Madison Gurkha

Your Security is Our Business

27 MEI 2016 UPDATE

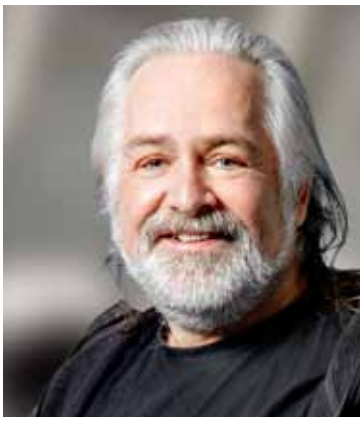
ITSX

23 juni 2016 gaat de Black Hat Sessions Part XIV van start! Zie pagina 4 en 5 voor het uitgebreide programma en de relatiekortingscode

In iedere Madison Gurkha Update vindt u een leuke en informatieve column, die de lezer een verfrissende kijk biedt op uiteenlopende onderwerpen rondom IT-beveiliging. Dit keer is het woord aan Hans Van de Looy.

DE COLUMN

"May you live in interesting times"



Als je de laatste maand(en) de media een beetje gevolgd hebt, kan het je niet ontgaan zijn dat Apple en de FBI een meningsverschil hadden over een zeer specifieke telefoon. Kort resumerend vroeg de FBI aan Apple om de telefoon van een dode terrorist zodanig te manipuleren dat zij toegang kregen tot de daarop opgeslagen gegevens. Apple weigerde dit en het kwam tot een gang naar de rechter. Maar nog voordat er een proces gevoerd werd was er al een media-circus van voor- en tegenstanders. Uiteindelijk heeft de FBI toegang gekregen tot de gegevens op het toestel zonder medewerking van Apple. Storm in een glas water? Of is er meer aan de hand?

Zelf stelde ik me een aantal vragen bij dit verhaal: zouden de Amerikaanse inlichtingendiensten werkelijk niet over eigen middelen beschikken om deze toegang te verkrijgen? Wat zou het gevaar kunnen zijn van een versie van iOS waarmee inlichtingendiensten eenvoudiger toegang konden krijgen tot een iPhone? Welk spel wordt hier gespeeld? Maar ook: Waarom maakt Apple zich zo druk over deze ene telefoon? Welke gegevens slaan we eigenlijk allemaal op op dergelijke apparatuur? Wat sturen we allemaal naar leveranciers van dergelijke apparatuur? Welke beveiligingsaspecten spelen hier eigenlijk allemaal een rol? Als je meer wilt weten over dit onderwerp raad ik je aan op 23 juni a.s. naar de ReeHorst in Ede te komen voor de veertiende editie van de Black Hat Sessions. Deze editie staat geheel in het teken van Mobile (In)security, zie ook de informatie elders in deze Update.

Zie hier één van de redenen dat er onvoldoende uren in een nacht zitten om de schijnbaar noodzakelijke 7+ uur slaap te halen. Informatiebeveiliging is een leuke hobby met een enorm spectrum aan mogelijke onderzoeksgebieden waar we allemaal rekening mee moeten houden om tot een zekere mate van vertrouwen te kunnen komen.

Uiteindelijk komt het er op neer dat ik nog steeds een groot voorstander ben van de bescherming van ons grondrecht op privacy; het recht door de staat en door andere personen met rust gelaten te worden. Maar vrouwe Justitia heeft niet voor niets een balans in haar hand. Er moet te allen tijde een evenwicht gevonden worden, en om dat te bewaken hebben we de rechterlijke macht. Dat Apple zich voordeed als beschermer van het recht op privacy kwam ze marketingtechnisch goed uit en ze hadden sterke argumenten. Dat de FBI dit voor de rechter wilde brengen is ook hun goed recht, want er moest een gewogen afweging gemaakt worden. Tot zover niets aan de hand. Maar wat gebeurde er daarna?

Na enkele weken dagelijks op de hoogte gehouden te worden door de media over de voors en tegens van de zaak FBI versus Apple, gaf de FBI te kennen dat ze Apple niet meer nodig hadden om de gevraagde toegang tot het apparaat te verkrijgen. In meer gespecialiseerde mailinglijsten waren er al lang meerdere mogelijkheden aangegeven waarop de beperking (maximaal tien keer proberen een code te raden waarna de geheime sleutel waarmee de gegevens versleuteld waren zou worden vernietigd) kon worden omzeild. Een extern clubje heeft dit klusje voor de FBI gedaan. Probleem opgelost zou je misschien in eerste instantie willen zeggen, maar er is meer aan de hand. Waar blijft de afweging door een rechter? Waar is die veiligheid ineens gebleven waar Apple zo trots op was? Wat hebben we hiervan geleerd?

Het eerste dat duidelijk naar voren komt is dat de marketing van Apple altijd zal proberen om een negatief bericht zodanig te manipuleren dat het positief uitpakt voor het bedrijf. Apple blijft weliswaar de privacy van hun gebruikers serieus nemen en continu verbeteringen aanbrengen om deze privacy te waarborgen, maar dit heeft duidelijk zijn grenzen. En daarnaast lijkt het er nu op dat overheidsdiensten commerciële dienstverleners in kunnen huren om deze maatregelen te omzeilen zonder tussenkomst van de eerder genoemde rechter en daar hoor ik verder niets meer over! Doordat Snowden duidelijk heeft gemaakt dat inlichtingendiensten wel vaker hun mandaat te buiten gaan mag dat laatste misschien wel als bekend worden verondersteld, maar dat mag toch niet betekenen dat we hiermee stilzwijgend instemmen?

Zeker niet wanneer je inziet welke informatie we tegenwoordig al dan niet bewust op dergelijke apparaten opslaan. Denk hierbij niet alleen aan je agenda, alle contactgegevens van familie, bekenden en bedrijfsrelaties, notities, (privé)foto's en filmpjes, historie van je browsers, zoektermen, allerlei gezondheidsgerelateerde gegevens en niet te vergeten route- en locatie-informatie. Waarschijnlijk weet dat apparaat meer van je dan je meest vertrouwde relatie!

Laten we er dus bewust mee omgaan, wetende dat bepaalde zaken uiteindelijk toegankelijk zijn voor grote leveranciers en overheden. De Chinese vloek -- "宁為太平犬，莫做亂离人 (nìng wéi tàipíng quan, mò zuò luàn lí rén)", vaak vertaald tot "May you live in interesting times" blijft onveranderd van kracht.

Veel leesplezier!

Hans Van de Looy
Partner, principal security consultant

Hands-on kennis opdoen is populair

Hoe veilig zijn je persoonlijke berichten? Die vraag staat centraal in de Hands-on Hacking Workshop: Secure messaging on your mobile, fact or fiction?
Tijdens deze workshop doen deelnemers onder leiding van security consultants van Madison Gurkha onderzoek naar een messaging-app voor Android. U leert hierbij als hacker te werken en ontdekt hoe (on)veilig je berichten zijn. De workshop wordt tweemaal per dag gegeven: een ochtendsessie van 11.00 – 13.00 uur en een middagsessie van 14.00 – 16.00 uur.

Wilt u meedoen met de hands-on hacking workshop tijdens de aankomende Black Hat Sessions op 23 juni a.s., dan is snel inschrijven raadzaam. De workshops zijn populair en er is maar een beperkt aantal plaatsen beschikbaar. Via het inschrijfformulier op www.blackhatsessions.com kunt u aangeven of de voorkeur uitgaat naar de ochtend- of middagsessie. Deelname aan de workshop is gratis voor bezoekers aan de BHS. Om deel te kunnen nemen is een laptop noodzakelijk.

Whitepaper

Everything you always wanted to know about IT security testing, but were afraid to ask.

In opdracht van SURFnet heeft Madison Gurkha begin dit jaar een whitepaper geschreven over alles wat er komt kijken bij het uitvoeren van technische IT security testen.

In de publicatie worden vragen besproken als: Waarom zijn beveiligingsonderzoeken nodig? Wat kan onderzocht worden? Welke onderzoeksmethoden er zijn? En wat is er nodig bij de uitvoering van een onderzoek? Hierbij is gekozen voor een pragmatische insteek waarbij theoretische kennis wordt gecombineerd met ervaringen van Madison Gurkha uit de praktijk. Dit whitepaper is geschreven voor medewerkers van onderwijs- en onderzoeksinstellingen die betrokken zijn bij IT-projecten, zowel vanuit een operationele rol als vanuit een regiefunctie. Wij kunnen dit whitepaper eigenlijk iedereen in alle organisaties aanraden die te maken heeft met technische IT security testen (of die dat zou moeten hebben).

Het whitepaper is te downloaden via de site van SURFnet:
https://www.surf.nl/kennisbank/2016/whitepaper-it-beveiligingsonderzoeken.html

Hieronder vermelden wij een aantal interessante bijeenkomsten/beurzen die de komende tijd zullen plaatsvinden.

26 mei 2016
NLUUG voorjaarsconferentie 2016security conferentie
Postillion hotel in Bunnik
Net als altijd zal de NLUUG-voorjaarsconferentie weer in het teken staan van devops, security, networking, configuration management, scalability, testing, continuous integration etc.
https://www.nluug.nl/events/vj16/

23 juni 2016
Black Hat Sessions Part XIV
De ReeHorst in Ede
Op 23 juni organiseert Madison Gurkha de veertiende editie van de Black Hat Sessions. Het imposante sprekersprogramma is de moeite waard en helemaal on topic voor het thema van dit jaar: Mobile (In)security.
www.blackhatsessions.com

2 en 3 november 2016
Vakbeurs Infosecurity.nl
Jaarbeurs in Utrecht
De vakbeurs haakt in op actuele vraagstukken over IT security en is een must voor iedere IT-professional. Ook dit jaar is Madison Gurkha aanwezig. Wij ontvangen u graag op onze stand C136 en bij onze seminars. Houd onze website in de gaten voor meer informatie.
http://www.infosecurity.nl/

HET COLOFON

Redactie
Ben Brücker
Daniël Dragičević
Remco Huisman
Matthijs Koot
Arnoud Koster
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 59
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.

