Madison Gurkha
Your Security is Our Business

16 SEPT 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 Remco Huisman over de businesscase.

DE COLUMN

De businesscase voor informatiebeveiliging

Tijdens gesprekken die ik met (potentiële) klanten heb, geven mijn gesprekspartners regelmatig aan dat IT-beveiliging binnen de organisatie wordt gezien als kostenpost. "Het voegt niks toe aan de business, het is lastig en het kost alleen maar geld." Vaak vragen ze mij wat de businesscase is voor IT-beveiliging. Daar is niet zomaar een antwoord op te geven. IT-beveiliging kost inderdaad geld, maar dat kost een brandverzekering ook. Deze laatste levert niks op, tenzij..... het kantoor afbrandt. Nu branden de meeste websites niet af, maar IT-beveiligingsincidenten zijn er te over. Deze incidenten van andere organisaties die de pers halen, maken meestal niet zo heel veel indruk, totdat het wat dichterbij komt. Zo zagen we na 'Lektober' een toename van aanvragen uit de (gemeentelijke) overheid en onlangs een toenemende vraag naar onze diensten vanuit de medische sector en arbeidsorganisaties.

Voor organisaties die gehackt zijn is het antwoord op de vraag van de business case ineens heel eenvoudig te beantwoorden. De imagoschade is vaak groot en de tijd en energie die in een (forensisch) spoedonderzoek moet worden gestoken is aanzienlijk. Bovendien wordt de directie/RvB onrustig, stelt prangende vragen en wil snel adequate antwoorden. Is een IT-omgeving of een webshop offline, dan is de schade door gederfde productiviteit c.q. omzet heel goed meetbaar. Organisaties die een 'hack' overkomt worden meestal onze beste klanten. Eindelijk nemen ze informatiebeveiliging voldoende serieus om de nodige maatregelen te nemen. Dat doet wel even pijn, maar er is vaak ook een grote inhaalslag te maken en heel veel te verbeteren om IT-beveiligingsrisico's structureel te identificeren, te verminderen en te voorkomen.

In sommige gevallen wordt de onderbouwing van de businesscase ondersteund door wet- en regelgeving waaraan organisaties moeten voldoen. Deze wet- en regelgeving is echter niet altijd even dwingend (er zijn weinig of geen sancties) of is tamelijk vrij interpreteerbaar. In de zorgsector ervaren wij NEN 7510:2011 niet als erg dwingend, terwijl de resultaten van onze onderzoeken in die sector over het algemeen laten zien dat aanscherping van de norm geen overbodige luxe is. De regels van De Nederlandsche Bank in de financiële wereld zijn al een stuk harder. Begin dit jaar heeft Logius een beveiligingsnorm opgesteld waaraan DigiD gebruikers zoals gemeenten en publieke instellingen moeten voldoen (hierover is in Update 15 al uitgebreid bericht). De kans is erg groot dat dit jaar Europese wetgeving van kracht wordt met betrekking tot digitale privacy. Meer over de nationale en Europese wet- en regelgeving leest u in het artikel van Matthijs Koot in de rubriek 'Het Inzicht' van deze Update. Deze nieuwe Europese telecomregels bevatten onder andere een meldplicht aan alle slachtoffers van een datalekkage en de EU kan tot 2% van de jaaromzet aan boetes opleggen in geval van ernstige nalatigheid. Staatssecretaris Fred Teeven loopt al op deze ontwikkeling vooruit met een wetsvoorstel dat het CBP toestaat om boetes tot EUR 450.000 op te leggen in geval van nalatigheid. Dit maakt het in ieder geval een stuk makkelijker om een businesscase te onderbouwen richting directie. Dáár wordt namelijk bepaald of en welke aandacht en het bijbehorende budget informatiebeveiliging en bescherming van persoonsgegevens krijgt.
Over privacy gesproken. Daniël Dragičević heeft in juni het Nationaal Privacy Debat bijgewoond. In deze Update doet hij kort verslag daarvan.

Ten slotte kan ik met trots melden dat ITSX versterking heeft gekregen van ir. Arthur Donkers (CISSP, CISA, CISM, ISO27K LA). Samen met Ralph Moonen zal hij de activiteiten van ITSX verder uitbreiden. Informatiebeveiliging beperkt zich namelijk bepaald niet tot de techniek. ITSX heeft met de toetreding van Arthur Donkers als partner meer slagkracht en capaciteit om diensten te leveren op het gebied van onder andere compliance (ISO 27001, NEN 7510, etc.) interim security management, beleid en procedures. Zie ook het uitgebreide interview met Arthur elders in deze Update.

