Deze expliciete toestemming is geformuleerd in onze (mantel)contracten en, voor het geval er derde partijen bij betrokken zijn, in een 'vrijwaring derde partij'. Hoewel Madison Gurkha vaak assisteert bij het verkrijgen van toestemming van derde partijen, blijft het primair de verantwoordelijkheid van u als klant om deze toestemming van de derde partijen te regelen. U heeft als het goed is contracten met deze derde partijen, bijvoorbeeld een hosting provider, en we raden dan ook aan in dit soort contracten afspraken over security audits vast te leggen.

Behalve dat we willen uitsluiten strafrechtelijk aangeklaagd te kunnen worden, is het ook noodzakelijk nog enige andere voorzorgen in acht te nemen. Een van de doelen van een security audit is meestal nagaan of kwaadwillenden onbedoeld of opzettelijk schade aan zouden kunnen richten. Madison Gurkha probeert dit aan te tonen dan wel aannemelijk te maken zonder die schade daadwerkelijk aan te richten.

Echter, er is altijd een kleine kans dat er door een security audit toch schade aangericht wordt. Zo kan het zijn dat Madison Gurkha onbewust tegen een nog niet eerder ontdekt (security-)probleem aanloopt, waardoor een ernstige verstoring of dataverminking optreedt. Verder kan het zijn dat een computersysteem zodanig slecht geconfigureerd en/of beheerd wordt, dat dit bij het minste of geringste 'omvalt'. Zonder het geheel uitsluiten van aansprakelijkheid voor dit soort directe en indirecte (gevolg) schade kan Madison Gurkha simpelweg haar dienstverlening niet juridisch verantwoord uitvoeren. Dit staat dan ook geformuleerd in onze contracten en vrijwaring derde partijen, met alleen een uitzondering voor opzet of grove nalatigheid aan de zijde van Madison Gurkha.

Omdat schade bij security audits nooit en te nimmer voor 100% uit te sluiten is, raden we onze klanten aan om indien mogelijk op een test/acceptatie-omgeving te laten testen. En ongeacht op welke omgeving er getest wordt, is het raadzaam recente backups te hebben, en dan het liefst backups waarvan aangetoond is dat ze ook correct en tijdig teruggezet kunnen worden.

Voor de goede orde: Madison Gurkha doet, zoals u van ons mag verwachten, haar uiterste best om securityrisico's in kaart te brengen zonder schadelijke gevolgen. Belangrijke factor hierin is natuurlijk onze jarenlange ervaring en 'track record' bij het succesvol uitvoeren van security audits.

Arjan de Vet
Partner, Principal Security Consultant

ICT in de rechtszaal

- SAMENVATTING-

Nog niet zo lang geleden stond ik voor de rechter. Niet als verdachte, maar als getuige-deskundige. Dat is, formeel gezegd, een getuige die onder ede wordt gehoord tijdens een rechtszaak omdat hij specialist is op een bepaald terrein. Hij getuigt dus zijn deskundigheid.

De verdachte in de zaak was een jongeman, verdacht van het inbreken op een computersysteem. Inbreken is strafbaar onder de Wet Computercriminaliteit. Toen ik erbij gehaald werd, speelde de zaak al 5 (!) jaar. Hoe kan dat gebeuren? Het blijkt dat bij de politie en de rechterlijke macht onbekendheid met de materie een groot struikelblok vormde. Het zorgde voor vertraging, maar ook voor een onvolledig en onduidelijk onderzoek. Hoe een firewall werkt, was in de zaak waar ik het hier over heb, bij de rechter in kwestie geheel onduidelijk. Als getuige-deskundige is het daarom van belang om, behalve het geven van een deskundig en eerlijk oordeel, dat zo duidelijk mogelijk te doen. Het belang van zo'n vertaalslag bleek tijdens de zaak waar ik het hier over heb.

Het bewijs voor de inbraak door de verdachte bestond uit een verklaring van een beheerder die "programma's had getraceerd naar een IP-adres" en dat IP-adres leidde uiteindelijk naar de verdachte. Hoe dat traceren door de beheerder precies in zijn werk ging werd niet vermeld, maar klaarblijkelijk was het enige aanknopingspunt de logging van een firewall. Hierin stond dat de firewall de hoeveelheid verkeer niet meer kon verwerken en dat er een poortscan aan de gang was (vanaf het IP-nummer van de verdachte).

Interessant om te weten is dat deze firewall niet bijhield wat er doorheen ging (alleen geblokkeerd verkeer werd genoteerd). Bovendien bleek uit de verklaringen dat het systeem waarop zou zijn ingebroken, vrijwel geheel openstond voor iedereen vanaf het hele internet. Aangezien elk systeem op internet ongeveer een aanval per minuut voor zijn kiezen krijgt, is het niet verwonderlijk dat er op wordt ingebroken, temeer daar het systeem niet werd beheerd (volgens de verklaringen).

Toch was de firewall logging blijkbaar voldoende om deze zaak jaren te laten slepen. Ander bewijs was er niet, ook geen bewijs dat de verdachte het niet had gedaan. Een grove fout tijdens het eerste onderzoek is geweest dat men wel de computer van de verdachte in beslag genomen en onderzocht heeft, maar niet het systeem van de aanklager, terwijl daar nu juist uit te halen was geweest op welke wijze en waar vandaan was ingebroken!

Kortom, de zaak stond of viel met de vraag: in hoeverre bewijst de firewall logging dat de verdachte inderdaad heeft ingebroken? Als getuige-deskundige kon ik de rechter eenvoudig duidelijk maken dat de firewall alleen melding maakte van een poortscan, en geen inbraak.

De verschillende manier waarop de rechter en ik tegen de materie aankijken, bleek wel toen de rechter specifiek wilde weten of de meldingen erop duidden dat er op de firewall werd ingebroken. Voor een techneut is het vanzelfsprekend dat een firewall verkeer wel of niet doorlaat, als een soort portier, maar dat de portier zelf normaal gesproken geen doelwit is.

Ook het idee dat er verschillende systemen achter een firewall staan, moest worden verduidelijkt. Hiervoor gebruikte ik eenvoudige analogieën. De rechter bedankte me voor mijn heldere uitleg en ik kreeg het idee dat de zaak voor het eerst in 5 jaar duidelijk was. De verdachte werd vrijgesproken.

Wellicht zijn er lezers die zich bezighouden met illegale zaken op computergebied. Er zijn bijvoorbeeld genoeg sites te vinden waar open-sourcesoftware en media worden aangeboden, waarbij dat volgens de licentie niet is toegestaan. Nu heb ik er geen problemen mee dat deze mensen worden berecht, maar een jarenlange, slepende gerechtelijke procedure wens ik niemand toe.