Op 23 juni a.s. organiseert Madison Gurkha voor de veertiende maal het inmiddels befaamde security congres Black Hat Sessions. Het thema dit jaar is: Mobile (In)security.

23 juni 2016 | De ReeHorst in Ede

Black Hat Sessions Part XIV
Mobile (In)security

BHS

Op 23 juni a.s. vindt de veertiende editie van de Black Hat Sessions plaats in de ReeHorst in Ede. Het thema van deze editie is "Mobile (In)security". Een zeer relevant onderwerp, want er is geen organisatie waar in meer of mindere mate een bring your own device-cultuur is ontstaan. Dat heeft voordelen, maar zeer zeker ook nadelen.

Mobiele apparaten, mobiele communicatie en het Internet of Things bieden onbegrensde mogelijkheden en daar maken we allemaal dankbaar gebruik van. Uiteraard zit er ook een keerzijde aan al het gemak. Tijdens de Black Hat Sessions Part XIV kunt u op informele wijze kennis opdoen over alles op het gebied van informatieveiligheid en mobiele technologie.

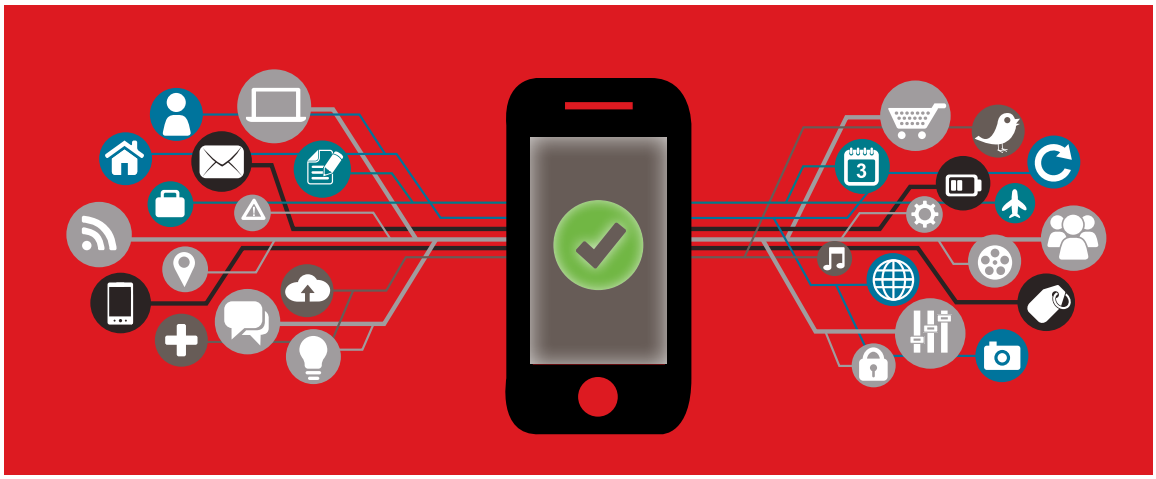
Vorig jaar kwamen zo'n vierhonderd deelnemers bijeen om in één dag kennis op te doen en te netwerken met vakgenoten. Met name de informele sfeer, de interactie met sprekers en deelnemers en het gevarieerde programma worden al jaren positief ontvangen door zowel IT-pro's als het management.

Mis het niet en laat u in één dag door nationale en internationale experts informeren over de risico's en mogelijkheden die mobiele technologie met zich meebrengt. Gaat u liever zelf aan de slag? Tijdens de hands-on hacking workshop: "Secure messaging on your mobile, fact or fiction?" wordt u meegenomen in een onderzoek naar een messaging-app voor Android. Leer als een hacker te werken en zie hoe (on)veilig uw berichten zijn.

Keynotesprekers Aral Balkan en **Kevin McPeake** zorgen deze editie voor een inspirerende opening en afsluiting van de dag. Ethisch ontwerper, professioneel spreker en digitale rechten activist Aral Balkan zet zich in voor open source alternatieven van sociale media waarin data van gebruikers zijn en niet van bedrijven als Google, Twitter of Facebook. Met zijn sociale onderneming Ind.ie ontwikkelt hij Heartbeat, momenteel in de ontwikkelingsfase. Aral gaf wereldwijd vele lezingen, op ongeveer 75 evenementen in 18 landen. Kevin heeft in de afgelopen 20 jaar zijn sporen verdiend als expert op het gebied van telecom en IT-security, onder andere als Senior Technical Security & Forensics Analyst bij Orange NL en Senior Information Security and Digital Forensics Specialist bij T-Mobile Nederland.

Het dagvullend programma bestaat naast de keynotes uit een technische track en een managementtrack. Uiteraard allemaal toegespitst op het thema van dit jaar: Mobile (In)security. Op deze manier kunt u zelf een interessant programma samenstellen passend bij de achtergrond en interesse.
Zie hieronder een korte samenvatting. Op www.blackhatsessions.com vindt u het volledige programmaoverzicht.
Zie ook bijgesloten leaflet met daarop de aankondiging van een extra keynotespreker!

De beveiliging van mobiele telefonie blijft een hot item. **Fabian van den Broek**, onderzoeker in de Digital Security groep aan de Radboud Universiteit Nijmegen, vertelt over **IMSI-catching**. Met IMSI-catchers kun je mobieltjes traceren en ze afluisteren.
Hoe veilig is mobiele telefonie nu eigenlijk nog? Werken 'IMSI-catcher-catchers'? En kunnen we IMSI-catching in zijn geheel voorkomen? **Victor van der Veen,** onderzoeker in de System and Network Security



Dagvullend programma over alles op het gebied van informatieveiligheid en mobile devices and communications.

Group aan de Vrije Universiteit Amsterdam, gaat in op de **BAndroid-kwetsbaarheid**. Hij zal de nodige details geven om de ernst van de zaak duidelijk te maken. Zie ook het uitgebreide interview met Victor elders in deze Update. **Raul Siles**, oprichter en senior security analist bij DinoSec en gecertificeerd SANS-instructeur, zal de techneuten onder ons verrassen met een dieptechnische lezing over **iOS** en **Maurice Aarts & Nikita Abdullin**, beide security analist bij Riscure, belichten in een aanval-verdedigingsduel zowel de kant van de aanvaller/hacker als die van de verdediger/ontwikkelaar om de risico's van **mobiele betalingen via NFC / HCE** aan te tonen.

Binnen de managementtrack vertelt **Dirk Jan van den Heuvel**, Divisie-Directeur Software & Security bij De Amerikaanse test- en certificatie-organisatie Underwriters Laboratories (UL), over de UL-cyberstandaarden en zal de toehoorders aan het denken zetten over het **testen van IoT-apparaten**. Mobiele applicaties behandelen steeds vaker vertrouwelijke gegevens. Welke typische kwetsbaarheden zien we in de praktijk bij deze toepassingen? **Rob van der Veer,** principal consultant bij SIG, gaat in op mobile app security vanuit een **secure coding** perspectief. **Ralph Moonen,** directeur van ITSX, geeft tekst en uitleg over **protocollen voor draadloze communicatie.**. Het Internet-of-Things (IoT) brengt nieuwere technologieën met zich mee: Zigbee, XBee en LoraWAN bijvoorbeeld, alsmede grote aantallen 'connected devices' via 3G of 4G. Ralph laat zien welke bedrijfsrisico's bestaan bij het inzetten van deze draadloze technologieën en welke belangrijke maatregelen genomen kunnen en moeten worden om ook in de toekomst een veilige omgeving te hebben. **Marianne Korpershoek**, partner en advocaat bij Louwers IP|Technology Advocaten, geeft inzicht in de **juridische aspecten rondom BYOD** en welke risico's u hierbij loopt in het kader van de meldplicht datalekken. Wat kun je doen om de risico's te mitigeren? Maar ook, wat doe je als organisatie met de informatie die wordt verkregen uit i-beacons, wearables etc. Wat mag wel? Wat mag niet?

Meld u aan als relatie van Madison Gurkha

Wij hopen dat u deze dag (wederom) samen met ons wilt doorbrengen in de ReeHorst in Ede. Uiteraard geldt voor relaties van Madison Gurkha een relatiekorting. Geef bij uw aanmelding via het inschrijfformulier de code **ns7wespu** op en de 10% korting wordt direct verrekend. Wellicht is dit congres ook interessant voor uw collega's? U kunt gebruikmaken van de extra geldende groepskortingen van 10% bij 5 tot 10 deelnemers. Meldt u meer dan 10 deelnemers tegelijkertijd aan, dan profiteert u van 15% extra groepskorting. Groepsaanmeldingen kunt u per e-mail aan bhs@congres4u.nl versturen.

Meer informatie over het congres en het inschrijfformulier vindt u op www.blackhatsessions.com.

Deze keer een interview met Victor van der Veen, promovendus aan de Vrije Universiteit Amsterdam over Android in aanloop naar zijn presentatie op de Black Hat Sessions.

