

14 JANUARI 2012

UPDATE

.....

DE COLUMN 2

Hans Van de Looy

HET NIEUWS 3

Vakbeurs groot succes

Internet der Dingen

HET COLOFON 3

HET INZICHT 4

Ward Wouts over het hacken met een

Teensy

HET EVENT 6

Black Hat Sessions Jubileumeditie,

4 april 2012, De Reehorst Ede

DE KLANT 8

Openhartig gesprek met een organisatie

binnen de centrale overheid

HET INTERVIEW 10

Elly van den Heuvel van het Nationaal

Cyber Security Centrum

(voorheen GOVCERT.NL)

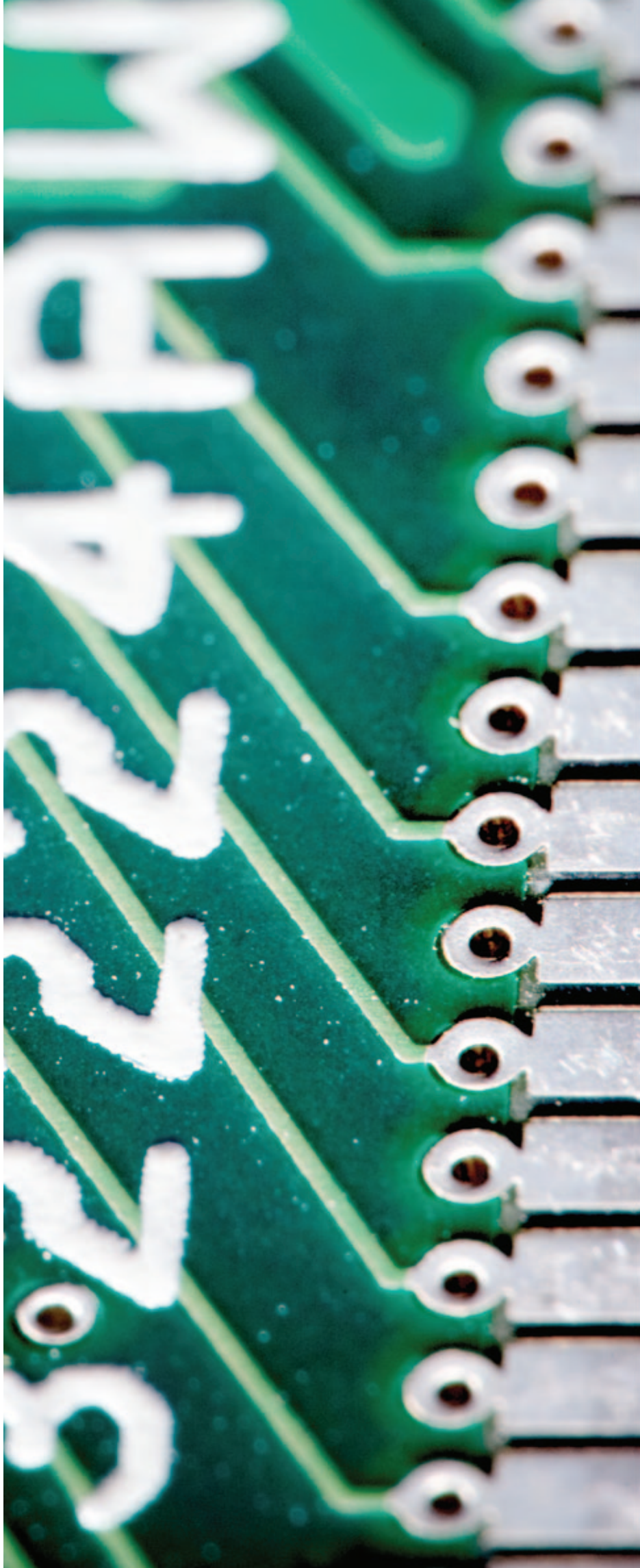
HET VERSLAG 11

Stefan Castille over zijn deelname aan

de training Industrial ICS Cybersecurity

Advanced Training in Idaho Falls

.....



14, een magisch getal

Nummer 14 heeft voor velen een speciale betekenis. Het is de som van de eerste drie kwadraten, waardoor het een kwadratisch piramide nummer is [zie: <http://home.wxs.nl/~hklein/somi2/chiops.htm>]. Het is tevens het atoomnummer van silicium (dat ook in de IT een grote rol speelt) [zie: <http://www.encyclo.nl/begrip/silicium>]. In veel gebouwen buiten Europa is het ook het nummer waarop je moet drukken als je naar de dertiende etage wilt. En het is het rugnummer van een belangrijke Nederlandse voetballer die, als ik dit schrijf, weer volop in de belangstelling staat door alle commotie bij Ajax. Nu ben ik geen voetbalfan en sinds ik het spel niet meer beoefen heb ik bijna alle interesse verloren, maar het blijft natuurlijk wel vreemd dat een raad van commissarissen (RvC) zo over elkaar heen rollend in de publiciteit komt dat bijna al het andere (werkelijke) nieuws erdoor overschaduwd wordt. Het heeft de taak om toezicht te houden op het beleid van de raad van bestuur (RvB) en op de algemene gang van zaken in de vennootschap en de ondernemingen die daaraan verbonden zijn. De term RvC wordt eveneens gebruikt voor een toezichthoudend orgaan in een vereniging of een coöperatie. Wanneer deze rechtspersonen een publiek-private doelstelling hebben wordt dikwijls de naam raad van toezicht (RvT) gehanteerd.

En dan komen we meteen bij de crux van deze column. Ik heb het er al vaker over gehad, maar wil het er hier toch weer een keer over hebben omdat het zo vreselijk belangrijk is. Wat hebben we gemerkt na de problemen met DigiNotar? Weet u het nog? Anders verwijs ik u naar de vorige Update waar het hele verhaal uitvoerig uit de doeken is gedaan [zie ondermeer: http://www.madison-gurkha.com/press/UPDATE_MG_herfst_2011.pdf]. De top van bedrijven en instellingen wil blijkbaar best budget ter beschikking stellen voor het laten toetsen van de beveiliging van bepaalde delen van hun automatisering, als een dergelijk rampenscenario uitgebreid in de media verschijnt. Echter, het zakt het daarna weer erg snel weg en men vervalt in de oude normen en waarden. Tevens vindt deze toetsing pas plaats net voor of na de ingebruikname van de omgeving en nog steeds maar zelden wordt er vanaf het begin van de ontwikkeling van een dergelijke dienst rekening gehouden met beveiliging door deze eis mee te nemen in het proces en te laten borgen door specialisten op dat gebied. Dat hier een aanzienlijke ruimte voor verbetering is mag duidelijk zijn. Dat bedrijven de beveiliging van hun ICT als kostenpost zien is op zijn minst problematisch te noemen.



