Madison Gurkha
Your Security is Our Business

15 APRIL 2012 UPDATE

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. Deze keer Guido van Rooij over de aanzienlijke gevolgen van onder andere DigiNotar en Lektober.

“We’re all doomed?!”

Op het moment dat ik dit schrijf is de lente weer begonnen. Tijd om de donkere winter achter ons te laten. Dat geldt niet alleen voor de natuur, maar zeker ook op beveiligingsgebied. In de tweede helft van vorig jaar werden we opgeschrikt door de problemen bij DigiNotar en de enorme nasleep daarvan. Daar bovenop kwam nog eens Lektober: de oktobermaand waarin Brenno de Winter op Webwereld het ene na het andere beveiligingsprobleem meldde. Bij veel gemeentes zijn toen beveiligingslekken aangetroffen met als gevolg dat (toen nog) minister Donner heeft ingegrepen en de getroffen sites afgesloten werden van DigiD met alle gevolgen van dien. Ook buiten Lektober om zijn er interessante problemen ontdekt zoals bijvoorbeeld het gebruik van standaard wachtwoorden op controleapparatuur van sluizen.

Wat zijn we nu uiteindelijk hiermee opgeschoten? In elk geval is door alle gebeurtenissen de ‘awareness’ van de problemen en risico’s groter geworden. Echter, ‘awareness’ is iets dat onderhouden dient te worden: we zullen continu mensen bewust moeten blijven maken en houden van IT-beveiligingsrisico’s. Aan de andere kant moeten we oppassen dat mensen en organisaties niet murw worden gemaakt en een soort fatalistische instelling krijgen, zoals in de uitspraak die ik ooit uit de mond van de Amerikaanse beveiligingsexpert Marcus Ranum heb gehoord: “We’re all doomed!”. Er zijn ook concrete stappen gezet door de overheid om de situatie te verbeteren. Zo heeft de DigiD beheerorganisatie Logius een norm opgesteld (getiteld ‘Norm ICT-beveiligingsassessments DigiD’) waarmee organisaties die gebruik maken van DigiD hun DigiD IT-omgeving kunnen (laten) toetsen. Deze norm is opgesteld op basis van de ‘ICT- beveiligingsrichtlijnen voor webapplicaties’ van het Nationaal Cyber Security Centrum. Deze Update is vrijwel volledig gewijd aan de DigiD beveiligingsnorm. Zo kunt u in de rubriek ‘Het Inzicht’ meer lezen over deze norm en onze visie erop. In de rubriek ‘De Klant’ vertelt IT security officer Rutger Heerdink over de uitdagingen van het UWV die als DigiD grootgebruiker eind 2012 getoetst moet zijn. Daarnaast is KING voor de gemeenten een project opgestart om de impact van de nieuwe Logius beveiligingsnorm rondom DigiD te bepalen. Lees hierover meer in het interview met Nausikaä Efstratiades van KING. Uiteraard mag een interview met Logius in deze uitgave niet ontbreken. Zie hiervoor het extra interview met Hans Verweij, Manager Productregie.

We zien ook ongewone ideeën ontstaan. Zo is er een voorstel gedaan om studenten overheidssites te laten hacken. Onlangs is dat door minister Spies verder geconcretiseerd in een brief aan de Tweede Kamer*. Nu lijkt dat op zich een goed idee: studenten doen op die manier ervaring op in de praktijk en de overheid krijgt gratis extra beveiligingsonderzoeken. Door de onderzoeken in een gecontroleerde omgeving te laten plaatsvinden zal de impact beperkt blijven bij eventuele problemen. Mijn inziens zitten er echter behoorlijk wat haken en ogen aan dit voorstel. Wanneer de overheid een gespecialiseerd bedrijf inhuurt om dit soort testen uit te voeren, dan is dat bedrijf verzekerd voor eventuele problemen die het veroorzaakt. Dat lijkt simpel, maar sinds 9-11 zijn in vrijwel alle verzekeringspolissen zogenaamde cyberclausules opgenomen waardoor schade bij hacken wordt uitgesloten. Hebben de studenten/faculteiten/universiteiten daar aan gedacht? Of neemt de overheid alle schade op zich, zelfs in verwijtbare situaties? Wordt voor iedere ingezette student een Verklaring omtrent Gedrag geëist of wellicht een screening? Hoe zal de geheimhouding van de rapportages worden geborgd? En van de tijdens het onderzoek verzamelde data? Die zal namelijk ongetwijfeld op een onversleutelde laptop van de student staan. Wat gebeurt er als die laptop wordt gestolen, of wordt verkocht?

Enfin, vragen genoeg. Maar welk probleem proberen we met behulp van de studenten eigenlijk op te lossen? De minister schrijft in haar brief dat gespecialiseerde bedrijven beveiligingsonderzoeken uitvoeren en dat de studenten als aanvulling daarop worden ingezet. Zoals ik het lees, hoopt de minister dat de inzet van studenten wellicht extra problemen aan het licht kan brengen, echter wel ten koste van extra risico’s (zie mijn vragen in de vorige alinea).

Mijn inziens is het veel verstandiger om studenten stage te laten lopen bij de gespecialiseerde bedrijven. De hele juridische, verzekeringstechnische infrastructuur is er dan al, inclusief het aanvragen van VoG. Bovendien zijn deze bedrijven gewend hoe om te gaan met vertrouwelijke gegevens.

Guido van Rooij
Partner, Principal Security Consultant

* http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/03/16/kamerbrief-voortgang-toekomstbestendigheid-identiteitsinfrastructuur.html

WORKSHOP MOBILE SECURITY & HACKING

Tijdens de Black Hat Sessions Jubileumeditie (zie ook **Het Verslag** elders in deze Update) hebben Ralph Moonen en Arthur Donkers (ITSX) al een voorproefje gegeven op deze tweedaagse workshop die op 17 en 18 september in Utrecht plaats zal vinden. Naast de reeds veelbesproken risico's van Bring-Your-Own-Device (BYOD) zullen de volgende onderwerpen aan de orde komen: 'Mobile Apps: hoe veilig zijn ze, en hoe zijn ze veilig te maken', en 'iPhone en Android zwakheden'. Ook het kraken van pincode beveiliging op iPhone, encryptie van smartphones en de beperkingen van remote-wipe functionaliteit worden aan de hand van praktische voorbeelden gedemonstreerd. Zie bijgesloten leaflet voor meer informatie!