Victor van der Veen is promovendus aan de Vrije Universiteit Amsterdam, in de vakgroep van Herbert Bos. Tijdens de Black Hat Sessions op 23 juni zal hij een technische lezing verzorgen over Android. In dit (technische) interview laat Victor zijn licht schijnen over de vragen die we hem in aanloop naar de conferentie vast stelden.

Kun je iets zeggen over het promotieonderzoek dat je aan de VU uitvoert?
De projecten waar ik vooral mee bezig ben geweest, gaan over Control-Flow Integrity (CFI) op binary-niveau. CFI is een verdedigingstechniek tegen geavanceerde aanvallen zoals Return Oriented Programming (ROP). Om een ROP-aanval te laten slagen, misbruikt een aanvaller bijvoorbeeld een "buffer overflow"-kwetsbaarheid om controle over een programma over te nemen. Bij een ROP-aanval injecteert de aanvaller zelf geen code, maar maakt hij gebruik van bestaande instructies van het programma [die reeds in het werkgeheugen zijn geladen, red.]. Door deze (blokken van) instructies in een bepaalde volgorde aan te roepen, neemt hij de controle over. CFI stopt zo'n aanval door te forceren dat instructies die een programma naar een andere locatie laten springen (control-flow instructies), alleen naar legitieme locaties (zoals oorspronkelijk bedoeld door de ontwikkelaar) kunnen springen. Een CFI-oplossing op binary-niveau betekent dat we geen broncode van het originele programma nodig hebben om het te beschermen.

De CFI-projecten waar ik aan heb gewerkt heten PathArmor en TypeArmor. PathArmor maakt gebruik van recente features in Intel processors om programma's te beschermen met een sterke variant van CFI: zogenaamde "context-sensitive CFI"[1]. Door gebruik te maken van hardwarefeatures heeft PathArmor een lage run-time overhead. TypeArmor focust op zogenaamde forward-edge control-flow instructies (indirect call instructies, in het bijzonder; instructies die je bijvoorbeeld ziet wanneer je een functiepointer aanroept). Met TypeArmor is het ons gelukt om een recent aanvalsmodel te stoppen (namelijk: Counterfeit Object Oriented Programming, oftewel COOP) [2].

Hoe is mobiele malware te herkennen?
Ik denk dat het tegenwoordig moeilijk is om mobiele malware te herkennen. Ik zal in mijn talk een demonstratie geven van (door ons geschreven) mobiele malware en ik denk niet dat een gebruiker deze malware met het blote oog kan herkennen. Ook automatische analyse kunnen we omzeilen; onze malafide app heeft een paar maanden in de Play-store gestaan en werd pas verwijderd nadat ik het hoofd van Android Platform Security een demonstratie filmpje heb laten zien.

Wat is een groter probleem: kwaadaardige applicaties die de gebruiker simpelweg om te veel rechten vragen, of applicaties die gebruik maken van kwetsbaarheden in het besturingssysteem? (Stagefright etc.)
In principe zou een gebruiker apps die om te veel rechten vragen gewoon kunnen weigeren tijdens installatie, en zou je zeggen dat kwetsbaarheden in het besturingssysteem een groter probleem zijn. Ik verwacht echter dat bestaande malware vaker gebruik maakt van een kwetsbare gebruiker (die alle permissies blindweg accepteert) dan van een kwetsbaar besturingssysteem.

Helpen mobiele anti-viruspakketten om gebruikers te beschermen tegen malware?
Slechts tot een zekere hoogte. Ik zou er niet blind op vertrouwen: ze kunnen veelal geen nieuwe malware detecteren.

Zie je trends in mobiele malware?
Ik heb me hier al een tijdje niet in verdiept, maar tot op heden staan vooral third-party markets erom bekend malware aan te bieden. Met name China heeft hier last van.

Gedurende je vorige onderzoeksprojecten ben je o.a. bezig geweest met geautomatiseerde analysetools voor Android-applicaties, zoals Andrubis. Hoe goed zijn deze tools in het analyseren/herkennen van malware, en hoe kunnen deze bedrijven helpen om veiliger te worden?
Andrubis geeft iedere app een rating tussen 0 (goedaardig) en 10 (kwaadaardig) en met de juiste threshold zijn de resultaten 'goed' te noemen. Van een sample set van 15.000 malware samples werd 98% correct gedetecteerd als kwaadaardig. Helaas is Andrubis ondertussen al aardig verouderd en worden grote apps of apps die gebruikmaken van nieuwere APIs niet ondersteund. Een bedrijf kan Andrubis gebruiken om het kaf van het koren te scheiden, maar er kunnen geen garanties gehangen worden aan of een app daadwerkelijk goed- of kwaadaardig is.

Hoe groot is het probleem van banking-trojans op mobiele devices, waar je onderzoek naar gedaan hebt? En hoe kan een gebruiker zich hiertegen beschermen?
Ik weet niet exact hoeveel verlies banken op dit moment lijden door banking-trojans, maar Eurograbber[3] is een goed voorbeeld van hoe fout het kan gaan: 36 miljoen euro gestolen.

Ik weet niet exact hoeveel verlies banken op dit moment lijden door banking-trojans, maar Eurograbber is een goed voorbeeld van hoe fout het kan gaan: 36 miljoen euro gestolen

Helaas heb ik geen goed nieuws en werkt Google tot op heden niet mee aan een manier om onze aanval te stoppen. Een radicale tip is het loskoppelen van je Android-account, met alle nadelen van dien, zoals geen Gmail meer op je telefoon.

Cryptolocker/ransomware is een steeds groter probleem voor traditionele computersystemen en netwerken. Verwacht je dat hier ook mobiele varianten op zullen komen, en waarom?
De mobiele varianten zijn er al, maar het is de vraag of dit net zo'n groot probleem gaat worden als op de desktop. Het lijkt erop dat Google er sinds Android 4.4 voor zorgt dat apps geen files kunnen verwijderen buiten hun eigen directory op de sdcard. Ze konden al niet bij normale data-directories van andere apps (niet op de sdcard), wat betekent dat ransomware alleen iets kan wanneer het onder root-rechten draait. Ransomware zou dus een root-exploit moeten bevatten; daar zou het bijvoorbeeld kingroot (http://www.kingroot.net) voor kunnen gebruiken.

Recentelijk heb je onderzoek gedaan naar kwetsbaarheden in tweefactorauthenticatie (2FA) wanneer deze op een mobiel device plaatsvindt. Kun je een korte samenvatting geven van je bevindingen?
We gaan uit van de situatie dat een aanvaller controle heeft over de browser van zijn slachtoffer. In deze situatie zorgt 2FA ervoor dat een aanvaller geen operaties kan uitvoeren die door 2FA beschermd worden (zoals het overmaken van geld van rekening A naar B). We hebben twee 'kwetsbaarheden' misbruikt om vanuit een geïnfecteerde browser ook controle te krijgen over de telefoon van een slachtoffer om zo phone-based 2FA te kraken. De eerste is de remote-install-feature van Google Play: je kunt een app installeren vanuit je browser door op de "Install"-button te klikken, en hoeft hierbij geen interactie uit te voeren op je telefoon (het accepteren van de permissies wordt in de browser voltrokken). Het tweede issue is de mogelijkheid om een app te activeren door op een link te klikken. Standaard is een app na installatie inactief; de app wordt pas actief zodra je deze opent, bijvoorbeeld door op het icoon te klikken of door op een speciale link te klikken die gekoppeld is aan de app. Omdat we controle hebben over de browser, en omdat alles tegenwoordig gesynchroniseerd wordt, kunnen we vanuit de browser bijvoorbeeld bookmarks van het slachtoffer overschrijven zodat ze, als deze geopend worden op een telefoon, redirecten naar onze app en deze activeren. De malafide app kan vervolgens sms-berichten afluisteren en TAN-codes doorsturen naar de aanvaller zodat hij midden in de nacht je bankrekening kan Leegtrekken. Dit onderzoek is trouwens ook onder de aandacht gekomen bij Slashdot[4, 5].

Zie je goede alternatieven voor de gebruikelijke manieren van 2FA?
Het is belangrijk om een tweede factor te gebruiken die los staat van de eerste factor (je PC/laptop). Een cardreader is daarom veiliger dan je smartphone (omdat de smartphone kan worden geïnfecteerd als je die koppelt met je PC/laptop).

Het Android platform wordt steeds meer gebruikt in apparaten, anders dan traditionele telefoons en tablets. Zie je hier gevaren?
Het is inderdaad te verwachten dat de komende jaren koelkasten en andere Internet of Things (IoT)-apparaten gehackt gaan worden. Hoe dit precies zal verlopen, durf ik niet te voorspellen, maar onze hack laat zien dat het verbinden van apparaten en synchroniseren van gegevens nieuwe aanvalsmodellen mogelijk maakt.

Victor van der Veen

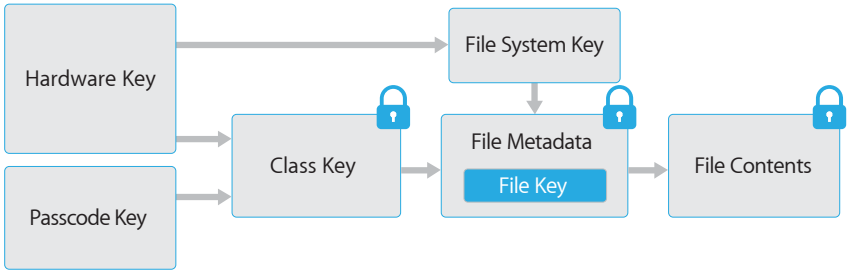
Victor is a PhD candidate in the System and Network Security Group at the VU University Amsterdam where he also obtained his MSc. degree in Computer Science in August 2013. Victor is currently under the supervision of prof. dr. ir. Herbert Bos.
His research focuses on - but is not limited to - malware on smartphones and is part of the Dutch-American Project Arrangement about cooperative research and development on cybersecurity. This means that he will spend a significant amount of time at the University of California Santa Barbara, where he will be advised by prof. dr. Christopher Kruegel. Besides mobile malware, Victor is interested in (low-level) system topics that enhance system security, as well as reverse engineering and analyzing malicious code. Aside from doing research on these topics, he also enjoys implementing related features in real systems.