Het zou dus goed zijn als zulke mensen er even stil bij zouden staan dat, als er een zaak tegen hen wordt aangespannen, dit een langdurige kwestie kan worden omdat de betrokkenen geen (of onvoldoende) kennis hebben van de techniek. Het onmiddellijk inschakelen van mensen met kennis van zaken en de kunde om dit te vertalen naar lekentermen, kan daarbij van groot belang zijn.

Auteur: Walter Belgers
Principal Security Consultant

Bron: Automatisering Gids nummer 17, april 2009

Jack Franken

Sinds 1 april is de afdeling Sales, binnen Madison Gurkha, versterkt met een nieuwe Senior Accountmanager.

Mijn naam is Jack Franken. Ik ben 42 jaar, getrouwd en ik heb twee kinderen. Nieuwe klanten zoeken en bekend maken met de diverse diensten van Madison Gurkha behoort tot mijn hoofdtaak. Daarnaast is het natuurlijk ook zaak om de relatie met bestaande klanten uit te bouwen. Het marktsegment internet security is nog steeds sterk groeiende en dus voor een accountmanager een interessant vakgebied. Madison Gurkha heeft de toekomst. In mijn vrije tijd squash en tennis ik. Dit doe ik al sinds mijn tijd op de TU Eindhoven. Daar ben afgestudeerd in de Elektrotechniek met als richting telecommunicatie. Daarna ben ik bij diverse bedrijven accountmanager en vestigingsmanager geweest.

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. Wie weet staat uw nieuwtje in de volgende Madison Gurkha Update!

Madison Gurkha Update interviewt voor iedere editie een gerenommeerd persoon in de ICT-beveiligingswereld om zijn of haar visie te delen over dit steeds belangrijker wordende onderwerp. Ditmaal een interview met Aldert Hazenberg over HAR2009.

Madison Gurkha is trotse sponsor van HAR2009

Aldert Hazenberg

Het is nu mei 2009 en je bent druk bezig met het organiseren van HAR2009. Even voor de mensen die het nog niet weten, wat is HAR precies en wie maken het mogelijk?
HAR2009 is een internationale conferentie over technologie en veiligheid; vier dagen vol lezingen, debatten en workshops. Technologie, apparaten en gadgets, maar ook ideologieën worden binnenstebuiten gekeerd, en iedereen gaat zelf aan de slag om verder te gaan waar anderen waren gebleven.

De kern van de organisatie is de Stichting Hxx, waarvan ik voorzitter ben. Maar feitelijk is de stichting niet meer dan een juridisch vehikel en een manier om de bijdragen van genereuze sponsors te kunnen ontvangen, de echte kracht komt van de vele vrijwilligers die samen de organisatie van het evenement doen. Het is lastig precies vast te stellen hoeveel dat er zijn, maar ik schat dat er nu zo'n 50 mensen bezig zijn om in augustus klaar te zijn, in de weken voor het evenement zijn dat er honderden.

Als ik besluit naar HAR te komen, waar moet ik me dan op voorbereiden? I.e. wat kan ik verwachten aan voorzieningen?
De 'outdoor conference' vindt plaats bij Vierhouten, op het voormalig socialistische jeugdkamp De Paasheuvel. Een grote hal, de Zonnehal (een monument) dient als podium voor lezingen, aangevuld met twee tenten van ongeveer gelijke capaciteit.

Er is ruime keus voor kampeerders. Van afgelegen plaatsen in het lommer tot grote velden. Douchegebouwen (gebouwen!) met douche en toilet staan verspreid over het terrein, en eigenlijk nooit ver weg. Diverse kleinere en grotere tenten en gebouwen vormen het toneel voor de rest van het programma en allerlei andere activiteiten.

Het logo heeft nogal een flower power uitstraling, ik denk dan aan muziekfestivals en niet aan een professioneel security en technologie congres. Hoe maak ik mijn werkgever duidelijk dat HAR voor een IT professional toch de moeite waard is?
Het logo geeft inderdaad de grass-roots origine van het evenement goed weer, maar dat doet niets af aan de waarde van het evenement voor de bezoekers.

Het idee achter hacken - technologie aanpassen zodat die aan jouw wensen en behoeften voldoet, en creatief gebruik maken van bestaande systemen - raakt meer vlakken dan technologie alleen. De behoefte om bij te blijven op het eigen vakgebied is de grote drijfveer voor ons publiek. Maar ook de kruisbestuiving tussen mensen die elkaar anders wellicht minder snel zouden ontmoeten. Welke werkgever ziet niet graag dat zijn eigen medewerkers zichzelf willen blijven verbeteren (upgraden)?

Dus ik kan bij wijze van spreken mijn kinderen gewoon meenemen naar HAR?
Ja zeker! Er is een family village, waar ouders voor hun kinderen activiteiten organiseren. Dit village slaat haar tenten op rondom een speeltuin.

Kinderen zijn de de hackers van morgen. We hopen dat de kleine bezoekertjes geïnspireerd raken, en wellicht later in het voetpad van hun ouders treden.

Licht eens een tipje van de sluier op voor onze lezers, wat voor sprekers kunnen ze verwachten, over welke onderwerpen?
Op dit moment wordt de stroom aan voorstellen voor lezingen en workshops beoordeeld en binnenkort zullen de eerste namen en onderwerpen aangekondigd worden. Om alvast een indruk te geven: het zal gaan over 'harde' technologie (IPv6, TOR), ideologie en praktijk (vrijheid van meningsuiting, delen van informatie op het internet) tot actuele zaken zoals de spraakmakende rechtszaak van FTD tegen BREIN.

Hoe denk je dat hackers en conferenties als HAR kunnen bijdragen aan de maatschappij?
Hackers zijn altijd kritisch. Bij een nieuwe technologie stellen ze vragen, of de technologie wel werkt zoals deze zou moeten werken. En of er ook andere mogelijkheden zijn.

Niet alleen op het technologische vlak zie je deze mentaliteit, maar bijvoorbeeld ook ten opzichte van de overheid. Hackers kunnen vaak onafhankelijk naar nieuwe ontwikkelingen kijken, of dat nu een nieuwe beveiligingsmethode is of een nieuwe wet over privacy of het filteren van datastromen.

Op een evenement als HAR2009 ontmoeten deze hackers elkaar, wisselen inzichten uit en gaan met hernieuwde kracht weer aan de slag in hun dagelijks leven. Of dat nu als netwerkbeheerder bij een multinational of een burgerrechtenorganisatie is. Zo versterkt een evenement de rol van hackers als waakhond.