Madison Gurkha testpartij bij Pilot Impactanalyse **DigiD**

Naar aanleiding van het aangekondigde beleid van Minister Spies moeten gemeenten jaarlijks een audit DigiD uitvoeren. Alle gemeenten moeten voor eind 2013 een DigiD audit hebben uitgevoerd. Om tot een gestandaardiseerde aanpak te komen, is KING in opdracht van BZK en de VNG gestart met een impactanalyse. Hierin wordt samengewerkt met negen gemeenten en betrokken audit- en pentestpartijen, waaronder Madison Gurkha. De negen deelnemende gemeenten aan de pilot zijn: Apeldoorn, Doetinchem, Eindhoven, Heerhugowaard, Lisse, Nieuwegein, Zuidplas, Zutphen en Zwolle. Madison Gurkha zal samen met Verdonck Klooster & Associates de gemeenten Eindhoven, Apeldoorn en Heerhugowaard auditen. Zie ook **Het Interview** met Nausikaä Efstratiades van KING elders in deze Update.

Geslaagde Jubileumeditie

Op 4 april jl. vond in Ede alweer de tiende editie van de Black Hat Sessions plaats! Zoals u ook in **Het Verslag** kunt lezen, kijken wij terug op een drukke, leuke en leerzame dag! Via de website www.blackhatsessions.com kunt u van de meeste lezingen de filmopnames bekijken en vindt u een korte foto-impressie. Wij danken alle deelnemers voor hun aanwezigheid en hopen u volgend jaar (weer) te mogen begroeten op de Black Hat Sessions Part XI!

9 mei 2012
Privacy zal ons een zorg zijn?
georganiseerd door Mitopics
BCN Utrecht
Seminar over privacy in de zorg toegespitst op het fenomeen datalekken. Walter Belgers van Madison Gurkha verzorgt hier een lezing *Datalekken voorkomen in de praktijk*. Deelnemen aan dit seminar is kosteloos.
http://www.mitopics.nl/weblog/

5 juni 2012
TEDxBrainport 2012, Making the Future
Evoluon Eindhoven
Ontdek de grootste en waanzinnigste nieuwe ideeën voor een betere wereld. Verschillende sprekers – waaronder Walter Belgers van Madison Gurkha – en presentatoren zullen hun 'grootste en waanzinnigste' nieuwe oplossingen aan het publiek voorleggen.
http://www.tedxbrainport.nl/

21 juni 2012
Test Automation Day
World Trade Center (WTC) Rotterdam
Deze editie staat in het teken van *The Future of Test Automation*. De plenaire lezingen worden verzorgd door niemand minder dan Scott Barber U.S., Elfriede Dustin U.S. (IDT) en Walter Belgers (Madison Gurkha).
http://www.testautomationday.com/

DEKLANT

In elke Madison Gurkha Update vragen wij een klant het spreekwoordelijke hemd van het lijf met betrekking tot zijn of haar relaties met IT-beveiliging.

Dit keer in deze rubriek geen anoniem interview zoals u gewend bent, maar een interview met één van de grootgebruikers van DigD. We gingen hiervoor in gesprek met Rutger Heerdink, IT security officer bij het UWV.

8 vragen aan ... Rutger Heerdink

1

In welke branche is uw organisatie actief?
Het UWV is ketenpartner in de sociale zekerheid. De organisatievorm is ZBO (Zelfstandig Bestuurs Orgaan) en valt daarmee in de categorie van de semi-overheid.

2

Wat zijn de 3 belangrijkste kwaliteiten waarover je moet beschikken om deze functie met succes te kunnen uitoefenen?
Voor het UWV zijn dit zondermeer: 1) Maatschappelijke betrokkenheid, ook al werk ik zelf met IT, is de hele organisatie gericht op maatschappelijke dienstverlening en dat merk ik ook in mijn dagelijkse werkzaamheden. 2) Iedere situatie heeft twee zijden: een IT security zijde, en een functionele wens. Niet altijd gaan die twee hand in hand. De kunst is om dan een goede balans te vinden tussen de beide kanten. 3) De drive om de organisatie continu te verbeteren op het gebied van informatiebeveiliging. In een omvangrijke organisatie als het UWV is dit goed mogelijk omdat de procesmatige aanpak die daarvoor vereist is, goed is ingebed in de organisatie.

3

Welke gebeurtenissen van afgelopen jaar hebben op jou - als informatiebeveiliger - veel indruk gemaakt?
De hack bij DigiNotar. De hack zelf was het begin van een reeks gebeurtenissen die de Nederlandse overheid wakker heeft geschud. Want naast het feit dat een systeem gekraakt was, moesten veel partijen overstappen naar andere leveranciers.
De aandacht als gevolg van 'Lektober' voor mijn vakgebied is toegenomen. Voor mijn omgeving (zowel zakelijk als privé) zijn dreigingen niet langer abstract en 'ver van mijn bed' maar mensen begrijpen wat er mis kan gaan en eisen - terecht - van 'hun' overheid scherpte en alertheid.

4

Hoe is informatiebeveiliging opgezet in uw organisatie?
Het UWV heeft informatiebeveiliging ingedeeld in een aantal pijlers. De beveiliging en privacy organisatie (B&P) is daarbij overkoepelend. B&P waakt over alle gegevens die het UWV verwerkt ongeacht of dit met IT gebeurt. Hierbij moet dus ook gedacht worden aan fysieke-, HRM- en juridische aspecten van informatiebeveiliging. Daarnaast stuurt de CISO de beveiliging van de UWV informatievoorziening aan. Verder heeft Concern ICT een specifiek IT security team onder leiding van Martin Franse, waar ik onderdeel van ben. De supervisie ligt bij de Commissie Informatiebeveiliging, waar de CIO en een aantal staf/ divisie directeuren in deelnemen. Tenslotte kan ik melden dat UWV trekker is van een Competence Center Informatiebeveiliging en dit samen met SvB, Belastingdienst en DUO opzet. Het Competence Center beoogt voor overheidspartners een uitwisselplatform te zijn voor kennis en expertise op het gebied van informatiebeveiliging.