Remco Huisman
Commercieel directeur

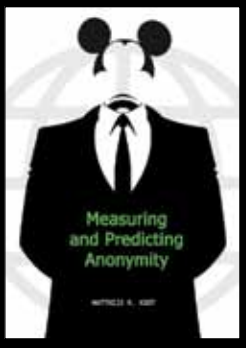
PS! In de vorige Update is al gemeld dat ik voor het goede doel (Bike to close the Gap) de Paterberg zou beklimmen. In drie uur tijd is me dat 23 keer gelukt. Dat de Paterberg een kuitenbijter van de eerste orde is, blijkt wel uit de foto bij deze column ;-)

Vakbeurs Infosecurity.nl 2012

Madison Gurkha en ITSX zijn ook dit jaar weer aanwezig op de vakbeurs Infosecurity.nl op 31 oktober en 1 november a.s. in de Jaarbeurs Utrecht. U bent van harte welkom op onze stand A107. Wij zullen u net als vorig jaar weer op een interactieve manier kennis laten maken met ons zeer complexe en snel veranderende vakgebied. Houd onze website in de gaten voor het actuele beursprogramma. Heeft u interesse om de beurs te bezoeken. Laat het ons a.u.b. weten dan sturen wij u een uitnodiging.

De Madison Gurkha Update voortaan (ook) **digitaal** ontvangen?!

In het kader van Maatschappelijk Verantwoord Ondernemen willen wij u als lezer de mogelijkheid bieden de Madison Gurkha Update voortaan (ook) digitaal te ontvangen. Als abonnee op de Madison Gurkha Update ontvangt u deze eerste digitale nieuwsbrief eenmalig binnenkort in uw mailbox met daarin een opt-in/opt-out mogelijkheid. Wij vragen u vriendelijk uw keuze door te geven, zodat wij u in de toekomst op de hoogte kunnen houden op de door u gewenste manier.



Matthijs R. Koot, Security Consultant bij Madison Gurkha, heeft op 27 juni 2012 zijn proefschrift verdedigd "Measuring and Predicting Anonymity" aan de Universiteit van A'dam. Matthijs heeft naar aanleiding van zijn proefschrift een artikel geschreven dat is opgenomen in het vaktijdschrift *Privacy & Compliance*. Op onze website vindt u de link naar het artikel "Kwantificatie van Herleidbaarheid".

Een goed begin nog veel werk te doen

Eerder dit jaar heeft KING in opdracht van BZK en VNG een impactanalyse uitgevoerd. Madison Gurkha heeft samen met VKA een bijdrage geleverd aan het onderzoek (zie Update 15 waarin we hier uitgebreid over berichten).
De eindrapportage hiervan is nu beschikbaar. Ga hiervoor naar de sectie 'Informatiebeveiliging' op de website van KING (www.kinggemeenten.nl). De rapportage geeft een beeld van de impact op gemeenten en doet bovendien een voorstel voor een mogelijk ondersteuningsaanbod vanuit KING aan gemeenten voor het assessment.

Hoe normering privacy beschermt

Een uitgebreide column door Walter Belgers in vaktijdschrift *Privacy & Compliance*. Om de digitale informatieverwerking in goede én veilige banen te leiden zijn (inter)nationale afspraken (normen) nodig. Een voorbeeld daarvan is de NEN 7510 voor in de zorg. En nu dan ook de normen en richtlijnen voor organisaties die een koppeling hebben met DigiD. Volgens Walter is het de 'por' in de goede richting. Op onze website vindt u de link naar het complete artikel.

Ministerie van ICT, een goed idee?

Volgens Hans Van de Looy (Madison Gurkha) wel

In een gesprek met ISP Today liet Hans weten wat zijn kijk is het op het plan van D66 om alle ICT-onderwerpen zoals privacy, cybercrime, internetvrijheid en telecom in een nieuw kabinet onder te brengen bij één ministerie. Wilt u meer lezen over dit plan en/of benieuwd naar de mening van experts uit de ISP-sector ga naar: http://www.isptoday.nl/nieuws/ministerie-van-ict-een-goed-idee (Gepubliceerd door ISP Today op donderdag 19 juli 2012)

In de rubriek 'Het Inzicht' stellen wij bepaalde (technische) beveiligingsproblemen aan de orde. Deze keer geeft Matthijs Koot meer inzicht in de ontwikkelingen op het gebied van nationale en Europese wet- en regelgeving.

Cookie wet

meldplicht en boete op privacyovertreding

Op 5 juni 2012 zijn de 'cookiewet' en 'meldplicht datalekken' van de nieuwe Nederlandse telecomwet in werking getreden. Hierbij een overzicht. De nieuwe wet regelt ook netneutraliteit, maar die treedt pas op een later moment in werking; dat onderdeel zal te zijner tijd ook in MG-Update worden besproken. Wel neem ik in dit artikel de in januari voorgestelde Europese Privacy Verordering in het kort mee.

