Madison Gurkha
Your Security is Our Business

26 JAN 2016 UPDATE

ITSX

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

DE COLUMN

Weer een jaar voorbij. Tijd om terug, maar vooral ook vooruit te blikken.

Laten we beginnen met een terugblik. 2015 was het jaar waarin Madison Gurkha haar 15-jarig bestaan heeft gevierd. In die vijftien jaar zijn we uitgegroeid van een kleine beloftevolle start-up tot een gerenommeerd technisch IT-beveiligingsbedrijf. Ons jubileum hebben we begin oktober met het hele team gevierd in Berlijn. Perfecte timing. Een lang weekend in oktober waarin het zonnig was en het 20 graden werd. We kwamen erachter dat de Oktoberfesten niet alleen in München worden gevierd, maar ook in Berlijn (op de Alexanderplatz vlak achter ons hotel). Als klap op de vuurpijl was het ook het weekend van 25 jaar Duitse eenwording, met een groot volksfeest bij de Brandenburger Tor.

2015 was ook het jaar dat Madison Gurkha is verhuisd. De Groene Toren is verkocht en daarmee ook de stek waar we vele jaren gevestigd waren. De eigenaar had andere plannen met de locatie en verzocht ons dringend te verhuizen. Zodoende zijn we sinds juni jl. gevestigd in een prachtig nieuw kantorenpand, 50 nummers verderop op de Vestdijk.

Ook het afgelopen jaar is duidelijk zichtbaar geweest dat security een hot topic is en dat de markt steeds volwassener wordt. Wat te denken van bijvoorbeeld de overnames van Pine en Fox-IT? Die laatste spreekt het meest tot de verbeelding met een overnamesom van ruim 130 miljoen euro, betaald door een Engels bedrijf. Ik ben benieuwd wat de Nederlandse overheid (en vooral de AIVD) daarvan vindt. Nog even en er is nog maar één gespecialiseerd zelfstandig technisch IT-beveiligingsbedrijf over.

Er is nog meer gebeurd in de wereld van informatiebeveiliging. Heel veel zelfs, maar laat ik me beperken tot een kleine bloemlezing van hacks in het afgelopen jaar: Vtech, Ashley Madison (nee dit heeft NIETS met Madison Gurkha te maken), SONY, de OPM data breach en Talk Talk. Er zijn nog genoeg andere hacks die het nieuws hebben gehaald en nog veel meer die het nieuws niet hebben gehaald. De meeste organisaties hangen beveiligingsincidenten namelijk liever niet aan de grote klok, maar houden ze onder de pet of vegen ze onder het tapijt. Zolang het maar niet bekend wordt.

Dit laatste is een mooi bruggetje naar een vooruitblik. Sinds 1 januari 2016 is de meldplicht datalekken van de Autoriteit Persoonsgegevens (voorheen: College bescherming persoonsgegevens) van kracht. Vanaf begin dit jaar is het nog maar de vraag of het verstandig is om incidenten onder het tapijt te vegen wanneer er persoonsgegevens in het spel zijn. Dat zou wel eens een dure beslissing kunnen zijn, met een prijskaartje tot € 810.000 of 10 procent van de netto-omzet. Heeft u al goed nagedacht over wat de meldplicht datalekken voor uw organisatie betekent? Uiteraard helpen wij u graag daarbij. Verderop in deze Update gaan we uitgebreid in op deze nieuwe meldplicht.

Er gaat nog veel meer gebeuren dit jaar, maar laat ik me niet al te veel wagen aan voorspellingen. Wat ik wel zeker weet is wat er verder nog in deze Update te lezen is. Zo gaat Thijs Hodiamont in de rubriek 'De Hack' in op fat-clients. Vaak lijkt de security daarvan aardig op orde totdat we verder kijken en de client decompileren en/of reverse engineeren. Dan blijkt opeens de hele beveiliging in de client te zitten. Van webapplicaties weten we al dat dit bepaald geen goed idee is. Rick van Bodegraven geeft inzicht in de meerwaarde van het inspecteren van de broncode bij een applicatieonderzoek. Met deze aanpak kan onder andere veel beter bepaald worden hoe robuust de beveiliging is. Zijn er her en der pleisters geplakt of is de beveiliging structureel opgelost? Mijn mede-compagnon Walter Belgers heeft de unieke Finse security conferentie T2.fi bezocht en daar een demonstratie over lockpicking gegeven. Het is hem gelukt om live op het podium een zeer lastig Assa Abloy slot te openen zonder daarbij geweld of sleutels te gebruiken. De unieke expertise van Walter komt ook regelmatig van pas bij geavanceerde onderzoeken waarbij fysieke beveiliging, social engineering, malware en IT-security bij elkaar komen.

Rest mij iedereen een heel goed nieuw en veilig jaar te wensen. Ik hoop dat het een jaar wordt waarin organisaties laten zien dat ze fatsoenlijk omgaan met privacygevoelige gegevens van u en mij. Die boetes van de Autoriteit Persoonsgegevens zouden toch helemaal niet nodig moeten zijn…?!

Remco Huisman
Partner, commercieel directeur

Madison Gurkha krijgt een **nieuwe website!**

Het vernieuwen van onze website staat al een tijd op onze to-do-lijst. De huidige website past niet meer bij de professionele en volwassen uitstraling die we als Madison Gurkha uitdragen. Bovendien ontbreken er voor ons belangrijke functionaliteiten. We zijn dan ook blij te kunnen melden dat de realisatie van onze nieuwe website op dit moment in volle gang is.

Naast een nieuwe 'look-and-feel' met een meer persoonlijke uitstraling hebben we aandachtig gekeken naar de juiste menustructuur en inhoud van de website. Alle aanwezige kennis wordt verzameld in een heuse 'kennisbank' zodat u straks op één plek alle informatie kunt vinden die voor u van belang is. Denk hierbij bijvoorbeeld aan een blogpost, klantencase of publicatie.

Op de hoogte blijven van de actualiteit, belangrijke ontwikkelingen en kennis op het gebied van IT security doet u voortaan niet alleen meer via de Madison Gurkha Update maar ook via ons blog waar we regelmatig interessante content zullen plaatsen. Natuurlijk is de nieuwe website geschikt voor mobiel gebruik zodat u de informatie prettig op telefoon of tablet kunt lezen.

We kunnen niet wachten tot we de nieuwe website in gebruik kunnen nemen en hopen dat u net zo enthousiast gaat zijn als wij. De vernieuwde www.madison-gurkha.com gaat naar verwachting komende maart live.

Vacatures

Madison Gurkha groeit gestaag door en dat betekent ruimte voor nieuwe gedreven, enthousiaste collega's die de schouders eronder willen zetten en mee willen groeien in onze organisatie.

Wij zijn per direct opzoek naar:

- **Security Consultants (SC)**
- **Senior Security Consultants (SSC)**
- **Junior Security Consultants (JSC)**
- **Werkvoorbereider**

Geïnteresseerd? Kijk voor meer informatie over de verschillende vacatures op onze website. Voor vragen en meer informatie neem je contact op via 040-2377990 of stuur je een mail naar jobs@madison-gurkha.com.