Hoe verwacht je straks op HAR terug te kunnen kijken?
Ik denk dat we in september kunnen terugkijken op een succesvol evenement, waar zo'n slordige 2500 mensen niet alleen naar goede sprekers kwamen luisteren, maar ook hun netwerk hebben uitgebreid met getalenteerde gelijkgestemden van over de gehele wereld.

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.

In de rubriek "De Hack" belichten we iedere Madison Gurkha Update een opmerkelijke situatie die tijdens een beveiligingsaudit werd aangetroffen. Deze keer het woord aan Jan Hendrikx over een hack met behulp van FireWire.

Light My Fire...

Enige tijd geleden werd Madison Gurkha gevraagd om een nieuw uit te rollen bedrijfslaptop te onderzoeken op kwetsbaarheden. De laptop zou op korte termijn ingezet worden en men wilde graag weten welke risico's er zaten aan het gebruik van deze laptop.

In de opdrachtomschrijving werd expliciet gevraagd om naast het besturingssysteem ook de verschillende aansluitingen op het apparaat mee te nemen in het onderzoek. De klant was er zich terdege van bewust dat fysieke beveiliging een belangrijk onderdeel is in de totale beveiliging van zo'n apparaat. Een laptop gaat immers mee op pad en staat op deze manier bloot aan heel andere gevaren dan bijvoorbeeld een systeem dat in een afgesloten serverruimte staat.
Onze medewerkers vinden het altijd leuk wanneer er hardware op bezoek komt en ook deze keer was het weer raak. Binnen no-time lag het hele apparaat in losse onderdelen op het bureau. (Natuurlijk met toestemming van de klant). Torx schroevendraaiers, diverse Linux distro's, (verloop)kabels en nog wat andere exotische hardware passeerden de revue.

Een paar koppen koffie

Wat we op de laptop aan beveiliging tegenkwamen, zag er goed uit. Een harde schijf die beveiligd was met een wachtwoord, sterke disk encryptie, een sterk BIOS wachtwoord en geen standaard mogelijkheid om de laptop op te starten vanaf andere opstartmedia dan de harde schijf. Ook na het resetten van het BIOS zagen we geen mogelijkheid om op korte termijn toegang te krijgen tot gebruikersdata op de harde schijf. Dan maar de wachtwoorden gebruiken die de klant ons gegeven had om deze eerste laag van beveiligingsmaatregelen te omzeilen. Misschien dat we na het opstarten van het besturingssysteem meer succes hadden.
Men had kennelijk ook nagedacht over de inrichting van het besturingssysteem want met de meegeleverde testaccounts viel ook relatief weinig eer te behalen. De beveiligingsinstellingen waren netjes gezet en als ingelogde gebruiker konden we alleen maar gebruik maken van de benodigde applicaties. Zou er dan werkelijk helemaal niets onveilig zijn aan deze laptop? Na wat lichte frustratie, ongeloof en een paar mokken koffie besloten we toch maar eens op zoek te gaan naar een alternatief. Het spel was nu immers begonnen en wij waren aan zet.
Op congressen en in vakliteratuur wordt sinds 2006 al regelmatig melding gemaakt van de beveiligingsproblemen van FireWire. De laptop in kwestie had zo'n aansluiting (ookwel IEEE-1394 aansluiting genaamd) en het lag voor de hand om eens uit te proberen of we iets gemeens met deze aansluiting konden doen. De filosofie achter FireWire is eigenlijk heel eenvoudig. Sta via de FireWire aansluiting directe toegang tot het RAM geheugen toe zodat gebruikers op een snelle manier data kunnen uitwisselen. Dat is fijn tijdens het maken van een complexe videomontage maar minder fijn wanneer mensen met verkeerde bedoelingen op deze manier ook direct toegang tot uw interne geheugen kunnen krijgen. Een korte zoektocht op het Internet bracht ons bij de website van Adam Boileau. Adam heeft als een van de eerste IT beveiligers, tijdens diverse live demonstraties, aangetoond dat je een computer daadwerkelijk kunt hacken via deze aansluiting. Daarnaast is Adam zo aardig geweest om de Python code waarmee hij dit destijds demonstreerde vorig jaar op zijn eigen website te plaatsen. Na het bestuderen van de verdere online documentatie kwam er een voorzichtige grijns op onze gezichten en besloten we om deze hack in praktijk te brengen.

lees verder op pag. 7

DE KLANT

In elke Madison Gurkha Update vragen wij een klant het spreekwoordelijke hemd van het lijf met betrekking tot zijn of haar relatie met ICT-beveiliging. Voor eenieder herkenbare verhalen uit de praktijk, uiteraard zo onherkenbaar mogelijk gebracht. Deze keer het woord aan meneer X van instelling Y.

In welke branche is uw organisatie actief?
Mijn organisatie is een semi-overheidsinstelling, die zich bezig houdt met het beheer en onderhoud van oppervlaktewater.

Hoeveel mensen houden zich in uw bedrijf bezig met informatiebeveiliging?
Informatiebeveiliging is hier, buiten mijn eigen functie, niet specifiek ingebed in functies. Verscheidene collega's houden zich hier echter vanuit hun vakgebied wel mee bezig. In totaal schat ik dat er 10 mensen mee bezig zijn.

Wat is uw functie?
Ik ben werkzaam als ICT adviseur met name op het gebied van de technische infrastructuur, daarnaast ben ik aangesteld als Security Officer voor ons digitale domein. Security zaken gerelateerd aan bijvoorbeeld fysieke toegang tot onze locaties zijn belegd bij andere collega's.

Wat zijn de drie belangrijkste kwaliteiten waarover men moet beschikken om deze functie met succes te kunnen uitoefenen?
Een top drie samenstellen is altijd lastig, vooral omdat de functie eigenlijk tweeledig is. Voor het adviesgedeelte zijn zaken als goede contactuele eigenschappen, uitgebreide marktkennis en ruime ervaring belangrijke zaken. Voor het security gedeelte komen zaken naar boven als actuele kennis van bijvoorbeeld exploits en ervaring als eerste naar boven in mijn hoofd. Maar het is zoveel meer. Zaken als risicoanalyse, bewustwording en dergelijke zijn evenzeer belangrijk.

Heeft u hiervoor een specifieke opleiding genoten?
Mijn opleiding was niet specifiek gericht op de ICT sector. Ik ben opgeleid tot elektrotechnicus, maar eigenlijk direct na mijn studie gaan werken in de ICT sector. Door middel van gerichte technische cursussen en opleidingen heb ik mij verder gespecialiseerd.