5

Hoeveel mensen houden zich in uw organisatie bezig met informatiebeveiliging?
In totaal zijn er organisatiebreed ruim 30 medewerkers specifiek met informatiebeveiliging bezig. De verantwoordelijkheden die voortkomen uit het beveiligingsbeleid zijn onderdeel van de lijnfunctie, waardoor dit aantal relatief beperkt kan blijven.

6

Op welke wijze maakt uw organisatie gebruik van DigiD?
De overheid zet in op E-dienstverlening, dit is een keuze die aan de ene kant hoort bij de kleine overheid, aan de andere kant hoort E-dienstverlening bij de 21ste eeuw. Het UWV biedt primair een tweetal internetportalen waar DigiD authenticatie wordt gebruikt. Dit zijn WERK.nl en het UWV Werknemersportaal te bereiken via UWV.nl. Met deze E-diensten behoort UWV tot de top van DigiD grootverbruikers.

7

Wat zijn in uw organisatie op dit moment de belangrijkste uitdagingen op het gebied van informatiebeveiliging rondom DigiD?
Logius (de organisatie verantwoordelijk voor DigiD, red.) heeft in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een set richtlijnen uit de NCSC beveiligingsrichtlijnen voor webapplicaties verplicht gesteld voor DigiD gebruikers. Daarmee zijn het voor ons normen geworden. Dit geldt voor alle organisaties die DigiD gebruiken. Eind 2012 moeten de grote overheidsorganen hieraan voldoen. Eind 2013 ook alle gemeenten in Nederland. Dit veroorzaakt hoe dan ook extra werk en dynamiek. Werkzaamheden die voortkomen uit dit normenkader komen bovenop de al ingeplande werkzaamheden. Toch ben ik ervan overtuigd dat het bijdraagt aan een veiligere en betere kwaliteit van E-dienstverlening, dus ik zie deze verplichting als een steun in de rug.

8

Welke maatregelen worden genomen om deze risico's onder controle te houden en hoe helpt Madison Gurkha daarbij?
Het NCSC normenkader richt zich op een breed scala van maatregelen. Van het beheerproces en tot technisch functioneren van portalen. Madison Gurkha is voor het UWV een belangrijke partner om onze portalen technisch op orde te houden. Zij signaleren dreigingen, adviseren ons en rapporteren ons met aanbevelingen.

KING en VNG gestart met Impactanalyse DigiD

Dit keer in deze rubriek een interview met Nausikaä Efstratiades, Coördinator Implementatie bij Kwaliteitsinstituut Nederlandse Gemeenten (KING). Gezien het belang van informatiebeveiliging voor gemeenten heeft KING besloten een project op te zetten. In dit project wordt de impact van de nieuwe Logius beveiligingsnorm rondom DigiD bepaald. Zodoende kan KING een gedegen advies uitbrengen aan de verschillende Nederlandse gemeenten. Nausikaä is binnen KING verantwoordelijk voor dit project.

Wat zijn de belangrijkste taken van KING?
KING is drie jaar geleden opgericht door de VNG om de kwaliteit van dienstverlening van gemeenten aan burgers en bedrijven te verhogen. KING heeft de afgelopen jaren een aantal standaarden ontwikkeld, geïmplementeerd en in beheer genomen. KING doet dat niet alleen. Deze worden samen met gemeenten ontwikkeld. Informatiebeveiliging is door de crises van DigiNotar en Lektober hoog op de agenda gekomen, zowel bij gemeenten als bij KING.

Welke rol speelt KING nu in het overleg tussen de gemeenten enerzijds en het Ministerie van Binnenlandse Zaken en Logius anderzijds?
KING vormt samen met de VNG het eerste contactpunt voor gemeenten. KING is naar aanleiding van het voorgestelde beleid van minister Spies van BZK (zie brief van de Tweede Kamer) gestart met een impactanalyse met negen gemeenten om van A tot Z het auditproces te doorlopen. Het betreft hier een gezonde mix van gemeenten met een diversiteit in ICT architectuur. Hierbij worden dan ook EDP-auditors, pentesters, CMS-leveranciers en hostingpartijen betrokken. De verwachting is dat dit tot een efficiënte en gestandaardiseerde aanpak zal leiden. De uitkomst van deze analyse zal dan ook vermoedelijk tot input leiden voor het vervolg van de audits voor de ruim 400 andere gemeenten. Te denken valt aan adviezen over hoe zij hun leveranciers moeten benaderen, het stimuleren van een gezamenlijke aanpak van gemeenten die dezelfde of vergelijkbare ICT-omgeving hebben, het aanbieden van de juiste documentatie etc. Gaandeweg zal blijken of er informatie of handreikingen missen. KING zal deze dan ontwikkelen. Organisaties als het waterschapshuis en IPO kunnen desgewenst aansluiten. De VNG en KING zullen de gemeenten voorzien van nieuws en informatie via de websites van KING en de VNG, de ledenbrief van de VNG, externe nieuwsbrieven, Twitter etc.

Welke doelstellingen heeft KING in dit kader voor haar zelf geformuleerd?
De VNG en KING zijn voornemens een informatiebeveiligingsdienst op te richten. Deze dienst heeft als doel gemeenten te ondersteunen bij het afhandelen van beveiligingsincidenten en de gemeentelijke informatiebeveiliging te verbeteren. Diginotar en Lektober hebben laten zien dat informatiebeveiliging in gemeenten kwetsbaar is. Een gecoördineerde aanpak voor het gemeentelijk veld is nodig. Dit is de aanbeveling van een Starting Gate die bureau Gateway van BZK eind maart in opdracht van de VNG en KING heeft uitgevoerd. De conclusies en aanbevelingen zijn:

- Werk snel een propositie uit en maak een businesscase;
- Organiseer een gecoördineerde incident- en crisisafhandeling voor gemeentelijk veld;
- Pak de informatiebeveiliging overheidsbreed aan;
- Organiseer en mobiliseer voor gemeenten de gespecialiseerde kennis van informatiebeveiliging;
- Gebruik het momentum om nu het inkoop- en leveranciersmanagement voor informatiebeveiliging te organiseren.