Zeker in de economische omstandigheden waar we ons nu in bevinden, waardoor de top van bedrijven toch al snel wordt gedwongen tot kostenbesparing om de aandeelhouders tevreden te kunnen blijven stellen. En dat terwijl een goede beveiliging van deze zelfde ICT juist noodzakelijk is om een groot gedeelte van de dagelijkse werkzaamheden correct en zonder problemen uit te kunnen voeren (denk hierbij natuurlijk aan de vertrouwelijkheid, integriteit en beschikbaarheid van de te verwerken gegevens).

Toch zijn er ook positieve veranderingen. De oprichting van het NCSC (Nationaal Cyber Security Centrum) dat op 1-1-2012 operationeel moet zijn [zie ook elders in deze Update het uitgebreide interview met Elly van den Heuvel, General Manager NCSC a.i.], heeft ondermeer kenbaar gemaakt dat beveiliging van SCADA (Supervisory Control and Data Acquisition) systemen een belangrijk onderdeel zal uitmaken van hetgeen waar dit centrum zich op zal richten. Dat de beveiliging van dergelijke systemen aanzienlijk achter loopt bij die van normale desktops en servers mag algemeen bekend worden verondersteld. Er is op dit gebied dus nog een lange weg te gaan. Om dit vroegtijdig aan te kunnen pakken heeft Madison Gurkha al enkele keren consultants laten meelopen in de National SCADA Test Bed Program in Idaho [zie: <http://www.inl.gov/scada/>]. Naast een uitgebreid artikel hierover vindt u natuurlijk ook in deze Update de andere bekende onderdelen die u hopelijk een aantal interessante en leerzame minuten zullen opleveren. Rest mij u te wijzen op de informatie over de jubileumeditie van de Black Hat Sessions, die Walter Belgers en ik al in 1998 zijn begonnen en inmiddels is uitgegroeid tot een welbekend seminar in de IT-beveiligingswereld.

Ik wens u bij deze een voorspoedig (ook in de huidige economische omstandigheden), maar vooral een veilig 2012!

Hans Van de Looy
Partner, Principal Security Consultant

Vakbeurs groot succes

Madison Gurkha participeerde afgelopen jaar samen met ITSX op vakbeurs Infosecurity.nl 2011 die plaatsvond op 2 en 3 november in de Jaarbeurs Utrecht. Wellicht heeft u in Update 13 al gelezen over onze deelname of heeft u zelf onze stand bezocht. Dit keer hebben we de bezoekers verrast met verschillende presentaties op de stand. Walter Belgers, Hans Van de Looy, Ralph Moonen en Stefan Castille hebben tijdens korte presentaties en live hacking demo's hun kennis gedeeld over onder andere Mobile (In) Security en Radio Frequency Identification (RFID).

Naast het bijwonen van interessante presentaties konden de bezoekers op de stand terecht om de fijne kneepjes van het "lockpicken" onder de knie te krijgen. We kijken terug op twee leuke, drukke maar bovenal succesvolle beursdagen. Bedankt voor uw bezoek!



Kijk op: <http://www.surf-academy.nl/> voor het complete programma, meer informatie over het evenement en om je in te schrijven.

Internet der Dingen

Het platform voor informatiebeveiligers in het onderwijs (SURFibo) en het incident response team van SURFnet (SURFcert) organiseren op 9 en 10 februari 2012 voor de vijfde keer een gezamenlijke conferentie die geheel in het teken staat van beveiliging in de omgeving van het hoger onderwijs en onderzoek. De conferentie wordt gehouden bij de SAXION Hogeschool te Deventer.

Het programma start op donderdagavond 9 februari met een boottocht over de IJssel. Tijdens het diner op de boot geeft Rob van Kranenburg een presentatie over

hoe het *Internet der Dingen* onze samenleving zal veranderen. Daarna wordt onder leiding van Jacques Schuurman gediscussieerd over hoe dit het security veld zal beïnvloeden.

Tijdens het dagprogramma op vrijdag 10 februari vinden verschillende presentaties plaats, waaronder die van Walter Belgers van Madison Gurkha. In zijn lezing 'IPv6 insecurities' vertelt hij over de beveiligingsaspecten van het nieuwe protocol. In de presentatie richt hij zich op de risico's die de invoering van het gebruik van IPv6 wellicht met zich mee brengt.

HET COLOFON

Redactie

Tim Hemel
Laurens Houben
Remco Huisman
Frans Kollée
Maayke van Remmen
Ward Wouts

Vormgeving & productie

Hannie van den Bergh /
Studio-HB

Foto cover

Digidaan

Contactgegevens

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

T +31 40 2377990

F +31 40 2371699

E info@madison-gurkha.com

Redactie

redactie@madison-gurkha.com

Bezoekadres

Vestdijk 9
5611 CA Eindhoven
Nederland

Voor een digitale versie van de Madison Gurkha Update kunt u terecht op www.madison-gurkha.com. Aan zowel de fysieke als de digitale uitgave kunnen geen rechten worden ontleend.

Hacken met een **TEENSY**

Een populaire social engineering aanval is het verspreiden van geprepareerde USB sticks om vervolgens met onder andere de autorun-functionaliteit malware uit te laten voeren.

Ook Madison Gurkha voert dit soort onderzoeken uit. Hierbij verspreiden wij of de klant een aantal door ons geprepareerde USB-sticks die, zodra ze in een laptop of pc worden gestopt, verbinding maken met een van onze systemen. Zo kunnen we zien of mensen deze USB-sticks in hun computer steken. In de praktijk is dat vaak het geval, want "wat kan het nu voor kwaad?". (Een recent onderzoek van Sophos, het anti-virus bedrijf, laat zien dat van 50 verloren USB-sticks 66% besmet was met malware.)

In dit artikel behandel ik een andere manier om via USB aanvallen uit te voeren. Voor ons is één van de leuke kanten van USB-aanvallen dat zowel het menselijk handelen als de hardware, factoren zijn waar we rekening mee moeten houden. Waar onze normale aanvallen zich vooral in softwareland afspelen krijgen we hier dan ook te maken met de hardwarekant.

Arduino

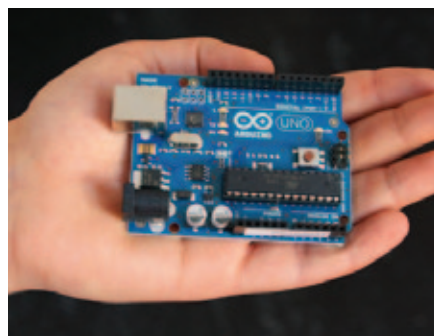
In 2005 is door Massimo Banzi en David Cuartielles het "arduino" project gestart. De vruchten van dit project zijn een stuk open hardware, het arduino-bord en een bijbehorende (open source) programmeeromgeving. Het bordje is een klein printplaatje met een chip erop. Het doel was om op een eenvoudige manier de functionaliteit van de chip bereikbaar te maken. Destijds is dit platform bedacht om studenten de mogelijkheid te geven om tegen geringe kosten ervaring op te doen met elektronische aansturingen en de interactie daarmee.