Wat vindt u het leukste aan uw functie?
De diversiteit. Door de combinatie van disciplines in mijn functie kom ik eigenlijk van alles tegen. De ene keer ben je bezig met een advies over een SSL-VPN appliance, terwijl je een dag later begint met het opstellen van een IP-nummerplan. Dit terwijl je net klaar bent met het aanbesteden van afdrukapparatuur en ik me al weer aan het voorbereiden ben op een aantal security awareness sessies.

Hoe is uw belangstelling voor informatiebeveiliging ontstaan?
Eigenlijk uit pure noodzaak. Naarmate we met elkaar steeds 'digitaler' gaan communiceren en ons steeds meer 'beschikbaar' stellen voor de buitenwereld, ga je jezelf steeds meer afvragen wat er met al die informatie gebeurd. Opeens kan de hele wereld bij je op de digitale deurmat staan en dat hoeft niet altijd met de beste bedoelingen te zijn. Die realisatie was voor mij de trigger om mij verder te verdiepen in het fenomeen.

Wat is volgens u het belangrijkste aspect van informatiebeveiliging?
Ik zou zeggen, de bewustwording in samenwerking met een risico analyse. Informatie staat tegenwoordig verspreid over vele locaties en systemen. Het je bewust zijn van welke informatie zich waar bevind, is in mijn ogen cruciaal. Je moet tenslotte niet alleen weten wat je beveiligd, maar ook waar en met welke onderlinge verbanden. En vaak als je gaat nadenken daarover, kom je nog wel eens voor verrassingen te staan. Informatie is vaak op meer plekken aanwezig/toegankelijk dan je denkt. Daarnaast is een gedegen risicoanalyse belangrijk. Niet alle informatie hoeft per definitie beveiligd te worden of is heel privacy gevoelig. Je schiet je doel voorbij als je voor duizenden euro's aan het beveiligen slaat, terwijl kosten bij verlies hooguit een paar honderd euro kosten. Helaas zijn echter zaken als imagoverlies wel moeilijk te calculeren.

Op welke manier heeft de opgedane kennis van uw vakgebied invloed op uw dagelijkse leven?
Op veel manieren eigenlijk. Ik ga bewuster om met allerlei online services. Ik denk na, voordat ik informatie over mijzelf vrijgeef bij dat soort services. Tegelijkertijd is bij mij thuis alles aan elkaar geknoopt en hebben vrienden en kennissen het over de digitale huishouding bij mij thuis.

Wat is het meest uitdagende probleem geweest waar u mee te maken heeft gehad tijdens de uitvoer van uw functie?
Het meest uitdagende tot nu toe is de implementatie van een nieuw IP-nummerplan. Dat is het moment, waarop alle disciplines bij elkaar komen en je de basis kunt leggen voor een veilig en gestructureerd netwerk. De toekomst zal leren of ik de goede keuzes gemaakt heb.

Hoe helpt Madison Gurkha daarbij?
Madison Gurkha helpt mij en onze organisatie op verschillende manieren. Zij hebben ons in eerste instantie geholpen met een uitstekende security audit. Deze audit gaf ons een goed en gedetailleerd inzicht in de 'gaten' in onze beveiliging. Daarnaast heeft Madison Gurkha ons geholpen met het opzetten en uitvoeren van een aantal awareness sessies. Deze hebben een hele belangrijke bijdrage geleverd aan de bewustwording van informatiebeveiliging bij al onze medewerkers. Deze bewustwording draagt in hoge mate bij aan de acceptatie van nieuwe veiligheidsmaatregelen. Op dit moment voert Madison Gurkha regelmatig een security scan uit, waardoor wij zelf 'scherp' blijven en ons bewust zijn van eventuele potentiële veiligheidsrisico's.

Wat zijn uw ervaringen met Madison Gurkha?
Tot nu toe louter positief. De informele en enthousiaste manier van communiceren, gekoppeld aan een hoge mate van professionaliteit is erg prettig samenwerken. Madison Gurkha heeft zich bij ons niet ontpopt tot een: "U vraagt, wij leveren" organisatie, maar zij denkt actief mee over security vraagstukken en de beste manier waarop deze aangepakt kunnen worden. Je hebt als klant het gevoel dat ondersteuning en samenwerken voorop staan en niet, zoals vaak wel het geval is, het eigen commerciële belang.

Welke trends voorziet u in de informatiebeveiliging voor de komende jaren?
Ik zie tot nu toe de trend tot het ontwikkelen en aanbieden van allerlei appliances, die

'instant security' aanbieden, maar zie dat wel als een kwalijke zaak. Security behelst niet alleen een apparaat of een stuk software. Ik hoop dat in de toekomst vooral veel meer aandacht aan security wordt besteed op het gebied van software. Lekken die er niet zijn, hoeven tenslotte ook niet gedicht te worden.

Wordt er in deze economisch mindere tijden nu meer of minder aandacht besteed aan informatiebeveiliging volgens u? En hoe komt dit denkt u?
Wat ik zo om mij heen zie, wordt er minder aandacht aan besteed. Het kost tenslotte geld en levert niet zo direct wat op. En deze korte termijn kosten/baten analyse viert in deze tijden helaas hoogtij. Maar volgens mij is dit juist het moment om te zorgen dat de algehele security up to date is. Want juist nu zijn er denk ik meer mensen bereid tot het nemen van short cuts om te komen aan informatie. Waarom het wiel opnieuw uitvinden als je het ontwerp bij de concurrent zo kunt weghalen, omdat deze zijn security niet goed voor elkaar heeft? Dat scheelt kosten en daar let men nu juist extra sterk op!

Madison Gurkha voert per jaar tientallen ICT-beveiligingsaudits uit voor uiteenlopende organisaties: van verzekeraars tot banken, van pensioenfondsen tot de overheid en van technologiebedrijven tot internetwinkels. Al onze klanten hebben één ding gemeen: ze nemen ICT-beveiliging 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 ICT-beveiligingsrisico's daarom dus ook structureel onderzoeken door Madison Gurkha.

vervolg van pag. 5

Kinderspel
Het bleek een kwestie te zijn van het verbinden van beide laptops via een FireWire kabel en het draaien van wat programma's en scripts. Daarna was het kinderspel om de reeds opgestarte Windows machine binnen enkele seconden over te nemen. Winlockpwn, zo heet Adams tool, maakt het ondermeer mogelijk om gelockte Windows sessies te unlocken en om het Windows login scherm te omzeilen. Belangrijk om hierbij te vermelden is dat men wel in het bezit moet zijn van een bestaande gebruikersnaam op het aan te vallen systeem omdat alleen de wachtwoordcontrole wordt omzeild. Ondanks dat Adams code de stabiliteit heeft van een vroege alpha release, bleek deze uiteindelijk goed genoeg voor onze aanval. Een kijkje in de "Documents and Settings" map met het door de klant verstrekte testaccount gaf ons uiteindelijk de gebruikersnaam die we nodig hadden om in te kunnen loggen als administrator.