KING KWALITEITS INSTITUUT NEDERLANDSE GEMEENTEN

De VNG en KING werken de komende weken samen met gemeenten een voorstel en een businesscase voor een Gemeentelijke Informatiebeveiligingsdienst verder uit.

Madison Gurkha testpartij bij pilot impactanalyse audit DigiD

Het is niet efficiënt om alle 415 gemeenten zelf hun audits te laten uitvoeren. Daarom wil KING onderzoeken met welke DigiD-koppelingen gemeenten werken, welke leveranciers daarbij betrokken zijn en hoe daarvoor een gestandaardiseerde auditaanpak ontwikkeld kan worden. Om dit te realiseren is KING in opdracht van BZK en de VNG gestart met een impactanalyse.

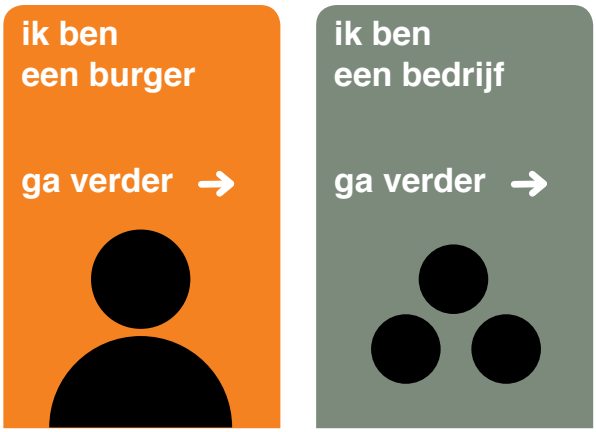
Negen representatieve gemeenten zijn geselecteerd om deel te nemen aan de pilot die functioneert als “testcase” om ervaring op te doen met het testen tegen de nieuwe DigiD beveiligingsnorm. De deelnemende gemeenten zijn: Apeldoorn, Doetinchem, Eindhoven, Heerhugowaard, Lisse, Nieuwegein, Zuidplas, Zutphen en Zwolle. Om gezamenlijk de negen audits uit te voeren zijn vier audit- en pentestpartijen aangesteld. Madison Gurkha zal samen met Verdonck Klooster & Associates de gemeenten Eindhoven, Apeldoorn en Heerhugowaard auditen.

De (totale) uitkomst van de impactanalyse verwacht KING in juni te presenteren.

In de rubriek "Het Inzicht" stellen wij bepaalde (technische) beveiligingsproblemen aan de orde. Deze keer geeft Walter Belgers meer inzicht in de nieuwe DigiD beveiligingsnorm en zijn visie daarop.

De nieuwe DigiD beveiligingsnorm

Alles liep zo lekker bij de gemeentes. Totdat opeens de ene na de andere lekke website in het nieuws kwam. Paniek alom! Gemeentesites werden afgesloten van DigiD. Managers moesten uitzoeken of 'hun' sites wel veilig genoeg waren. En wie bepaalt dan wat 'veilig genoeg' is?



Met recht kun je spreken van een 'wake-up call'. In de praktijk zie ik maar al te vaak dat beveiliging iets is waar mensen pas mee aan de slag gaan als daar lichte dwang mee gemoeid gaat. Jaren terug zorgde SOX voor een hoop activiteit in de beveiliging. Meer recent de NEN7510-norm in de zorg. En nu: normen en richtlijnen voor instellingen die een DigiD koppeling hebben.

Altijd in het vizier

Maar beveiliging hoort niet iets te zijn dat je, als iemand je in de ribben port, er maar even bij doet met tegenzin. Beveiliging is iets dat je altijd in het vizier moet hebben. Bij het ontwerp, bij de implementatie, bij elke upgrade en elke test. Of het nu gaat om een desktopcomputer of om bedrijfsprocessen, ze zullen veilig genoeg moeten zijn.

Kort door de bocht is beveiliging: 'het doet niet wat het niet hoort te doen'. Functionaliteit is complementair: 'het doet wat het hoort te doen'. Dat de focus bij het bouwen van een systeem of inrichten van een proces bij functionaliteit ligt, is logisch, maar dat betekent nog niet dat beveiliging maar helemaal genegeerd kan worden. Als software geschreven wordt door iemand die beveiligingsbewust is, kan het nog wel goed uitpakken. Heel vaak echter levert het lekke applicaties op, zonder dat men zich daar van bewust is.

Een groot gevaar is namelijk dat het ontbreken van beveiliging niet direct zichtbaar is. Het ontbreken van functionaliteit daarentegen, valt wel op. Het is ook heel eenvoudig om uit te leggen aan de manager dat er tijd en geld vrijgemaakt moet worden om een functioneel probleem op te lossen. Bij beveiliging ligt dat moeilijker. Geld en tijd loskrijgen is lastig omdat de beveiliging geen direct aanwijsbaar effect heeft. De business case (die er wel is), is lastiger te verkopen.

Goed hang- en sluitwerk

Op de een of andere manier is beveiliging in de IT ook niet iets dat mensen wakker houdt. Dit in tegenstelling tot andere terreinen waar beveiliging van belang is. Iedereen begrijpt het belang van goed hang- en sluitwerk in huis (terwijl je waarschijnlijk best een tijdje je huis onafgesloten kunt laten zonder dat er problemen optreden). En vrijwel iedereen heeft een brandverzekering, terwijl de kans op brand minimaal is. Wat dat betreft is het opzeggen van een brandverzekering bij een bezuinigingsronde even voor de hand liggend als bezuinigen op IT-beveiliging. Beiden voegen niets functioneels toe en kosten geld. Maar in de gedachte van een manager heeft een brandverzekering meer waarde dan IT-beveiliging.