De eerste versie van deze hardware werd geprogrammeerd door het bordje met een seriële kabel (RS-232) met een PC te verbinden. Destijds een logische keuze, aangezien de chip op het bordje direct met die seriële verbinding geprogrammeerd kan worden. Al snel werd dit vervangen door op de bordjes een extra chipje op te nemen dat een USB/serieel-vertaalslag kan maken. Vanaf toen konden de bordjes via een USB-poort geprogrammeerd en aangestuurd worden. Iets wat ik heel handig vind, aangezien mijn Apple laptop al jaren geen seriële-poort meer heeft.

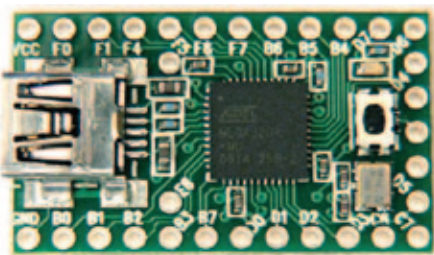
In een nog latere versie is het chipje dat de USB/serieel-vertaalslag maakt (oorspronkelijk een specialistische "FTDI"-chip) vervangen door een meer algemeen en programmeerbare chip. Een groot voordeel hiervan is dat het arduino-bordje nu niet alleen serieel via USB kan communiceren, maar zich nu in principe ook kan gedragen als andere USB-apparaten. Bijvoorbeeld als een muis, een toetsenbord of een joystick.

Naast al deze hardwareontwikkelingen heeft de arduino ook een hoop culturele ontwikkelingen in gang gezet. Door zowel de hardware als de software open, eenvoudig en goedkoop te houden zijn veel mensen in aanraking gekomen met het bouwen van besturingen, die daar anders wellicht nooit aan begonnen zouden zijn. Zo wordt de arduino, bijvoorbeeld, regelmatig gebruikt in kunstprojecten.

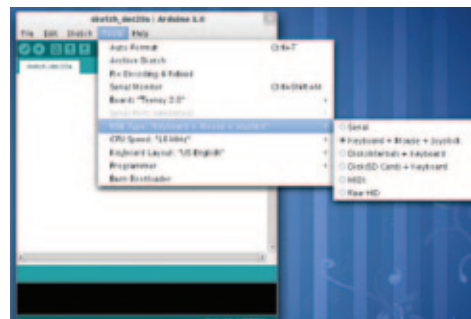
Aangezien de hardware open is, zijn er ondertussen ook een groot aantal arduino-



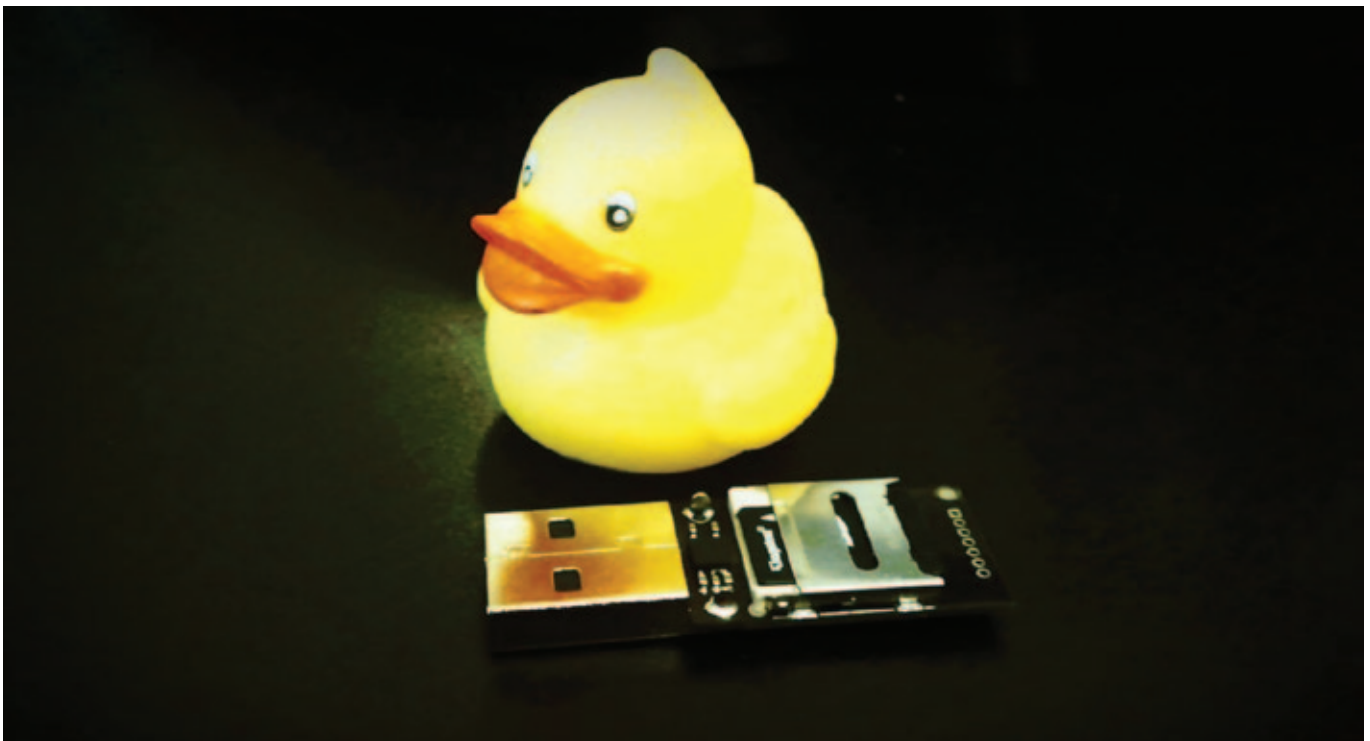
Arduino



Teensy



Installeren teensyduino



klonen op de markt. Sommigen willen simpelweg een goedkoper alternatief zijn, zoals bijvoorbeeld de "seeeduino". Anderen voegen netwerkmogelijkheden toe, zoals de "nanode". Weer anderen bieden meer aansluitmogelijkheden of zijn dusdanig flexibel dat ze in kleding gestikt kunnen worden.