Suggesties
Hoewel we tijdens de hierboven beschreven aanval te maken hadden met een Windows versie die gevoelig was voor Winlockpwn zijn ook andere besturingssystemen in principe kwetsbaar voor dit type aanval. Een interessant detail hierbij is dat we nu eens niet te maken hebben met een bug in het besturingssysteem. Het is simpelweg de filosofie achter FireWire die de hack mogelijk maakt.
Nu zult u zich wellicht afvragen wat u tegen deze hack kunt doen. Hier een aantal suggesties. Zorg ervoor dat het besturingssysteem niet kan opstarten zonder het invoeren van een wachtwoord. Hiermee voorkomt u dat een reeds uitgeschakelde laptop, na het opnieuw inschakelen, kan worden aangevallen zonder tussenkomst van de eigenaar. Voor reeds opgestarte laptops ligt dit weer anders. Het simpelweg uitschakelen van de FireWire poort in het BIOS en het BIOS vervolgens beveiligen met een wachtwoord blijkt niet afdoende. Het BIOS valt in de meeste gevallen te resetten en ook losse PCMCIA FireWire kaarten blijken te werken. Dit laatste maakt zelfs dat laptops zonder een eigen FireWire aansluiting kwetsbaar zijn voor de hack. Het fysiek onklaar maken van de FireWire poort met behulp van wat epoxy hars biedt daarom ook geen soelaas. Wellicht is de beste oplossing nog wel het uitschakelen van de FireWire poort, PCMCIA adapter en de OHCI controller ondersteuning binnen het besturingssysteem zelf. Vervolgens dient u er natuurlijk wel voor te zorgen dat eindgebruikers deze wijzigingen niet ongedaan kunnen maken.

Flexwerkplekken
Wanneer dit alles om welke reden dan ook niet mogelijk is, zal men er dus zelf voor moeten zorgen dat er geen kwaadwillenden in de buurt van het apparaat kunnen komen. Dit geldt overigens niet alleen wanneer men op pad is want ook binnen de eigen vertrouwde kantooromgeving zijn er voldoende momenten waarop laptops gevaar lopen. Denk bijvoorbeeld maar aan vergaderingen, het ontvangen van bezoek en middagpauzes waarbij mensen hun laptop locken en deze vervolgens onbeheerd achterlaten. Mede door de invoering van flexwerkplekken worden deze risico's eigenlijk alleen maar groter omdat men steeds minder vaak in ruimtes werkt die afgesloten kunnen worden. Hierdoor wordt het ook voor collega's onderling steeds eenvoudiger om stiekem eens een kijkje op elkaars systeem te nemen, met alle gevolgen van dien.

In de rubriek "Het Inzicht" stellen wij meestal bepaalde technische beveiligingsproblemen aan de orde. Ditmaal beschrijft Tim Hemel echter geen specifiek technisch probleem, maar geeft hij antwoord op de vraag, hoe u zich het beste kan voorbereiden op een audit.

Het **voorbereiden** van een audit

Bij het plannen van een audit proberen wij zo duidelijk mogelijk aan onze klanten te communiceren wat de consultants van Madison Gurkha zoal nodig hebben om hun onderzoek goed te kunnen uitvoeren. In veel gevallen gaat dit probleemloos, maar soms zien we dat een aantal zaken niet geregeld zijn op het moment dat onze audit van start gaat.

Vaak worden deze zaken snel opgelost met een flinke dosis creativiteit en flexibiliteit om het onderzoek zoveel mogelijk waarde te geven in de tijd waarbinnen dit moet worden uitgevoerd. Tijd verliezen tijdens een audit is niet fijn voor onze klanten en voor onszelf frustrerend, aangezien wij aan ons werk het meeste plezier beleven als dit goed en efficiënt wordt uitgevoerd. Daarom bespreken we hier het belang van een aantal voorbereidingspunten.

Bij Madison Gurkha voeren we verschillende soorten audits uit: Black, Grey en Crystal Box op verschillende onderzoeksgebieden zoals infrastructuren of (maatwerk)(web)applicaties. Wat precies de verschillen zijn tussen deze audits, is te lezen in onze brochure en offertes. Per type audit geven we hier een checklist met aandachtspunten voor de voorbereiding.

Black Box Infrastructuur Audit

Bereikbaarheid van de systemen
Het komt wel eens voor dat systemen niet bereikbaar zijn. Bij het voorbereiden is het essentieel om te kijken waar de systemen zich bevinden en hoe deze te benaderen zijn: via het internet of alleen op de locatie zelf?

Netwerkaansluitingen
Wanneer een audit onsite plaatsvindt, moeten netwerkaansluitingen met bijbehorende IP-adressen geregeld worden, zodat wij onze laptops kunnen aansluiten om de scans uit te voeren. Dit gaat tegen menig security policy in, maar wij maken gebruik van gespecialiseerde tools die op onze laptops aanwezig zijn en niet op een standaard PC. Daarnaast is één van de doelen van een audit vaak om uit te vinden wat een aanvaller kan doen wanneer de security policy wordt omzeild. Uiteraard zorgen wij dat alleen de doelsystemen worden onderzocht en dat er zo min mogelijk verstoringen van de systemen optreden. Ons doel is immers het onderzoeken van de beveiliging van het systeem en niet het aanrichten van schade.

Firewalls die verkeer filteren
Indien het verkeer naar systemen verloopt via firewalls, dan zullen de scans op de systemen ook verlopen via deze firewalls. In dat geval wordt de totaalsituatie van het systeem en firewall getest. Wellicht was het de bedoeling om de beveiliging van het systeem zelf te testen. In dat geval beperken de firewalls de tests. Het is een goed idee hier rekening mee te houden.