Cookies

Naar het nieuw ingevoegde wetsartikel 11.7a wordt ook wel verwezen als 'cookiewet'. Nederland heeft, strenger dan de Europese ePrivacy-richtlijn voorschrijft, gekozen voor een opt-in model voor cookies. Dit opt-in model verplicht websites tot het vragen van toestemming aan de gebruiker via een 'vrije, specifieke en op informatie berustende wilsuiting', conform de privacywet. Dat impliceert twee eisen:

1. informatie: de gebruiker dient te worden geïnformeerd over wie het cookie plaatst, dat het cookie wordt geplaatst en waarom het cookie wordt geplaatst[1] ('cookieverklaring')
2. toestemming: de gebruiker moet (vervolgens) om toestemming worden gevraagd.

Pas na toestemming mag het cookie worden geplaatst. Eén categorie cookies is hiervan uitgezonderd: geen toestemming is nodig voor cookies die uitsluitend tot doel hebben elektronische communicatie tot stand te brengen, of strikt noodzakelijk zijn voor het ten uitvoer brengen van de door de gebruiker gevraagde dienst. Voorbeelden van zulke uitzonderingen zijn sessiecookies, cookies voor het bijhouden van een online winkelwagentje of een taalkeuze, en cookies om ingelogd te blijven na beëindiging van browsesessie. De noodzaak wordt overigens beoordeeld vanuit de bezoeker, niet vanuit de aanbieder[2]. Voor alle andere cookies, waaronder (dus) ook het cookie van Google Analytics, is in principe toestemming vereist. Ook als de trackingfunctie van Google Analytics is uitgeschakeld[3].

Hoe werkt het vragen van toestemming in de praktijk? Zoals Arnoud Engelfriet van ICTRecht observeerde[4] heeft het Fok.nl forum gekozen voor een tussenpagina die de gebruiker om toestemming vraagt. Financial Times heeft gekozen voor een semi-transparant ja/nee keuzeschermpje dat als sluier over de website is gedrapeerd. Telegraaf.nl heeft gekozen voor een horizontaal balkje onderaan

De OPTA heeft zelf al aangegeven alleen *schrijnende gevallen* te willen aanpakken

Hoe groot moet het algemeen belang zijn om gevreesde reputatieschade-door-openbaarmaking te rechtvaardigen?

de pagina waaruit blijkt dat zij, in principe in strijd met de huidige wet, een model van impliciete toestemming (blijven) hanteren. NRC.nl heeft zich op moment van dit schrijven nog beperkt tot het verstrekken van informatie over het gebruik van cookies; er wordt niet om toestemming gevraagd, maar ook geen opt-out aangeboden. De wet en de praktijk lopen momenteel nog behoorlijk uiteen. Wat betreft handhaving valt het risico voor uw organisatie wellicht mee: OPTA is weliswaar sinds 5 juni 2012 bevoegd om de cookiewet te handhaven en kán een boete opleggen van EUR 450.000 per overtreding, maar heeft zelf al aangegeven alleen 'schrijnende gevallen' te willen aanpakken.

Meldplicht

De nieuwe wet bevat tevens een nieuw hoofdstuk 11a getiteld 'Continuïteit'. Die regelt een zorg- en meldplicht voor aanbieders van openbare elektronische telecommunicatienetwerken en/of -diensten. Bij 'inbreuk op de veiligheid' en 'verlies van integriteit' zijn aanbieders nu verplicht daarvan melding te maken aan de overheid. De wet stelt tevens dat indien openbaarmaking in het algemeen belang is, de overheid de melding openbaar kan maken c.q. de aanbieder tot openbaarmaking kan verplichten. Op 6 juli jl. maakte de NCTb bovendien bekend[5] dat er nog dit jaar een veel bredere wettelijke meldplicht komt, namelijk voor organisaties in zes vitale sectoren: elektriciteit, gas, drinkwater, telecom, transport (waarbij Schiphol en mainports Rotterdam expliciet worden genoemd), en keren en beheren oppervlaktewater. De reden voor die meldplicht is dat de impact van een verstoring in die sector groot kan zijn en dat er bij uitval in deze sectoren 'al zeer snel' sprake is van een cascade-effect naar andere sectoren, waardoor 'grootschalige maatschappelijke ontwrichting een reëel risico vormt'. Het zal me benieuwen hoe uitwisseling van incidentinformatie in praktijk gaat uitwerken, ook met de wettelijke mogelijkheid om openbaarmaking af te dwingen in gedachten. Hoe groot moet het algemeen belang zijn om gevreesde reputatieschade-door-openbaarmaking te rechtvaardigen? Hoe wordt 'algemeen belang' eigenlijk gekwalificeerd en/of gekwantificeerd? Ook bestaat in Amerika het fenomeen 'overdisclosure': uit angst om niet te voldoen aan de meldplicht die daar geldt melden organisaties allerlei zaken waarvan de ernst, welbeschouwd, onvoldoende is om melding te rechtvaardigen. Kan Nederland op dit punt lering trekken uit de Amerikaanse praktijk?