Bij een oud en door en door bekend vakgebied als mechanische sloten heb je een SKG-keurmerk met 1, 2 of 3 sterren. De beveiliging wordt getest aan de hand van duidelijke regels waarin toegestane gereedschappen, inbraaktechnieken en hoeveelheid tijd zijn vastgelegd. Bij een jong en complex

> Een groot gevaar is namelijk dat het ontbreken van beveiliging niet direct zichtbaar is

norm

De DigiD beveiligingsnorm is bedoeld voor organisaties die DigiD gebruiken en jaarlijks een ICT-beveiligingsassessment moeten doen. De norm[1] is een selectie van richtlijnen uit het document "ICT-beveiligingsrichtlijnen voor webapplicaties[2]" van het Nationaal Cyber Security Centrum (NCSC). Deze richtlijn bestaat uit twee documenten. Het eerste deel bevat de daadwerkelijke richtlijnen, het tweede deel de toelichting met aanbevelingen daarop.
De norm is vastgesteld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties in overleg met Logius, Rijksauditdienst en NCSC. De beveiligingsrichtlijnen van NCSC zijn breed toepasbaar voor ICT-oplossingen die gebruikmaken van webapplicaties. In het kader van DigiD zijn de richtlijnen die de meeste impact hebben op de veiligheid van DigiD en de met DigiD ontsloten gegevens gekwalificeerd als de norm en onderdeel van de toetsing.
Logius adviseert echter de hele set van richtlijnen van NCSC te adopteren.

Het doel zou moeten zijn om continu veilig te werken: veilig te ontwerpen, te implementeren en te onderhouden

vakgebied als IT-beveiliging is dit veel en veel complexer. Het aantal mogelijke aanvalsvectoren is vele malen groter. Hierdoor is voor het testen van de beveiliging van een (maatwerk)applicatie ook heel veel meer specialisme nodig dan het testen van een slot. Het zorgt er ook voor dat een SKG-sterrensysteem eigenlijk niet uitvoerbaar is, er zijn gewoonweg te veel manieren om beveiliging te doorbreken.
Tenzij je een heel generiek lijstje van mogelijke lekken maakt. Je zou bijvoorbeeld kunnen zeggen: de tien veel voorkomende problemen in webapplicaties die in de OWASP top-10 worden genoemd, mogen niet voorkomen. Het testen hiervan kost echter veel tijd en het is dan zaak een optimum te vinden tussen de besteedde tijd en de mate van verkregen zekerheid dat alle belangrijke kwetsbaarheden zijn gevonden.

Nieuwe norm voor beveiliging
De norm die opgelegd gaat worden aan instellingen die met DigiD koppelen heeft ook last van deze complexiteit. Je kunt geen norm opstellen die zo specifiek is, dat een test op de norm kan worden uitgevoerd met een soort afvinklijst. Door de norm generieker te maken, laat je echter weer ruimte voor interpretatie. Met recht een probleem om je haren uit je hoofd te trekken. Maar hoe de norm ook uitpakt, het feit blijft dat daarmee wel het probleem wordt aangepakt dat er vaak niet genoeg redenen worden gezien om iets aan beveiliging te doen. Wat dat betreft is het feit dat zo'n norm bestaat, ongeacht de inhoud, al voldoende om de algehele beveiliging te verbeteren.

Continue veilig werken
De norm richt zich overigens niet alleen op technische zaken, maar ook op de procedures rondom (technische) beveiliging. Eigenlijk is dat het belangrijkste. Het doel zou niet moeten zijn om te slagen voor een beveiligingstest. Het doel zou moeten zijn om continu veilig te werken: veilig te ontwerpen, te implementeren en te onderhouden. Op de lange termijn is daar ook de meeste winst te halen. Eigenaars van websites die zijn afgesloten van DigiD hebben inmiddels wel een idee van de hoeveelheid inspanning en kosten die erbij komen kijken om beveiligingsproblemen op te lossen.

Problemen voorkomen is altijd goedkoper en bespaart u zaken als slechte publiciteit en veel moeite om de norm te halen. Denk daarbij aan bewustwordingscampagnes, aan opleidingen in het veilig programmeren, design reviews voordat er aan implementatie wordt begonnen, het opstellen van beveiligingseisen naast functionele eisen in ontwikkelprojecten, het gebruik van abuse cases in de opleveringsfase van een project, het laten uitvoeren van beveiligingstesten voordat iets in productie wordt genomen, en zo meer.
Met een veilig fundament is het vrij eenvoudig om aan specifieke eisen, die mogelijk in de toekomst nog opgelegd worden, te voldoen.

1 http://www.logius.nl/fileadmin/logius/product/digid/documenten/assessments/120221_norm_ict-beveiligingsassessments_digid.pdf
2 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

Waar de rest van deze editie in gaat op DigiD en de uitdagingen die daar bij komen kijken, gaat Ward Wouts in deze rubriek 'De Hack' in op het vaak onderbelichte interne netwerk.

Onderbelichte interne netwerken

De meeste IT-afdelingen zijn er tegenwoordig van doordrongen dat het periodiek uitrollen van beveiligingsupdates op alle systemen een must is. Met name op het vlak kantoorautomatisering wordt dit tegenwoordig vaak centraal aangestuurd en is dit redelijk onder controle. Hoewel we ook regelmatig bedrijven zien waar een grote diversiteit aan systemen gebruikt wordt, waar dit minder goed geregeld is. Virusscanners en firewalls zijn gemeengoed geworden. Zelfs mijn mailbox laat me nog maar zelden een ongefilterd spambericht zien. Ik zou er bijna vrolijk van worden. Maar als het dan zo goed geregeld is, waarom zien we dan nog steeds zo veel problemen op interne netwerken?