Meldplicht datalekken van kracht

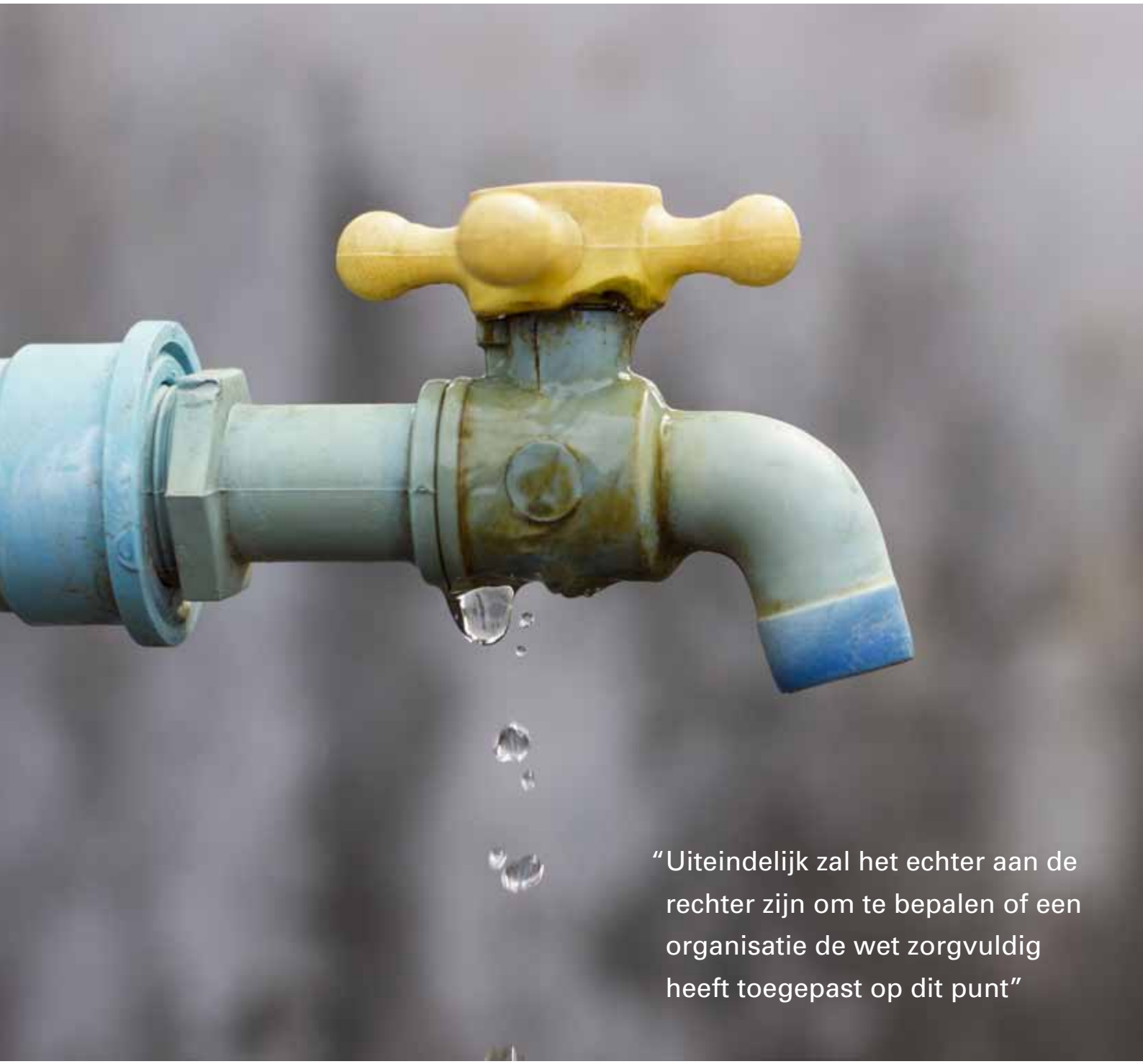
Alle bedrijven en overheden die persoonsgegevens verwerken op grond van de Wet bescherming persoonsgegevens (Wbp) zijn sinds 1 januari 2016 verplicht om een ernstig datalek direct te melden aan de Autoriteit Persoonsgegevens.
Het CBP heeft in december 2015 de definitieve beleidsregels voor de meldplicht datalekken gepubliceerd. Aan de hand van deze regels kan uw organisatie vaststellen of er sprake is van een datalek en aan wie u dit moeten melden.
Wij kunnen ons voorstellen dat het nogal wat vragen oproept. Bent u goed voorbereid en weet u welke stappen u moet ondernemen? In het interview op pagina 4 van deze Update geeft Louwers IP|Technology Advocaten uitgebreid uitleg en praktische tips. Zie ook de ITSX-rubriek op pagina 16 waar Marloes Kwakkel vertelt over de QuickScan Meldplicht Datalekken.

Namens alle Gurkha's een succesvol en veilig nieuw jaar gewenst!

Ook in 2016 staan we graag voor u klaar om meer grip te krijgen op uw digitale veiligheid en weerbaarder te worden voor geavanceerde aanvallers.

Deze keer een interview met Huub de Jong, advocaat en partner bij Louwers IP|Technology Advocaten over de meldplicht datalekken.

Klaar voor



"Uiteindelijk zal het echter aan de rechter zijn om te bepalen of een organisatie de wet zorgvuldig heeft toegepast op dit punt"

een datalek?

Sinds 1 januari 2016 bent u wettelijk verplicht datalekken te melden. Weet u wat u moet doen? Wij vroegen Huub de Jong, advocaat bij Louwers IP|Technology Advocaten om de nodige uitleg en praktische tips.

Wat houdt de meldplicht datalekken nu precies in?

Per 1 januari jl. zijn organisaties (zowel bedrijven als overheden) verplicht bepaalde datalekken te melden. Het gaat dan om datalekken waarbij persoonsgegevens zijn betrokken en waarbij degene die verantwoordelijk is voor de verwerking in Nederland is gevestigd. Een dergelijk datalek moet gemeld worden aan de Autoriteit Persoonsgegevens (voorheen: College bescherming persoonsgegevens) en in bepaalde gevallen ook aan de gedupeerde (betrokkene). Tegelijkertijd met de invoering van de meldplicht datalekken maakt de nieuwe wet het mogelijk dat de Autoriteit Persoonsgegevens hoge boetes op kan leggen. Deze boetes kunnen niet alleen opgelegd worden bij het niet melden van een datalek, maar ook bij andere schendingen van de Wet bescherming persoonsgegevens (Wbp) zoals de beveiligingsplicht.

Welke incidenten dienen er gemeld te worden en bij wie?

De organisatie die verantwoordelijk is voor de verwerking van persoonsgegevens moet de Autoriteit Persoonsgegevens in kennis stellen van inbreuken op de beveiliging die ernstig nadelige gevolgen hebben voor de bescherming van persoonsgegevens of inbreuken die tot een aanzienlijke kans hierop leiden. Ook de betrokkene moet op de hoogte gebracht worden, wanneer de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer. De praktische toepassing van deze wettelijke criteria zal nog niet altijd eenvoudig zijn.

Er wordt geschreven: "De inbreuk moet bovendien 'ernstig' zijn – en wat ernstig is, is een eigen afweging" Hoe maak je als organisatie deze afweging?

De wet heeft het niet over 'ernstig' maar kijkt vooral naar de gevolgen, zoals ik hierboven beschrijf. Dat maakt het nog niet eenvoudig om te bepalen waar de grens ligt tussen wat wel of niet gemeld dient te worden. Uiteindelijk zal ieder bedrijf daarin zijn eigen afweging moeten maken eventueel in samenspraak met zijn adviseurs. De Autoriteit Persoonsgegevens heeft beleidsregels gepubliceerd waarin ze aangeeft hoe de toezichthouder meent dat organisaties deze afweging moeten maken. Uiteindelijk zal het echter aan de rechter zijn om te bepalen of een organisatie de wet zorgvuldig heeft toegepast op dit punt.

Biedt de wettekst wel aanknopingspunten hiervoor?

Ja op bepaalde punten wel. Indien er passende technische beschermingsmaatregelen zijn getroffen hoeft een datalek niet gemeld te worden aan de betrokkene (wel aan de toezichthouder). Je kunt daarbij bijvoorbeeld denken aan het verlies van een usb-stick die degelijk met encryptie is beveiligd. Er moet dan wel een kopie beschikbaar zijn, want het verlies van persoonsgegevens kan ook een datalek opleveren. Om die reden dient het in beginsel bijvoorbeeld ook gemeld te worden indien een systeembeheerder per ongeluk een database met persoonsgegevens verwijdert waarvan geen kopie voorhanden is.

Een ander opvallend punt is de uitzondering voor financiële ondernemingen. Deze organisaties hoeven op basis van deze wet een datalek ook niet te melden aan de betrokkene. Een algemene meldplicht zou in de praktijk volgens de wetgever voor ongewenste situaties kunnen zorgen. Denk aan een bankrun. Financiële ondernemingen kunnen op basis van specifiek voor hen geldende regels overigens alsnog gehouden zijn een datalek te melden.

Hoe groot is de kans dat er daadwerkelijk boetes uitgedeeld gaan worden?

Dat zal de praktijk moeten uitwijzen. Aangezien de Autoriteit Persoonsgegevens een relatief kleine toezichthouder is, zullen er door de toezichthouder keuzes gemaakt moeten worden. Organisaties die veel en/of

CV

Huub de Jong is als advocaat gespecialiseerd in technologierecht. Hij heeft ruim vijftien jaar ervaring met het adviseren over juridische aspecten van complexe technologievraagstukken, het opstellen en beoordelen van (inter)nationale contracten, het oplossen van geschillen en zo nodig het voeren van procedures. Huub zet zijn juridische kennis en gevoel voor technologie graag in voor de strategische belangen van cliënten. Zijn aandachtsgebieden zijn IT- en internetrecht, security, privacy, auteursrecht en telecomrecht.

