

UPDATE

WWW.MADISON-GURKHA.COM

.....

DE COLUMN **2**

Walter Belgers

HET NIEUWS

Gebruik virtualisatie bij penetratietesten **3**

Jan Hendrixx **3**

Sponsoring kinderopvang Nepal **5**

DE KLANT **4**

Uit de industrie

HET INTERVIEW **6**

Han Fey

HET INZICHT **7**

Zijn SSL websites nog te vertrouwen?

DE HACK **8-9**

Herinner mij - Gebruikersgemak
geeft aanvalsmogelijkheid

HET VERSLAG **10-11**

Chaos Communication Congress

DE AGENDA **11**

HET COLOFON **11**

.....



Ethisch Hacken

Mensen vragen mij wel eens wat ik voor werk doe. Als mensen echt geïnteresseerd zijn vertel ik ze over al puzzelend applicaties onderzoeken, over cursussen security awareness geven, over gebouwen proberen binnen te lopen en forensisch onderzoek doen op gehackte systemen. Maar soms weet je al dat de vragensteller een kort antwoord verwacht. Dan vertel ik dat ik "ethisch hacker" ben.

Hoewel dat de lading niet helemaal dekt, bevat het toch wel twee kernpunten uit ons werk. Allereerst "hacker". Ik bedoel dat in de originele betekenis. Tegenwoordig worden criminele computervandalen "hackers" genoemd, maar de term heeft van origine niets met criminele activiteiten te maken. Het ontstond in de jaren '60 op het Massachusetts Institute of Technology (MIT) en een hacker was daar "iemand" die er plezier aan beleefde om de details te begrijpen van programmeerbare systemen en hun mogelijkheden op te rekken. Dit in tegenstelling tot normale gebruikers die alleen het minimale willen leren. Een hacker heeft dus een onderzoekende geest en een creatieve instelling.

Dat zijn precies de mensen die bij Madison Gurkha werken. Standaard programma's gebruiken die kwetsbaarheden in websites opsporen kan iedereen, dat is een kwestie van de juiste knopjes indrukken. Wij gebruiken dat soort programma's ook. Maar daarna komt het interpreteren van de resultaten en, nog belangrijker, het uitvoeren van aanvullend onderzoek door precies uit te vinden hoe het systeem werkt en waar de zwaktes zitten. En dat is precies "de details begrijpen" en "de mogelijkheden oprekken" zodat die mogelijkheden, die eigenlijk niet gewenst zijn, aan het licht komen. Zoals de mogelijkheid geld van andermans rekening over te maken in een e-banking applicatie.

Een hacker ben je of je bent het niet. Je herkent ze gemakkelijk. Kent u in uw omgeving iemand die zijn nieuwe laptop na aankoop onmiddellijk helemaal uit elkaar haalt om te zien wat erin zit? Die probeert uit te vinden welke knopjes je tegelijk moet indrukken in de auto om de geheime menu's te krijgen op de boordcomputer? Een hacker.

Zoals ik al zei, hebben veel mensen bij het horen van het woord "hacker" associaties met iets crimineels. Vandaar dat we duidelijk maken dat we niet zomaar hacken, maar ethisch hacken. Die ethiek vind je op meerdere plekken terug. Computerinbraak is strafbaar, daar is de wet heel duidelijk over. De tweede wet computercriminaliteit is daarin weer wat strenger geworden, hoewel de maximale straf gelijk is gebleven met vier jaar gevangenisstraf. Het werk dat wij verrichten valt onder die wet. Vandaar dat wij heel secuur te werk gaan om voor elke opdracht heel goed duidelijk te krijgen wat er binnen de opdracht valt, wie de eigenaar is van de systemen of netwerken en daar dan ook een vrijwaring van te ontvangen. Alleen als wij een vrijwaring hebben is wat we doen legaal.

Deze ethiek in ons werk is eigenlijk heel logisch. Er zijn



wetten die computerinbraken strafbaar stellen, dus hebben we een goedkeuring nodig om dat te kunnen doen. Maar onze ethiek gaat verder dan wat in de wet staat. Is het u al opgevallen dat we op onze website geen namen van klanten noemen? Ook dat is ethiek. Als klant wilt u niet onnodig aandacht vestigen op wat u aan beveiliging doet. Wij begrijpen dat, dus we zullen die namen niet zomaar publiceren, zelfs als dat commercieel interessant voor ons zou zijn. Voor ons is dat een tweede natuur.

Toch lees ik nog te vaak verhalen in de krant over mensen die deze ethiek er blijkbaar niet op na houden. Nog niet zo lang geleden werd de mailbox van een staatssecretaris gekraakt. Dit gebeurde in opdracht van een tijdschrift en werd uitgevoerd door iemand die zichzelf ethisch hacker noemde. Hij bouwde een "Trojan Horse" programma waarmee hij 14.000 systemen infecteerde en zo een "Botnet" creëerde. Hiermee kraakte hij het wachtwoord, door gewoon maar miljoenen mogelijke wachtwoorden te proberen. De ethiek is hier ver te zoeken. Er is illegaal ingebroken op 14.000 systemen. De dader kan vier jaar de cel in verdwijnen voor zijn daad. Hij vertelde er in het artikel nog eens bij dat hij wel eens onbeveiligde draadloze netwerken opspoorde en dan de desktop achtergrond van de systemen aanpast met reclame voor zijn bedrijf ("u heeft een beveiligingsprobleem, bel ons!").