Uitzonderingssysteem

Een van de meest voorkomende problemen blijft het uitzonderingssysteem. Vaak een pc die maar voor een kleine specifieke taak gebruikt wordt en om de een of andere reden niet geüpdatet 'kan' worden. De specialistische software die er op draait werkt niet op een up-to-date besturingssysteem. De software die er op draait is zo kritiek voor een bedrijfsproces dat niemand er aan durft te komen. Er wordt bijzondere hardware gebruikt die nergens anders mee werkt. Dit zijn allemaal begrijpelijke argumenten om zo'n uitzondering te accepteren. Vanuit beveiligingsoogpunt levert dit echter wel problemen op als dit er voor zorgt dat dit uitzonderingssysteem gebruikt kan worden om andere systemen aan te vallen. Bijvoorbeeld via de zogenaamde pass-the-hash techniek met metasploit. Mijn collega's Frans en Stefan hebben dit onlangs op de Black Hat Sessions (zie ook 'Het Verslag' op pagina 11 van deze Update) nog gedemonstreerd. Vaak kan dit het beste ondervangen worden door het specifieke systeem af te scheiden van de 'normale' netwerken; er een soort quarantainestatus aan geven dus. Daarnaast is het goed om na te denken over het opvangen van storingen. Als een systeem zo belangrijk is dat het niet geüpdatet kan worden, wat gebeurt er dan als bijvoorbeeld de hardware het laat afweten? Werkt de software überhaupt nog op nieuwere systemen? Mijn ervaring met beheer en beveiliging vertelt me dat dit soort uitzonderingen zelden de extra kopzorgen en bijkomende kosten waard zijn.

Embedded software

Naast de uitzonderingssystemen, waarvan de meeste beheerafdelingen wel weten dat ze er zijn, maar liever de andere kant op kijken, zien wij een grote uitdaging bij het beheer van embedded software. De grote nieuwe NAS- of SAN-machine wordt in het algemeen initieel nog goed geconfigureerd. Printers in alle maten worden echter vaak alleen ingeprikt en zodra ze een IP-adres hebben aan hun lot overgelaten. Hierbij wordt vergeten dat deze printers vaak ook over het netwerk beheerd kunnen worden. We hebben onlangs de controle kunnen krijgen over een volledige repro-afdeling door, vrijwel uitsluitend, default wachtwoorden te gebruiken. Op ongeveer de helft van de printers was het wachtwoord leeg. Nu klinkt dat niet perse als schokkend, tot je op de printers de uitgaande post kunt meelezen.

Een beetje printer heeft tegenwoordig een ingebouwde harde schijf en wordt vaak geleased. Op de harde schijf komen de te printen documenten al dan niet tijdelijk te staan. Dit is gezien de functie van zo'n printer heel logisch en volledig verklaarbaar. Zo'n apparaat moet gewoon productie draaien en als ie stuk is moet een monteur het, liefst zo snel mogelijk, repareren. Hiermee ontstaat echter wel een achterdeur naar interessante gegevens, in ieder geval interessant genoeg om af te drukken. In de gevallen waar we zien dat de printers wel correct met wachtwoord geconfigureerd zijn (vergeet niet SNMP af te schermen!), zien we dat er in het algemeen geen updates geïnstalleerd worden. In feite is de printer hiermee een uitzonderingssysteem geworden. Naast het wel installeren van eventuele updates raden we aan dit soort systemen in aparte subnetten te plaatsen en het verkeer van en naar de printers strikt te filteren. Vaak kan het zinnig zijn om een pc als soort stepping-stone in te richten en als printserver te gebruiken voor de daadwerkelijke printers. Zo kan een redelijk afgebakende datastroom gecreëerd worden.

'Vergeten' systemen

Overigens zien we dat ook de andere appliances op interne netwerken (ze worden gelukkig maar zelden direct aan het internet gehangen) vaak nauwelijks tot niet geüpdatet worden. Denk bijvoorbeeld aan (kleine) NAS-systemen, draadloze access-points en telefoonsystemen. Van al dit soort 'vergeten' systemen hebben we regelmatig 'misbruik' kunnen maken. Helaas is hier geen eenvoudige oplossing voor. De beheerorganisatie kan niet anders dan periodiek (laten) controleren of dit soort systemen veilig geconfigureerd zijn, of er beveiligingsupdates uitgebracht zijn en als het mogelijk is ze zo goed mogelijk van de normale netwerken afscheiden.

Hans Verweij

In deze uitgave waarin DigiD centraal staat, laten wij belanghebbenden aan het woord. Omdat de beheerorganisatie Logius in dit kader niet mag ontbreken, hebben we Hans Verweij, Manager Productregie bij Logius bereid gevonden een aantal vragen te beantwoorden. Binnen zijn functie is Hans verantwoordelijk voor de totale lifecycle van verschillende e-Overheid producten, waaronder DigiD. Aangezien beveiliging één van de thema's is die van belang zijn bij de lyfecycle, licht Hans een en ander toe over de nieuwe beveiligingsnorm van Logius rondom DigiD.

Er bleken in Lektober veel overheidswebsites kwetsbaar te zijn, die gebruik maken van DigiD. Bij een aantal sites heeft Logius besloten deze af te sluiten van DigiD. Wat zijn hierbij de overwegingen van Logius geweest?
Logius heeft 39 websites tijdelijk afgesloten van DigiD. Er werd tijdens Lektober namelijk bekend dat deze sites mogelijk ernstige beveiligingsrisico's liepen. Daarbij werd gesproken over het overnemen van DigiD sessies. In overleg met de VNG en KING en in afstemming met NCSC heeft Logius besloten de dienstverlening van DigiD aan de betreffende gemeenten op te schorten.

In onze optiek is, door de aandacht in o.a. Lektober, het bewustzijn van DigiD gebruikende organisaties t.a.v. IT-beveiliging toegenomen. Hoe ziet Logius deze ontwikkeling?
Logius vindt dit een positieve ontwikkeling en herkent dit. Organisaties beseffen steeds meer dat ze opereren in ketens die grotendeels digitaal zijn en dat ze een verantwoordelijkheid hebben om hun IT-beveiliging op orde te hebben zodat de ketens niet verzwakken. Lektober heeft daarnaast hardhandig en terecht blootgelegd dat we de keten als geheel moeten beveiligen in plaats van alleen de afzonderlijke schakels. Vandaar ook de norm voor organisaties die DigiD gebruiken. Zo wordt de dienstverleningsketen, waar DigiD altijd in gebruikt wordt, in ieder geval sterker.