His personal website, that includes a list of publications, can be found at http://vvdveen.com/.

1 http://vvdveen.com/publications/PathArmor.pdf
2 http://vvdveen.com/publications/TypeArmor.pdf
3 http://www.bankinfosecurity.com/interviews/darrell-burkey-i-1730/op-1
4 https://it.slashdot.org/story/16/04/08/1735240/anywhere-computing-makes-2fa-insecure-on-ios-and-android
5 https://news.slashdot.org/story/16/04/10/237215/academics-claim-google-android-2fa-is-breakable

Apple versus FBI

In februari jl. beval de FBI Apple mee te werken aan het doorzoeken van de iPhone van één van de (omgekomen) daders van de schietpartij in San Bernardino. Apple weigerde dat. De FBI ondernam juridische stappen, maar maakte vlak voor de eerste hoorzitting bekend de telefoon te kunnen ontgrendelen via een (vooralsnog) onbekende methode die tegen betaling is verworven van een (vooralsnog) onbekende derde. Hoe zat het precies met het FBI-bevel aan Apple? In dit Inzicht de zaken nog eens op een rijtje, met aandacht voor een aantal technische details van iOS.



Figuur 1: Diagram van sleutels en versleuteling op iOS. Bron: [Apple2015]

Versleuteling: de UID en passcode
De telefoon van de dader betreft een iPhone 5c met iOS 9. Sinds iOS 8 is de 'Data Protection'-functie, opslagversleuteling, standaard ingeschakeld. Op iOS 9 werkt dat op hoofdlijnen als volgt [Apple2015].

Er is sprake van twee geheime codes. De eerste geheime code is de 'Passcode Key', kortweg 'passcode': dat is de code die de gebruiker instelt bij ingebruikname van het iOS-device. iOS 9 vraagt de gebruiker een 6-cijferige code in te stellen, maar de gebruiker kan ook een veel langere alfanumerieke code opgeven.

De tweede geheime code is de 'Hardware Key', ook wel 'Unique Identifier' of kortweg 'UID': dat is een 256-bits AES-sleutel die tijdens het fabrikageproces van de CPU-chipset (A6, A7, A8, enz.) wordt gegenereerd en in de hardware zit ingebakken. Op iOS-devices met een A7-chipset of nieuwer, zoals de iPhone 5s en de iPhone 6, bevindt de UID zich in de 'Secure Enclave', een co-processor met een door Apple geminimaliseerde versie van ARM TrustZone. De iPhone 5c, het model waar het bij San Bernardino om gaat, heeft geen Secure Enclave. (Om dit Inzicht ook relevant te houden voor gebruikers van nieuwere iOS-devices, wordt toch enkele malen gerefereerd aan de Secure Enclave.)

Figuur 1, afkomstig uit Apple's documentatie, geeft weer welke sleutels worden gebruikt. Op iOS vindt de versleuteling plaats op bestandsniveau, afhankelijk van de 'Protection Class' die aan een bestand is toegewezen. Voor elk bestand wordt een random sleutel gegenereerd, de 'File Key': daarmee worden de gegevens in het bestand feitelijk versleuteld. Er zijn vier klassen: 'Complete Protection', 'Protected Unless Open', 'Protected Until First User Authentication' en 'No Protection'. Elke klasse heeft een eigen sleutel, de 'Class Key', die wordt gebruikt om de 'File Key' te versleutelen. De versleutelde 'File Key' wordt opgeslagen in de metadata van het bestand. Die metadata zelf is versleuteld met een 'File System Key', die wordt gegenereerd tijdens de installatie van iOS en wordt opgeslagen in een snel wisbaar gedeelte van het flashgeheugen. De 'File System Key' dient louter als schakel in het mechanisme voor remote wipe en auto-erase. Wanneer de gebruiker de passcode wijzigt, wijzigt alleen de versleuteling van de 'Class Keys'. Die werkwijze voorkomt dat bij elke wijziging van de passcode alle bestanden volledig opnieuw moeten worden versleuteld. De 'File Key' wijzigt dus niet. (Het is niet bekend hoe iOS de random sleutels genereert en hoe random deze precies zijn; bij iOS 7.)

Van de passcode en de UID wordt via PBKDF2 een sleutel afgeleid. Het aantal PBKDF2-iteraties is volgens Apple zo afgestemd dat 80ms(hardwarematige) vertraging per inlogpoging wordt geïntroduceerd. Bestanden met de klasse 'Complete Protection' maken gebruik van een 'Class Key' die is versleuteld met een sleutel die wordt afgeleid van de passcode en UID. Dat geldt ook voor bestanden met de klassen 'Protected Unless Open' en 'Protected Until First User Authentication'. Alleen bij bestanden met de klasse 'No Protection' is dat anders: de 'Class Key' van deze bestanden is versleuteld met alleen de UID. Dat is bijvoorbeeld nodig voor om het besturingssysteem te kunnen laten booten tot aan het passcodescherm. De 'File Key' en 'Class Key' worden vanaf A7-chipsets nimmer in het normale geheugen verwerkt; de 'key wrapping' (conform RFC 3394) vindt daar plaats binnen de Secure Enclave, en de Secure Enclave spreekt met minder vertrouwde delen van de hardware tijdelijke sleutels af als 'toegangscontrole' voor het versleutelen en ontsleutelen.

Hoe kom je achter de UID en passcode?
Hoe achterhaal je de passcode? Hoe random de passcode is, en of iets of iemand meegluurde toen de gebruiker deze instelde en sindsdien invoerde, is op voorhand niet te zeggen. Als de passcode alleen bij de (in dit geval overleden) dader bekend is, dan zal in beginsel moeten worden gedacht

aan brute-force proberen. Het brute-forcen van een alfanumerieke passcode van 6 cijfers en kleine letters zou volgens Apple vanwege de 80ms(hardwarematige) vertraging maximaal 5.5 jaar duren. Gemiddeld zal het in de helft van die tijd lukken. Natuurlijk kunnen voor hand liggende combinaties eerst worden geprobeerd: '000000', '123456', '654321', betekenisvolle datums, postcodes, enz.; met een beetje geluk is het dan veel eerder raak. Heel soms zal keyspace-reductie mogelijk zijn op basis van vetvlekken op het schermpje, daar waar zich toetsen van het on-screen toetsenbord bevinden.

Een eerste probleem bij het brute-forcen is dat iOS na 5 passcode-pogingen een minuut blokkering oplegt voordat een volgende poging kan worden gedaan; na 6 pogingen een blokkering van vijf minuten, etc.; en na 9 pogingen een blokkering van een uur. Na 10 foute pogingen moet het device op iTunes worden aangesloten om een restore uit te voeren. Daarbij gaan gegevens die op het device zijn toegevoegd sinds de laatste backup verloren, net als bijvoorbeeld de cache van on-screen toetsaanslagen (die, voor zover bekend, niet in de backup staat). Daarna zijn opnieuw 10 pogingen mogelijk. Op die manier kan een passcode in principe brute-force worden achterhaald, maar erg praktisch is dat niet.

Een tweede probleem is de auto-erase-functie: indien deze is ingeschakeld (standaard uitgeschakeld), dan wordt na 10 foute passcode-pogingen de 'File System Key' gewist. Op dat moment kunnen de bestandsmetadata en bestanden met de klasse 'No Protection' niet meer worden ontsleuteld, en het besturingssysteem daarom niet meer booten. (De documentatie van Apple vermeldt overigens niet wat bij de auto-erase gebeurt met de versleutelde bestanden en metadata, waaronder dus ook gebruikersgegevens; vermoedelijk blijven deze, versleuteld, in het flashgeheugen aanwezig.)

Dan de UID. Hoe achterhaal je die? Hoe random de UID is, en of iets of iemand meegluurde bij het fabricageproces, is niet bekend. Volgens Apple wordt de UID niet vastgelegd bij Apple of Apple's leveranciers[Apple2015]. Op iOS-devices met de A6-chipset, zoals de iPhone 5c van de dader, is de UID volgens Snowden te achterhalen via 'chip decapping'([Snowden2016]). Het is denkbaar dat de UID ook kan worden gevonden door deze uit het werkgeheugen van de A6-chipset te dumpen, mits de relevante pin-outs kunnen worden geïdentificeerd en chocola kan worden gemaakt van de signalen op die pins. Op devices met een Secure Enclave wordt de UID volgens Apple nooit in het werkgeheugen verwerkt, en zou dan (nog) veel moeilijker te achterhalen zijn.

Als de UID niet bekend is, dan zou ook díe moeten worden geraden, wil men kunnen brute-forcen via het rechtstreeks aanspreken van het flashgeheugen in plaats van de normale kanalen. Aangezien de UID 256 bits lang is, is dat onwerkbaar. Vanaf de A7-chipset zou het vanwege de Secure Enclave bovendien niet mogelijk zijn om op deze wijze een brute-force-aanval uit te voeren, omdat de extra vertraging per inlogpoging dan niet door de iOS-software, maar door de Secure Enclave wordt afgedwongen. Om die vertraging te omzeilen zou aangepaste Secure Enclave-firmware nodig zijn.