Is het u al opgevallen dat wij nooit bellen nadat een lek is vastgesteld? Wij vinden het onethisch om ongevraagd de beveiliging te controleren met als doel de verkoop van onze diensten, nog even afgezien van de vraag in hoeverre je dat kunt zonder overtreding van de wet (het voorbeeld van de draadloze netwerken hierboven is een duidelijk geval van illegale praktijken). Maar ook als u onverhoopt in het nieuws komt door een beveiligingslek, zullen wij u niet bellen. Wij vinden dat ongepast. We hebben u graag als klant, maar dan omdat u onze kwaliteit kent en waardeert waardoor u het initiatief neemt om ons te bellen.

Walter Belgers
Partner, Principal Security Consultant

Gebruik virtualisatie bij penetratietesten

-SAMENVATTING-

In eerste instantie lijken de begrippen virtualisatie en penetratietesten wellicht weinig met elkaar te maken hebben. Toch blijken ze tegenwoordig meer en meer met elkaar verbonden te worden. Vooral omdat virtualisatie het hectische leven van iemand die de technische beveiliging van ICT-systemen moet beoordelen een stukje aangenaamer kan maken.

Door middel van virtualisatie wordt het met de huidige beschikbare hardware mogelijk om meerdere omgevingen (bijvoorbeeld besturingssystemen, maar ook de applicaties die gebruikmaken van besturingssystemen) gelijktijdig aan te spreken. De systemen waarover dit artikel gaat, zijn de huidige generatie laptops en software die daarvoor beschikbaar is. In de meeste gevallen wordt gebruik gemaakt van de Intel architectuur en draaien de virtuele omgevingen, weliswaar netjes gescheiden van elkaar, met bijna dezelfde snelheid als wanneer ze zelf direct van de hardware gebruik zouden maken.



Noodzakelijk is het gebruik van virtualisatie natuurlijk niet. Maar handig is virtualisatie wel! Vooral als de tools die je gebruikt of moet gebruiken niet alleen beschikbaar zijn, of in veel gevallen "juist niet" beschikbaar zijn, onder een van de Microsoft besturingssystemen. Om de belangrijkste tools onder handbereik te hebben (en liefst gelijktijdig te kunnen gebruiken) tijdens een penetratietest, zouden we dus zowel een Windows systeem als een Linux systeem en – in bepaalde gevallen – ook nog een *BSD en/of OSX ter beschikking moeten hebben. Door middel van virtualisatie kan een laptop al deze omgevingen bevatten en, wanneer nodig, beschikbaar stellen. In veel gevallen (als de apparatuur krachtig genoeg is) zelfs gelijktijdig. Vroeger werkten we vooral met multi-boot systemen. Door op de schijf bijvoorbeeld Linux, OpenBSD en Windows te installeren, konden we toch gebruikmaken van alle tools,

maar kostte het wel regelmatig een reboot van het volledige systeem. Het gebruik van virtuele omgevingen maakt reboorten overbodig en zorgt ervoor dat een beveiligingsspecialist veel efficiënter kan werken.

Ook bij het geven van demonstraties kan virtualisatie van pas komen. Het komt regelmatig voor dat ik een lezing moet houden waarbij het publiek door middel van een live demonstratie van bepaalde methoden en technieken veel sneller en duidelijker begrijpt waar het werkelijk om draait dan wanneer ik het tracht uitteleggen aan de hand van tientallen Powerpoint, of liever Keynote, slides. Hierdoor wordt het wisselen tussen demonstratie en presentatie ook eenvoudiger omdat er geen beamer gewisseld moet worden.

Volgens de wet Computercriminaliteit 2 is hacken strafbaar. Hierdoor wordt het natuurlijk erg lastig voor iedereen, zowel studenten als specialisten, die interesse heeft in het testen en kunnen beoordelen van de technische beveiliging van ICT-systemen om tools uit te proberen en te leren gebruiken. Hierdoor ontstaat er al snel de behoefte aan een LAB. Een omgeving waarin verschillende configuraties eenvoudig kunnen worden opgebouwd om daarna gebruikt te worden als "target-practice". Virtualisatie in combinatie met Live CDROMs, biedt ook hier uitkomst. Dit levert een aanzienlijke besparing op voor wat betreft hardwarekosten, terwijl de beschikbare (krachtigere) hardware ook efficiënter wordt ingezet.

Aan virtualisatie dienen natuurlijk ook een aantal beveiligingseisen te worden gesteld. Eén van de meest in het oog springende zal zijn dat de ene omgeving op geen enkele manier een andere omgeving direct mag beïnvloeden.

Hans (J.C.G.) van de Looy
Partner, Principal Security Consultant

Bron: Informatiebeveiliging nummer 7, november 2008

Jan Hendrikx



Mag ik me even voorstellen? Ik ben Jan Hendrikx, 32 jaar en sinds 1 januari jl. werkzaam als Security Consultant bij Madison Gurkha. Na een aantal jaar werkzaam te zijn geweest als Risk & Control officer bij een multinational, ben ik opzoek gegaan naar een andere baan met meer technische diepgang. Iets dat ik steeds meer begon te missen omdat ik me meer en meer met security management bezig moest gaan houden en steeds minder met de techniek. Toevallig kwam ik op het Internet een vacature tegen van het bedrijf waar ik tijdens mijn vorige baan een auditrapport van had gelezen. Juist ja, Madison Gurkha. Destijds had ik tijdens het lezen van het auditrapport al zoiets van: "Dat werk lijkt me nu echt iets voor mij!" In mijn vrije tijd houd ik me natuurlijk bezig met computers en alles wat daarmee te maken heeft. Met name FreeBSD vind ik een erg interessant besturingssysteem om dingen mee te doen. Die interesse is begonnen tijdens mijn opleiding Hogere Informatica aan Fontys Hogescholen. Maar er is meer in het leven. Zo ben ik bijvoorbeeld ook een groot muzikieliefhebber. In het verleden heb ik daarom ook een opleiding afgerond aan het Koninklijk Conservatorium. Niet dat ik daar momenteel nog erg veel mee doe maar ik vind het prettig om een bredere achtergrond en interesse te hebben dan alleen maar techniek.