Boete

Op Europees niveau wordt ondertussen verder gesleuteld aan privacyregels. De in januari voorgestelde Europese Privacy Verordening beschrijft een verplichting om datalekken binnen 24 uur te melden en een m.i. ietwat wereldvreemde verplichting tot het aanstellen van een functionaris gegevensbescherming voor bedrijven vanaf 250 medewerkers. Eén van de onderdelen die zich daar op extra veel belangstelling mag verheugen is de potentieel gigantische maximumboete die op het overtreden van privacyregels komt te staan: tot 2 procent van de wereldwijde jaaromzet van de organisatie die de regels overtreedt. Als die boete inderdaad wordt ingevoerd zal het onderwerp compliancy nog nadrukkelijk aanwezig zijn op de agenda's van het management. De vrees bij strengere privacyregels is dat ze de markt ondermijnen. Persoonlijk zie ik juist kansen voor Privacy by Design, en bestendiging van (consumenten)vertrouwen die verdere ontwikkeling en groei mogelijk maakt.

Afsluitend

De beschreven ontwikkelingen op nationale en Europese wet- en regelgeving tonen dat de wetgever (consumenten)privacy en veiligheid serieus neemt. Er zijn ontwikkelingen die (burger)privacy mogelijk onder druk zetten, zoals de vernieuwing van Wet op de inlichtingen- en veiligheidsdiensten en eventuele voortvloeisels uit het Europese INDECT-project. Die materie bewaren we voor een volgende Update.

Aanbevolen links

1. Cookiewet
   http://maxius.nl/telecommunicatiewet/artikel11.7a

2. Meldplicht datalekken
   http://maxius.nl/telecommunicatiewet/artikel11a.2

Cookierecht.nl
http://www.cookierecht.nl/

DDMA handleiding Cookiewet 'Wet en werkelijkheid' (mei 2012) http://www.ddma.nl

De meldplicht voor datalekken in de Telecommunicatiewet,
F.J. Borgesius, Computerrecht, 2011/4
(vindbaar via uw zoekmachine)

1 http://www.wieringa-advocaten.nl/nl/we-blog/2012/06/06/cookie-aanbieden-eerst-netjes-vragen
2 idem
3 http://www.solv.nl/weblog/nog-meer-misverstanden-over-de-nieuwe-cookiewet/18902
4 http://blog.iusmentis.com/2012/06/06/werkelijk-niemand-heeft-trek-in-de-cookiewet/
5 http://www.nctb.nl

In de rubriek "Het Verslag" laten wij u delen in onze ervaringen, seminars en trainingen. Deze keer doet Daniël Dragičević verslag van het Nationaal Privacy Debat. Fotografie door: Sebastiaan ter Burg

4x privacy

Onder het motto 'Bekijk privacy eens van alle kanten' hield Webwereld op maandag 11 juni jl. het eerste Nationaal Privacy Debat. Bedrijfsleven, overheid, politiek en opsporingsdiensten waren het over één ding eens: privacy, de omgang met en beveiliging van persoonsgegevens, moet beter worden geregeld.

In het World Forum in Den Haag waren er paneldiscussies met onder meer Tweede Kamerleden Arjan El Fassed (GroenLinks), André Elissen (PVV) en Kees Verhoeven (D66) en werden er verschillende keynotes gegeven met aansluitend vragen uit het publiek. Vanzelfsprekend waren betrokken organisaties als het College Bescherming Persoonsgegevens, Bits of Freedom en Privacy First ook aanwezig. De overige gasten waren journalisten, academici, advocaten en professionals uit de ict-wereld.

Hans Van de Looy en Daniël Dragičević van Madison Gurkha waren als toehoorders bij het Nationaal Privacy Debat aanwezig. Hieronder doet Daniël inhoudelijk verslag van de verschillende keynotes en paneldiscussies.
Op de website van het Nationaal Privacy Debat (www.nationaalprivacydebat.nl) vindt u de link naar de open webcast om het debat van 11 juni terug te kijken.

Brenno de WInter

Privacy en Opsporing

Keynote: Pim Takkenberg (Korps Landelijke Politie Diensten)

Dhr. Takkenberg gaat in zijn presentatie in op de werkzaamheden van de politie en maakt duidelijk dat de politie haar werk niet kan uitvoeren zonder de privacy van burgers te schenden. Hierbij werd aangegeven dat dit wel binnen de juiste juridische kaders hoort te gebeuren.
Een medewerker van XS4ALL geeft aan dat de databewaarplicht is ingevoerd, maar dat na alle investeringen erg weinig bevraagd wordt. Dhr. Takkenberg geeft aan dat er nog een leercurve bij de politie is bij het opvragen en inwinnen van deze gegevens. Ook geeft dhr. Takkenberg aan dat het de politie niet gaat om het inwinnen van zoveel mogelijk gegevens. Liever heeft ze zo specifiek mogelijke gegevens aangaande de zaak die op dat moment speelt.