Teensy

Een van de arduino-klonen, de teensy, legt de focus op een zo klein mogelijk formaat (30x18mm). Voor het gebruiken van de teensy in de arduino-programmeeromgeving is het nodig om wat extra software te installeren, "teensyduino" genaamd. Deze software voegt het teensy-bordje toe aan de arduino-programmeeromgeving, samen met de optie om diverse USB-types in te stellen. De ondersteunde types zijn:

- serieel;
- toetsenbord, muis en joystick;
- disk (internal) en toetsenbord;
- disk (SD card) en toetsenbord;
- MIDI;
- Raw HID.

Wanneer een van de toetsenbord-types gekozen wordt, kan het teensy-bordje zo geprogrammeerd worden dat het, na het aansluiten, toetsenbordaanslagen naar een PC stuurt. Het ziet er op het scherm dan ook uit alsof er iemand commando's zit in te tikken. Dit kunnen alle commando's zijn die de programmeur graag uitgevoerd ziet. In ons

geval is dat vaak iets als Windows-R (om de run-box te krijgen). Gevolgd door "iexplore" om internet explorer te starten. Daarna een paar tellen wachten om internet explorer de tijd te geven te starten. Dan F6, om naar de locatiebalk te springen, gevolgd door "http://www.madison-gurkha.com". Dit is niet om de hits op onze website op te schroeven, maar om aan te tonen dat het mogelijk is om op deze manier kwaadaardige software uit te laten voeren.

Nu zullen de meeste mensen niet zomaar een printplaatje aan hun computer hangen. Dat ziet er te vreemd uit. De kunst is dan ook om er een aantrekkelijke behuizing omheen te bouwen. Bijvoorbeeld een mooie muis, zoals gedemonstreerd door Netragard.

SET

Wij zijn niet de enigen die zich met dit soort zaken bezig houden. Veel mogelijke social engineering technieken zijn gebundeld in de Social Engineering Toolkit (SET). Deze toolkit kan kant en klare programmacode voor de teensy genereren, ook voor spannendere zaken dan een URL bezoeken. Deze code kan vervolgens met de arduino-programmeeromgeving in het teensy-bordje worden geladen. De door SET gegenereerde code maakt gebruik van de Windows ALT-codes, om via het numerieke toetsenbord de commando's op te geven. Dat is zo geïmplementeerd omdat het SET-project er tegenaan

liep dat niet alle toetsenborden hetzelfde zijn. In Nederland zien we vooral US International toetsenborden, maar bijvoorbeeld Duitse of Vlaamse toetsenborden zijn heel anders. Via de ALT-codes zagen ze een manier om toch steeds dezelfde karakters in te geven. Hier zit wel een nadeel aan: als num-lock uit staat werkt het niet. Zo kent de SET code nog enkele onhebbelijkheden, maar al met al is het een erg leuk startpunt.

USB Rubber ducky

Een alternatief voor het programmeren van een teensy en het zelf bedenken van een aantrekkelijke behuizing is de USB Rubber ducky. De rubber ducky ziet er uit als een normale USB-stick (ook verkrijgbaar als eendje). De ducky maakt gebruik van micro-SD-kaartjes met een simpel tekst bestand met de gewenste toetsaanslagen.

Zie ook

- <http://nakedsecurity.sophos.com/2011/12/07/lost-usb-keys-have-66-percent-chance-of-malware/>
- <http://arduino.cc/>
- <http://www.seeedstudio.com/>
- <http://nanode.eu/>
- <http://www.pjrc.com/teensy/>
- <http://pentest.snosoft.com/2011/06/24/netragards-hacker-interface-device-hid/>
- <http://www.social-engineer.org/>
- <http://www.usbrubberducky.com>

Dit jaar organiseert Madison Gurkha de 10e editie van de Black Hat Sessions.
Deze jubileumeditie mag u niet missen!

HET EVENT

4 april 2012, De Reehorst Ede

Black Hat Sessions JUBILEUMEDITIE



Dit jaar organiseert Madison Gurkha alweer de 10e editie van de Black Hat Sessions. Wat ooit begon als een middag waarop consultants van Madison Gurkha hun kennis deelden is uitgegroeid tot een welbekend seminar in de IT-beveiligingswereld. In deze jubileumeditie op 4 april 2012 laten we de stand van beveiliging in de ICT-wereld de revue passeren, van verleden via het heden naar een blik in de toekomst

Bestemd voor ú

De bijeenkomst wordt georganiseerd voor beheerders van systemen, netwerken en applicaties, security officers, interne auditors, het management en andere geïnteresseerden. Dit jaar hebben wij in het programma voldoende ruimte vrijgemaakt voor parallelle tracks, zodat zowel technische als niet-technische bezoekers een interessant programma kunnen volgen.

Kosten

Voor deze speciale jubileumeditie van de Black Hat Sessions, hebben wij de prijs verlaagd. Vorig jaar betaalde u € 315,- voor het seminar, dit jaar zijn de kosten voor deelname € 265,- (excl. BTW) per persoon. Documentatie, lunch en koffie zijn inbegrepen. Uiteraard geldt ook dit jaar voor alle relaties van Madison Gurkha een korting van € 35,-. Zo betaalt u dus maar € 230,- (excl. BTW)

08.30 u **Ontvangst en registratie**

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

09.30 u **Keynote: Heel Nederland blijft lek**

Brenno de Winter, onderzoeksjournalist met bijzondere aandacht voor beveiliging en privacy, journalist van het jaar 2011
Als we kijken naar de huidige situatie in de Nederlandse IT-industrie dan lijkt het mantra 'insecurity by design' wel de norm te zijn. Het regent trieste voorbeelden van onveilige situaties, identiteitsdiefstal die erg eenvoudig is, gevoelige systemen die niet online horen te zijn en minimaal horen te beschikken over basale beveiliging. Sinds Lektober is de outline van de problematiek bekend, maar de inkleuring begint nu pas vorm te krijgen.

10.30 u **Parallele tracks**

Shenandoa a Forensics Challenge

Wim Verloop en/of Huub Roem, Managing Partners & Senior Forensic Analysts, Digital Investigation B.V.

Deze presentatie neemt je mee in een case van een groot-schalig digitaal forensisch onderzoek. De melding: we zijn gehackt, de business ligt stil en er worden enorme inkomsten gemist, ruim 100 servers lijken besmet te zijn er lekt informatie. Wat is er gebeurd? Welke uitdagingen komen de Emergency Incident Responders tegen? Hoe stel je ruim 100 servers forensisch veilig? Wat is de onderzoeksvraag die beantwoord moet worden door de forensisch analisten? Welke middelen, tools en acties zijn door de hacker(s) gebruikt en uitgevoerd? Deze presentatie geeft een antwoord op deze vragen, stelt conclusies en doet aanbevelingen zodat u kunt starten met 'Forensic Readiness'

Social Engineering

Walter Belgers, Partner en Principal Security Consultant, Madison Gurkha

Technical people look at security mostly from a technical standpoint. Are systems fully patched? Have SQL-injection problems been eliminated? Truth is, the technical aspect of security is just a small part of the problem. People are probably the biggest security problem to fix. Social engineering is conning people into giving you information or access to systems or buildings. It is, in most cases, far more easy than breaking in electronically. In this talk, we will look at what makes social engineering

work, how to come up with working scenario's and how to try to avoid these problems. The lecture includes examples from actual social engineering assignments and some hilarious clips from the internet. After the talk, the attendees will hopefully understand the importance of security awareness within their companies, being more alert to attacks at the same time.