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!



In welke branche is uw organisatie actief?

In de industrie branche.

Hoeveel mensen houden zich in uw bedrijf bezig met informatiebeveiliging?

In totaal houden er 8 mensen binnen dit bedrijf zich bezig met informatiebeveiliging.

Wat is uw functie?

Ik ben Information security specialist. Samen met mijn collega's ben ik verantwoordelijk voor het opstellen van richtlijnen en het uitvoeren van risicoanalyses binnen ons bedrijf.

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

Naast doorzettingsvermogen, geduld en overredingskracht moet je goed een probleem kunnen analyseren en moet je klantgericht zijn. Daarnaast moet je ook helder en duidelijk kunnen communiceren. Deze vaardigheden gecombineerd met een goede kennis van informatiebeveiliging en risicomanagement zijn vereist voor de functie van informatiebeveiliging.

Heeft u hiervoor een specifieke opleiding genoten?

Ik heb hier geen specifieke opleiding voor genoten, mijn vooropleiding is TH Wiskunde. Daarnaast heb ik het vak in de praktijk geleerd (training on the job).

Wat is volgens u het belangrijkste aspect van informatiebeveiliging?

De mens is toch wel het belangrijkste aspect van informatiebeveiliging. Je kunt namelijk

nog zoveel technische maatregelen treffen om informatiebeveiliging op een hoger niveau te brengen, mensen kunnen het altijd omzeilen. Er is dus bewustzijn nodig anders komt er niets terecht van informatiebeveiliging en wordt het ook niet serieus genomen.

Hoe is uw belangstelling voor informatiebeveiliging ontstaan?

Ik heb nooit echte specifieke belangstelling gehad voor het vak. Ik ben op een gegeven moment een vacature tegengekomen met betrekking tot informatiebeveiliging, deze leek me interessant en ik ben er dus zodoende ingerold.

Wat vindt u het leukste aan uw functie?

Het leukste aan mijn functie is, dat ik me overal mee mag bemoeien en dus zo overal binnen onze organisatie kom. Zodoende krijg ik ook met verschillende mensen te maken.

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

Mensen overtuigen van het nut van security maatregelen blijft het meest uitdagende probleem. Dat is iedere keer anders en er

worden ook steeds weer nieuwe tegenargumenten bedacht. Het is hierbij de uitdaging om niet rigide te zijn (dan kan niemand meer werken) en ook niet te flexibel (dan staat alles open), maar om een goede mix te kiezen zodanig dat onnodige risico's voor de organisatie worden voorkomen.

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

Ik draaf hier gelukkig niet erg in door, maar mijn thuisverbinding is bijvoorbeeld wel netjes encrypted. En ook tijdens het browsen op internet let ik erop dat ik niet overal op klik.

Hoe helpt Madison Gurkha daarbij?

Madison Gurkha doet voor ons met name Security Audits op applicatie niveau. Dus telkens als wij een nieuwe applicatie hebben, laten we deze testen door Madison Gurkha.

Wat zijn uw ervaringen met Madison Gurkha?

Ik heb goede ervaringen met Madison Gurkha en we hebben een prettige samenwerking.

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.

Madison Gurkha heeft een geldbedrag gedoneerd aan Stichting Veldwerk om te besteden aan de bouw van een kinderopvang in de Kathmandu vallei in Nepal.



foto Michelle Peeters - www.deuxbleus.nl

Madison Gurkha sponsort kinderopvang Nepal

De stichting, opgericht door Nederlander René Veldt, voert allerlei projecten uit in Nepal die de lokale bevolking steunen. Het opvanghuis, waar 45 kinderen kunnen worden opgevangen, is er daar een van. De stichting richt zich op het verbeteren van de leefomstandigheden van gehandicapten, kinderen en vrouwen. Kasteloze (wees)kinderen hebben namelijk nauwelijks een toekomst in Nepal. Ook is er veel sterfte onder vrouwen door slechte omstandigheden tijdens bevallingen. Daardoor sterven er in Nepal ongeveer 4 vrouwen per dag.

Madison Gurkha kwam in aanraking met de stichting doordat partner en Principal Security Consultant Walter Belgers in november meewerkte als vrijwilliger. Hij hielp mee om in de bergen van Nepal te bouwen aan een gemeenschapscentrum. Dit centrum is er één van zes die gebouwd worden om dienst te zullen doen als onder andere kinderopvang en EHBO-centrum. Hier kunnen ook vrouwen op hygiënische wijze bevallen. De bouw van deze gemeenschapscentra is eveneens een initiatief van Stichting Veldwerk.

Walter over zijn ervaring: "De mensen in de binnenlanden van Nepal zagen er gelukkig en gezond uit, ondanks het harde werken. Ze zijn allemaal zelfvoorzienend met eigen rijst- en

aardappelvelden. Stroom of gereedschappen zijn er niet. Echter, als iemand een been breekt, kan er niets gedaan worden: om in een ziekenhuis te komen moet er drie uur door de bergen gelopen worden en dan nog een paar uur liftend naar de stad gereden. Mensen kunnen en willen dat niet, met als gevolg dat zelfs een beenbreuk al fataal kan worden."