Ten overvloede: bestanden met de klasse 'No Protection' zijn toegankelijk voor een ieder met fysieke toegang tot het device, zonder de passcode te kennen. De FBI kan dus reeds bij de gegevens in die bestanden; maar zal daar weinig spannends vinden. (Ontwikkelaars van iOS-apps beslissen trouwens zelf welke klasse ze toepassen voor opslag van gebruikergegevens, en zouden dus ook 'No Protection' kunnen kiezen; in dat geval zijn de gegevens niet beschermd bij diefstal of verlies van het device.)

Het FBI-bevel

De FBI eiste van Apple een methode die 1) "will bypass or disable the auto-erase function whether or not it has been enabled", en 2) "will enable the FBI to submit passcodes to [the device] for testing electronically via the physical device port, Bluetooth, Wi-Fi, or other protocol available on [the device]" (want de passcode kan normaal alleen via het on-screen toetsenbord worden ingevoerd), en 3) "will ensure that when the FBI submits passcodes to [the device], software running on the device will not purposefully introduce any additional delay between passcode attempts (...)". De FBI wil dus ongelimiteerd en zonder softwarematig geïntroduceerde vertraging tussen passcode-pogingen geautomatiseerd passcodes kunnen uitproberen via een kabeltje, Bluetooth of Wi-Fi, zonder te riskeren dat de auto-erase-functie wordt getriggerd.

Technisch gezien kan Apple aan de eis van de FBI voldoen door een aangepaste versie van iOS

Er is op iOS-devices sprake van twee geheime codes: de *Passcode Key* en de *Hardware Key*

De FBI eiste iOS-firmware die auto-erase en passcode delays uitschakelt, en toestaat passcodes (geautomatiseerd) uit te proberen zonder die op het scherm in te toetsen

beschikbaar te stellen. Een Apple-executive sprak in die context over "GovtOS", anderen trokken "FBI" en "iOS" samen tot "FBiOS". Het iOS-beveiligingsmodel maakt dat nieuwe iOS-firmware door een iOS-device alleen wordt geaccepteerd indien deze digitaal is ondertekend onder Apple's eigen root CA, waarvan het certificaat op iOS-devices is opgeslagen (in de BootROM). Zonder zo'n ondertekening weigert een iOS-device de firmware. Een door Apple ondertekende variant van iOS zou via de Device Firmware Upgrade-functie (DFU) als ramdisk in het werkgeheugen van een inbeslaggenomen device moeten worden geladen en uitgevoerd. Dat kan zonder passcode. Indien de gebruiker de Find My iPhone-functie heeft ingeschakeld, zijn Apple ID-credentials nodig, maar daarvoor zou Apple eventueel een bypass kunnen maken voor de FBI.

Op devices met een A7-chipset of nieuwer worden de extra vertraging en auto-erase afgedwongen door de Secure Enclave. Maar naar verluidt zou de L4-firmware die in de Secure Enclave draait door Apple zelf te updaten
zou zijn, zónder dat gebruikersdata wordt gewist [Guido2016, Kelley2016]. Als dat klopt, wat toch enigszins saillant zou lijken, dan kan Apple technisch gezien ook voor devices met een A7-chipset of nieuwer voldoen aan dit FBI-bevel.

De FBI stelt in haar bevel dat de aangepaste iOS-firmware alléén moet kunnen worden uitgevoerd op het device waarop het bevel betrekking heeft, gebaseerd op unieke identifiers: "serial numbers, ECID, IMEI, etc.". Door de aangepaste firmware te binden aan unieke identifiers wordt het risico op misbruik teruggebracht, aangenomen dat de gebruikte identifiers op een vergrendeld device niet zomaar te vervalsen zijn. Maar de FBI heeft dus niet gevraagd om generieke firmware die tegen om het even welk iOS-device kan worden ingezet.

Het uitlekken van zo'n GovtOS-image heeft, op 't eerste oog, alleen gevolgen voor de veiligheid van één device. Het manipuleren van dat image om het geschikt te maken voor een ander device, of generiek te maken, eist ten minste dat een aanvaller het image zo weet te manipuleren dat een collision optreedt in het hashalgoritme dat wordt gebruikt bij het genereren van de ondertekening (de 'SHSH-blob'). De kans dat zo'n aanval kan worden uitgevoerd vóórdat de hele wereld alweer op de volgende versie van iOS draait, en de uitgelekte GovtOS-image z'n waarde heeft verloren, is waarschijnlijk klein, maar ook niet uit te sluiten. De FBI stelt in haar bevel (daarom?) dat de firmware on-site bij Apple zelf, dus op de Apple-campus in Cupertino, op het device mag worden geladen. Als de firmware de fysieke grenzen van de Apple-campus nimmer verlaat, is er minder gelegenheid voor ongewenste distributie (resteert de insider threat).

Het werken met een device-specifiek GovtOS-image betekent dat voor elk toekomstig te onderzoeken device een nieuw image moet worden gemaakt. Tenzij de FBI toegang heeft tot de iOS-broncode en de private key die Apple gebruikt voor ondertekening, moet Apple dat doen. Het is best mogelijk een voldoende veilige interface op te zetten tussen de FBI en Apple. De FBI zou de relevante versie-informatie en unieke identifiers aan Apple kunnen toezenden, en Apple vervolgens, eventueel na een out-of-band controle, een nieuw GovtOS-image genereren.

Als de FBI de rechtszaak had voortgezet en Apple was blijven weigeren, zou de FBI volgens mediaberichten van plan zijn bruutweg toegang te eisen tot de iOS-broncode en Apple's private key. Volgens weer andere mediaberichten zou dat bij andere bedrijven reeds zijn gebeurd, op grond van de FISA.

Backdoor-light

Het feit dat Apple in staat is een iOS-variant te maken die via DFU kan worsden geladen, kan in zekere zin al worden opgevat als backdoor. Zij het eentje waarbij nog steeds de passcode moet worden geraden; een backdoor-light, zeg maar.

Het is niet uitgesloten dat andere methoden bestaan om gegevens te achterhalen of de passcode te brute-forcen; voor de iPhone 5c bleek dat laatste het geval. Indien een gebruiker iCloud-backups heeft ingeschakeld, dan staat een gedeelte van de gegevens op servers van Apple, versleuteld met een sleutel die bekend is bij Apple (dus zonder passcode of UID). En indien een device binnen 48 uur sinds de laatste ontgrendeling niet is uitgeschakeld of gereboot, en wordt gekoppeld met een computer die door het device reeds wordt vertrouwd, is het eveneens mogelijk om toegang tot sommige

gegevens te krijgen: dan start de synchronisatie namelijk zonder dat de passcode opnieuw hoeft te worden ingevoerd. Maar dat zijn toevalstreffers die zich in de opsporingspraktijk vermoedelijk zelden voordoen, en waarbij bovendien onbekend blijft of er belangrijke gegevens op het device staan die niet in de backup staan. (Bij San Bernardino bleek dat trouwens niet het geval.)

Techbedrijven en overheden

Bij San Bernardino staat buiten kijf dat het gaat om een dader van de moord op 14 personen, is de betrokkene dood, en heeft de eigenaar van de telefoon, de werkgever van de dader, toestemming gegeven voor ontgrendeling. Tóch weigert Apple. 'Apple vs FBI' gaat dus niet over de (on)mogelijkheid om toegang te krijgen tot gegevens op deze ene iPhone, maar om de vraag in hoeverre van techbedrijven mag worden verlangd dat zij inspanningen leveren ter ondersteuning van opsporings- en inlichtingenwerk. Ook de (legitieme) vijand gebruikt moderne technologie en kan beschikken over een niveau van beveiliging dat, kijkend naar bijvoorbeeld iOS-devices met de Secure Enclave, toch behoorlijk hoog begint te worden. Dat is niet goed of fout; het is gewoon een realiteit.

Dat Apple zegt zes tot tien engineers twee tot vier weken te moeten inzetten om de gevraagde software te maken, soit; dat gaat over kosten en beschikbaarheid van personeel. Er zijn belangrijkere vragen: als Apple dit verzoek inwilligt, moeten dan ook andere techbedrijven dit soort verzoeken tegemoet zien? Moet een medewerkingsplicht zich kunnen uitstrekken tot het op afstand laten inschakelen van een microfoon of camera? En tot toegang tot broncode en geheime sleutels? Moeten verzoeken van andere landen worden ingewilligd? Wie beslist daarover, en hoe?

Betogen dat techbedrijven per definitie geen medewerking moeten verlenen aan opsporingsdiensten en inlichtingen- en veiligheidsdiensten, staat gelijk aan het ontkennen van de rechtsstaat. In een rechtsstaat worden belangen immers altijd tegen elkaar afgewogen, en zijn er geen belangen die te allen tijde als troefkaart kunnen worden gespeeld. In verschillende rechtsstaten, waaronder Nederland, is reeds sprake van bepaalde medewerkingsplichten: bijvoorbeeld de plicht voor aanbieders van openbare communicatienetwerken om aftapbaar te zijn. Discussie over medewerkingsplichten ging en gaat, ook in het debat over de Wiv20xx, niet of nauwelijks om een principieel 'voor' of 'tegen', maar vooral over voorwaarden (kosten, verantwoordelijkheden, beveiliging, schade), toezicht, en wettelijke waarborgen (bescherming van grondrechten, noodzaak/proportionaliteit/subsidiariteit).

