29 NOVEMBER 2016
THE HAGUE SECURITY DELTA CAMPUS

review

CYBER SECURITY EVENT 2016

Beveilig uw organisatie tegen cybercrime en datalekken en voorkom imago en reputatieschade voor uw organisatie!

WWW.SBO.NL/CYBERSECURITY

Studiecentrum voor Bedrijf en Overheid

Review 29 november 2016

Beste lezer,

Op 29 november 2016 vond op The Hague Security Delta Campus in Den Haag, de internationale stad van vrede, recht en veiligheid, het Cyber Security Event plaats waar ervaringsdeskundigen en experts werkzaam bij de overheid, wetenschap en het bedrijfsleven samenkwamen om kennis en ervaringen uit te wisselen over cyber security en de aanpak van cybercrime en datalekken om zo van elkaar te leren.

Een belangrijke les van het event was dat overheid, bedrijfsleven en wetenschap elkaar nodig hebben om tot innovatieve oplossingen te komen voor een veiligere (virtuele) wereld. The Hague Security Delta Campus, het grootste veiligheidscluster van Europa, speelt hierbij een belangrijke rol door overheden, innovatieve bedrijven en toonaangevende kennisinstellingen samen te brengen om producten, diensten en kennis te ontwikkelen voor de aanpak van cybercrime en datalekken.

Met het Cyber Security Event boden we een podium aan overheden, bedrijven en kennisinstellingen om deze kennis, producten en diensten met elkaar te delen. In deze review op het event worden de opgedane kennis en ervaringen voor u nog eens op een rij gezet, zodat u deze kunt toepassen in uw dagelijkse praktijk.

Veel leesplezier!

Met vriendelijke groet,

Frank van Summeren, congres- en opleidingsmanager veiligheid bij het Studiecentrum voor Bedrijf en Overheid en organisator van het Cyber Security Event

Xander Beenhakkers, programmamanager bij The Hague Security Delta Campus en dagvoorzitter van het Cyber Security Event

Bas de Kroon, partnershipmanager bij het Studiecentrum voor Bedrijf en Overheid

Cyber Security Challenge

Het Cyber Security Event werd geopend door **Joris den Bruinen**, plaatsvervangend directeur van The Hague Security Delta, het grootste veiligheidscluster van Europa, waar bedrijven, overheden en kennisinstellingen samenwerken om producten, diensten en kennis te ontwikkelen voor een veilige wereld. Na de opening van het event gingen de deelnemers bij de Cyber Security Challenge in teams onder begeleiding van experts aan de slag met een complex vraagstuk op het terrein van cyber security.

Het betrof een fictieve maar waarheidsgetrouwe casus waarbij een stroomstoring, veroorzaakt door een gerichte cyberaanval, ervoor zorgt dat ongeveer 200.000 huishoudens en bedrijven zonder stroom zitten. Daarnaast heeft de stroomstoring gevolgen voor allerlei openbare voorzieningen. Zo is het openbaar vervoer ernstig ontregelend, zijn ziekenhuizen noodgedwongen op noodstroom overgegaan en staat het verkeer op verschillende plaatsen vast omdat de verkeerslichten zijn uitgevallen. De deelnemers aan de Cyber Security Challenge maakten onderdeel uit van het Quick Emergence Response Team. Het was de taak van de teams om dit incident snel en grondig te onderzoeken en te verhelpen. Dit deden de teams door de aard en omvang van het incident te achterhalen en een pakket van maatregelen op te stellen om de stroomstoring ongedaan te maken en mogelijke gevolgen zoals economische en ecologische schade en maatschappelijke ontwrichting (waar mogelijk) te beperken.

Een belangrijke les uit de Cyber Security Challenge is dat overheid en bedrijfsleven elkaar nodig hebben om dergelijke incidenten waar mogelijk te voorkomen en waar nodig te bestrijden. Voor een effectieve samenwerking is het van belang dat zij bekend zijn met elkaars belangen, rollen, taken en (on)mogelijkheden. Daarnaast werd tijdens de Cyber Security Challenge duidelijk dat vroegtijdige detectie van cruciaal belang is om de schade te beperken en dat het opstellen van mogelijke scenario's kan helpen bij het inzichtelijk krijgen van de mogelijke gevolgen van het incident.