Inmiddels zijn vijf van de zes gemeenschaps-huizen afgebouwd. Deze zullen draaiende worden gehouden door de lokale bevolking: de stichting probeert alles zo snel mogelijk over te dragen.

Het project dat door Madison Gurkha gesponsord wordt, houdt zich bezig met de opvang van kasteloze weeskinderen. Hoewel het kastensysteem wettelijk niet meer bestaat in Nepal, is het er in de praktijk nog wel. Een kasteloos kind mag niet het huis binnengaan van iemand die wel tot een kaste behoort. De kansen voor een kasteloos kind zijn minimaal, zeker als het ook nog gehandicapt is. Deze kinderen moeten leven van de straat en eindigen vaak in de goot.

Walter vertelt: "In Kathmandu zagen we inderdaad jongeren op straat die verstoten waren en alleen nog maar op de been bleven door lijm te snuiven. Het is triest om te zien.

De Nepalezen bekommeren zich niet om deze kinderen, terwijl ze met relatief weinig middelen verder geholpen kunnen worden." Het opvanghuis van Stichting Veldwerk voorziet hierin. De kinderen krijgen opvang en les. Ook biedt het huis plek aan vrouwen die er kunnen leren naaien. Hiermee kunnen ze (eventueel met een microkrediet) een eigen winkel beginnen. Ook wordt, op het bijbehorende land, geleerd hoe men winstgevend gewassen kan verbouwen.

Toen Walter dit project in november bezocht, was men bezig de laatste hand te leggen aan het grootste gebouw, het project bestaat uit meerdere gebouwen. Het idee is om een soort zelfvoorzienend dorp te maken, genaamd Hamro Gaun. Met behulp van een kleine waterkrachtcentrale wordt stroom opgewekt voor LED-verlichting. De akkers leveren voedsel voor de inwoners.

Kinderen met potentieel kunnen later worden gesponsord om een opleiding te volgen. Zo kunnen deze kinderen in de toekomst volwaardig meedraaien in de Nepalese maatschappij.

Wilt u Stichting Veldwerk ook sponsoren, kijkt u dan op <http://www.stichting-veldwerk.org/>.



Han Fey

in dit slot zitten acht draaiende magneten die in een goede stand moeten worden gezet.

Naast mechanische sloten zie je ook steeds vaker elektronische sloten. Hebben mechanische sloten hun langste tijd gehad?

Wat we zien is dat het kraken van een elektronisch slot moeilijker is dan het kraken van een mechanisch slot, waardoor aanvallers zich meestal op het mechanische gedeelte dat ook in elk elektronisch slot zit concentreren. Door een extern aangebrachte trilling of magnetisch veld kan mogelijk iets in het slot worden bediend waardoor het open zou kunnen gaan. Meerdere sloten hebben hier last van gehad. Zoals het een goede fabrikant betaamt, wordt het slot meteen aangepast zodat het dan ook weer beschermd is tegen die aanvallen.

Wat is jouw indruk van het gemiddelde bedrijf: wordt daar voldoende aandacht aan de sloten besteed?

Beveiliging is vaak een sluitpost binnen bedrijven. Het is één van de dingen waar "onzichtbaar" op kan worden bezuinigd, zo is de gedachte van veel facility managers. Een veilige organisatie krijg je pas als je gebruik maakt van het zogenaamde "preventiewiel". Het preventiewiel wordt gevormd door 4 kwadranten (beleid, organisatie, voorzieningen en cultuur) die evenwichtig en onlosmakelijk met elkaar zijn verbonden. Naast "voorzieningen" (waaronder sloten vallen), zijn die andere drie kwadranten ook belangrijk.

In de softwarewereld zie je dat dezelfde programmeerfouten steeds weer opnieuw gemaakt worden. Is dat bij sloten ook zo?

Helaas is het zo dat fabrikanten grote investeringen hebben gedaan in machines die maar een bepaald soort product kunnen maken. Daarom wordt een nieuw slot meestal ontwikkeld binnen randvoorwaarden van die machines. Grote veranderingen zijn meestal niet mogelijk in de lopende productie. We hebben wel eens een fout in een slot aangetroffen waardoor een aanvaller een speciaal werktuigje, een "kam", kon gebruiken om alle pinnen uit de kern van het cilinderslot te duwen, waardoor de kern kan draaien en het slot opent. Door langere pinnen in het cilinderhuis te plaatsen, kon deze openingstechniek worden voorkomen. Fabrikanten zijn dus nog

wel geneigd een dergelijk verbetering door te voeren. Omdat nieuwe slotenontwikkelaars vaak niet bekend zijn met deze kamtechniek, komt deze fout keer op keer weer voor bij de verschillende slotenfabrikanten.

Je kunt een productiefout dus niet zomaar repareren als de sloten al verkocht zijn. Doen slotenfabrikanten extra moeite om hun sloten vooraf te testen?

We zien dat slotenfabrikanten steeds meer "hobbyisten" loslaten op hun slot in een vroegtijdig stadium van de productie. We krijgen dan de vraag of wij het reeds ontwikkelde product willen testen op manipulatie. Wordt er iets gevonden, dan wordt dit direct teruggekoppeld naar de fabrikant die dan een verbeterde versie ontwikkeld, voordat het op de markt wordt gebracht.

Open Standaarden zorgen voor uitwisselbaarheid. Is er in de slotenwereld ook sprake van "Open Source"?