Dat misbruik niet is uit te sluiten, bleek ook bij tapvoorzieningen: zo werd de mobiele telefoon van de premier van Griekenland aldaar illegaal afgeluisterd via (zeer verfijnde) spyware op een tapvoorziening bij de betrokken telecomaanbieder [Spectrum2005]. Zo'n incident is echter geen bewijs dat tapvoorzieningen massaal onveilig zijn en worden misbruikt door onbevoegden (of bevoegden). Gezonde skepsis over opsporings- en inlichtingenbevoegdheden is een deugd, maar vooralsnog moet worden vastgesteld dat er weinig voorbeelden bekend zijn van (overtuigende) casussen van misbruik. Als het klopt dat bij de NSA in een decennium tijd een dozijn LOVEINT-incidenten hebben gespeeld, en er niet óók tientallen of honderden niet-opgemerkte gevallen van oneigenlijk gebruik zijn, is dat toch niet heel slecht voor zo'n enorme organisatie. Zonder daarmee de ernst van die incidenten te ontkennen of te concluderen dat de status quo helemaal jofel is. Het blijft tandenknarsen.

Afsluiting

Had Apple moeten meewerken aan het verzoek van de FBI? Er zijn op z'n minst heldere voorwaarden, waarborgen en effectief toezicht nodig. De huidige situatie, waarin de FBI vertrouwt op een (generieke) 0-day is in elk geval minder florissant dan dat de FBI is genoodzaakt tot (specifieke) medewerking van Apple. Het is denkbaar dat de FBI de derde partij al langer voor handen had en simpelweg hoopte dat Apple onder druk zou buigen voor het bevel, zodat de FBI meer dan één methode zou hebben zonder daadwerkelijk een juridisch precedent te veroorzaken. Want ook voor de FBI is de uitkomst van zo'n rechtszaak onzeker, zoals hen duidelijk zal zijn geworden uit de massale bijval die Apple vanuit de (advocaten van de) Amerikaanse techsector en burgerrechtenbewegingen wist aan te wakkeren.

[Apple2015] (versie september 2015, bezocht 2 april 2016), https://www.apple.com/business/docs/iOS_Security_Guide.pdf
[Guido2016] https://blog.trailofbits.com/2016/02/17/apple-can-comply-with-the-fbi-court-order/
[Kelley2016] https://twitter.com/JohnHedge/status/699882614212075520
[Snowden2016] http://www.ibtimes.co.uk/apple-vs-fbi-snowden-says-decapping-can-crack-iphone-used-by-san-bernardino-attacker-syed-farook-1545397
[Spectrum2005] http://spectrum.ieee.org/telecom/security/the-athens-affair

In elke Madison Gurkha Update vragen wij een klant het spreekwoordelijke hemd van het lijf met betrekking tot zijn of haar relatie met IT-beveiliging. Dit keer 8 vragen aan Ton Bogerd van VECOZO.

8 vragen aan ...

... Ton Bogerd, ICT-manager bij VECOZO, het digitale knooppunt voor ketenpartijen in de zorg.

1 Wat doet VECOZO?

VECOZO is hét landelijk communicatiepunt voor de zorg. VECOZO zorgt voor een veilige en kwalitatief hoogwaardige omgeving waarin ketenpartijen administratieve gegevens uitwisselen. De organisatie is opgericht door een aantal zorgverzekeraars vanuit de behoefte aan administratieve lastenverlichting voor de hele keten. Alle zorgverzekeraars, zorgkantoren, bijna alle zorgaanbieders en (indirect) gemeenten zijn bij VECOZO aangesloten. In 2015 zijn via VECOZO meer dan 2 miljard berichten uitgewisseld in het zorgdomein.

2 Je bent ICT-manager bij VECOZO. Wat houdt deze functie precies in?

Ik ben verantwoordelijk voor het realiseren van de doelstellingen van de afdeling Informatie- & Communicatietechnologie. Hiertoe houd ik me bezig met het opstellen van afdelingsbeleid, plannen voor de middellange termijn en het inrichten en aansturen van een afdeling van medewerkers met gevarieerde vaktechnische werkzaamheden. Als ICT-manager maak ik deel uit van het managementteam en ben ik nauw betrokken bij de informatiebeveiliging binnen VECOZO.

3 Waar ben je trots op?

VECOZO is altijd in beweging. Op dit moment nemen we een mooie stap voorwaarts richting een toekomstvaste infrastructuur. Daarmee lopen we innovatief voorop met ons Software Defined Datacenter (SDDC) en applicatielandschap. Tijdens de verbouwing is de winkel natuurlijk open. Het is echt een grote prestatie dat VECOZO dit project samen met OpenLine, EMC en CISCO binnen 1 jaar heeft gerealiseerd.

"Tijdens piekmomenten behandelen we 815 klantverzoeken per seconde"

4 Hoe is informatiebeveiliging opgezet binnen de organisatie?

VECOZO heeft haar informatiebeveiliging ingericht conform onder andere WebTrust (certificaatuitgifte) en de norm NEN7510. Op basis hiervan hebben we een pakket van technische en organisatorische maatregelen getroffen. Een Information Security Management System (ISMS) staat centraal, van waaruit beheersdoelstellingen- en maatregelen worden opgesteld, beheerd en geaudit.
We hebben een robuuste security-architectuur en gelet op de aard van onze dienstverlening is dit niet meer dan vanzelfsprekend. Bovendien wordt VECOZO jaarlijks door een externe partij geaudit, voeren we continue geautomatiseerde pentests uit en laten we onze ICT-omgeving regelmatig door Madison Gurkha onderzoeken.

5 Hoeveel mensen houden zich bezig met informatiebeveiliging?

Naast de fulltime functies bestaande uit een Compliance en Risk Officer, Security Officer en Security Coördinator zijn er drie beveiligingscoördinatoren die een deeltaak vervullen rondom informatiebeveiliging. En daarnaast eigenlijk elke VECOZO-medewerker! Informatiebeveiliging is namelijk in welke functie dan ook onderdeel van het werk. We moeten ons allemaal bewust zijn van informatiebeveiliging en hiernaar handelen.

6 **Wat zijn de belangrijkste uitdagingen op het gebied van informatiebeveiliging?**

VECOZO is een innovatief bedrijf dat inzet op een hoge mate van automatisering binnen ICT, dat zie je ook terug in onze ICT-security-maatregelen. We zitten momenteel in een omschakeling van handmatige naar meer geautomatiseerde preventie en detectie. Er zijn te veel leveranciers die vooral willen verkopen op basis van FUD (Fear, Uncertainty and Doubt). Het is voor ons essentieel dat we díe producten inzetten die echt iets toevoegen aan onze security-architectuur.

7 **Welke maatregelen worden genomen om bestaande IT-beveiligingsrisico's onder controle te houden?**

VECOZO hanteert een set aan preventieve en detectieve maatregelen. Denk hierbij aan maatregelen als change-management, patchmanagement, anti-malware, exploit-preventie en -mitigatie, pentesting, etc., maar ook het continu monitoren van dreigingen en kwetsbaarheden.

8 **Hoe ondersteunt Madison Gurkha daarbij en wat zijn je ervaringen tot nu toe?**

Madison Gurkha voert voor VECOZO pentests uit, zowel op nieuwe diensten voor we deze in productie nemen, als voor bestaande diensten. Bestaande diensten worden, afhankelijk van hun classificatie, periodiek opnieuw onderzocht. Zo zorgen we ervoor dat onze diensten veilig zijn en veilig blijven.

We hebben hierbij goede ervaringen met Madison Gurkha. Het is een professionele partij die met ons meedenkt op het gebied van allerlei beveiligingsvraagstukken. De rapporten zijn helder en goed leesbaar.

"Op dit moment nemen we een mooie stap voorwaarts richting een toekomstvaste infrastructuur. Daarmee lopen we innovatief voorop met ons Software Defined Datacenter (SDDC) en applicatielandschap."

In dit extra Inzicht gaat security consultant Ben Brücker in op de technische risico's van Bring Your Own Device.

KEERZIJDE van

Mobiele apparaten zijn niet meer weg te denken uit werkplekken en kantoren. Deze apparaten bieden mogelijkheden om de productiviteit van uw werknemers te verhogen, maar brengen ook hun eigen risico's mee. Hebben uw werknemers telefoons en tablets van de zaak? Of neemt iedereen zijn eigen apparaat mee? In dit artikel kijken we naar de mogelijke risico's en geven we tips hoe deze geminimaliseerd kunnen worden.

Mobiele apparaten zullen vanwege hun kleine formfactor en het gebruiksgemak bijna overal mee naartoe worden genomen door de werknemers. Ook zijn ze ontwikkeld om permanent in verbinding te staan met het internet. Dit kan via Wi-Fi, maar ook via Bluetooth, usb-kabels of zelfs de traditionele ethernetkabel. Omdat veel functionaliteit afhangt van de internetverbinding zal het apparaat regelmatig worden verbonden met netwerken die minder veilig zijn dan uw bedrijfsnetwerk. Denk hier aan de gratis Wi-Fi-netwerken in de trein en koffiezaken, maar ook het thuisnetwerk van de werknemer.

Wanneer werknemers eigen tablets en mobiele telefoons meenemen en aansluiten op het bedrijfsnetwerk, dan valt dat onder de noemer `bring your own device' (BYOD). BYOD maakt het voor IT-afdelingen aanzienlijk lastiger om controle en inzicht te houden over het eigen netwerk. Deze apparaten beslaan namelijk een groot spectrum van verschillende hardware, besturingssystemen en software.