Paneldiscussie

Bits of Freedom hekelt tijdens de paneldiscussie het gebrek aan openheid door politiekorpsen en verantwoordelijke ministers over statistieken van gegevensopvragingen bij providers en social media. Dhr. Takkenberg geeft aan dat deze openheid toekomstige onderzoeken kan schaden en dat dit niet in het belang is van de opsporingsinstanties. Uit de zaal komt de vraag wat BoF met de tapgegevens wil bereiken. BoF wil deze cijfers relateren aan het aantal opgeloste zaken en daarmee de ineffectiviteit van het opsporingsmiddel aantonen. Dit lijkt moeilijker dan in eerste instantie gedacht, omdat het aantal opgeloste zaken niet altijd relatief is aan het aantal telefoontaps.

Privacy en Bedrijven

Keynote: Anthony House (Google)

De eerste keynote werd verzorgt door dhr. Antony House van Google. Besluiten van een groot bedrijf als Google hebben zijn weerslag op grote groepen gebruikers. Google is zich daar ook van bewust. Het multidisciplinaire team dat zich bij Google met privacy bezighoud, probeert verder te gaan dan wat privacywetgeving van hun eist. Dit heeft geresulteerd in features als `Google Dashboard', `SSL by default' en `Google Account Activity statements'. Het idee om gebruikers meer inzicht in de gegevens te geven waar Google over beschikt wekt vertrouwen en geeft de gebruiker een bepaalde controle over zijn/haar gegevens.

Paneldiscussie

Tijdens het vragenrondje schokte dhr. Kanters van de NS met de opmerking dat privacywetgeving zo complex is dat bedrijven moeite hebben met de naleving ervan bij het invoeren of wijzigen van bedrijfsprocessen. De paneldiscussie ging over het volgende vraagstuk: moeten bedrijven meer aan zelfregulering doen, of dient er meer regelgeving te komen ten aanzien van privacybescherming? Tijdens de discussie wordt een vergelijking gemaakt tussen digitale dienstverlening en drugs, waarbij gebruikers de gevaren van het gebruik niet kunnen inzien. Hierbij wordt aangegrepen dat privacy een fundamenteel recht is waarop niet mag worden ingeleverd. Concreet dient een bedrijf transparant te zijn door het publiceren van de gehanteerde privacy policy waarin in duidelijke taal hoort te staan wat er precies met de verzamelde gegevens wordt gedaan.

Overheid en Privacy

Keynote: Bart de Koning

Schrijver Bart de Koning haalt in zijn presentatie een aantal projecten van de overheid aan waarbij privacybezwaren niet of nauwelijks zijn meegenomen. Denk hierbij aan de vingerafdrukken in het paspoort, de kilometerregistratie en de databewaarplicht. Ook stelt dhr. De Koning dat incompetentie een groter risico is dan bewust beleid.

Paneldiscussie

Tijdens de derde paneldiscussie horen we dat de overheid stelselmatig 'Recht op eerbiediging van privé-, familie- en gezinsleven Art. 8' overschrijdt. De afweging voor het inbreuk maken op de persoonlijke levenssfeer door de overheid is in iedere situatie anders. Dit is een reden dat er geen beleid op kan worden geschreven.

Privacy en Beveiliging

Keynote: Joost Farwerck (KPN)

Tijdens de presentatie van dhr. Farwerck werd ingegaan op de hack bij KPN. In navolging op dit incident heeft KPN een privacymissie en cyber security office opgesteld. Hiermee worden zowel interne controles, reacties op incidenten en communicatie naar klanten, overheden en andere instanties verbeterd. Het publiek geeft meermaals aan dat er nog te weinig gecommuniceerd wordt naar klanten, wanneer een incident zich heeft voorgedaan. Hierbij lopen klanten risico omdat ze niet weten welke gegevens op straat liggen en zich niet kunnen voorbereiden op eventueel misbruik ervan.

Paneldiscussie

Gesteld werd dat bij het opstellen van regelgeving controle-instanties meer slagkracht moeten krijgen voor handhaving. Verbaasd was men dat dataminimalisatie geen onderdeel uitmaakt van de discussie, wat er niet is hoeft ook niet te worden beveiligd. Dhr. Kanters (NS) geeft aan dat de OV-chipkaart hieraan voldoet. Er worden geen gegevens bewaard die de privacy kan schaden. In een verhitte discussie werd aangegeven dat de klant bepaalt wanneer zijn privacy geschonden wordt, niet de leverancier.

Madison Gurkha interview voor iedere editie een gerenommeerd persoon in de ICT-beveiligingswereld. Deze editie een interview met Arthur Donkers die vanaf 1 juli 2012 officieel zijn intrede heeft gedaan bij ITSX.