T +31 70 2400 836
M +31 6 1099 2888
E dejong@louwersadvocaten.nl
W www.louwersadvocaten.nl

"Wij adviseren organisaties om een op maat gemaakt draaiboek klaar te hebben liggen"

gevoelige gegevens verwerken zullen eerder het risico lopen beboet te worden. Hetzelfde geldt voor organisaties waarover geklaagd wordt bij de toezichthouder of organisaties die om een andere reden op bijzondere aandacht van de toezichthouder kunnen rekenen. Een goede beveiliging blijft uiteraard de beste remedie om de kans op boetes te verkleinen.

Wat valt er contractueel te regelen met afnemers en leveranciers?
Met afnemers en leveranciers zullen afspraken gemaakt dienen te worden over de uitvoering van de meldplicht. Dit is niet alleen verstandig, maar vaak ook wettelijk verplicht. De exacte invulling van deze afspraken is afhankelijk van de eigen capaciteit, beleid en de verdere contractuele relatie. Feitelijk vormen deze afspraken een uitbreiding op de bestaande verplichting om goede afspraken te maken over de beveiliging van persoonsgegevens met afnemers en leveranciers.

Is eventuele schade bijvoorbeeld te verhalen of verzekerbaar?
De markt die specifiek deze risico's afdekt is nog volop in ontwikkeling. De afgelopen tijd hebben diverse verzekeraars een cybercrimeverzekering op de markt gebracht. Hoewel de polisvoorwaarden per verzekering uiteenlopen wordt veel schade die een organisatie kan oplopen door een dergelijke verzekering gedekt. Het is zelfs niet ongebruikelijk dat de eventuele boetes die men krijgt vanwege schending van de meldplicht door de verzekeraar vergoed worden.

Welke consequenties heeft deze meldplicht concreet voor organisaties?
Voorheen hadden bedrijven meer ruimte om te bepalen of ze een datalek wilde melden aan de gedupeerden en zo ja, op welke manier. Deze ruimte is nu verregaand beperkt door de nieuwe wet, waarbij meestal ook de toezichthouder (Autoriteit Persoonsgegevens) geïnformeerd moet worden. Daarnaast kon de toezichthouder in het verleden geen boete opleggen wanneer een datalek niet werd gemeld. Per 1 januari jl. is zowel het niet melden van een datalek of het niet op orde hebben van de beveiliging van persoonsgegevens als andere schendingen van de Wbp fors gesanctioneerd met een boete tot EUR 810.000 en in uitzonderlijke situaties zelfs 10 procent van de netto-omzet.

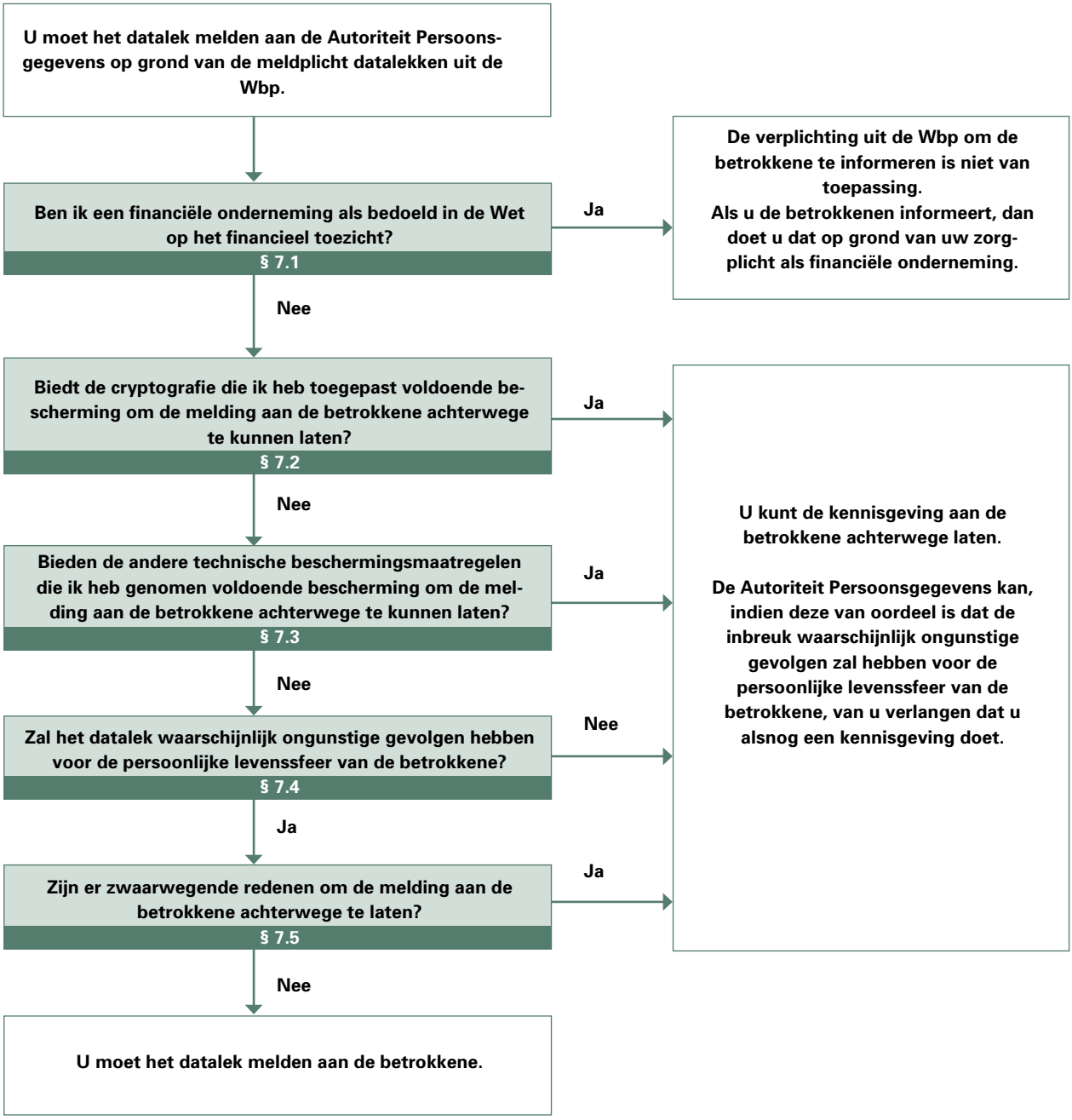
Hoe kunnen organisaties zich het beste voorbereiden?
Een datalek gaat vaak gepaard met onrust, terwijl een gedegen en tegelijk voortvarende aanpak op zo'n moment noodzakelijk is. Wij adviseren organisaties dan ook een op maat gemaakt draaiboek klaar te hebben liggen. Door een draaiboek weet iedere medewerker die betrokken moet zijn bij het managen van het lek en de gevolgen, wat er wanneer van hem of haar verwacht wordt en welke afwegingen er gemaakt moeten worden. Ook is het nodig om de eerder genoemde contracten na te lopen. Verder kan het zinvol zijn te oefenen hoe een organisatie reageert in het geval van een incident. Cyber security experts zeggen vaak dat het meer de vraag is wanneer een organisatie gehackt wordt dan of een organisatie gehackt wordt.

Wat vindt Louwers Advocaten van de meldplicht?
Dat zal ervan afhangen hoe de meldplicht in de praktijk vorm gaat krijgen, welke effecten deze teweegbrengt en welke opstelling de toezichthouder daarbij kiest. Op zichzelf is er niets mis met transparantie op dit punt en kan dit bijdragen aan het beoogde vertrouwen in de zorgvuldige verwerking van persoonsgegevens. Zeker wanneer organisaties besluiten om extra aandacht te schenken aan de beveiliging van de aan hen toevertrouwde persoonsgegevens om een verplichte melding van een datalek te voorkomen. Mocht het effect voor de praktijk echter zijn dat we overspoeld gaan worden met pro forma meldingen dan zou het effect weleens nihil kunnen zijn. In dat geval is het alleen een extra administratieve last voor bedrijven.

De praktijk zal nog flink moeten worstelen met de praktische implicaties van de meldplicht. De Autoriteit Persoonsgegevens noemt als voorbeeld dat een kwetsbaarheid in een webapplicatie als gevolg waarvan medische gegevens kunnen worden ingezien gemeld dient te worden aan de toezichthouder. Ook hanteren ze als vuistregel dat het lekken van gevoelige persoonsgegevens aan de betrokkene gemeld dient te worden. Betekent dit nu tezamen dat iedere SQL-injectie kwetsbaarheid die door een ethische hacker gevonden wordt in een portal waar gevoelige persoonsgegevens worden verwerkt aan de betrokkene gemeld dient te worden volgens de Autoriteit Persoonsgegevens, tenzij kan worden aangetoond dat hiervan geen misbruik is gemaakt? Dat zou nogal wat consequenties hebben voor de praktijk. We zullen de komende tijd ongetwijfeld nog interessante vragen krijgen van cliënten.