Een van de redenen waarom ik sloten verzamel is de verschillende technieken in deze sloten. Ieder land gebruikt zijn eigen type cilinder, we hebben bijvoorbeeld Scandinavia Oval en Round, Europrofiel, Mortise, Rim, Deadbolt cilinders, etc. Ook wat er in het slot zit, verschilt nogal. Elke fabrikant heeft zo zijn specialiteit qua gebruikte technieken. Indien een fabrikant een nieuwe techniek patenteert, heeft hij 15 jaar alleenrecht op het gebruik van deze techniek. Marketingtechnisch en verkooptechnisch wordt dan alles uit de kast gehaald om het product in die periode te verkopen en te promoten. Na die 15 jaar mag iedereen deze techniek gebruiken omdat het patent dan verlopen is. In mijn verzameling heb ik sloten, waarin technieken zitten van andere fabrikanten van wie het patent is verlopen. Een voorbeeld daarvan is het DOM-ix systeem. Nadat het patent verlopen is, maakt de Spaanse fabrikant STS in licentie nog steeds dezelfde sloten. Maar in principe is het dus een bedrijfstak met nauwelijks open standaarden.

.....
**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.**

Kun je in het kort vertellen wie je bent?

Mijn naam is Han Fey en ik heb een bijzonder uitgebreide verzameling van meer dan 3000 verschillende sloten. Met mijn achtergrond in werktuigbouwkunde kijk ik graag naar verbeteringspunten in mechanische producten dus ook in hang- en sluitwerk. Het kijken naar verbeteringen brengt automatisch met zich mee dat je ook kijkt naar zwakke punten.

Bij software is het heel lastig om te zien hoe veilig het is. Hoe zit dat met sloten?

Met sloten is het ongeveer hetzelfde. Het duurste slot hoeft niet per definitie het beste slot te zijn. Bij sloten zijn er wel keurmerken zoals het SKG-keurmerk. Bij deze keuring gebruikt men alleen vaste testpatronen en een vaste gereedschapskoffer. Het kennisniveau van de gemiddelde mens is zo toegenomen door internet, dat er door de creativiteit van mensen geheel nieuwe aanvalsmethoden ontstaan waar niet op wordt getest. Commerciële belangen in productiemachines en verhoging van kosten van het eindproduct en advertentiecampagnes maken dat veel fabrikanten niet mee willen doen aan deze wapenwedloop. Maar, je moet je ook afvragen hoeveel beveiliging je eigenlijk nodig hebt.

Wat vind je het veiligste slot en waarom?

Puur alleen naar mechanische cilinder gekeken, zijn er verschillende merken die goed aan de vwg timmeren. Het veiligste slot van nu, hoeft morgen niet meer het veiligste slot te zijn. Als ik als voorbeeld de Abloy Protec neem, dan is dat naar mijn mening een van de veiligste en meest flexibele sloten. Heel veilige sloten oefenen wel aantrekkingskracht uit op fanaten uit heel de wereld die proberen de beveiliging te omzeilen. Er is altijd wel een slimme geest die een zwakke plek vindt en via internet wordt deze kennis snel verspreid. Een andere veilige cilinder is de EVVA MCS,

Zijn SSL websites nog te vertrouwen?

Banken, verzekeringen, webwinkels en extranetten maken allemaal gebruik van verbindingen die met SSL worden beveiligd. Deze is, vertrouwend op de controle door de webbrowser, in staat om te bepalen of de gebruiker een versleutelde verbinding heeft met de beoogde server en niet met een malafide nagebootste website. Het gebruik hiervan wekt vertrouwen bij de gebruikers.

Tijdens het 25e Chaos Communication Congress (25C3) afgelopen december 2008 (zie "Het Verslag" op pagina 10), werd er door een internationale groep onderzoekers een presentatie gegeven van een MD5 aanval. Het was een vervolg op de MD5 collision¹ onderzoeken van voorgaande jaren. Het doelwit was de op MD5 gebaseerde certificaten die veelal worden gebruikt door SSL webserver (HTTPS protocol).

In voorgaande jaren was het al gelukt om meerdere verschillende documenten te maken waarbij de cryptografische MD5 hashes hetzelfde waren. Hierdoor was aangetoond dat MD5 voor de toekomst beter niet meer gebruikt kon worden voor het verifiëren van elektronische documenten, waaronder ook certificaten die door SSL webserver worden gebruikt.

De aanval is niet gericht op de SSL webserver zelf, maar maakt gebruik van een kwetsbaarheid in de Public Key Infrastructuur (PKI). In theorie zijn dan ook andere toepassingen waarbij gebruik wordt gemaakt van PKI kwetsbaar. In het geval van het gebruik van certificaten bij SSL webserver, is de aanval mogelijk doordat de meeste webbrowser de controle van de certificaten uitvoeren zoals die door de webserver worden gepresenteerd. De uitslag van de webbrowser is positief indien aan een aantal voorwaarden is voldaan.

Een van deze voorwaarden is dat het certificaat betrouwbaar is. Dit wordt nagegaan door de in het certificaat genoemde naam van de webserver en de elektronische handtekening waarmee het certificaat is ondertekend te controleren. De ondertekening van certificaten kan door middel van een hiërarchie, waarbij er een of meerdere tussenliggende Certificate Authority's (CA) ondertekenen. Door het volgen van deze ketting van tussenliggende certificaten, wordt uiteindelijk de laatste ondertekening gedaan door één "Root CA". De meeste webbrowser zijn voorzien van de benodigde "Root CA" certificaten zodat de uiteindelijke ondertekening kan worden geverifieerd. Alleen indien de hele keten van handtekeningen geldig is, zal deze controle door de webbrowser een positief resultaat hebben.