IDS/IPS
Een soortgelijke opmerking is van toepassing op Intrusion Detection/Prevention Systemen (IDS/IPS). Onze scans genereren over het algemeen veel verkeer en een groot deel hiervan wordt door zo'n systeem gezien als kwaadaardig. De kans is dus groot dat er een vals alarm wordt gegenereerd of dat het systeem de toegang automatisch blokkeert. In beide gevallen kan dit de tests frustreren. Het liefst voeren wij scans uit zonder dat hier een IDS/IPS bij betrokken is, tenzij het natuurlijk de bedoeling van de test is om te kijken hoe snel er alarm geslagen wordt en of het IDS/IPS überhaupt goed functioneert.

IP-adressen van de targets
Uiteraard kan zonder targets geen scan worden uitgevoerd. Bij een infrastructuurscan zijn de IP-adressen van belang en wel op de adressen die voor de auditors bereikbaar zijn: het geven van interne IP-adressen wanneer vanaf het internet wordt gescand heeft weinig zin.

Crystal Box Infrastructuur Audit

De methode die bij een Crystal Box Infrastructuur Audit - in aanvulling op de Black Box aanpak - wordt toegepast is het inspecteren van systeemconfiguraties. Hierbij wordt eerst zoveel mogelijk informatie verzameld, die dan offline wordt geanalyseerd. Voor het verzamelen van deze informatie heeft Madison Gurkha tooling ontwikkeld, waarmee het onderzoek efficiënter kan verlopen en er dus meer onderzocht kan worden dan wanneer deze informatie handmatig moet worden verzameld.

Firewall configuraties
Voor het inspecteren van firewalls voldoen vaak de firewall regels die betrekking hebben op de doelsystemen. Het komt in de praktijk echter voor dat firewall regels op een andere plaats in de configuratie van toepassing blijken te zijn op de doelsystemen. Juist deze regels zorgen voor de beveiligingsproblemen en zijn dus wel degelijk van belang. Het liefst ontvangen wij de regels in een elektronische vorm waarop analyse tools kunnen worden toegepast. Een papieren uitdraai voldoet ook, maar is minder efficiënt.

Systeemtoegang/beheerder die scripts draait
Voor server-systemen heeft Madison Gurkha zogenaamde "checklist scripts", die zoveel mogelijk systeeminformatie verzamelen van een server. Deze scripts dienen als super user (bijvoorbeeld administrator of root) op het systeem te worden gedraaid. Meestal laten we dit door een beheerder doen. Deze kent de details van het systeem en na het inspecteren van ons script kan hij aanpassingen maken om te voorkomen dat het script tijd verspilt aan het verzamelen van informatie die niet van belang is. Na afloop van het script heeft de beheerder de gelegenheid om verzamelde informatie uit de uitvoer te verwijderen indien deze erg gevoelig is. Uiteraard gaan wij zorgvuldig om met deze informatie: opslag gebeurt op een versleutelde harde schijf en na gebruik wordt deze informatie veilig vernietigd.

Webapplicatie Audit (Black/Grey/Crystal)

Bereikbaarheid applicatie
Net als bij infrastructuur audits is ook de bereikbaarheid van de webapplicatie belangrijk. Kan de applicatie van buiten worden benaderd of alleen vanaf het interne netwerk? Zijn er firewalls of proxies die moeten worden geconfigureerd zodat de auditors de applicatie kunnen benaderen? Is er een IDS/IPS dat de tests zou kunnen beïnvloeden? Kortom, soortgelijke vragen als bij een infrastructuur audit.

Target URL
Zonder de URL van de applicatie kan weinig onderzocht worden. Deze URL moet uiteraard op te vragen zijn vanaf onze systemen die gebruikt worden voor het onderzoek.

Accounts: voor iedere rol twee
Om te testen op autorisatieproblemen in de applicatie, vragen we voor iedere rol binnen de applicatie twee accounts. Hiermee kan worden gecontroleerd of controles horizontaal (dezelfde rol, andere gebruiker) en verticaal (zelfde gebruiker, andere rol) geïmplementeerd zijn. Uiteraard is het aanwezig zijn van testdata ook belangrijk.

Proxies, integrated authentication
Wanneer vanaf een netwerk onsite moet worden getest, komen we wel eens een situatie tegen waarin gebruik wordt gemaakt van authenticatiemethodes (NTLM) die alleen beschikbaar zijn op de Windows netwerk PC's. Helaas ondersteunen een aantal van onze tools deze niet standaard en kan de applicatie niet worden getest vanaf onze laptops. In zo'n geval dient de testsoftware op een netwerk PC geïnstalleerd te worden. Ook dat is niet altijd mogelijk, in verband met security policies. Het is verstandig om na te gaan of hiervan sprake is en eventueel voorzieningen te treffen om de test te kunnen uitvoeren. In de praktijk komt dit zelden voor, maar het zou zonde zijn om een test te moeten afbreken om deze reden.

Stabiele applicatie, invloed van/op andere tests
Onze tests worden vaak voor een release uitgevoerd. Dit is een tijd waarin nog allerlei laatste kleinigheidjes worden opgelost en de applicatie dus wordt aangepast. In verband met het reproduceren van testresultaten is het belangrijk dat de applicatiecode zo min mogelijk wijzigt. Vaak is het nodig een test meerdere keren uit te voeren om de oorzaak te bepalen. Wanneer de applicatie tussendoor wijzigt, kunnen deze resultaten anders zijn en zien wij "onverklaarbare resultaten". Daarnaast is het soms zo dat andere tests gelijktijdig worden uitgevoerd op hetzelfde testsysteem. Indien gebruik wordt gemaakt van andere datasets, zitten de tests elkaar meestal niet in de weg.

Broncode (indien afgesproken)
Indien bij een applicatie audit ook broncode wordt bekeken, dient deze beschikbaar te zijn. Deze broncode analyseren we het liefst op onze eigen systemen. Uiteraard gelden hiervoor dezelfde regels als voor al onze klantendata: opslag op een versleutelde harde schijf en veilige vernietiging van de gegevens na gebruik.

Persoon beschikbaar voor vragen over broncode
Omdat broncode soms moeilijk te begrijpen is in de relatief korte tijd waarbinnen een audit wordt uitgevoerd, is het raadzaam een ontwikkelaar ter beschikking te hebben die vragen over de broncode kan beantwoorden. Deze persoon hoeft niet constant aanwezig te zijn, maar wanneer er vragen zijn is het fijn als de auditors deze persoon kunnen bereiken.