Schematisch overzicht meldplicht datalekken

Het onderstaande schema geeft de vragen weer die u moet beantwoorden om vast te stellen of u een specifiek datalek moet melden aan de betrokkenen. Iedere vraag uit het schema correspondeert met een paragraaf uit het document "Beleidsregels meldplicht datalekken voor toepassing van artikel 34a van de Wbp" dat in december 2015 door de Autoriteit Persoonsgegevens is gepubliceerd. Deze en andere publicaties over de beveiliging van persoonsgegevens en over de meldplicht datalekken vindt u op de website van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl.



bron: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken.pdf

Dit keer in rubriek De Hack geeft security consultant Thijs Hodiamont een heldere uitleg over het onderzoeken van fat-clients.

Fat-client Hack

Recentelijk hebben we de kans gehad om in opdracht van een SaaS-ontwikkelaar de door hen ontwikkelde fat-client te onderzoeken op kwetsbaarheden. Dit artikel beschrijft dat proces en de uitdagingen die hierbij komen kijken.

Madison Gurkha voert regelmatig onderzoeken uit op een zogenaamde fat-client. Het onderzoeksdoel: het vaststellen van het niveau van technische IT-beveiliging, wijkt niet af van onze gangbare onderzoeken op webapplicaties. Echter, de manier van onderzoeken is wel degelijk anders en is vaak arbeidsintensiever dan een meer gangbaar grey box onderzoek.

Definitie

Het begrip 'fat-client' is, zoals bij veel termen in IT, relatief/subjectief/aan inflatie onderhevig (haal door wat niet van toepassing is). Voor dit artikel hanteren we de volgende definitie: 'Een applicatie die is ontworpen volgens een client-server-model en daarbij ook een niet-triviaal deel van de functionaliteit delegeert aan de client.' Fat-clients komen voor in de vorm van bijvoorbeeld Java-applets, .NET-applicaties en C++-applicaties. In de praktijk zien we vaak applicaties voor specifieke bedrijfsprocessen die veelal gerelateerd zijn aan betalingen en/of vermogensbeheer. Een ander kenmerk is dat deze fat-clients vaak niet via het internet gebruikt worden maar enkel via een intern netwerk of een VPN-verbinding. Dit is echter geen gouden regel want Java-applets vormen daar weer een uitzondering op.

Onderzoeksmethoden

De traditionele manier van onderzoeken die we toepassen op webapplicaties, door het uitvoeren van een man-in-the-middle (MitM)-aanval op het netwerkverkeer tussen client en server, heeft zijn beperkingen. Fat-clients maken vaak gebruik van niet-standaard-protocollen, beschermen de communicatie of maken gebruik van andere mitigerende maatregelen om de beveiliging te waarborgen. Het onderzoeken van een fat-client is vaak een combinatie van de volgende drie methoden:

1. **MitM**
   Inspecteren van communicatie tussen client en server. In enkele gevallen zijn er nog steeds opties om verkeer te manipuleren en daarmee security controls te omzeilen. De communicatie tussen client en server geeft ook inzicht in de interne werking van de fat-client. Deze informatie kan gebruikt worden in andere aanvallen.

2. **Disassembly/decompilatie**
   Het disassemblen en/of decompileren van de fat-client. Bij Java-applets en .NET-applicaties is het over het algemeen triviaal om deze applicaties te decompileren tot leesbare broncode. Met deze broncode kunnen we de interne werking van de fat-client onderzoeken met als doel kwetsbaarheden te vinden en security controls te omzeilen. Ontwikkelaars kunnen maatregelen nemen om decompilatie te voorkomen of lastiger te maken, maar een aanvaller met meer tijd kan hier omheen werken.

3. **Debugging**
   Het debuggen van een draaiende applicatie stelt ons in staat om de mechanismen van de applicatie te gebruiken. Wanneer een applicatie bijvoorbeeld de communicatie ondertekent met een cryptografische hash (controlecijfer) dan kunnen we het bericht aanpassen voordat het ondertekend wordt. Client-side controles en autorisaties kunnen op deze wijze ook omzeild worden. Het grote nadeel van deze methode is dat de moeilijkheidsgraad van zeer gemakkelijk (Java-applets) tot zeer moeilijk (C++) gaat. Ontwikkelaars kunnen maatregelen nemen om debuggen te bemoeilijken, maar een aanvaller met meer tijd zal in staat zijn deze maatregelen te omzeilen.

Het onderzoeken van een fat-client, of een willekeurig stuk software, met behulp van bovenstaande methoden noemen we 'reverse engineering'.

Casus

Een aantal jaar geleden hebben we in opdracht van de klant een onderzoek uitgevoerd op een SaaS-applicatie, in de vorm van een fat-client van ontwikkelaar ACME (fictieve naam). Uit dit onderzoek waarbij we gebruik hebben gemaakt van de traditionele MitM-methode, kwamen een aantal bevindingen naar voren. De gevonden kwetsbaarheden stelden een aanvaller in staat om door het verkeer tussen de fat-client en de backend te manipuleren, gegevens van andere klanten in te zien, te wijzigen en te verwijderen. Ook was het mogelijk om SQL-queries die door de fat-client werden opgesteld aan te passen met als resultaat willekeurige informatie uit de achterliggende database. Het resultaat van dit onderzoek is destijds door de klant teruggekoppeld aan ACME waarna een gepatchte versie van de software werd opgeleverd. Een heronderzoek, in beperkte tijd, toonde aan dat alle risico's gemitigeerd waren.

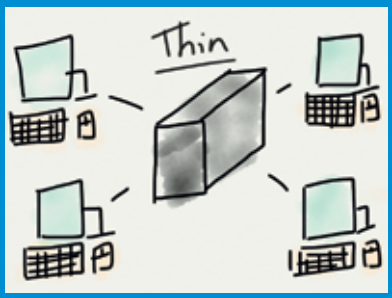
Afgelopen jaar benaderde ACME ons direct om naar aanleiding van het eerder uitgevoerde onderzoek een nieuw onderzoek uit te laten voeren. Met de resultaten van dit onderzoek wilde zij aan haar klanten kunnen aantonen dat de door hun ontwikkelde SaaS-oplossing geen kwetsbaarheden bevat. De SaaS-applicatie betreft een Java-applet waarvan gebruikers met verschillende functierollen gebruik kunnen maken. Ook het rollen-, rechten- en gebruikersbeheer wordt via een Java-applet uitgevoerd.

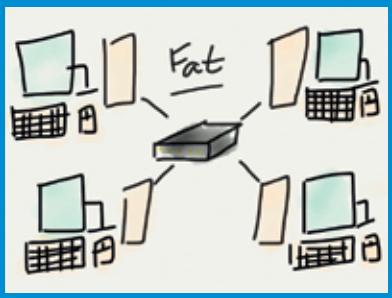
De uitdaging

De fat-client (de Java-applet) bevat de functionaliteit voor alle rollen en bepaalt op basis van de informatie van de backend welke informatie en/of functionaliteit weergegeven mag worden. Een gebruiker met beperkte rechten zal minder functionaliteit zien dan een beheerder.

De uitdaging: hoe krijg ik als aanvaller met rechten van een normale gebruiker toegang tot de functionaliteit van een beheerder? Dit gaat over verticale autorisaties. Daarnaast maakt een SaaS-applicatie veelal gebruik van een gedeelde omgeving. Hoe kan een aanvaller met de rechten van klant A toegang krijgen tot de gegevens van klant B? Dit noemen we horizontale autorisaties.

In de eerste fase van een onderzoek zijn dit de twee punten waar we op focussen.





Definitie fat-client

Het begrip *fat-client* is, zoals bij veel termen in IT, relatief/subjectief/aan inflatie onderhevig (haal door wat niet van toepassing is).

Voor dit artikel hanteren we de volgende definitie: *Een applicatie die is ontworpen volgens een client-server-model en daarbij ook een niet-triviaal deel van de functionaliteit delegeert aan de client.*

Onderzoek
We starten het onderzoek met het inspecteren van het verkeer tussen de fat-client en de backend. Wanneer we aanpassingen maken in het verkeer, bijvoorbeeld het aanpassen van een identifier voor een organisatie, volgt er direct een foutmelding. Nadere inspectie laat zien dat de berichten van de fat-client een checksum/controlecijfer bevatten op basis van het cryptografische SHA256-algoritme. Met behulp van dit controlecijfer kan de backend vaststellen of het bericht tussentijds is aangepast. Bovendien wordt een foutmelding gegenereerd als het meegestuurde controlecijfer niet overeenkomt met het berekende controlecijfer. Een MitM-aanval wordt hiermee voor een zeer groot deel gemitigeerd. Daarmee is onze interesse gewekt want we zien geen verschil in de berichtenstructuur ten opzichte van de 'kwetsbare' fat-client zoals die de eerste keer is onderzocht.