Schematisch ziet dit er als volgt uit:

Certificate chain:

```
|
|- s:/C=NL/ST=Noord-Brabant/L=Eindhoven/O=Madison Gurkha B.V./
  OU=Webserver Team/CN=secure.madison-gurkha.com
  i:/C=NL/O=Madison Gurkha B.V./CN=Madison Gurkha B.V. PKI CA
|
|- s:/C=NL/O=Madison Gurkha B.V./CN=Madison Gurkha B.V. PKI CA
  i:/C=ZA/ST=Western Cape/L=Cape Town/O=Thawte Consulting cc/
  OU=Certification Services Division/CN=Thawte Premium
  CA/emailAddress=premium@thawte.com
```

In bovenstaand voorbeeld wordt een tussenliggend certificaat gebruikt.

Tijdens de controle door de webbrowser, zal het certificaat op naam van "secure.madison-gurkha.com" worden geverifieerd met behulp van de publieke sleutel van de instantie die het certificaat heeft ondertekend, in dit geval "Madison Gurkha B.V. PKI CA". Dit is echter een tussenliggend certificaat dat is ondertekend door "Thawte Premium CA". Dit rootcertificaat is binnen de webbrowser aanwezig zodat de ondertekening kan worden geverifieerd.

De MD5 aanval is gericht op het tussenliggende certificaat. De aanvalder maakt zelf een valide webservercertificaat en laat dit op legitieme wijze ondertekenen door een van de in webbrowser bekende "Root CA's". Deze doet de ondertekening² op basis van een MD5 hash. Dit webservercertificaat is zodanig van opzet, dat er een tweede certificaat bestaat dat als tussenliggend certificaat kan worden gebruikt en waarop een MD5 collision van toepassing is met het webservercertificaat. Nadat het webservercertificaat door de "Root CA" is ondertekend, wordt deze handtekening gebruikt en gekopieerd naar het tussenliggende certificaat. Dit tussenliggende certificaat kan vervolgens worden ingezet om willekeurige (webserver) certificaten te ondertekenen. De controle van een dergelijk certificaat door de webbrowser zal positief uitvallen en de gebruiker zal het certificaat vervolgens vertrouwen. Deze heeft dan ook niet in de gaten dat er met een andere server wordt gecommuniceerd en dus het slachtoffer is van een zogenaamde "Man-In-The-Middle" aanval.

Het alternatief voor MD5 is op dit moment SHA-1 of SHA-2. SHA-1 wordt door de meeste CA's en programmatuur (webbrowser) ondersteund wat niet kan worden gezegd van SHA-2. Daar tegenover staat wel dat het slechts een kwestie van tijd is voordat ook SHA-1 op eenzelfde wijze zal worden aangevallen. SHA-2 is voor de langere termijn de betere oplossing en zal dan ook steeds meer ondersteund gaan worden.

1. Een MD5 (Message Digest Algorithm 5) hash is een 128-bit waarde die middels een cryptografische functie wordt berekend over een bestand of in dit geval over een elektronisch certificaat. Indien er twee of meer certificaten worden gemaakt waarbij de waarde van de MD5 hash identiek is, dan spreken we van een collision.
2. Bij de ondertekening van een certificaat worden slechts bepaalde onderdelen zoals serienummer, geldigheidsduur, issuer (CA), subject (website), publieke sleutel en nog een aantal specifieke kenmerken van het certificaat ondertekend. Niet de gegevens zelf, maar een MD5 hash die aan de hand van deze gegevens wordt bepaald, wordt ondertekend.

.....

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.



Herinner mij

Gebruikersgemak geeft aanvalsmogelijkheid

Steeds meer gebruikersapplicaties worden via het internet ontsloten en zijn toegankelijk middels een standaard webbrowser. Een gebruiker dient zich vaak te identificeren voordat er van de applicatie gebruik kan worden gemaakt. Hiervoor is een gebruikersidentificatie vereist, in de vorm van een wachtwoord of ander authenticatiemechanisme.

Om een volgend bezoek te vereenvoudigen, bieden applicaties vaak de mogelijkheid om de gebruikersidentificatie op te slaan zodat deze bij een volgend bezoek automatisch wordt ingevuld. Gebruikersvriendelijk of een mogelijkheid voor kwaadwillenden?

Over het algemeen maken deze applicaties gebruik van gebruikersidentificatie in combinatie met een wachtwoord voor het verkrijgen van toegang. Hierbij is er vaak vanuit de applicatie aandacht besteed ten aanzien van het gebruik en beheer van deze gegevens. De webapplicatie biedt dan functionaliteiten aan zoals: versleutelde verbindingen, het gebruik van niet voor de hand liggende gebruikersidentificaties, eisen ten aan-

zien van de toegestane wachtwoorden, mogelijkheid tot het wijzigen van wachtwoorden en beperking van het maximaal toegestane aantal foutieve aanmeldingen binnen een bepaald tijdsbestek. De mogelijkheid voor het lokaal opslaan van het wachtwoord op het systeem van de gebruiker is hier niet aan de orde en we zien dan ook dat deze functionaliteit over het algemeen niet door de webapplicatie wordt aangeboden.

Tijdens de technische audits van webapplicaties, zien we vaak dat met name de gebruikersidentificatie lokaal op het systeem van de gebruiker wordt opgeslagen. Soms gebeurt dit geheel automatisch zonder dat de gebruiker hier invloed op heeft en soms heeft de gebruiker de mogelijkheid om aan

te geven dat hij/zij wil dat deze informatie bij een volgend bezoek automatisch wordt ingevuld. Het betreft hier de zogenaamde "Herinner mij" of "Remember me" keuzemogelijkheid.