Overig

Vrijwaringen derde partijen
Strikt genomen is het onderzoeken van IT-beveiliging, zelfs in opdracht, strafbaar. Daarom voeren wij een onderzoek niet uit zonder dat hiervoor een vrijwaringsverklaring is getekend. Bij klanten is deze vrijwaring opgenomen in het contract, maar soms komt het voor dat de systemen die worden gescand eigendom zijn van een derde partij. In dat geval dient deze partij ook een vrijwaringsverklaring te tekenen. Dit is vaak een ingewikkeldere taak dan het lijkt. Ten eerste dient bekend te zijn wie de derde partijen zijn. Deze informatie kan alleen door de klant worden aangeleverd. Daarna moet de vrijwaring daadwerkelijk worden getekend. De meeste derde partijen hebben hiermee niet zo'n moeite, maar soms kost het meer tijd dan aanvankelijk werd gedacht. Om vervelende situaties te voorkomen helpt het om dit traject zo vroeg mogelijk te starten. Zie ook de column op pagina 2 voor meer informatie over de juridische aspecten van ons werk.

Hopelijk geven deze checklists meer inzicht in de wijze waarop Madison Gurkha haar onderzoeken zo goed mogelijk kan uitvoeren en kunnen ze bruikbaar zijn bij de voorbereiding van een audit die soepel, efficiënt en prettig verloopt. Deze checklist is niet volledig en in de praktijk zijn onze audits vaak toegespitst op een bepaalde situatie. Wanneer er specifieke vragen zijn over bovengenoemde zaken, aarzel dan vooral niet contact op te nemen: een goed voorbereide audit is voor iedereen belangrijk.

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.

De Black Hats Session VII staat alweer voor de deur. Daarom vonden wij het gepast om u een preview te geven van wat u allemaal kunt verwachten op 16 juni in Ede. Walter Belgers licht een tipje van de sluier voor u op.

Black Hats Session VII

Gehackt?! En wat nu?

Op dinsdag 16 juni houdt Madison Gurkha, in samenwerking met Array Seminars, weer een Black Hats Session. Het zal de zevende keer zijn dat dit seminar georganiseerd wordt. Wat ooit begon als een middag waarop consultants van Madison Gurkha hun kennis deelden, is uitgegroeid tot een dagvullend seminar met meerdere lezingen van externe sprekers en leveranciers.

Elke Black Hats Session heeft een eigen thema. De vorige keer stonden botnets en rootkits centraal, deze keer zullen dat incident response en IT forensics zijn. Daarbij proberen we de vraag te beantwoorden: "wat moet er gebeuren na een inbraak?"

Daartoe zal Walter Belgers (Madison Gurkha) laten zien hoe je met eenvoudige freeware tools een beperkt onderzoek kunt uitvoeren. Hierbij zullen ter plekke forensische gegevens verzameld worden. Arnoud Engelfriet (ICTRecht) zal ingaan op de huidige wetgeving rondom computercriminaliteit. Wanneer is een inbraak strafbaar? Hoe kan digitaal bewijs worden ingezet?

Na de lunch zullen Marnix Kaart en Erwin van Eijk (Nederlands Forensisch Instituut) dieper ingaan op de eisen waaraan digitaal bewijs moet voldoen om stand te kunnen houden in een rechtszaak. Ze zullen ook technieken laten zien om bewijsmateriaal van goede kwaliteit te verzamelen. Tot slot zal Roland Vergeer (Digital Intelligence) vertellen over een recent fraudeonderzoek en welke verrassingen daarbij optraden. De fouten die in dat onderzoek gemaakt zijn, kunt u zelf de volgende keer voor zijn. Zoals gezegd, zijn er naast deze vier lezingen, ook nog vendorsessies die door leveranciers worden ingevuld. Zo zullen Eddie Willems (Kaspersky) en Rolf van Gent (Netasq) beide een sessie verzorgen. Evenals Bernhard van der Feen (Microsoft) en Pete Herzog (Outpost24).

Het programma beslaat een hele dag. Registratie is mogelijk vanaf 8:30 en de laatste lezing is om 16:30 afgelopen, waarna een afsluitende borrel plaatsvindt. De Black Hats Session zal gehouden worden in congrescentrum De Reehorst in Ede. Aanmelden kan via de URL http://www.arrayseminars.nl/. Alle relaties van Madison Gurkha krijgen bovendien een korting bij aankoop van het toegangsbewijs. Wij hopen u op 16 juni te mogen begroeten in Ede tijdens de Black Hats Session VII.

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.

Vacatures

Madison Gurkha is een jonge, groeiende en veelbelovende organisatie op het gebied van (technische) IT security. Madison Gurkha levert kwalitatief zeer hoogwaardige diensten aan grotere organisaties zoals landelijke opererende overheidsinstellingen, (beursgenoteerde) multi-nationals en financiële instellingen.

Kijk voor meer informatie over de verschillende vacatures op onze website.

Door onze aanhoudende groei zijn wij dringend op zoek naar:
→ Junior Security Consultant (JSC)
→ Security Consultant (SC)
→ Senior Security Consultant (SSC)

Kandidaten met aantoonbare security kennis van Microsoft producten en technologieën hebben op dit moment onze voorkeur.

Ben jij degene die we zoeken?
Stuur dan snel je CV met sollicitatiebrief naar hrm@madison-gurkha.com.

16 juni 2009
Black Hats Sessies VII, Ede
www.madison-gurkha.com
Deze zevende editie van de welbekende Black Hats Sessies wordt georganiseerd door Array Seminars en Madison Gurkha en staat volledig in het teken van Incident Response & IT forensics. Ging het programma van de vorige editie in op de duistere en criminele kant van het Hacken: HACKING FOR PROFIT, deze keer gaan we in op de gevolgen: GEHACKT! En wat nu? Kijk voor het complete programma op onze website.

18 t/m 26 juni 2009
Klassikale training Secure Programming, Veenendaal
www.madison-gurkha.com
Op 18 en 26 juni geeft Madison Gurkha weer een klassikale variant van onze gerenommeerde Secure Programming training. Kijk voor meer informatie op onze site en schrijf snel in.

13 t/m 16 augustus 2009
Hacking At Random, Vierhouten
http://har2009.org/
Van 13 tot 16 augustus 2009 is er weer een hacker camp gepland, ditmaal zal het evenement in Vierhouten plaatsvinden. Hacking at Random (HAR) belooft een vier dagen durend feest van onder andere "technoanarchisme", ideologische debatten en hands-on tinkering te worden. Madison Gurkha is tevens een trotse sponsor van dit evenement. Voor degene die geïnteresseerd zijn: de "call for papers" staat nog open.