11.15 u **Koffiepauze / Informatiemarkt**

11.45 u **Parallele tracks**

Hardware security testing – When to stop?

Job de Haas, Director Embedded Technology, Riscure BV
Security testing has a strong connotation with software vulnerabilities and exploits. But also hardware is tested on security. The secret keys embedded in smart cards and System-on-Chips are valuable. This presentation shows how far such security testing goes. From measuring power consumption to firing lasers. From using acid to etch them open to using Focussed-Ion-Beams to change the chips themselves.

2012 en verder: doelwit bent u altijd, maar wie is de aanvaller?

Edwin van Buuren, Adviseur informatiebeveiliging, National Cyber Security Centrum (NCSC)

In zijn presentatie zal Edwin kort met nostalgie terugkijken op het verleden: virussen die zichzelf rondmailden? Lastig, maar wat zouden we graag willen dat het weer 2001 was, af en toe. En waar staan we dan nu? Daar gaat Edwin uitgebreid op in. Voor wie moeten we bang zijn, wat willen ze eigenlijk, en waarom zijn we kwetsbaar voor de snode plannen die ze hebben? Of is het allemaal een hype? Het feit dat er vanaf januari 2012 een National Cyber Security Centrum bestaat, suggereert van niet en Edwin zal u daarvan overtuigen. Tenslotte zal Edwin, als er tijd voor is, u aan de hand van een korte quiz inzage geven in zijn kristallen bol en u volledig ontspannen achterlaten.

12.30 u **Lunch / Informatiemarkt**

13.30 u **Parallele tracks**

Security en het einde van de computer die alles kan, mag en doet wat jij wil

Bert Hubert, Cybersecurity Architect NetScout, Founder PowerDNS

Vroeger, toen de meeste computers geen belangrijke dingen

FOTO: TONY THUIS





per persoon. Voor studenten hebben wij een speciaal tarief van € 55,- mogelijk weten te maken. Geef bij uw online-inschrijving aan dat u een relatie of student bent, en het juiste tarief wordt verrekend.

Vroegboekvoordeel

Als u zich uiterlijk vijf weken voor het evenement registreert, wordt u beloond met 10% korting op de deelnemersprijs.

Deze JUBILEUMEDITIE van de Black Hat Sessions mag u niet missen! Meldt u snel aan via het inschrijfformulier op www.blackhatsessions.com.



deden, kon deze ook niet zo veel. Met de komst van webbrowsers, gevolgd door SSL en certificaten, konden we gaan bankieren op internet. Onze belastingen, verzekeringen, pensioenen en politieaangiften volgden snel. Inmiddels verzadigen spam en malware onze 'general purpose' en is ook SSL niet meer te vertrouwen (denk aan Diginotar). Toch gaan we niet aanstonds onze belastingen weer op papier invullen. In dit praatje wordt uitgelegd hoe het zo ver gekomen is, en welke oplossingen mogelijk zijn als de security industrie zijn best doet. En wat er gebeurt als we dat niet doen – het einde van de computer die doet wat je wil.



If you generate 4% of all global traffic, how do you handle abuse?

mr. Alex de Jooode, Security Officer, LeaseWeb BV
What do you need to do become a good netizen? How do you ensure abuse is handled in a timely fashion and what programs has LeaseWeb developed to fight CyberCrime. This presentation will give you an insight on how one of the largest self-managed dedicated hosting companies on a daily basis fights cybercrime in all its facets.

14.30 u **Parallele tracks**



RFID Security taken for granted

drs. ing. Roel Verdult, onderzoeker die als student bekend werd door de OV-chipkaart te hacken, Institute for Computing and Information Sciences Radboud University Nijmegen, The Netherlands

Het dagelijkse leven van een gemiddelde Nederlander zit vol met RFID apparaten. Denk hierbij bijvoorbeeld aan toegangsbeveiliging van het kantoor, reizen met de OV-chipkaart, startonderbreker in auto's, mobiel betalen en het uitlezen van pacemakers. We gebruiken veel van deze apparatuur zonder er bij na te denken. Het werkt goed en voelt zelfs een beetje magisch, draadloos en op afstand een deur kunnen openen. Dit geeft al snel een gevoel van veiligheid. Het ziet er indrukwekkend en ingewikkeld uit, dan zal het wel moeilijk zijn dit te misbruiken of na te maken. Het tegendeel blijkt waar. In zijn presentatie zal Roel Verdult enkele voorbeelden uitleggen en aantonen waarom we met een wereld vol slecht beveiligde apparatuur leven. Doordat we ons hebben laten opzadelen met slechte producten lijkt "alles wel te kraken". Het probleem zit hem vaak niet in de beschikbare technologie, maar in de keuze die we de industrie voor ons laten maken!



Hacken; toen, nu en straks

Koen Martens, Woordvoerder, VNHO (Verenigde Nederlandse Hackerspaces en Organisaties)

Wie de media er op na slaat, zal het misschien niet denken: maar hackers hebben sinds jaar en dag grote invloed gehad op de technologische ontwikkeling en zijn het gemeengoed geworden van ICT. De rijke hacker-cultuur kent vele kleurrijke figuren en visionaire denkers. Koen Martens zal in vogelvlucht een blik werpen op de herkomst van het woord hacker en uit de doeken doen wat een hacker beweegt. Een recent fenomeen, hackerspaces, brengt hackers samen. De verschillende perspectieven die zo samen komen, leveren interessante en ambitieuze projecten op om te reageren op hedendaagse uitdagingen op het gebied van ruimtevaart, communicatie en milieu.