De gebruikersidentificatie die kan bestaan uit een klantnaam, klantnummer of willekeurige reeks karakters, wordt in een cookie opgeslagen. De opgeslagen informatie wordt bij een volgend bezoek aan de webapplicatie gebruikt. Het gebruik van cookies is afhankelijk van meerdere factoren en er zijn verschillende beveiligingslagen actief. Een deel daarvan is geïmplementeerd in de browser, een ander deel wordt bepaald door de webapplicatie.

Doordat de inhoud van een dergelijk cookie bij juist gebruik alleen door de webapplicatie kan worden bepaald, wordt in de praktijk invoervalidatie op dat cookie nauwelijks toegepast. Indien een aanval echter door een andere zwakte in de webapplicatie, bijvoorbeeld door Cross Site Scripting, toegang heeft tot dit cookie, dan opent dit mogelijkheden voor een aanval.

De impact van de combinatie van twee afzonderlijke zwakheden blijkt ineens een enorm beveiligingsrisico. Het volgende scenario is een voorbeeld van een aanval die meerdere malen succesvol tijdens een audit, door de security consultants van Madison Gurkha, is ingezet. Onderstaand voorbeeld illustreert dat geen enkele invoer door de webapplicatie kan worden vertrouwd.

Gedurende de audit werd in een URL een mogelijkheid gevonden om JavaScript code toe te voegen aan een parameter. Deze JavaScript code werd door de browser uitgevoerd. Tevens werd vastgesteld dat er geen invoervalidatie plaatsvond op de inhoud van het cookie dat er voor zorgde dat de gebruikersidentificatie na het aanroepen van de inlogpagina automatisch werd ingevuld. De volgende stappen werden gevolgd voor het succesvol uitvoeren van een aanval waarbij niet alleen de gebruikersidentificatie maar ook het bijbehorende wachtwoord werd verkregen zonder dat de gebruiker dit opmerkte.



Stap 1 Voorbereiding

Er wordt een speciale webpagina gecreëerd die "interessante" informatie bevat. Het bestaan van deze speciale pagina wordt middels de verschillende communicatiekanalen bekend gemaakt (sociale netwerken, blogs, e-mail enzovoorts). Deze webpagina oogt onschuldig maar bevat in werkelijkheid JavaScript code die gebruik maakt van de eerder gevonden Cross Site Scripting mogelijkheid. Deze pagina zorgt ervoor dat de browser ongezien een URL van de webapplicatie opvraagt (Cross Site Request Forgery). Tijdens deze aanroep wordt er door de browser JavaScript code uitgevoerd in de context van de webapplicatie. Deze

JavaScript code zorgt ervoor dat het "Herinner mij" wordt voorzien van een nieuwe waarde: wederom JavaScript code.



Stap 2 Infectie van het "Herinner mij" cookie

Een gebruiker wordt verleid tot het bezoeken van de zojuist gecreëerde pagina. De gebruiker vindt dat de informatie toch niet zo interessant is en vervolgt zijn weg zonder dat deze heeft geconstateerd dat er een cookie van een andere webapplicatie is aangepast. Het eerste gedeelte van de aanval is hiermee voltooid.



Stap 3 Activering

Op een later tijdstip, waarbij het dus niet uitmaakt of de gebruiker zijn systeem opnieuw heeft opgestart, bezoekt hij/zij de webapplicatie waarbij het inlogscherf wordt getoond. Hierbij wordt het bijbehorende cookie inclusief de geïnjecteerde code automatisch naar de webapplicatie gestuurd.



Stap 4 Voltooiing

De gebruiker voert zijn wachtwoord in, de gebruikersidentificatie is namelijk al ingevuld door de webapplicatie, en klikt op "inloggen". In plaats van de standaard inlogroutine, wordt er door het eerder geprepareerde cookie een gemodificeerde inlogroutine aangeroepen. Hierdoor wordt er een URL opgevraagd waarbij de invoervelden zoals gebruikersidentificatie en wachtwoord meegestuurd worden. Tevens wordt er voor gezorgd dat de oorspronkelijke inlogpagina wordt aangeroepen, waarbij de gebruiker wordt ingelogd. Deze kan met de webapplicatie aan de slag, niet wetende dat zijn inloggegevens nu bij een derde partij bekend zijn.

Aanvallen zoals hierboven beschreven zijn in verschillende variaties mogelijk doordat er onvoldoende invoervalidatie is en doordat er wordt vertrouwd op standaardtechnieken, waarbij er geen rekening wordt gehouden dat deze mogelijk omzeild kunnen worden. In sommige gevallen wordt een deel van de verantwoordelijkheid bij de gebruiker gelegd door het aanbieden van bijvoorbeeld een "Herinner mij" optie. Een reguliere gebruiker zal zich niet bewust zijn van de mogelijke beveiligingsrisico's en zal in vele gevallen kiezen voor functionaliteit. Het is dan ook de vraag of deze verantwoordelijkheid bij een gebruiker moet komen te liggen zonder dat er een duidelijke beschrijving van de mogelijke risico's wordt gegeven. Een en ander wordt nog eens bevestigd door het feit dat veel gebruikers hun wachtwoord in de browser opslaan indien een applicatie deze mogelijkheid biedt.