7 t/m 8 september 2009
FRHACK, Besançon
www.frhack.org/
FRHACK is de eerste internationale IT security conferentie door hackers, voor hackers in Frankrijk. De conferentie zal gehouden worden in Besançon, een plaats nabij de Zwitserse grens. FRHACK is niet commercieel, maar juist uiterst technisch van aard. De conferentie is bedoeld voor iedereen die te maken heeft met IT security (van security officers tot software ontwikkelaars). FRHACK is erop gericht om de industrie, overheid, academici en hackers bij elkaar te brengen voor kennisdeling omtrent IT security en alles wat daaraan is gerelateerd. FRHACK zal zowel nationale als internationale sprekers aan het woord laten, allemaal met uiteenlopende vaardigheden en specialismen.

Redactie
Marnix Aarts
Walter Belgers
Tim Hemel
Jan Hendrikx
Remco Huisman
Frans Kollée
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.

DINSDAG 16 JUNI 2009 – DE REEHORST EDE

BLACK HATS SESSION PART VII

GEHACKT?

INCIDENT RESPONSE & IT FORENSICS

MET SPREKERS: WALTER BELGERS - MADISON GURKHA › ROLAND VERGEER - DIGITAL INTELLIGENCE › ARNOUD ENGELFRIET - ICTRECHT › MARNIX KAART EN ERWIN VAN EIJK - NEDERLANDS FORENSISCH INSTITUUT


Walter Belgers


Roland Vergeer


Arnoud Engelfriet


Marnix Kaart


Erwin van Eijk

Deze zevende editie van de welbekende Black Hats sessies wordt georganiseerd door Array Seminars en Madison Gurkha en staat volledig in het teken van Incident Response & IT Forensics.

Ging het programma van de vorige editie in op de duistere en criminele kant van het Hacken: HACKING FOR PROFIT, deze keer gaan we in op gevolgen: GEHACKT! En wat nu?

Het wordt CSI Ede op 16 juni. Walter Belgers van Madison Gurkha zal een presentatie geven over incident response "light". Hoe kunt u eenvoudig incident response onderzoek doen met freeware tools? Roland Vergeer (Digital Intelligence) geeft een mooi voorbeeld uit de praktijk over een forensisch onderzoek naar een interne fraude (die niet intern bleek te zijn), Arnoud Engelfriet (ICTRecht) gaat in op bewijsvoering in een rechtszaak, wat de criteria zijn voor computervredebreuk of denial-of-service en wat er dus nodig is om een aangifte te kunnen doen of een civiele zaak om schadevergoeding te kunnen beginnen. Het Nederlands Forensisch Instituut zal een lezing over forensisch onderzoek geven.

BESTEMD VOOR Ú

De bijeenkomst wordt georganiseerd voor beheerders van systemen, netwerken en applicaties, security officers, interne auditors en andere geïnteresseerden. Na dit seminar heeft u geleerd hoe u zelf eenvoudig incident response kunt doen en wat er bij een volledig forensisch onderzoek komt kijken. Ook leert u waar u aan moet denken als u een onderzoek voor de rechter wilt brengen.

PROGRAMMA DINSDAG 16 JUNI 2009

09.30 Opening door de dagvoorzitter

09.50 Incident response "light"
Walter Belgers, Madison Gurkha
Een systeem gedraagt zich raar. Er komen meldingen van derden over inbraakpogingen. Wat zou er aan de hand zijn? In deze lezing zullen simpele (freeware) tools de revue passeren, waarmee incident response kan worden gedaan. Hoe is de aanval in zijn werk gegaan? Welke sporen vind ik nog op de disk of in het geheugen? Zijn er rootkits achtergebleven? Een "light" onderzoek probeert antwoorden op die vragen te vinden maar heeft niet als doel een uitgebreid forensisch onderzoek te doen.

10.50 Pauze en informatiemarkt

11.10 Opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk
Arnoud Engelfriet, ICTRecht
Hacks en cracks worden steeds subtieler, maar de wet is en blijft een bot instrument. De Wet Computercriminaliteit is in 2006 grondig herzien, waarbij met name de regels rond virussen en DDoS-aanvallen aangescherpt zijn. Ook het meesurfen bij de buren is nu vaak strafbaar, hoewel nog niet duidelijk is wanneer nu precies. Maar voordat we weten of een XSS exploit nu "binnendringen in een geautomatiseerd werk is", zijn er nog wel een paar proefprocessen nodig. Wat houden die wetten en regels nu in? Hoe kan digitaal bewijs daarbij worden ingezet? En hoe voorkom je dat jij het proefproces wordt?

12.10 Vendorsessies

12.40 Lunch en informatiemarkt

13.40 Forensisch onderzoek in hacking zaken
ir. Marnix Kaart en ir. Erwin van Eijk CISSP, Nederlands Forensisch Instituut
Het NFI krijgt regelmatig het verzoek onderzoek te doen in zaken die betrekking hebben op hacking of pogingen daartoe. Meer dan eens is het aangeleverde materiaal van matige kwaliteit en dit heeft over het algemeen een negatieve invloed op de bewijswaarde. Voorbeelden hiervan zijn het ontbreken van een goede audittrail, gebrek aan mogelijkheden tot integriteitscontrole van aangeleverde logbestanden, onduidelijkheid over de betrouwbaarheid van datum- en tijdsinstellingen, onvolledige informatie met betrekking tot de aanwezige infrastructuur, etc. Deze presentatie beoogt de toehoorders meer inzicht te geven in randvoorwaarden waar bewijsmateriaal aan dient te voldoen. Ook worden er enkele praktische methoden en technieken gedemonstreerd waarmee bewijsmateriaal van goede kwaliteit verzameld kan worden ten tijde van een incident. De nadruk zal hierbij liggen op het vastleggen van netwerkverkeer en geheugenacquisitie. Er wordt uitgelegd op welke wijze dit materiaal een bijdrage kan leveren aan het forensisch onderzoek.

14.40 Vendorsessies

15.10 Pauze en informatiemarkt

15.30 Digitale criminelen gesnapt
Roland Vergeer, Digital Intelligence
Bij cybercrime is niets wat het lijkt. Een eenvoudig geval van interne fraude kan uiteindelijk uitmonden in een onderzoek, waarbij meerdere organisaties gecompromitteerd blijken te zijn. Aan de hand van een recente zaak laat Roland Vergeer zien hoe een digitaal forensisch onderzoek verloopt, en welke verrassingen de onderzoeker en zijn opdrachtgever kunnen tegenkomen. Aan bod komen onder andere de werkwijze van hackers, de gebruikte onderzoeksmethodiek, en gemaakte fouten bij beide partijen.

Array SEMINARS

Madison Gurkha Your Security is Our Business

Sponsor: TSTC TSHUKUDU TECHNOLOGY COLLEGE