Er worden door organisaties als KING pilots voorbereid met het toetsen volgens de nieuwe norm. Wat zijn de verwachtingen van Logius t.a.v. eventuele aanpassingen van de norm na het uitvoeren van deze pilots?
De verwachting van Logius is dat de norm stevig staat en dat daar weinig tot geen aanpassingen op komen. Wel verwachten wij dat n.a.v. de pilots van KING het toetsingsproces meer gestroomlijnd kan worden door het slim organiseren van toetsingen bij leveranciers en gemeenten.

De verwachting van Logius is dat de norm stevig staat en dat daar weinig tot geen aanpassingen op komen

Mogelijk volgen nog wel wijzigingen in de aanpak in 2013, dit is afhankelijk van de resultaten over 2012 en eventueel daaropvolgende beleidsmatige en politieke aanvullende afspraken.

Grotere gebruikersorganisaties van DigiD moeten eind 2012 aan de norm voldoen, kleinere eind 2013. Wat is de overweging van Logius geweest om deze periode zo lang te laten zijn?
De deadlines zijn zo gekozen dat prioriteit wordt gegeven aan de grote gebruikersorganisaties en om kleine organisaties een realistische kans te geven hun omgevingen op orde te maken, ondersteund door KING en de VNG.

Wat zijn de consequenties voor organisaties als ze niet tijdig aan de norm voldoen?
Logius kan na het ontvangen van een rapport met bevindingen een onderzoek instellen of de beveiliging van DigiD gevaar loopt. Bij een duidelijke bedreiging van de integriteit van DigiD zal Logius de DigiD aansluiting opschorten.
Organisaties worden, net als tijdens Lektober, van DigiD afgesloten zodra sprake is van een geconstateerde inbraak in hun ICT-systeem.

Welke ontwikkelingen op korte en lange termijn ziet Logius voor DigiD en het al daar niet strenger worden van de norm?
Op korte termijn verwacht Logius geen aanpassing van de norm. Op langere termijn (één of meer jaren) verwacht Logius dat de norm langzaam strenger zal worden. Het is een groeimodel.

Welke verdere ondersteuning biedt Logius aan de gebruikers van DigiD-toepassingen?
Wij helpen DigiD gebruikende organisaties door ze zo goed mogelijk te informeren over de assessments. Hierbij zullen we ook zeker gebruik maken van de ervaringen uit de assessments bij grootgebruikers in 2012 en de pilot van KING/VNG bij een tiental gemeenten.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

In de rubriek "Het Verslag" laten wij u delen in onze ervaringen tijdens conferenties, seminars en trainingen. Deze keer doet Daniël Dragičević verslag van de Black Hat Sessions Part X Jubileumeditie.

Black Hat Sessions Part X
Jubileumeditie

Op 4 april 2012 vond alweer de tiende editie van de Black Hat Sessions plaats in congrescentrum de Reehorst te Ede. In grote getale hebben we deze speciale jubileumeditie gevierd waarin we de stand van beveiliging in de ICT-wereld de revue hebben laten passeren, van verleden via het heden naar een blik in de toekomst. Daniël Dragičević van Madison Gurkha vertelt hoe hij deze dag heeft beleefd.

De conferentie werd ook dit jaar geopend door dagvoorzitter Walter Belgers (Madison Gurkha). Er werd stilgestaan bij het overlijden van Harry Onderwater in december 2011. Harry Onderwater zou als hacker en beveiligingsexpert van het eerste uur komen spreken op deze editie van de Black Hat Sessions.

Het overvolle programma bestond uit meerdere parallelle tracks. Helaas hebben we te weinig ruimte om alle presentaties hier te behandelen. We zullen daarom in dit verslag enkele presentaties voor u eruit lichten. Inmiddels kunt u de meeste lezingen alsnog beleven door de opnames ervan te bekijken via de website www.blackhatsessions.com. Ook kunt u hier terecht voor de hand-outs van de presentaties en een korte foto-impressie.

Brenno de Winter trapt af

De eerste keynote, getiteld "Heel Nederland blijft lek" werd gegeven door journalist van het jaar 2011 Brenno de Winter. Tijdens deze presentatie werd pijnlijk duidelijk hoe in Nederland wordt omgegaan met persoonsgegevens. Het feit dat veel bedrijven en overheden zich schuldig maken aan bovenmatige gegevensverzameling is een zorgelijke ontwikkeling. Wanneer je daarbij de grote aantallen terugkerende beveiligingslekken als gevolg van SQL injection of slecht patchbeleid bij optelt, wordt duidelijk dat datalekken - en als gevolg daarvan identiteitsdiefstal - een grotere problemen zijn dan over het algemeen wordt gedacht.

Brenno maakte een interessante vergelijking tussen het IT-beveiligingswerkveld en de luchtvaart. Wanneer er in de luchtvaart een ongeluk of een 'near miss' plaatsvindt, wordt dit tot op de bodem uitgezocht en worden de resultaten gepresenteerd. Op basis van deze resultaten worden zowel technische als procedurele verbeteringen doorgevoerd. Waarom is het in de IT-beveiliging zo dat de onderzoeken in het geheim plaatsvinden en dat bevindingen vaak niet of nauwelijks naar buiten komen? Waarom leren we niet van onze fouten? *"If you think safety is expensive, try an accident"*, zoals Brenno het treffend wist te citeren.

Black Hat Sessions Part X werd mede mogelijk gemaakt door de Sponsoren
ITSX, PvIB, SCOS, GGB, AT Computing, TSTC en Media Partners: Ngi, SecureLink en Certified Secure

Madison Gurkha bedankt
Brenno de Winter, Huub Roem, Wim Verloop, Walter Belgers, Job de Haas, NCSC, Bert Hubert, Roel Verdult, Koen Martens, Frans Kollée en Stefan Castille

Een duik in de wereld van de mobiele beveiliging

Ralph Moonen en Arthur Donkers (ITSX) zijn tijdens hun presentatie in de wereld van de mobiele beveiliging gedoken. Encryptie op mobiele platformen wordt weinig gebruikt waardoor gegevens op dit soort apparaten gemakkelijk te achterhalen zijn met standaard forensische tools. Ook kwamen de verschillen tussen Google's Open Android en Apple's "walled garden" ter sprake, gevolgd door de risico's die het zogenaamde 'rooten' van apparaten met zich meebrengt. Ter afsluiting kregen we een live demonstratie te zien waarbij de heren toegang konden krijgen tot een 'gelockte' iPad door een bruteforce-aanval uit te voeren op het wachtwoord waarbij ook de automatische wipe-functie werd omzeild. Deze presentatie was een voorproefje van de later in het jaar te houden workshops (zie ook het nieuwsitem op pagina 3 van deze Update en de bijgesloten leaflet).