Omdat het een Java-applet betreft hebben we de mogelijkheid om deze met publiekelijk beschikbare tools als JD-GUI te decompileren tot leesbare code. Een publiekelijk beschikbare tool voor .NET-applicaties is ILSpy. Voor C/C++-applicaties moet een aanvaller terugvallen op decompilers als Hex-Rays Decompiler (commercieel) of Snowman (open-source).

We besluiten de Java-applet te decompileren met behulp van JD-GUI om de logica van de fat-client te kunnen achterhalen. Wanneer een gebruiker inlogt krijgt de fat-client van de backend te horen welke rol de gebruiker heeft en bij welke organisatie de gebruiker hoort. De rolinformatie wordt door de fat-client gebruikt om functionaliteit wel of niet te tonen. De organisatie-informatie wordt in ieder request naar de backend meegezonden. Wanneer de gebruiker zijn dashboard wil zien zal het verzoek aan de backend zijn: 'Geef me het dashboard voor organisatie A'. Als we het dashboard van organisatie 'B' willen inzien moeten we 'A' dus aanpassen naar 'B'. Dit kunnen we doen door onze eigen client te schrijven of door de fat-client te debuggen en de waarde 'A' aan te passen naar 'B' voordat het controlecijfer berekend wordt. Met behulp van Eclipse, een Java IDE, debuggen we de applet en passen we de waarde aan. De backend honoreert ons verzoek en we krijgen het dashboard van organisatie 'B' te zien. Hiermee is ontbrekende horizontale autorisatie aangetoond.

Vervolgens testen we nog een aantal andere handelingen zoals het toevoegen van gebruikers aan andere organisaties en het inzien van transacties van andere organisaties. Bij alle handelingen ontbreekt de horizontale autorisatiecontrole. In de broncode van de backend die tijdens het onderzoek is aangeleverd zien we bovendien dat er geen verticale autorisatiecontroles zijn geïmplementeerd. Hierdoor kan een normale gebruiker bijvoorbeeld mutaties op andere gebruikers met een administratieve rol uitvoeren. Ook nu is het mogelijk om SQL-queries aan te passen en hiermee informatie te verzamelen. Op basis van onze bevindingen concluderen we dat ACME na ons initiële onderzoek enkel een controlecijfer heeft toegevoegd op de berichten tussen de fat-client en de backend en dat de gehele applicatie nog steeds kwetsbaar is.

Hoe nu verder?
ACME heeft met behulp van onze input een hoop aanpassingen gedaan, waardoor de backend nu niet langer impliciet aanneemt dat de invoer van de fat-client vertrouwd is. Bij ieder verzoek moeten er zowel horizontale als verticale autorisatiecontroles worden gedaan. Onze onderzoeken hebben laten zien dat dit ook echt nodig was en dat het niet voldoende is om een controlecijfer voor de berichten te gebruiken. Tevens is alle SQL-functionaliteit verplaatst naar zogenaamde 'prepared statements' in de backend. Dit alles resulteerde in een arbeidsintensieve klus voor ACME.

Fat-clients zijn, voor zover wij kunnen bepalen, op dit moment nog een ondergeschoven kindje omdat het aanvalsoppervlak vaak klein is. Ze worden dikwijls op een intern netwerk gebruikt door een beperkte groep mensen en de klanten zijn vaak niet op de hoogte van de mogelijke kwetsbaarheden in dit soort software. Gecombineerd met het feit dat de onderzoeken arbeidsintensiever zijn dan 'normale' applicatie-onderzoeken leidt dat ertoe dat bedrijven ervoor kiezen om deze fat-clients niet te laten onderzoeken. Hopelijk hebben we u aan het denken gezet.

Verticale autorisaties:
Hoe krijg ik als aanvaller met rechten van een normale gebruiker toegang tot de functionaliteit van een beheerder?

Horizontale autorisaties:
Hoe kan een aanvaller met de rechten van klant A toegang krijgen tot de gegevens van klant B?

Save the Date!

23 juni 2016 | Black Hat Sessions Part XIV | Mobile (in)security | De ReeHorst, Ede

Had u kunnen denken dat mobiele apparaten en communicatie zo'n vlucht hadden kunnen nemen? Zo'n dertig jaar geleden moest je om mobiel bereikbaar te zijn rondlopen met een koffertje waar een telefoonhoorn aan verbonden was. Tegenwoordig is je smartphone vele malen sneller dan een pc uit die tijd en met een schermresolutie waar je toen alleen maar van kon dromen.

Snoeren aan apparaten zijn lastig dus boden Wifi en Bluetooth uitkomst. Wifi is inmiddels niet meer weg te denken en de beschikbaarheid ervan is voor velen een must: "Ik ben online dus ik besta". Bluetooth is gemeengoed en we gebruiken het allemaal dagelijks voor de draadloze communicatie met muizen, toetsenborden, smartwatches, headsets, luidsprekers etc.

We staan eigenlijk nog maar aan het begin van het Internet of Things. Al die "dingen" op het internet zitten meestal niet aan een draadje vast. Er is inmiddels een veelheid aan protocollen/transport mechanismes ontstaan om "dingen op het internet" te laten communiceren. Denk bijvoorbeeld aan Zwave, 6LowPAN, Zigbee, LoRa, etc. Maar laten we RFID ook niet vergeten. Het communiceert dan wel niet over grote afstanden, maar het is draadloos en wordt in veel belangrijke toepassingen gebruikt en is niet meer weg te denken.

Mobiele apparaten, mobiele communicatie en het Internet of Things bieden stuk voor stuk voor mogelijkheden en daar maken we allemaal dankbaar gebruik van. Uiteraard zit er ook een keerzijde aan al dit gemak.

Tijdens deze veertiende editie van het jaarlijkse security congres "Black Hat Sessions" gaan we in op de IT-beveiligingsrisico's die mobiele apparaten en communicatie met zich meebrengen. Smartphones en tablets zijn eigenlijk gewoon computers, met alle risico's die we al kennen en waarschijnlijk nog meer. Wifi is in het verleden erg lek geweest en hoe veilig is het nu? GSM is heel makkelijk afluisterbaar en hoe staat het eigenlijk met die nieuwe protocollen? De communicatie op het "Internet of Things" moet immers licht en efficiënt? Is dat nog wel veilig?

Zowel voor techneuten als het management bieden we een interessant programma met toonaangevende sprekers uit het veld, hands-on hacking workshops en voorbeelden uit de praktijk. Het is natuurlijk ook een uitgelezen kans om te netwerken en met vakgenoten van gedachten te wisselen over al deze onderwerpen.

BHS

De Black Hat Sessions is het jaarlijkse security congres van Madison Gurkha. Wat veertien jaar geleden begon als een middag ter kennisdeling is uitgegroeid tot een succesvol evenement in de IT-beveiligingswereld. Vorig jaar kwamen zo'n 400 deelnemers bijeen om in één dag kennis op te doen en te netwerken met vakgenoten. Met name de informele sfeer, de interactie met de sprekers en deelnemers en het gevarieerde programma wordt al jaren positief ontvangen door zowel IT Pro's als het management.

Reserveert u vast 23 juni 2016 in uw agenda
Meer informatie over het programma en het inschrijfformulier zijn binnenkort te vinden op: www.blackhatsessions.com

Dit keer geeft Rick van Bodegraven, security consultant bij Madison Gurkha, inzicht in de meerwaarde van het inspecteren van de broncode bij een applicatieonderzoek.

HET INZICHT

Voorkom ad-hoc **brandjes blussen**

Madison Gurkha voert jaarlijks veel verschillende IT-beveiligingsonderzoeken uit. Bij al deze onderzoeken is één aspect voor ons altijd hetzelfde; het speuren naar kwetsbaarheden in de applicaties of infrastructuur die 'in scope' zijn. Afhankelijk van de hoeveelheid beschikbare informatie, hanteren we hierbij verschillende onderzoeksmethoden. Dit varieert van een black box onderzoek dat vergeleken kan worden met een aanval zoals digitale inbrekers die zouden uitvoeren tot een diepgaand crystal box onderzoek waarbij we vooraf beschikking krijgen over alle mogelijke informatie. In dit artikel geven we inzicht in de onderzoekswijze die gehanteerd wordt tijdens een crystal box applicatieonderzoek, ook wel bekend als whitebox onderzoek.