15.15 u **Koffiepauze / Informatiemarkt**

15.45 u **Live demo van hedendaagse aanvalsmethoden**

Frans Kollée, Senior Security Consultant en Stefan Castille, Medior Security Consultant, Madison Gurkha

De afgelopen jaren zijn de aanvallen op (IT) omgevingen veranderd. Zo zagen we een periode waarbij de aanvallen vooral gericht waren op netwerkapparatuur. Deze werden daardoor beter beveiligd en de aanvallen verschoven zich al vrij snel naar de aangeboden services en serversystemen. Ook deze zijn in de afgelopen jaren steeds beter beveiligd en het merendeel van de hedendaagse aanvallen zijn gericht op de aangeboden applicaties en (browser) clients. Andere aanvalsvectoren zijn social engineering en het verkrijgen van toegang tot interne netwerken van gebruikers, zowel op privé- alsook zakelijke netwerken. Het toenemende gebruik van mobiele apparaten, heeft ervoor gezorgd dat ook deze in toenemende mate worden aangevallen. Tijdens deze presentatie wordt kort teruggegaan in de tijd naar aanvallen zoals deze tijdens de Black Hat Sessions III in 2004 gedemonstreerd zijn. De toen gedemonstreerde aanvallen zijn tegenwoordig slechts in beperkte mate toepasbaar. Al snel zullen Frans en Stefan overgaan tot een aantal aanvallen zoals deze vandaag de dag worden uitgevoerd. Zij belichten daarbij de werkwijze van de aanval, maar ook die van de beveiliging van IT-omgevingen.

16.30 u **Afsluiting door de dagvoorzitter**

16.40 u **Borreluur / Informatiemarkt**



In welke branche is uw organisatie actief?

Onze organisatie is actief binnen de centrale overheid.

Wat is uw functie?

Information Security Manager

Hoeveel mensen houden zich in uw organisatie bezig met informatiebeveiliging?

Uiteraard zijn alle medewerkers in meer of mindere mate betrokken bij (onderdelen van) informatiebeveiliging. Daarnaast zijn ongeveer 15 medewerkers binnen de organisatie beroepsmatig met informatiebeveiliging bezig.

Hoe is informatiebeveiliging opgezet in uw organisatie?

Informatiebeveiliging is een samenhangend geheel van processen, organisatie, mensen en middelen. Security Management zorgt voor sturing, managementrapportage en escalatie.

De **processen** zijn gebaseerd op ITIL (ITIL staat voor Information Technology Infrastructure Library). Security Management neemt een centrale positie in ten opzichte van de operationele en tactische ITIL deelprocessen.

In de **organisatie** is er een strikte scheiding aangebracht tussen de ontwikkeling van ICT en de productieomgeving. Aan de ontwikkelkant zijn dedicated security specialisten bezig met de ontwikkeling, het beheer en het beschikbaar stellen van ICT volgens vastgestelde beveiligingskaders zoals ISO 27001/2. Security operations specialisten waken 7 * 24 uur over het beveiligingswelzijn van de productiesystemen.

De **mensen**: er wordt in dit verband niet alleen aandacht besteed aan ICT-specialisten, die vaak vergaande autorisaties hebben en dus een zeer interessante doelgroep zijn. We kijken ook met name naar de gebruikers van 'onze' ICT. Informatiebeveiliging is allang niet meer een "ICT feestje". Informatiebeveiliging is grotendeels afhankelijk van de factor mens. Bewustwording, houding en gedrag zijn daarom

voornaamste speerpunten geworden met betrekking tot het informatiebeveiligingsbeleid.

De **middelen**, de laatste component, bestaat uit de ICT, de techniek en de beveiligingsinstellingen daarvan. Ook de tooling voor bijvoorbeeld monitoring, analyzing en reporting valt onder deze component.

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

Gezond wantrouwen, geduld, overtuigingskracht en niet te vergeten, maar bijna vanzelfsprekend, integriteit.

Wat vindt u de leuke en wat de minder leuke kanten van uw functie?

De dynamiek die het vak met zich mee brengt, vind ik het leukst. Geen dag verloopt zoals de vorige. De media-aandacht van de afgelopen tijd versterkt dat nog een keer. Deze dynamiek ontstaat doordat enerzijds de ICT voortdurend in beweging is. Er komt voortdurend allerlei nieuwe functionaliteit (b.v. mobility) op de markt. Anderzijds levert dat aan de kant van informatiebeveiliging weer heel wat uitdagingen op; vooral als blijkt dat vastgestelde uitgangspunten op grond van informatiebeveiliging in contrast staan met die nieuwe functionaliteit. Ik krijg helaas geen tijd om over minder leuke kanten van het vak na te denken.

Wat zijn in uw organisatie op dit moment de belangrijkste uitdagingen op het gebied van informatiebeveiliging?

Er zijn twee zaken die onze ruime aandacht hebben. In de eerste plaats zijn dat de externe bedreigingen. Wij zijn en blijven uiterst alert op acties van kwaadwillenden die gericht zijn op misbruik van vertrouwelijke gegevens of die een nadelige invloed kunnen hebben op de beschikbaarheid van onze diensten. Ten tweede is dat de houding en het gedrag van medewerkers en gebruikers. Die moet steeds gericht zijn op het verantwoord omgaan met vertrouwelijke informatie en informatiesystemen. Mensen bewust maken is weliswaar een eerste stap, maar dat is nog niet voldoende. Met gerichte opleidingen en adequaat reageren van het management op ongewenst gedrag, wordt het geheel wat dwingender en minder vrijblijvend.

Welke maatregelen worden genomen om deze risico's onder controle te houden en hoe helpt Madison Gurkha u daarbij?

Madison Gurkha helpt ons om, met behulp van de laatste stand van de technieken en methoden van kwaadwillende, mogelijke kwetsbaarheden op te sporen en ons daartegen te wapenen.

Wat zijn uw ervaringen met Madison Gurkha?

De ervaringen zijn prima. Madison Gurkha beschikt over de juiste kennis en kunde en is uitstekend in staat om deze te vertalen naar onze organisatie. De persoonlijke contacten tussen de specialisten van beide organisaties werken over en weer erg versterkend en inspirerend.

Dit keer in deze rubriek een interview met Elly van den Heuvel van het Nationaal Cyber Security Centrum (voorheen GOVCERT.NL). De in oktober bekend geworden lekken in verschillende overheids(gerelateerde) websites, zijn aanleiding geweest voor het Ministerie van Binnenlandse Zaken om aanvullende maatregelen te treffen. Binnen deze maatregelen speelt het Nationaal Cyber Security Centrum (NCSC) een belangrijke rol. Om de taken en activiteiten van het NCSC met een breed publiek te delen vroegen wij Elly van den Heuvel, General Manager NCSC a.i., het spreekwoordelijke hemd van het lijf.

Elly van den Heuvel

Wat zijn de belangrijkste taken van het NCSC?

De belangrijkste taken van het NCSC bevinden zich op een drietal vlakken: expertise en advies, response op dreigingen en incidenten en versterking van de crisisbeheersing. Je kunt dan concreet denken aan het in samenwerking met publieke en private partners uitvoeren van monitoring, afhandelen van incidenten en alerteren over dreigingen, maar ook het regulier beoefenen van crisisstructuren. Het NCSC doet dit vanaf de start primair voor de rijksoverheid en de vitale sectoren.

Eind 2011 is het NCSC gestart. In hoeverre verandert dit wat GOVCERT.NL doet?