RFID Security taken for granted

Roel Verdult (Radboud Universiteit Nijmegen), die als student bekend werd door de OV-chipkaart te hacken, benoemde in zijn presentatie verschillende problemen in RFID security. Zowel de hack van de OV-chipkaart als de werking van verschillende andere commercieel verkrijgbare RFID-oplossingen kwamen ter sprake. RFID wordt steeds vaker gebruikt als authenticatie methode voor fysieke beveiliging maar ook in andere toepassingen zoals bijvoorbeeld casinochips.

De besproken implementatiefouten variëren van het gebruik van een identieke sleutel voor elk product, de output van een functie die voorspelbaar is of toepassingen waarbij encryptie helemaal ontbreekt. Roel bevestigde ook twee bekende spreuken die in de cryptografie vaak geopperd worden: "gesloten protocollen komen de veiligheid niet ten goede" en "de sleutellengte heeft geen grote impact als de implementatie van het protocol niet goed is toegepast". Deze technische lezing heeft mij in ieder geval genoeg stof tot nadenken gegeven.

Hedendaagse aanvalsmethoden

Het programma werd afgesloten met een live hacking demo verzorgd door Frans Kollée en Stefan Castille (Madison Gurkha). Zij demonstreerden meerdere hacks waaronder het achterhalen van *WPA-sleutels*. Een andere soort hack die ze lieten zien was *Pivoting*, waarbij een gecompromitteerd systeem wordt gebruikt om het interne netwerk te scannen, werkte erg goed. Ook de *pass-the-hash*, het inloggen op een systeem door gebruik te maken van een hashwaarde, bemachtigd op een ander systeem bleek een interessante aanvalsmethode te zijn. De hack met de geprepareerde USB-hub werd als laatste gedemonstreerd. De USB-hub was voorzien van een Teensy-microcontroller. Deze werd gebruikt om toetsaanslagen naar de PC te sturen. Tijdens de koffie- en lunchpauzes konden de deelnemers bij de stand van Madison Gurkha een antwoord geven op de prijsvraag: "Hoeveel security audits voerde Madison Gurkha in 2011 uit? De winnaars werden tijdens deze presentatie bekend gemaakt en kregen als "gelukkige" winnaar een USB-hub uitgereikt. Hopelijk voor hen een niet-geprepareerde, want Frans en Stefan hebben laten zien wat de gevolgen kunnen zijn als de USB-hub voorzien is van extra elektronica.

Met een kort afsluitingswoord bedankte Walter Belgers ten slotte iedereen voor zijn/haar aanwezigheid in de vorm van een borrel in de wintertuin. Het was een drukke, gezellige en leerzame dag!

HET COLOFON

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

Vormgeving & productie
Hannie van den Bergh / Studio-HB

Foto cover
Digidaan

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

T +31 40 2377990
F +31 40 2371699
E info@madison-gurkha.com

Redactie
redactie@madison-gurkha.com

Bezoekadres
Vestdijk 9
5611 CA Eindhoven
Nederland

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



Bent u klaar voor de DigiD audit?

DigiD Audit Readiness Scan

Met de DigiD Audit Readiness Scan helpt ITSX u bij het tijdig vaststellen van verbeterpunten en ondersteunt u bij de audit voorbereidingen.

Ter bescherming van persoonsgegevens van burgers heeft Logius een beveiligingsnorm opgesteld waaraan DigiD gebruikers zoals gemeenten en publieke instellingen moeten voldoen.

Beveiligingsincidenten in DigiD gerelateerde applicaties kunnen leiden tot het rigoureus afsluiten van DigiD met alle gevolgen van dien. Het is daarom van belang dat wanneer u DigiD gebruikt binnen uw organisatie, u de IT-beveiliging op orde heeft en op tijd klaar bent voor de verplichte audit. Deze audit dient dit jaar, of voor kleinere organisaties volgend jaar, te zijn afgerond.

Het vergt een aanzienlijke inspanning van organisaties om aan de norm te kunnen voldoen. Omdat de norm nog zo nieuw is, is er bovendien nog weinig kennis over beschikbaar. Daarom is het goed om te weten dat ons moederbedrijf Madison Gurkha betrokken is bij een pilot van KING (Kwaliteits Instituut Nederlandse Gemeente) om een drietal gemeenten te auditen tegen de DigiD norm. Op basis van de kennis en ervaring die dit oplevert kan ITSX uw organisatie ondersteunen met de DigiD Audit Readiness Scan. De scan bekijkt de mate waarin uw organisatie klaar is voor de audit en voldoet aan de normen. Deze 'gap-analyse' levert een concreet verbeterplan en een 'roadmap' op om de audit succesvol te laten verlopen. ITSX en Madison Gurkha kunnen u uiteraard ook de helpende hand bieden bij het uitvoeren van het verbeterplan.

De DigiD Audit Readiness Scan vergt een geringe investering maar bespaart u een langdurig, moeizaam en duur traject om uw IT-beveiliging op orde te krijgen en te voldoen aan de DigiD norm.

Indien u vragen heeft of een afspraak wilt maken, kunt u contact met ons opnemen via www.itsx.com of info@itsx.com.

ITSX en haar consultants leveren diensten over de gehele breedte van het vakgebied informatiebeveiliging, waaronder de deelgebieden Information Security Management, IT-Audit en Compliance, Testen, Opleiding en Training.

Madison Gurkha
Your Security is Our Business