Bij een crystal box onderzoek van (web)applicaties beschikken we vooraf over alle mogelijke informatie waaronder configuratiebestanden, interne (ontwerp) documentatie en de volledige broncode van de te onderzoeken applicatie. Doordat de code beschikbaar is kunnen we relatief snel kwetsbaarheden aantreffen die normaal gesproken pas na vele uren van traditioneel pentesten (speurwerk) naar boven komen. Of nog erger, pas aan het licht komen als ze door een volhardende aanvaller uitgebuit worden. Ook is het mogelijk om specifieke ontwerpkeuzes en eventuele kwetsbare instellingen in een vroeg stadium te onderzoeken, wanneer logbestanden, configuratiebestanden en ontwerpdocumenten worden aangeleverd. Dit type onderzoek heeft de meeste diepgang en zal dan ook de meeste resultaten en mogelijke verbeterpunten opleveren.

Hoe gaat het in zijn werk?

Bij aanvang van het onderzoek bekijken we hoe groot de broncode is. Hiervoor gebruiken we tools die regel voor regel inspecteren in welke programmeertaal de betreffende regel is geschreven. De tool laat vervolgens een totaaloverzicht zien van het aantal regels per programmeertaal. Hierdoor krijgen we een globaal beeld van de omvang en de structuur van de aangeleverde broncode.

Vervolgens begint het 'echte' onderzoek waarbij de focus ligt op het onderzoeken van kwetsbaarheden vanuit het perspectief van de applicatie. Wanneer we vermoeden dat een aangetroffen kwetsbaarheid structureel in de applicatie aanwezig is, kijken we in de broncode of dit daadwerkelijk het geval is. Mochten we gedurende het onderzoek van de applicatie een vermoeden ontwikkelen dat er iets niet helemaal in de haak is, dan biedt de broncode uitkomst om dit vermoeden te bevestigen of te ontkrachten. Hierdoor kunnen we een kwetsbaarheid die in de praktijk lastig uit te buiten is, snel opsporen zodat de

opdrachtgever passende maatregelen kan nemen om het beveiligingsprobleem op te lossen.

Controleren hoe bepaalde zaken zijn opgelost
Een voordeel van de crystal box methode is dat er ook toekomstige problemen mee voorkomen kunnen worden. Doordat alle broncode en eventuele configuratiebestanden geïnspecteerd kunnen worden, kunnen we bijvoorbeeld afwijkingen van best practices detecteren. Een voorbeeld hiervan is de ingestelde encryptie in configuratiebestanden of de complexiteit van wachtwoorden voor verbindingen met achterliggende databases. Ook het zoeken naar veel voorkomende beveiligingsrisico's als SQL-injectie, cross-site request forgery (CSRF) of cross-site scripting (XSS) kan een stuk efficiënter wanneer de broncode beschikbaar is. Veel van de oorzaken van deze drie risico's zijn al langer in het vakgebied bekend, waarbij vaak ook specifieke functies in bepaalde talen als boosdoener worden genoemd. Het zoeken naar deze risico's kan hierdoor aangevuld worden met het doorzoeken van de gehele broncode op bekende kwetsbare functies.

Het beschikbaar hebben van de broncode levert voordelen op wanneer vanuit het perspectief van de applicatie wordt getest. Indien er tijdens het onderzoek een kwetsbaarheid wordt gevonden, kunnen we precies traceren welk stuk code in dat geval verantwoordelijk is. Op deze manier kan veel duidelijker de oorzaak aangewezen worden. En op basis hiervan kunnen we vervolgens de gehele broncode doorlopen om te zien of de kwetsbaarheid ook op andere plaatsen aanwezig is waar dezelfde code is hergebruikt. Ook wanneer kwetsbaarheden niet aanwezig blijken te zijn levert een crystal box onderzoek voordelen op. We kunnen namelijk tot op de bodem uitzoeken en aantonen waarom dat het geval is, waarbij vaak zelfs de verantwoordelijke regels code aangewezen kunnen worden.

Een kanttekening is hier overigens wel op zijn plaats. Het uitvoeren van een crystal box onderzoek is nadrukkelijk niet hetzelfde als het uitvoeren van een code review. Bij een code review wordt iedere regel code nauwgezet onderzocht, met behulp van tooling die daar speciaal voor ontwikkeld is. Bij dit type onderzoek zijn ook andere aspecten dan alleen beveiliging van belang. Software engineering principes zoals onderhoudbaarheid en complexiteit voeren de boventoon tijdens een code review. Indien er een volledige code review uitgevoerd moet worden, doen we dit vaak in samenwerking met de specialisten van onze partner SIG (Software Improvement Group).

Toekomstig niveau van IT-veiligheid
Zoals hierboven genoemd is, zijn er naast het crystal box onderzoek nog twee andere onderzoeksmethoden die gehanteerd worden. Dit zijn de grey- en black box onderzoeken. Bij een grey box onderzoek beschikken we over credentials waarmee we kunnen inloggen op de applicatie. Bij een black box onderzoek is alleen de url van het te onderzoeken systeem bekend. Eén van de nadelen van dit type onderzoeken is het feit dat de afwezigheid van een kwetsbaarheid nooit kan worden gegarandeerd. Alleen in het geval van aanwezigheid kan dit worden bewezen. Dit kan een vals gevoel van veiligheid opleveren. Er zijn immers geen kwetsbaarheden gevonden, dus kunnen ze ook niet aanwezig zijn… toch?

Dit alles betekent uiteraard niet dat wij onze klanten aanraden om voortaan alleen nog maar crystal box onderzoeken uit te laten voeren. Ieder onderzoek vraagt immers om een eigen kwalitatief hoogwaardige aanpak die past bij de zichtbaarheid van de organisatie en het afbreukrisico. Voor het uitvoeren van een crystal box onderzoek is specifieke kennis nodig. Omdat niet alle consultants per definitie op iedere opdracht ingezet kunnen worden, is het bij een crystal box onderzoek lastiger om een flexibele planning te kunnen bieden. De kwaliteit van het uitgevoerde onderzoek staat immers voorop en moet van het niveau zijn dat u van ons mag verwachten.

Er zijn immers geen kwetsbaarheden gevonden, dus kunnen ze ook niet aanwezig zijn... toch?

Het **technische beveiligingsonderzoek**; wat komt hierbij kijken?

Er zijn diverse redenen aan te wijzen om een beveiligingsonderzoek uit te laten voeren. Het vernieuwen van de technische infrastructuur, het invoeren van een nieuw portaal of bijvoorbeeld een mobiele applicatie. Ook een audit kan aanleiding geven tot het uitvoeren van een dergelijk onderzoek. Maar voordat u het rapport met bevindingen in handen heeft, gaat er heel wat aan vooraf. Ook hier geldt: een goede voorbereiding is het halve werk. Tamara Brandt, teamleider bij Madison Gurkha, geeft meer inzicht in het proces. Dit geeft u handvatten om het beveiligingsonderzoek zo goed mogelijk te laten verlopen.

Een belangrijk uitgangspunt is dat een beveiligingsonderzoek alleen in opdracht kan worden uitgevoerd. Dit vloeit voort uit het strafrecht: het inbreken op andermans computers en netwerken is in beginsel bij wet verboden. En dat is nu juist precies wat er tijdens een beveiligingsonderzoek gebeurt, zij het dus op verzoek en onder voorwaarden. Elk opzettelijk en wederrechtelijk binnendringen in computersystemen is strafbaar. Dit is een belangrijke reden om zorg te dragen voor een juiste voorbereiding. Onderdeel van deze voorbereiding is helder krijgen op welke URL of IP-adres(sen) het onderzoek plaats zal vinden. Aan de hand hiervan wordt een controle uitgevoerd om vast te stellen of er een aanvullende vrijwaring nodig is voor het onderzoek. Dit kan bijvoorbeeld het geval zijn wanneer een derde partij juridisch eigenaar is van het systeem dat getest wordt, of wanneer vrijwaring niet voldoende wordt afgedekt door middel van het verstrekken van de opdracht. Ook wordt de informatie over het doelsysteem gebruikt om de opdracht in te schatten. Vragen die hierbij beantwoord dienen te worden zijn onder meer: Wat is de omvang van het te testen systeem? Hoeveel dagen zijn er nodig om dit systeem te testen? En: welk specialisme moet er worden ingezet?