Wij willen een **partner** zijn

juli 2012 - heden
mede-eigenaar en directeur ITSX

1991 - heden
Zelfstandig / onafhankelijke specialist, onder meer van Le Reseau netwerksystemen

1988 - 1991
BSO / AT (Technische automatisering)

1986 - 1988
ICT Novotech
(detachering o.a. in Eindhoven)

ITSX
Annie M.G. Schmidtweg 12
1321 JE Almere
www.itsx.com
info@itsx.com
gsm +31 (0)6 533 151 02

Wie ben je?
Ik ben Arthur Donkers, woon boven Groningen (wel plannen om naar 'de stad' terug te verhuizen), ben getrouwd, heb twee kinderen en een meer dan warme belangstelling voor informatiebeveiliging.

Je naam klinkt bekend.... vertel...
Ik ben al sinds 1996 bezig met informatiebeveiliging, en ben vanuit de technische hoek doorgegroeid naar ook de niet-technische aspecten van het vak. 'Vroeger' was het uitvoeren van een portscan al een bijzonder iets (in de tijd voordat er Nmap was) en vond je soms hele interessante zaken zoals Telnet-toegang zonder wachtwoord. Tegenwoordig is het andersom; als je internetsysteem nu niet permanent wordt gescand vanaf het internet is waarschijnlijk je verbinding kapot. Deze ontwikkeling heb ik deels via Le Reseau netwerksystemen meegemaakt, een bedrijf dat ik zelf heb opgericht. Tegenwoordig verricht ik mijn werkzaamheden via 1Secure BV en vanaf 1 juli 2012 direct vanuit ITSX.

Waarom ITSX?
Als zelfstandig consultant deed ik al veel langer projecten via ITSX. Ik ken Ralph Moonen, eigenaar van ITSX, al een hele tijd en de samenwerking verliep en verloopt altijd heel prettig. Zowel Ralph als ik wilden al langer een echte security practice opzetten zodat we meer kunnen bieden dan alleen het 'uurtje factuurtje' werk. Daarnaast zijn ITSX en 1Secure op allerlei gebieden goed met elkaar vergelijkbaar, waardoor je weinig cultuurschokken hoeft te verwachten. Voor mij een logische keuze dus. In de loop van een aantal gesprekken is het plan zo ontstaan en vanaf 1 juli 2012 is dat nu officieel van kracht.

Wat bedoel je met: meer dan alleen het 'uurtje factuurtje' werk?
ITSX wil meer zijn dan een bemiddelingsbureau dat tegen een uurtarief specialisten inzet. Wij willen een partner zijn waarop onze klanten kunnen bouwen en terecht kunnen voor advies bij alle aspecten van informatiebeveiliging, van diep technische vraagstukken tot het vervullen van de rol van strategische partner bij het bepalen van het juiste informatiebeveiligingsbeleid. Samen vinden we zo de juiste oplossing voor de vraagstukken die er spelen bij de klant. ITSX, en daarmee haar klanten, heeft een groot netwerk aan kennis en ervaring achter zich staan. Hierdoor is ITSX meer dan een leverancier van uren.

Waarmee onderscheidt ITSX zich van de concurrentie?
ITSX positioneert zich als een partner op informatiebeveiligingsgebied. Naast de klassieke interimdiensten en de grote implementatietrajecten biedt ITSX ook gestandaardiseerde diensten aan zoals ISO 27001 GAP analyses en de DigiD Audit Readiness Scan (DARS). Deze diensten zijn gebaseerd op een pragmatische en doelgerichte aanpak van een specifiek vraagstuk. Op basis van

Eerder dit jaar hebben wij voor UNI Strategic een Mobile Hacking en Security Lab verzorgd in Kuala Lumpur. Deze succesvolle workshop is in april jl. herhaald in Abu Dhabi en zal op 17 en 18 september a.s. ook hier in Nederland worden gehouden. (Voor meer informatie en om je in te schrijven ga je naar: www.itsx.nl/workshops/.

een aantal reeds uitgevoerde projecten zijn deze diensten gegroeid naar een bewezen en effectieve manier om snel de juiste informatie boven tafel te krijgen.

Hiermee onderscheidt ITSX zich van andere spelers in de markt: de kennis en ervaring van ITSX wordt omgezet in diensten die bijna als een standaard product kunnen worden ingezet. Het wiel hoeft niet iedere keer opnieuw te worden uitgevonden, met als nuttig effect dat er weinig tot geen overhead in deze diensten zit en de beschikbare tijd zo efficiënt mogelijk kan worden ingezet.

Nieuwe slogan?