Uiteindelijk is het meest voorkomende probleem dat medewerkers hun mobiele apparaten verliezen. Dit kan per ongeluk gebeuren, maar kan ook het resultaat zijn van diefstal. Denk eens na wat voor gegevens van uw bedrijf hierop achterblijven. Het gaat hier om onder andere e-mails, gevoelige documenten, contactgegevens en zelfs GPS-data.

Wat kan een aanvaller?

Mobiele apparaten zijn computers. Ze zijn daarom ook kwetsbaar voor `ouderwetse' aanvallen via software. Denk daarbij aan malafide applicaties of kwetsbaarheden die worden uitgebuit door op een link in een e-mail te klikken.

Naast de traditionele aanvalsvectoren via software hebben mobiele apparaten het bijkomende risico dat een gebruiker ze altijd bij zich heeft. Hierdoor is de kans dat het apparaat wordt gestolen of verloren groter dan bijvoorbeeld bij pc's. Wanneer een apparaat in handen van een kwaadwillend persoon valt, dan zijn er afhankelijk van het apparaat, besturingssysteem en configuratie verschillende mogelijkheden om de data van de gebruiker te achterhalen.
De authenticatie is de eerste laag van bescherming die de aanvaller moet omzeilen. Als er geen pincode, wachtwoord of andere vorm van authenticatie wordt gebruikt zal de aanvaller kinderlijk eenvoudig gevoelige informatie kunnen inzien. Zo kan hij applicaties openen waarin de gebruiker is ingelogd. Hierdoor is er toegang tot onder andere e-mails, opgeslagen bestanden, bezochte websites en foto's.

Ook is het mogelijk om een back-up van alle data te maken op een systeem van de aanvaller. Als hij het systeem terugbrengt voordat het wordt gemist dan kan in alle rust de data worden bekeken zonder dat de gebruiker weet dat er iemand toegang heeft gehad. Ook wanneer de authenticatie niet direct kan worden omzeild zijn er toch mogelijkheden. Zo is de sd-kaart, die voor extra opslag dient, over het algemeen niet versleuteld. Hier worden zaken zoals foto's en downloads opgeslagen die door iedereen uit te lezen zijn.

Er zijn gebruikers die hun mobiele apparaten `rooten' of `jailbreaken'. Hierdoor zijn modificaties aan het besturingssysteem mogelijk en kan men applicaties installeren die, in het geval van iOS, niet uit de officiële App Store komen. Van deze `root'-toegang zal een aanvaller gebruik maken om, onder andere, de lokale opslag van applicaties uit te lezen. In deze lokale opslag zijn vaak logingegevens of persoonlijke informatie opgenomen. Ook als een gebruiker zijn apparaat niet zelf heeft `geroot' zijn er vooral in oudere versies van de besturingssystemen kwetsbaarheden beschikbaar waarmee `root'-toegang kan worden verkregen. Een voorbeeld hiervan is de `Android Futex Requeue'-kwetsbaarheid die in het Metasploit-framework is opgenomen.

Is beleid een oplossing?

Na het opnoemen van de risico's die aan het gebruik van dit soort apparaten zijn verbonden lijkt het misschien de beste oplossing om het zakelijk gebruik hiervan te verbieden. Dit is waarschijnlijk het slechtste dat u kan doen. Mensen maken nou eenmaal graag gebruik van dit soort nieuwe technologieën en zullen het gemak hiervan missen, waardoor ze om het bedrijfsbeleid heen gaan werken. Hierdoor heeft de IT-afdeling nog minder zicht op wat er allemaal met apparaten en data op het netwerk gebeurd.

BYOD-gemak

Op het internet zijn er voldoende lijsten te vinden met nuttig beleid omtrent dit soort apparaten. We zullen er hier een aantal bespreken:

Maak gebruik van sterke wachtwoorden
Een wachtwoord of pincode is de eerste horde die een aanvaller moet nemen om bij gevoelige data te komen. Het is hier van belang om te kiezen voor sterke wachtwoorden, en niet voor korte pincodes.

Zoals te zien is in de zaak tussen de Amerikaanse FBI en Apple is het in moderne versies van iOS niet eenvoudig om de pincode-beveiliging te omzeilen. Wanneer gebruikers echter hun eigen apparaten meenemen is de kans groot dat er ook oudere apparaten worden gebruikt waarbij dit wel te omzeilen valt.

Zo mogelijk, kies dan ook voor de optie dat de informatie op het apparaat wordt gewist na te veel foutieve inlogpogingen. Op deze manier is men beschermd tegen brute-force-aanvallen.

Denk ook na of u vingerafdrukken wilt toestaan als authenticatiemiddel. Hierbij is het een extra risico dat de benodigde vingerafdrukken meestal op het apparaat zelf aanwezig zijn.

Ga na welke beschermingen er zijn tegen `lockscreen-bypass'-aanvallen
Ook al kan een aanvaller het wachtwoord niet raden, toch zijn er vaak manieren om beperkte functionaliteit van het apparaat te bereiken. Zo is er een uitgebreide lijst te vinden van `lockscreen-bypass'-aanvallen per iOS versie en worden er mogelijke beschermingen aangedragen.

Zorg dat het bestandssysteem is versleuteld.
Als een aanvaller de data niet kan benaderen door de authenticatie te omzeilen kan deze proberen het bestandssysteem direct uit te lezen. Door gebruik te maken van encryptie kan dit worden tegengegaan.

Gebruik software waarmee apparaten op afstand gewist kunnen worden.
Wanneer apparaten in verkeerde handen vallen is het van belang om een aanvaller zo weinig mogelijk tijd te geven om hiervan misbruik te maken. Er bestaat software waarmee u de data die op een apparaat staat opgeslagen, op afstand kunt verwijderen. Het is nuttig om deze optie te hebben, maar vertrouw er niet blindelings op. Deze techniek werkt namelijk niet wanneer het apparaat niet met het internet verbonden is.

Stimuleer het snel melden van het verlies van een apparaat.
Als werknemers bang zijn voor negatieve consequenties bij het verliezen van een apparaat zullen ze geneigd zijn om het niet direct te melden, in de hoop dat ze het toch nog terugvinden. Hierdoor heeft een aanvaller meer tijd om het apparaat te kraken.

Maak gebruik van veilige/privacy-vriendelijke software
Werknemers hebben bepaalde use-cases voor hun apparaten. Inventariseer welke behoeften er zijn en kijk naar software om deze behoefte te vervullen. Gebruiken de werknemers Dropbox om bestanden uit te wisselen en Whatsapp om te communiceren? Bekijk dan of het gebruik van deze software past binnen het bedrijfsbeleid. Zo niet, geef dan geschikte alternatieven.

Wat het beleid ook is, het is van belang om dit beleid klaar te hebben liggen. Tijdens een incident is het niet de juiste tijd om hierover na te denken omdat er dan overhaaste beslissingen worden genomen.

Mobile Device Management

Een goed beleid voor dergelijke punten is belangrijk om te hebben. Maar in bedrijven is het moeilijk om het gebruik hiervan bij iedereen af te dwingen. Daarom bestaat er speciale software, zogenaamde `mobile device management' (MDM)-software, om apparaten te beheren. Met dit type software kan men applicaties, data, configuraties en patches distribueren over de aangesloten apparaten. In de basis mag van deze softwarepakketten verwacht worden dat de volgende configuraties kunnen worden afgedwongen:

- Gebruik van sterke wachtwoorden;
- Minimaal patch-level van het apparaat;
- Gebruik van bestandsversleuteling;
- Blokkeren van `rooted' of `jailbroken' apparaten.

Daarnaast is functionaliteit voor het vinden van verloren apparaten, en het wissen hiervan ook redelijk standaard. Natuurlijk zijn er ook pakketten die extra functionaliteit bieden, zoals extra versleuteling van applicaties in `containers'.

Helaas zijn ook MDM-oplossingen niet bulletproof. Dit is bijvoorbeeld te zien in de presentatie Practical Attacks against Mobile Device Management Solutions van het bedrijf Lacoon Security. Ze demonstreerden hier een aanval hoe zowel iOS als Android apparaten `geroot' konden worden zonder dat dit problemen opleverde met de aanwezige MDM-software. Hierna waren ze in staat om de beveiligde e-mails te benaderen.

Conclusie

Zoals bij veel gevallen in de IT-wereld is er helaas geen geheel veilige oplossing voor de omgang met mobiele apparaten. Maar het is wel mogelijk om risico's te minimaliseren en gevolgen te mitigeren. Hiervoor is het van belang om over de volgende zaken na te denken:

- Wat zijn de mogelijke risico's?
- Welk beleid helpt om deze risico's te mitigeren?
- Welke software helpt om dit beleid te implementeren?

Mobile is een noodzakelijk kwaad, maar biedt vooral ook veel mogelijkheden om productiviteit en efficiëntie te verhogen. Start daarom vandaag met het bepalen van het beleid en voorkom onnodige beveiligingsrisico's.

Goed om te weten: tijdens de Black Hat Sessions Part XIV: 'Mobile (In)security' op 23 juni a.s. zal door externe experts zowel verbreding als verdieping worden gezocht rondom dit onderwerp.

In de ITSX-rubriek vertelt Ralph Moonen, directeur van ITSX, over de laatste ontwikkelingen in de IT-beveiligingswereld en rondom ITSX in het bijzonder.