Een ander belangrijk punt is het plannen van de opdracht. Vaak zijn er voorwaarden zoals een datum waarop livegang plaatsvindt of een wettelijke verplichting tot wanneer een audit uitgevoerd moet zijn. Ook is het van belang dat alle betrokken partijen op de hoogte zijn van het tijdsframe waarbinnen een opdracht wordt uitgevoerd. Zo kan men elkaar informeren bij bijzonderheden en kunnen verdachte acties worden verklaard.

Voor een succesvol onderzoek is het verder goed te weten op welke manier het doelsysteem of -netwerk te bereiken is: vaak kan dat via internet, maar soms is het noodzakelijk om het onderzoek op locatie uit te voeren. Ook zijn vaak inloggegevens nodig om in het systeem te kunnen. Dit is afhankelijk van het type onderzoek dat overeengekomen is. Bij een zogeheten black box onderzoek test men een systeem zonder te beschikken over geldige inloggegevens. Bij andere typen onderzoek wordt vooraf informatie gegeven over het systeem, zoals inloggegevens, documentatie, en/of broncode. Kan het onderzoek via het internet uitgevoerd worden dan is het soms nodig het doelsysteem bereikbaar te maken voor de onderzoekers door IP-adressen te whitelisten in de firewall. In het tweede geval zijn er nog een aantal extra zaken voor te bereiden: op welke locatie en bij wie mogen de onderzoekers zich melden? Is er een werkplek geregeld met een netwerkaansluiting, en is er een contactpersoon die hen bij vragen bij kan staan?

Er komt dus heel wat kijken bij een goede voorbereiding van een beveiligingsonderzoek. Alle voorbereidingen staan in het teken van het zo succesvol en effectief mogelijk laten verlopen van het onderzoek.

In de ITSX-rubriek vertelt Marloes Kwakkel, Risk consultant & Certified Compliance Officer bij ITSX, over de QuickScan Meldplicht Datalekken.

QuickScan Meldplicht Datalekken

Eerder in deze Update heeft u uitgebreid kunnen lezen over de meldplicht datalekken. De meldplicht gaat er vanuit dat organisaties hun best doen om datalekken te voorkomen en dat zij deze op een gecontroleerde wijze kunnen oplossen, mocht zich onverhoopt toch een datalek voordoen.

Marloes Kwakkel, Risk consultant & Certified Compliance Officer bij ITSX, legt in dit artikel de focus op de praktische kant van het verhaal. Wat betekent het concreet voor uw organisatie? En belangrijker nog: welke maatregelen passen het beste bij uw organisatie?

Want vraagt u zich ook niet af:

- In hoeverre voldoen we al aan deze wetgeving?
- Op welke punten gaat de meldplicht datalekken impact hebben op onze organisatie?
- Welke risico's lopen wij?

Tool en rapport
Om deze vragen op korte termijn te kunnen beantwoorden heeft ITSX een QuickScan tool ontwikkeld. Deze 'QuickScan Meldplicht Datalekken' is een slimme vragenlijst over de belangrijke onderwerpen op het gebied van privacy en informatiebeveiliging. Het geeft een beeld over de 'readiness' binnen de organisatie en gaat in op zowel organisatorische-, procedurele- als technische aspecten.
Uit deze tool komt een rapport met de vragen en antwoorden, aanbevelingen en follow-up/acties. De expert van ITSX voegt hier een korte managementsamenvatting aan toe, die rekening houdt met de context van de organisatie en het uitgevoerde onderzoek. In deze samenvatting staan de meest dringende zaken en welke verbeteringen nodig zijn.

Samenwerking
Om tot dit resultaat te komen werken de experts van ITSX samen met de opdrachtgever en wordt een dag ingepland om alle benodigde informatie te verzamelen en vragen te beantwoorden. Deze dag heeft het karakter van een workshop, waarin via interviews informatie wordt gehaald. De focus ligt op het bespreken van de onderwerpen, delen van kennis, samen bepalen van de aandachtspunten en het verhogen van de bewustwording.

Aanwezigen
Vanuit de opdrachtgever zullen verschillende rollen/personen aanwezig zijn. Hier kan het bijvoorbeeld gaan om een security officer, IT manager en/of functionaris gegevensbescherming. Belangrijk is dat deze mensen kennis hebben over de organisatie en de onderwerpen die besproken worden en daar ook een zekere mate van bevoegdheid en/of verantwoordelijkheid voor dragen. Op basis van de informatie die zij verstrekken worden immers conclusies getrokken en aanbevelingen gedaan.

Onderwerpen
Tijdens deze QuickScan worden meerdere onderwerpen besproken. Er wordt gestart met het bepalen van de context. Om welke persoonsgegevens gaat het, waar staat wat, waar zitten koppelingen/verbindingen en welke belanghebbenden (stakeholders) zijn op verschillende manieren betrokken bij de organisatie.

Na deze eerste verkenning worden de volgende onderwerpen inhoudelijk besproken:

Hoe gaat uw organisatie om met:
- **Privacy management, persoonsgegevens en betrokkenen;**
- **Stakeholders, externe partijen en afspraken;**
- **Informatiebeveiliging;**
- **Governance;**
- **Risicomanagement;**
- **HR;**
- **Beleid;**
- **Toegangsbeveiliging (Fysiek en logisch);**
- **Beheersing van kwetsbaarheden;**
- **Versleuteling;**
- **Logging en monitoring;**
- **Incidentenbeheer;**
- **Continuïteit, crisismanagement en crisiscommunicatie;**
- **Specifieke meldplicht procedures;**
- **Bewaren en vernietigen van gegevens;**
- **Naleving, controle en testen.**

Voordelen

Deze aanpak heeft een aantal specifieke voordelen, namelijk:
- **Door het samenbrengen van kennis ontstaat er een beter begrip van de situatie en de risico's;**
- **Het is niet heel ingrijpend, terwijl de aandachtspunten duidelijk naar voren komen;**
- **Er wordt weinig tijd gevergd van de betrokkenen;**
- **Het betreft een relatief lage investering;**
- **Resultaat is een overzichtelijke rapportage met een duidelijke oplossingsrichting en actielijst.**

Een belangrijk eerste voordeel van deze aanpak is het direct creëren van bewustwording en momentum!

Het eerst genoemde voordeel, over het krijgen van een beter begrip van de situatie en de risico's, is essentieel. Het is gebleken dat de verschillende personen die aanwezig zijn bij zo'n workshop allemaal bekend zijn met een aantal risico's in hun eigen domein. Tijdens de workshop blijkt vaak dat tussen deze risico's een beperkte overlap zit en er feitelijk meer risico's zijn dan voor eenieder onafhankelijk van de ander inzichtelijk was. Een belangrijk eerste voordeel van deze aanpak is daarmee het direct creëren van bewustwording en momentum!

Mocht u vragen hebben over dit onderwerp neemt u dan contact met ons op via info@itsx.com of via telefoonnummer 088-8883111.

ITSX

Walter Belgers doet verslag van t2 infosec dat vorig jaar plaatsvond in Helsinki. Hij heeft hier zelf een presentatie gegeven over lockpicking en IT-beveiliging.

t2 infosec

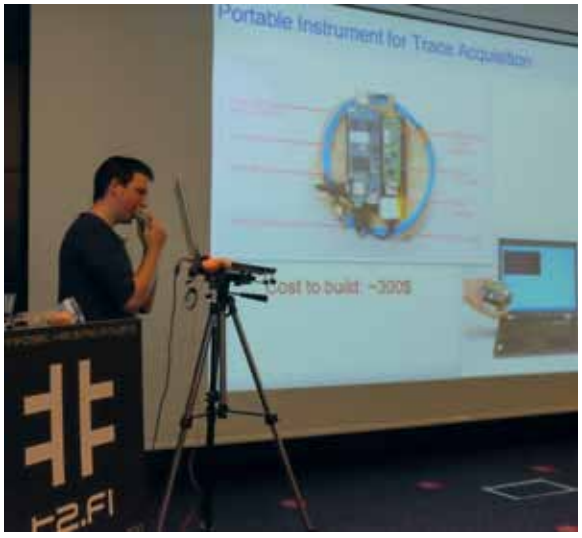
Op 29 en 30 oktober 2015 vond de 12e editie van de jaarlijkse conferentie t2 infosec plaats in Helsinki. Aan het roer van deze conferentie staat Tomi Tuominen, een Fin die bedacht dat hij in zijn land een conferentie over ICT-beveiliging zou kunnen houden, kleinschalig en met goede sprekers. Dat concept werkt nog steeds.