25C3

Nothing to hide

Toen ik voor het eerst het CCC (Chaos Communication Congress) bezocht, in 1997 in Hamburg, was dit een relatief kleine bijeenkomst met een paar honderd bezoekers. De sfeer was informeel, hackers toonden elkaar nieuwe trucs en wat er buiten het officiële programma (voor zover daarvan sprake was) gebeurde was minstens zo belangrijk als de lezingen die mensen gaven.

Het congres deed zijn naam "Chaos Communication Congress" eer aan, want ondanks het feit dat er niet veel bezoekers waren in vergelijking met latere jaren, was het een drukte van jewelste en werd er twee jaar later uitgeweken naar een nieuwe locatie in Berlijn.

In de afgelopen jaren is ook daar het aantal bezoekers van het congres flink toegenomen. Dit jaar waren er ongeveer vierduizend bezoekers en waren de dagkaarten op de tweede dag van het congres al "ausverkauft", zoals dat in goed Duits heet.

Men zou verwachten dat na vijftwintig jaar ervaring dit congres een professioneel en zakelijk tintje zou krijgen, zodat het vergeleken kan worden met Blackhat Europe en de SANS conferenties. De oorspronkelijke chaotische en informele sfeer is echter blijven hangen, wat deze conferentie uniek maakt qua grootte en doelgroep.

De meer zakelijke conferenties zijn voornamelijk gericht op ICT-beveiligingsprofessionals, oftewel mensen die beroepsmatig bezig zijn met ICT-beveiliging. Aan de ene kant behelst dit werk het controleren van policies, het managen van processen en het inschatten en vermijden van risico's. Aan de andere kant bevinden zich de ICT-beveiligingstesters, die de informatiebeveiliging onderzoeken. Voor deze laatste groep is het belangrijk op de hoogte te zijn van de laatste ontwikkelingen op het gebied van ICT-beveiliging. Waar zijn deze beter op te doen dan tussen een groep mensen die, omdat ze tijd en moeite investeren om beveiligingen diepgaand te onderzoeken, tot nieuwe inzichten komen en anderen inspireren verder onderzoek te doen? Het CCC is hiervoor dus de ideale gelegenheid.

Met als thema "Nothing to hide" was het programma veelbelovend. Er werden dan ook zeker een aantal belangrijke zaken onthuld, die nog niet publiekelijk bekend waren. Op bijeenkomsten als deze zijn bekende beveiligingsonderwer-



Ook in Cisco's IOS zijn nog steeds kwetsbaarheden te vinden.

pen namelijk niet meer interessant. Zo was er bijvoorbeeld geen enkel praatje dat specifiek over virussen ging, er was één presentatie over botnets en een onderwerp als social engineering wordt alleen op het programma geplaatst als er iets nieuws en creatiefs te melden is.

Om deze creativiteit te stimuleren, is het uitermate belangrijk dat hackers de gelegenheid krijgen te experimenteren in een ontspannen atmosfeer. Deze werd gecreëerd door het geven van presentaties over hoe technologie kan worden toegepast in andere gebieden dan de informatietechnologie, zoals bijvoorbeeld een lezing over het genetisch modificeren van voedsel en de maatschappelijke gevolgen hiervan. Veel technologieën zijn namelijk niet zonder risico en op het congres wordt daarom ook aandacht besteed aan de maatschappelijke gevolgen van technologie en in het bijzonder natuurlijk de



Slapen op het congres scheelt hotelkosten en zorgt dat je het programma niet mist.

informatietechnologie.

Wat dat betreft hadden een aantal onthullingen een aanzienlijke impact op de maatschappij. Het DECT-protocol bijvoorbeeld, waarvan iedereen aanvankelijk vermoedde dat dit telefoongesprekken afdoende beveiligde, blijkt af te luisteren te zijn en in sommige situaties blijkt niet eens versleuteling te worden toegepast. Een andere schokkende onthulling, die voor veel lezers waarschijnlijk niet meer als een verrassing komt, was de presentatie over het maken van een SSL-certificaat dat leek te zijn gesignd door een van de root CA's en op die manier door iedere browser geaccepteerd zou worden. Aangezien veel webapplicaties, zoals e-banking, afhankelijk zijn van SSL, heeft dit behoorlijke gevolgen. De onderzoekers die dit presenteerden hielden zich dan ook niet helemaal aan het thema "Nothing to hide" aangezien de inhoud pas op het laatste moment bekend werd gemaakt en het gefalsificeerde certificaat uiteraard niet bekend gemaakt werd.

Wegens de drukte was het soms niet meer mogelijk presentaties te volgen; een situatie die vergelijkbaar was met het eerste congres dat ik bezocht. Het verschil met toen, is dat alle presentaties tegenwoordig op video vastgelegd worden en later te bekijken zijn. Bij Madison Gurkha worden deze video's ook goed bekeken en besproken. Degenen die vanwege de economische crisis tijd over hebben, kunnen meer informatie vinden op: <http://events.ccc.de/congress/2008/>.

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.

15 t/m 16 mei 2009

CONFidence, Krakau

<http://2009.confidence.org.pl/>

De 5e editie van de Poolse ICT-beveiligingsconferentie CONFidence, zal plaatsvinden op 15 en 16 mei 2009 in Krakau. De gastsprekers bij dit evenement zijn onder andere Bruce Schneier en Joanna Rutkowska. Walter Belgers van Madison Gurkha zal een lezing geven over lockpicken, het openen van sloten zonder sleutel.

16 juni 2009

Black Hats Sessions, 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: GE-HACKT! En wat nu? Kijk voor het complete programma op onze website.

18 en 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 degenen die geïnteresseerd zijn: de "call for papers" staat nog open.

Redactie

Marnix Aarts
Walter Belgers
Tim Hemel
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

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.