Klaar voor de toekomst

ITSX heeft de laatste maanden naast zeer interessante projecten ook een flinke personeelswisseling ondergaan. Ralph Moonen, directeur van ITSX, geeft u een persoonlijke update om de veranderingen mee te delen en iets over de strategie van ITSX in de komende tijd te vertellen.

Directie

Binnen de directie heeft een wijziging plaatsgevonden. Arthur Donkers die in 2013 als partner bij ITSX is aangetreden, heeft om persoonlijke redenen besloten om uit de directie van ITSX te stappen. Hij zal nog wel als associate voor ITSX opdrachten blijven uitvoeren maar Arthur's wens is om daarnaast ook andere ventures te starten en op te bouwen. Hij heeft daarom per februari 2016 zijn bestuursfunctie opgegeven. Wij wensen hem het beste toe in zijn toekomstige ondernemingen. Ralph Moonen en Remco Huisman vormen hiermee het voltallige bestuur van ITSX.

Consultants

Ook bij de consultants is het nodige veranderd. Marcus Bakker heeft een nieuwe positie aanvaard bij de ING Bank, maar daar staat tegenover dat we twee nieuwe consultants hebben aangenomen. De eerste, die reeds is gestart, is Arjan van den Ham. Arjan is zijn carrière begonnen bij Deloitte en is de laatste jaren Operations Manager geweest van het SOC van Unisys. ITSX wil met de komst van Arjan de dienstverlening rondom Security Operations en Security Management consultancy een boost geven.

De tweede nieuwkomer bij ITSX is Enrico Kleijbeuker. Enrico komt van T-Mobile alwaar hij security specialist was en veel ervaring heeft opgedaan met standaarden, compliance en privacy.

Account Management

Na het vertrek van Thorgal Nicasia is de account management positie een tijdje onvervuld geweest. We hebben echter onlangs een nieuwe account manager aangesteld die zich op korte termijn hier aan jullie zal voorstellen.

Al met al dus een tamelijk turbulente tijd voor ITSX, maar wel een periode die ons de kans geeft om onze groeistrategie te verwezenlijken en focus te herwinnen. We kijken dan ook uit naar de komende maanden met veel nieuwe projecten en nieuwe mensen!

Projecten

ITSX heeft in het eerste kwartaal een zeer sterke stijging gezien van het aantal projecten dat aan de nieuwe privacy wetgeving is gerelateerd (meldplicht datalekken). Het valt hierbij op dat sommige (met name kleinere) organisaties nog helemaal niet weten van het bestaan van de meldplicht. Wij

hebben daarom vrijwel al onze klanten hierover persoonlijk geïnformeerd. Dit heeft in diverse gevallen geleid tot aanpassingen in processen en procedures.

Naast de privacywetgeving heeft ITSX recent diverse projecten uitgevoerd op het gebied van Internet of Things (IoT). De draadloze communicatie tussen apparaten (bijvoorbeeld home-automation systemen, voertuig volg- en meetsystemen of smartphones) en een back-end systeem waar de verzamelde gegevens verwerkt worden, moet tenslotte ook worden beveiligd. Bijkomend probleem is dat kwetsbaarheden in die systemen ook met secure software updates, op afstand, moeten worden beveiligd. Dit is niet altijd eenvoudig waardoor een gedegen analyse noodzakelijk is om alle risico's te identificeren.

Black Hat Sessions: "Look Ma, no wires"

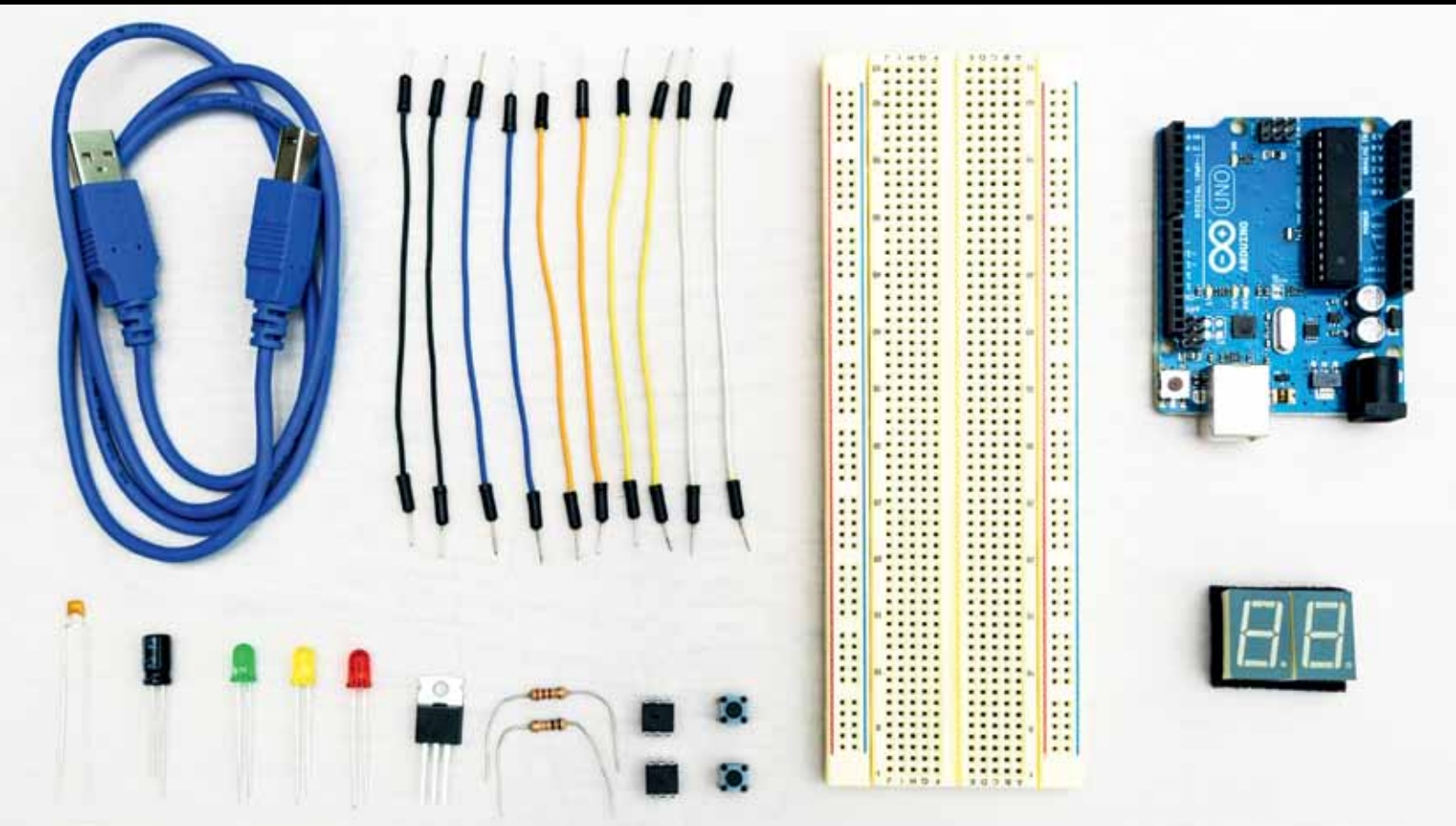
Met name de recente ervaring op het laatstgenoemde onderwerp (draadloze communicatie) zal het onderwerp zijn van mijn presentatie op de aankomende Black Hat Sessions. Ik zal hier vertellen over de nieuwste draadloze technologieën, waarbij de nadruk ligt op het beheersen van de risico's. In de laatste jaren zijn diverse nieuwe technologieën op de markt gekomen zoals 4G, ZigBee, XBee, LoraWan en anderen. Deze worden gebruikt voor onder andere telefonie home-automation, sensor netwerken of het besturen van drones. Sommige van de apparaten hebben zelfs een directe internetverbinding waarbij vaak gebruik gemaakt wordt van de nieuwere IPv6 standaard in plaats van de bekendere IPv4 standaard. Ook dit brengt risico's met zich mee. De presentatie zal zeker een technische component hebben maar zal voornamelijk gericht zijn op het bespreken van de essentiële maatregelen voor beveiliging (en monitoring) van deze nieuwe ontwikkelingen.

Dat ITSX aan de start van een nieuwe periode staat zal duidelijk zijn: sterker en beter gefocust, met een zeer ervaren team van gemotiveerde en senior consultants. Wij hebben er erg veel zin in!

ITSX

Heb jij de juiste hackers-mindset?

Wil je het liefst elk stukje techniek dat je tegenkomt meteen ontrafelen?
Reverse engineer je je eigen CV-ketel om deze met een Arduino aan te kunnen sturen?
In een inspirerende omgeving met echte ethical hackers kun je je bij ons verder bekwamen.



Wij zijn per direct opzoek naar:

Security Consultants (SC)

Senior Security Consultants (SSC)

Junior Security Consultants (JSC)

Wij bieden:

- Een interessante functie binnen een toonaangevend IT-beveiligingsbedrijf
- Werk aan uitdagende projecten voor grote (internationale) organisaties
- Minstens 1 dag per week tijd voor "NERD" Never-Ending Research and Development
- Kansen om je kennis voortdurend uit te breiden en jezelf te ontwikkelen
- Een leuk team met passie voor het vak

Kijk voor meer informatie over de verschillende vacatures op onze website.
Heb je interesse, stuur dan snel je motivatie met CV naar jobs@madison-gurkha.com.

Madison Gurkha
Your Security is Our Business

www.madison-gurkha.com