Vorig jaar was ik voor het eerst op de t2 infosec conference en sprak toen over de parallellen tussen beveiliging in de fysieke wereld en in de ICT (zie ook het verslag in Update 23). Dit jaar wilde de organisatie me graag weer hebben en zelf keek ik ook uit naar deze conferentie. De sprekers worden zeer goed behandeld en de conferentie is intiem en leerzaam. Er worden slechts 99 bezoekers toegelaten en de conferentie is jaarlijks uitverkocht. De (noodzakelijke) sponsoren zijn onopvallend aanwezig en hebben geen invloed op het programma. De sprekers worden gekozen op basis van onderwerp maar ook hoe ze kunnen presenteren.

Tomi stemde toe in een lezing over fysieke penetratietests, mits ik een Assa Abloy slot zou openen. Deze sloten, die je overal in Finland tegenkomt, zijn bijzonder lastig open te krijgen. Het kostte me de nodige hoofdbrekens, maar het is me gelukt om als eerste live op het podium zo'n slot te openen zonder geweld en zonder sleutel. Maar er was nog veel meer interessants te zien, vandaar een beknopt verslag van de meest in het oog springende zaken.

De keynote was van **Morgan Marquis-Boire**. Zoals de bedoeling bij een keynote, werden we geprikkeld met wat stellingen en open vragen, zoals de vraag wanneer het omslagpunt er was van hackers naar staten als aanvallers. Als je Stuxnet en Regin bekijkt, is dat zeker al vanaf 2002 aan de gang, en misschien al wel sinds 1996 als je zaken als domein-registraties voor deze malware bekijkt. Een belangrijker omslagpunt is recenter: de onthullingen van Snowden. Want op dat moment leefden we al in een "panopticon": een staat waarin we op elk moment afgeluisterd en bekeken kunnen worden, maar pas op dat moment wisten we het ook (en dat is een voorwaarde voor een panopticon). Zo'n panoptische maatschappij kan functioneren (kijk naar de UK), maar wanneer is het teveel (zoals in Oost-Duitsland)? Kan de technologie ons nog helpen? (Want de politiek zal dat niet doen.)

Georg Wicherski gaf uitleg over het bouwen van een wegwerp-laptop die je mee op reis kunt nemen. Bij grote(re) bedrijven is het nu al zo dat CEO's e.d. een wegwerplaptop gebruiken, maar



Georg wilde er eentje hebben van maximaal 300 dollar. Uiteindelijk is dat gelukt met een Chromebook laptop met wat modificaties, zodat de bootchain veiliger is. We weten nu dat de NSA programma's heeft ("IRATEMONK" en "SWAP") om laptops bij de douane te infecteren.

De lezing van **David Chismon** ging over Threat Intelligence. Dit is het nieuwe modewoord, maar wat is het nou precies en wat heb je er aan? Voor veel mensen is het "we kopen threat-feeds en proberen APT's te detecteren". De feeds die je kunt kopen, blijken vrijwel disjunct, de vraag is dus wat je er aan hebt. Bovendien moet je je eerst de vraag stellen: wat wil je ermee? Threat Management kun je op allerlei niveaus doen. Op strategisch niveau heb je het over traditionele "intelligence" en dat is erg moeilijk. Op operationeel niveau heb je het over logging en events, die door de verdedigers kunnen worden gebruikt. Op een tactisch niveau gaat het over malware samples, informele contacten e.d. die leiden tot adviezen voor architecten en systeembeheerders. Op technisch niveau gaat het ten slotte om rulesets voor firewalls die je bouwt aan de hand van feeds. Let wel: de systemen in feeds blokkeren, levert je alleen bescherming tegen zaken die heel makkelijk te omzeilen zijn, namelijk hashes, IP-adressen en domeinnamen.

Lev Pachmanov van Tel Aviv University sprak over side channel attacks op PC's. Boeiend, maar vaak niet zo aanschouwelijk. Lev had echter een paar werkende demo-opstellingen. Zo kon hij PGP-sleutels uit een PC halen door gegevens die lekken via aardstroom, af te vangen door fysiek te koppelen met metalen onderdelen van de laptop. Deze lekstroom kan ook door een mens lopen, of zelfs door een worst zoal Lev liet zien (ik moet erbij zeggen dat deze typische Finse worst officieel is geclassificeerd als groente vanwege te weinig vlees). Ook met een microfoon die geluiden uit spoeltjes en condensatoren opving, wist hij de sleutels te achterhalen, totdat door applaus in de zaal de microfoon overstuurt raakte. Dit werkt ook met de microfoon in een mobieltje op 30cm.

Dit is slechts een bloemlezing. Wil je meer weten, kijk dan op t2.fi. Hier worden ook de handouts beschikbaar gesteld. De volgende conferentie is op 27 en 28 oktober 2016.

> "Het kostte me de nodige hoofdbrekens, maar het is me gelukt om als eerste live op het podium zo'n slot te openen zonder geweld en zonder sleutel"
>
> *Walter Belgers*

HET COLOFON

Redactie
Daniël Dragičević
Laurens Houben
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

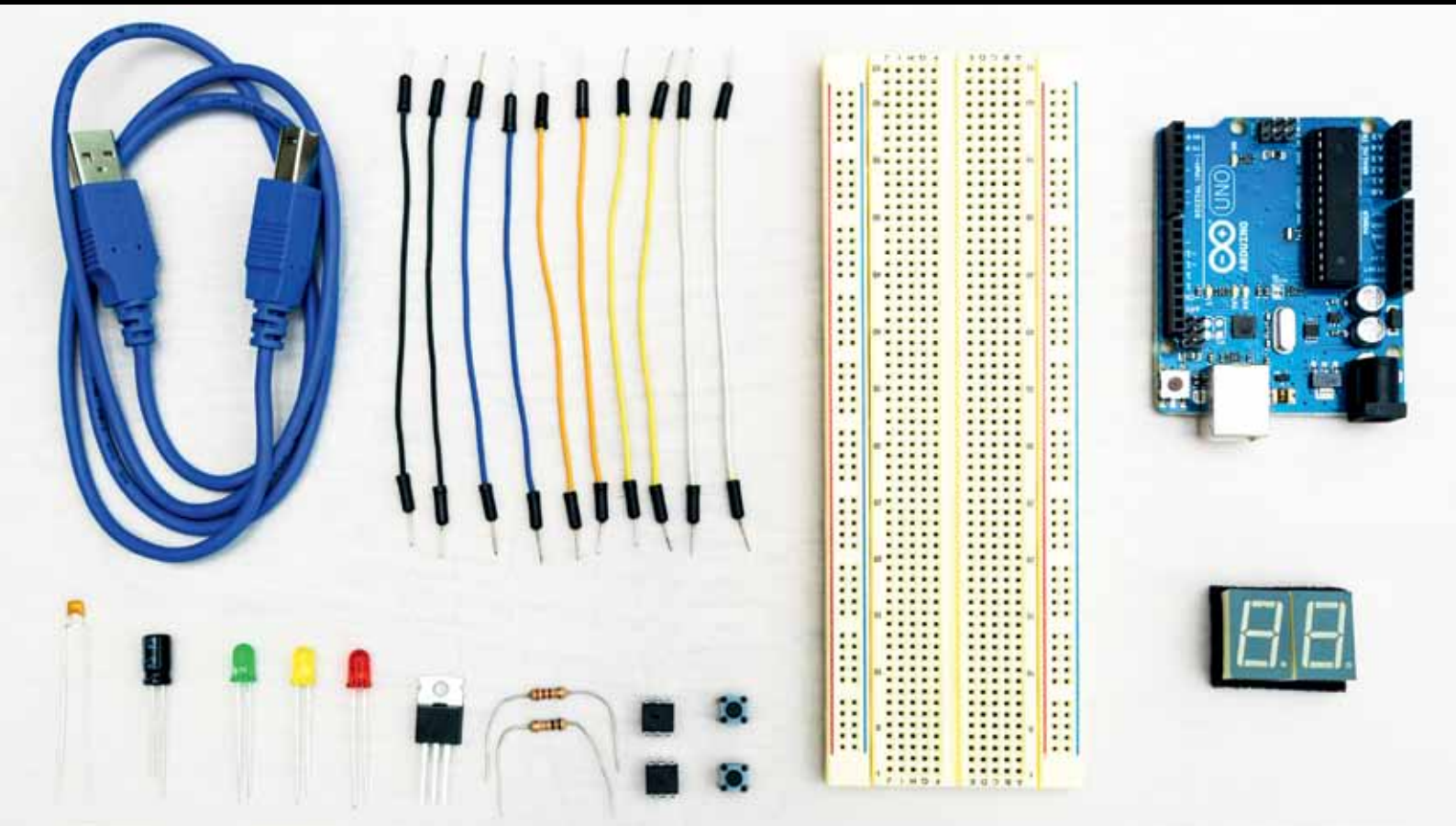
Redactie
redactie@madison-gurkha.com

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.

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