Deze partnership benadering vind je inderdaad ook terug in onze nieuwe slogan 'Understanding the Tools, the Players and the Rules'. Dit is precies die kennis en ervaring die ITSX meeneemt naar haar klanten om daarmee een passende oplossing te vinden voor de beveiligingsvragen die er spelen. Vergelijk het met onderhoud aan je huis of auto. Een aantal zaken kun je zelf doen, maar soms is het sneller, beter en goedkoper om een specialist in te huren. Zo werkt het ook bij ITSX. Natuurlijk kunnen klanten zelf al hun beveiligingsvragen beantwoorden, maar je weet nooit zeker of je wel voor de juiste oplossing hebt gekozen en of je niet te veel tijd en geld hebt uitgegeven om tot die oplossing te komen. Door ITSX in te schakelen maak je direct gebruik van de kennis en ervaring in het ITSX netwerk zonder dat je daar zelf in hoeft te investeren.

Daar waar Madison Gurkha zich met veel succes heeft gespecialiseerd in technische IT-beveiligingsonderzoeken en -testen, richt dochterbedrijf ITSX zich meer op de zachte kant van informatiebeveiliging: beleid, procedures, compliancy en interim-management.

Hierin vullen Madison Gurkha en ITSX elkaar goed aan en kunnen we onze klanten helpen in alle verschillende facetten van de beveiligingscyclus. Madison Gurkha en ITSX werken veelvuldig samen in grote multidisciplinaire onderzoeken.

In elke Madison Gurkha Update laten wij een klant aan het woord.
Deze keer geven we graag het woord aan Ed de Myttenaere, Manager ICT-automatisering bij Ymere.

Ymere werkt al enige jaren samen met Madison Gurkha en ITSX aan het structureel identificeren, verminderen en voorkomen van technische IT-beveiligingsrisico's. Hiertoe zijn er door Madison Gurkha verschillende onderzoeken uitgevoerd op onder andere de externe IP-ranges, de website en het interne netwerk. ITSX heeft bovendien een ISO 27001 GAP- en risicoanalyse voor Ymere uitgevoerd.

7 vragen aan ... Ed de Myttenaere

1 ***In welke branche is uw organisatie actief?***
Ymere werkt als maatschappelijk ondernemer aan wijken met perspectief waar bewoners willen wonen, leven en groeien. Ymere is actief in de metropoolregio Amsterdam, met als kerngemeenten Almere, Amsterdam, Haarlem en Haarlemmermeer, Leiden en Alkmaar. Ymere bezit rond de 85.000 verhuureenheden, waarvan ongeveer 76.000 woningen.

2 ***Hoeveel mensen houden zich in uw organisatie bezig met informatiebeveiliging?***
Informatiebeveiliging is ingebed in de gehele organisatie. Dit houdt in dat alle medewerkers, bewust of onbewust bezig zijn met informatiebeveiliging. Daarnaast zijn er diverse medewerkers die binnen hun standaard verantwoordelijkheid, inhoudelijk betrokken zijn bij (onderdelen van) informatiebeveiliging. Er is echter geen verantwoordelijke binnen de organisatie die hier full-time mee bezig is, in de rol van bijvoorbeeld een security officer.

3 ***Wat is uw functie?***
Mijn functie is Manager ICT-automatisering. Het is mijn verantwoordelijkheid te zorgen voor een goede IT-dienstverlening. Met andere woorden: ICT zo naadloos mogelijk laten aansluiten op de werkprocessen binnen de organisatie, binnen de gegeven randvoorwaarden, noodzaak en budget.

4 ***Hoe is informatiebeveiliging opgezet in uw organisatie?***
Informatiebeveiliging is het samenspel tussen de business requirements en de kaders en richtlijnen gesteld door onze afdelingen informatisering en ICT-automatisering waarbij ook de risico's in kaart zijn gebracht.
We zijn momenteel bezig om data te classificeren zodat we op basis van een volledige dataclassificatie inzicht hebben of we als organisatie wel of geen beveiligingsmaatregelen moeten nemen om data te beschermen.

5 ***Wat zijn in uw organisatie op dit moment de belangrijkste uitdagingen op het gebied van informatiebeveiliging?***
De belangrijkste uitdaging blijft altijd om de juiste balans te vinden tussen een goed informatiebeveiligde (ICT-)omgeving met een zo hoog mogelijke gebruiksvriendelijkheid, waarbij we ook rekening moeten houden met de huidige trends en ontwikkelen zoals "BYOD" en "Cloud". Daarnaast is het belangrijk dat iedereen – van hoog tot laag in de organisatie – het belang van informatiebeveiliging blijft inzien. Dat is iets waar we continu aan blijven werken.