GOVCERT.NL is per 1 januari opgehouden te bestaan en volledig opgegaan in het opgerichte cyber security centrum. Alle activiteiten die GOVCERT.NL uitvoerde, worden nu dan ook uitgevoerd door het centrum in samenwerking met publieke en private partijen. Daarnaast geldt 2012 als eerste fase van het groeimodel van het centrum en wordt het gezien als het transitiejaar waarin (gezamenlijk met partners) meerjarige programma's worden opgestart om nadere invulling te geven aan de kerntaken en activiteiten.

Er bleken in "Lektober" veel gemeente websites kwetsbaar te zijn, die gebruik maken van DigiD. Deze zijn destijds door Logius afgesloten van DigiD. Hoe heeft GOVCERT.NL deze gemeenten kunnen helpen?

Lektober is voor veel partijen een zeer ingrijpende maand geweest. GOVCERT.NL heeft specifiek voor de getroffen gemeenten een checklist ontwikkeld waarmee de gemeenten zelf inzicht konden krijgen op welke specifieke punten de beveiliging van hun website verbeterd kon worden. Je kunt dan denken aan veelal technische aspecten, zoals access management of de beveiliging van netwerk, besturingssystemen of webap-

plicaties. Daarnaast heeft GOVCERT.NL, op basis van de uitgevoerde checklist, specifiek aanvullend advies kunnen geven wanneer dat nodig was. Overigens heeft GOVCERT.NL in veel gevallen uiteraard ook direct gecommuniceerd met de applicatieontwikkelaars zelf.

Wat moeten gemeenten in de toekomst doen om ervoor te zorgen dat ze niet meer worden afgesloten van DigiD?

GOVCERT.NL is momenteel, in samenwerking met publieke en private partners, bezig met de ontwikkeling van een norm voor de beveiliging van websites. Deze norm zal zeker de aspecten bevatten die ik eerder noemde, maar uiteraard breder zijn dan dat. De verwachting is dat Logius deze norm vanaf het einde van het eerste kwartaal van 2012 zal gaan gebruiken als een van de aansluitvoorwaarden voor DigiD.



Wat kan een bedrijf als Madison Gurkha bijdragen aan de publieke en private samenwerking die het NCSC voor ogen heeft?

Met bedrijven als Madison Gurkha werken we al samen, bijvoorbeeld in het kader van trendrapportages. Specifiek voor het centrum zouden securitybedrijven kunnen bijdragen door het delen van informatie ten behoeve van situational awareness. Securitybedrijven hebben vanuit hun rol eigen inzichten in wat er op het vlak van cybersecurity speelt en waar opdrachtgevers mee te maken hebben. Zij zouden daarnaast ook kennis en kunde beschikbaar kunnen stellen, op structurele of incidentele basis, bijvoorbeeld bij grote incidenten of een crisis. Ten slotte kunnen partners input leveren ten behoeve van de strategische dialoog omtrent de rol van het NCSC en de uitvoering daarvan.

Edwin van Buuren zal een presentatie geven op de Black Hat Sessions op 4 april 2012. Wat kunnen bezoekers verwachten?

Het thema van de Black Hat Sessions is "Past Present Future" – Edwin zal aandacht besteden aan alle drie de aspecten, maar de focus leggen op het heden: wat zijn nou dreigingen waar wij nu mee te maken hebben en waar moeten we ons dus tegen beschermen? Daarnaast zal hij ook enkele factoren belichten die ertoe bijdragen dat we kwetsbaar zijn voor die bedreigingen.

GOVCERT.NL



Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie



Een virtuele eekhoorn

Dit jaar kreeg ik de mogelijkheid om, op uitnodiging van het NICC en het Department of Homeland Security, een training te volgen in Idaho Falls, zo'n 8 tijdzones van Nederland verwijderd. Daar werd namelijk de cursus 2011 *International ICS Cybersecurity Advanced Training* gegeven, verzorgd door het Idaho National Laboratory.

In 2010 is de 'worm' Stuxnet uitgebreid in het nieuws gekomen. Deze 'worm' is specifiek ontwikkeld om bepaalde SCADA (Supervisory Control and Data Acquisition) systemen aan te vallen en te manipuleren. (zie ook Update 10 waarin we uitgebreid aandacht hebben besteed aan Stuxnet). Sinds de ontdekking van Stuxnet zijn verschillende varianten ontdekt die andere systemen aanvallen.

Omdat deze systemen ook bij onze klanten aanwezig zijn, is het belangrijk om de nodige kennis in huis te hebben. De ICS Cybersecurity Advanced Training was voor mij de ideale gelegenheid om meer te leren over de specifieke bedreigingen voor procesnetwerken en de mogelijkheden om de beveiliging hiervan te verbeteren. De groep van ongeveer 40 cursisten bestond uit security

consultants zoals ik, onderzoekers, beheerders en IT-managers. Een gevarieerde club met verschillende achtergronden.

Cursus

Tijdens de eerste dagen van de cursus werden verschillende onderwerpen in een snel, maar degelijk tempo doorlopen. Zo kwamen eerst de Industrial Control Systems zelf aan bod. De verschillende componenten en veelgebruikte protocollen werden aangehaald en de werking van de systemen werd kort onder de loep genomen.

Vervolgens werd er aandacht besteed aan het aanvallen van netwerken, systemen en aan de tools die daarvoor gebruikt worden. Hands-on oefeningen zorgden voor een eerste kennismaking met de deze tools voor de deelnemers die hiermee niet bekend

waren. Om de oefeningen vlot te laten verlopen was een aangepaste versie van het populaire 'backtrack' systeem aanwezig. De oefeningen vonden plaats op een daarvoor ingericht testnetwerk waar ook procescontrollers aanwezig waren. Op deze manier konden we aan de hand van de pompen, lampen en meters zien wat het effect van onze eerste hackpogingen waren.

Red team / Blue team

Op donderdag vond het hoogtepunt van de cursus plaats, gevolgd door een 'lessons learned' op vrijdag. Een 12 uur lange sessie op donderdag stond in het teken van de Red team/Blue team oefening. De groep was eerder in de week opgesplitst in een blauw (verdedigend) team en een rood (aanvallend) team.

in Idaho Falls

Het blauwe team, waar ik deel vanuit maakte, kreeg de verantwoordelijkheid om een simulatie van het bedrijfsnetwerk met daarin een chemische installatie in stand te houden en ervoor te zorgen dat de productie van een geheim chemisch product doorgang vond. Punten werden uitgereikt voor elke geproduceerde 'batch', maar ook voor het detecteren van aanvallen, het installeren van patches en het veiliger maken van het netwerk. Het netwerk bestond niet alleen uit het productienetwerk, maar was een goed uitgewerkt bedrijfsnetwerk met een DMZ, een kantoorgedeelte en een afgescheiden productienetwerk. De hele bedrijfsstructuur werd gesimuleerd, waarbij ook de nodige verantwoordelijkheid bij de managers werd gelegd.