6 ***Welke maatregelen worden genomen om de beveiligingsrisico's onder controle te houden?***
Naast beleids- en kaderstelling worden de ICT-infrastructuren en (web)applicaties jaarlijks onderworpen aan een IT-beveiligingsonderzoek. Dit gebeurt op diverse manieren. De website en de portals laten wij onderzoeken middels een grey box aanpak. Zo kunnen wij ook laten controleren of er autorisatieproblemen binnen onze applicaties te vinden zijn. Ymere wil uiteraard absoluut vermijden dat data van bijvoorbeeld onze ene cliënt kan worden ingezien door een andere cliënt. De belangrijke delen van onze IT-infrastructuur laten wij diepgaand volgens de crystal box methodiek onderzoeken. Tijdens zo'n onderzoek wordt een hack-achtige aanpak gecombineerd met een diepgaande inspectie van de systemen en de inrichting van ons netwerk. Op deze manier kunnen wij een robuustere beveiliging realiseren die voldoet aan belangrijke beveiligingsprincipes, zoals een gelaagdheid van verdediging, compartimentering en minimale privileges. Wij zijn dan wel niet De Nederlandsche Bank o.i.d., maar wij willen binnen Ymere informatiebeveiliging wel op orde hebben. Dat zijn wij verplicht naar onze stakeholders toe, maar ook naar onze medewerkers en partners. Daarnaast gaat het bij projecten waar wij als Ymere bij betrokken zijn om zeer aanzienlijke investeringen. Informatie daarover moet ook goed worden beschermd.

7 ***Wat zijn uw ervaringen met Madison Gurkha en ITSX?***
Ik ben zeer te spreken over Madison Gurkha en ITSX. In korte tijd wordt veel werk verzet. Het is prettig met hen samenwerken en de geleverde werkzaamheden zijn van een prima niveau.

Als u op de hoogte wilt blijven van de laatste ontwikkelingen in de IT-beveiligingswereld dan zijn beurzen en conferenties de ideale gelegenheid om uw kennis te verrijken en om contacten op te doen. In de Madison Gurkha Update presenteren wij een lijst met interessante bijeenkomsten die de komende tijd zullen plaatsvinden.

20 en 21 oktober 2012

EuroBSDcon 2012

Warschau Polen

http://2012.eurobsdcon.org

EuroBSDcon is de technische conferentie in Europa, bedoeld voor gebruikers en ontwikkelaars van op BSD-gebaseerde systemen. EuroBSDcon is een unieke gelegenheid om meer te leren over de krachtige BSD-systemen die we dagelijks gebruiken en om in contact te komen en ervaringen uit te wisselen met andere ontwikkelaars uit de hele wereld. Als organisatie steunt Madison Gurkha de doelstellingen van EuroBSDcon. Wij vinden het belangrijk om kennis te delen en bij te dragen aan open source projecten. Madison Gurkha sponsort dit project dan ook van harte.

31 okt en 1 nov 2012

Infosecurity.nl / Storage Expo / Tooling Event

Jaarbeurs Utrecht

http://www.infosecurity.nl/nl-NL/Bezoeker.aspx

Tegenwoordig worden bedrijven bijna dagelijks geconfronteerd met allerlei vraagstukken op het gebied van IT-beveiliging. Vraagstukken waar de vakbeurs Infosecurity.nl op inhaakt en een absolute must voor elke ICT-professional. Samen met de vakbeurzen Storage Expo en Tooling Event bieden marktleiders, verenigingen, sprekers en andere ICT-professionals u hun ideeën, technieken, diensten en visie aan op de meest actuele IT-beveiligingsthema's. Zoals u elders in deze Update kunt lezen is ook dit jaar Madison Gurkha samen met ons dochterbedrijf ITSX aanwezig op de vakbeurs Infosecurity.nl U bent van harte welkom op onze stand A107 (wanneer u na de entree direct linksaf gaat, dan vindt u onze stand al snel aan uw linkerhand).

Madison Gurkha
Your Security is Our Business

VACATURES

Madison Gurkha is een jonge, groeiende en veelbelovende organisatie op het gebied van (technische) IT-beveiliging. Madison Gurkha voert jaarlijks meer dan driehonderd projecten uit voor zeer diverse organisaties. Hoewel deze organisaties zeer verschillend zijn, delen zij met elkaar dat zij veel belang hechten aan IT-beveiliging en alleen met topspecialisten genoegen nemen. Madison Gurkha doet onder andere zaken met beursgenoteerde bedrijven, banken, (zorg)verzekeraars, ministeries en gemeentes.

Door onze aanhoudende groei zijn wij op zoek naar:

- **Teamleider / werkvoorbereider**
- **Security Consultant (SC)**
- **Senior Security Consultant (SSC)**
- **Junior Account Manager**

Voor de consultants geldt dat kandidaten met aantoonbare beveiligingskennis van Microsoft-producten en -technologieën, en zij die source code reviews kunnen uitvoeren op dit moment onze voorkeur hebben.

Meer informatie over bovenstaande vacatures kun je vinden op onze website www.madison-gurkha.com.

Voldoe jij aan het profiel en ben je echt goed, stuur dan je CV met sollicitatiebrief naar hrm@madison-gurkha.com.

HET COLOFON

Redactie
Daniël Dragičević
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.



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