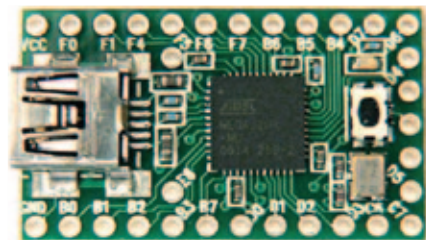
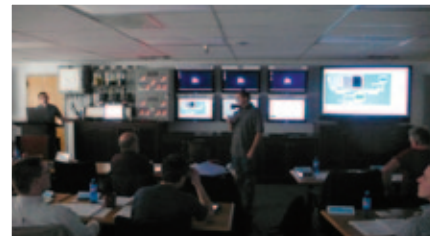
Het rode team had een ander doel: namelijk het saboteren van de productie en zoveel mogelijk schade toe te brengen aan het bedrijf door bijvoorbeeld het lekken van bedrijfsgegevens, het uitschakelen van diensten of door het verstoren van de productie.

Na een chaotisch begin kregen we grip op de situatie en bleven we het rode team telkens een stap voor. Totdat plots de stroomvoorziening werd uitgeschakeld.

Even paniek, maar al snel bleek dat het rode team niet verantwoordelijk was. Een virtuele eekhoorn had een kortsluiting veroorzaakt in de centrale van het bedrijf. Aan het management de taak om deze centrale zo snel mogelijk te vinden en de stroom weer in te schakelen. Na een paar minuten lichtten onze beeldschermen op en konden we weer verder werken. Ondertussen was de score in het voordeel van het rode team waarop we besloten in de tegenaanval te gaan. We namen een poging om de elektriciteit van de tegenstanders uit te schakelen en zetten een honeypot op die het productiesysteem moest nabootsen. Een half uurtje later kwam dan eindelijk de verlossing; het blauwe team had met enkele punten voorsprong gewonnen.

Lessons learned

Op vrijdag werd de oefening geëvalueerd. Beide teams gaven hun visie op de oefening en lieten aan elkaar zien wat er tijdens de oefening was gebeurd. Ook de organisatie, het zogenaamde witte team, kwam aan bod en gaf uitleg over het werkelijke netwerk van de organisatie. Zoals ook in de praktijk het geval is, was het blauwe team bewust voorzien van onvolledige informatie. Tijdens de uitleg bleek pas hoe nauwgezet de



simulatie was voorbereid, en hoe levensecht alles was opgezet.

Hoewel de eerste drie dagen erg interessant waren, is voor mij de Red team / Blue team oefening het meest leerzaam geweest. Door fouten te maken, maar ook vooral door samen te werken met mensen met een andere achtergrond, wordt je kennis naar een hoger niveau getild.

GEORGANISEERD DOOR MADISON GURKHA



4 april 2012 | De Reehorst in Ede

Black Hat Sessions JUBILEUMEDITIE

SPREKERS ZIJN

Edwin van Buuren, Brenno de Winter, Walter Belgers, Wim Verloop, Huub Roem, Job de Haas, Bert Hubert, Roel Verdult, Alex de Joode, Koen Martens, Frans Kollée, Stefan Castille

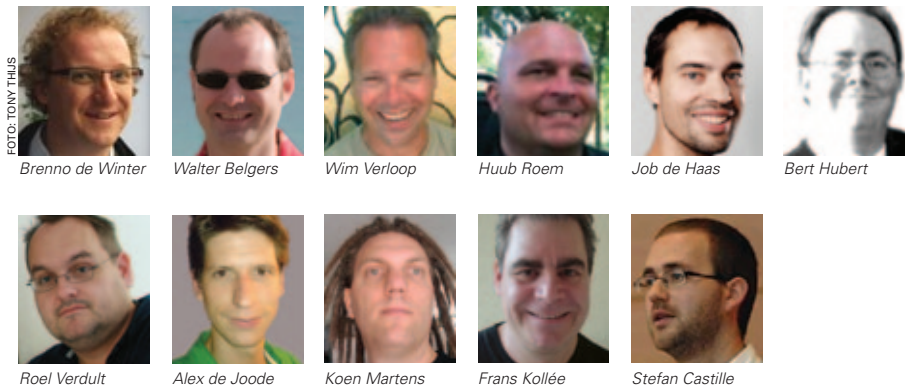


FOTO: TONY THUIS

Brenno de Winter

Walter Belgers

Wim Verloop

Huub Roem

Job de Haas

Bert Hubert

Roel Verdult

Alex de Joode

Koen Martens

Frans Kollée

Stefan Castille



Bijna 15 jaar geleden deelden Hans Van de Looy en Walter Belgers hun kennis over aanvalstechnieken in de IT onder de naam Black Hat Sessions. Sinds de oprichting van Madison Gurkha zijn de sessies uitgegroeid tot een volwaardig seminar waarbij interessant gastsprekers uit Nederland en daarbuiten hun kennis delen over de nieuwste ontwikkelingen op het gebied van technische IT-beveiliging.

Dit jaar organiseert Madison Gurkha voor de tiende keer de Black Hat Sessions, een jubileumeditie dus. Het dagvullend programma bestaat uit meerdere parallele tracks, waardoor u, ongeacht uw technische achtergrondkennis, interessante lezingen kunt volgen. De lezingen worden door onafhankelijke sprekers gegeven en zijn niet commercieel. De onderwerpen zijn uiteenlopend, variërend van forensics tot abuse afhandeling, van hackerspaces tot NCSC, van hardware hacking tot RFID en van DNS tot social engineering.

De dag begint met een keynote door journalist van het jaar 2011, Brenno de Winter, die het afgelopen jaar heel wat stof deed opwaaien in beveiligingsland. Ook de plenaire afsluiter mag er zijn: een live demonstratie van enkele courante aanvalstechnieken, belicht vanuit zowel de aanvaller alsook de verdediger.

Het belooft een interessante editie te worden. We hopen dat u deze dag samen met ons wilt doorbrengen in Ede.

DATUM

4 april 2012

LOCATIE

De Reehorst in Ede

TIJD

09.30 tot 17.00 uur

INFORMATIE EN REGISTRATIE

www.blackhatsessions.com

BESTEMD VOOR Ú

De bijeenkomst wordt georganiseerd voor beheerders van systemen, netwerken en applicaties, security officers, interne auditors, het management en andere geïnteresseerden. Dit jaar hebben wij in het programma voldoende ruimte vrijgemaakt voor parallele tracks, zodat zowel technische als niet-technische bezoekers een interessant programma kunnen volgen.