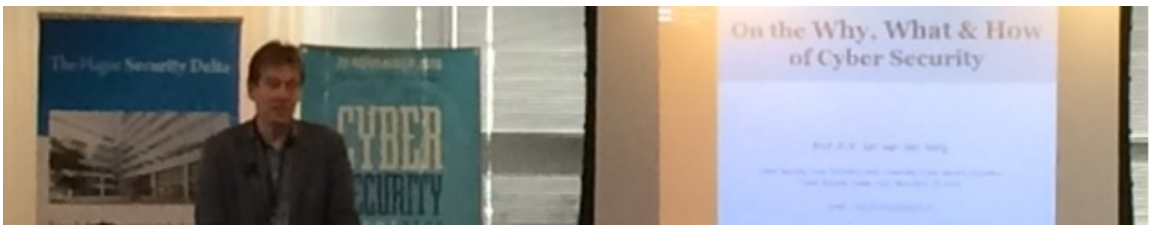
Na de Cyber Security Challenge werd het Cyber Security Event voortgezet onder leiding van Xander Beenhakkers, programmamanager bij The Hague Security Delta Campus en dagvoorzitter van het event.

Cyber Security

De eerste plenaire lezing van het Cyber Security Event werd verzorgd door **Jan van de Berg**, hoogleraar Cyber Security bij de Technische Universiteit Delft en bij de Universiteit Leiden, wetenschappelijk Directeur van de Stichting Cyber Security Academy en Opleidingsdirecteur van de masteropleiding Cyber Security.

Jan van de Berg ging tijdens zijn presentatie in op het hoe en waarom van cyber security dreigingen. Enkele dreigingen die naar voren kwamen waren cyber activisme (bijvoorbeeld wikileaks), DDOS attacks, hacks, cybercrime en spionage. Slachtoffers van deze dreigingen zijn burgers, bedrijven, vitale infrastructuur en overheden. Jan van de Berg pleitte tijdens zijn presentatie voor een gebalanceerde aanpak van deze bedreigingen, waarbij aandacht is voor preventieve en repressieve maatregelen op technisch, sociaal en organisatorisch terrein.

Om slachtofferschap van cyberdreigingen te voorkomen is het volgens Jan van de Berg van belang om vitale bedrijfsprocessen in kaart te brengen, potentiele dreigingen en kwetsbaarheden te identificeren, acceptabele risiconiveaus te definiëren, afspraken te maken over taken, rollen en verantwoordelijkheden met betrekking tot de aanpak van de gedefinieerde risico's, de voorgenomen maatregelen te implementeren en te monitoren op hun effectiviteit.



Privacy & Cyber Security

Mireille Hildebrandt, hoogleraar Interfacing Law & Technology aan de Vrije Universiteit Brussel en hoogleraar ICT en Rechtstaat aan de Radboud Universiteit Nijmegen, stelde tijdens haar presentatie dat de ingrijpende veranderingen in de informatie- en communicatietechnologie kansen maar ook risico's opleveren voor de privacy van burgers.

Er zijn verschillende technologische innovaties om de informatie van burgers te beschermen en hun privacy te waarborgen, maar de meest eenvoudige en ook effectieve maatregel is dat overheden en bedrijven alleen die data van burgers opslaan en gebruiken die daadwerkelijk relevant is voor hun activiteiten. Ieder probleem dat niet wordt geschept, hoeft immers ook niet te worden opgelost aldus Mireille Hildebrandt. Dit betekent concreet dat overheden en bedrijven van veel data (Big Data) verzamelen een omslag moeten maken naar het verzamelen van relevante data (Smart Data) en van gedachteloos naar doelbewust bewaren van data.

Cybercrime

De volgende plenaire lezing werd verzorgd door **Peter Zinn**, cyber security Specialist en adviseur van het Team High Tech Crime bij de Nationale Politie.

Peter Zinn ging in zijn presentatie in op de belangrijkste vormen van cybercrime en wat de impact hiervan is op onze samenleving. Daarnaast liet Peter Zinn zien hoe overheden en bedrijven kunnen komen tot een cyber security strategie voor de aanpak van cybercrime. Hierbij benadrukte hij dat alles veranderd en niets nieuw is. Dit betekent dat overheden en bedrijven zich moeten blijven ontwikkelen om cybercrime nu en in de toekomst het hoofd te kunnen bieden. Door mee te gaan in de technologische ontwikkelingen en barrières op te werpen, kunnen zij cybercrime waar mogelijk voorkomen. Een belangrijke randvoorwaarde voor een succesvolle aanpak van cybercrime is volgens Peter Zinn om de cyber security zo simpel mogelijk te organiseren. Hoe complexer deze wordt, hoe onvoorspelbaarder veranderingen zijn en hoe moeilijker het is om in control te blijven.

Gaming helpt cybercrime te (h)erkennen en te voorkomen

Foppe Vogd, Ambassadeur van de awareness game informatieveiligheid namens CIO Platform Nederland, de beroepsvereniging van CIO's en IT eindverantwoordelijken van private en publieke organisaties in Nederland, verzorgde tijdens het Cyber Security Event een presentatie over hoe gaming kan helpen bij het (h)erkennen en voorkomen van cybercrime.

De game die is ontwikkeld door 40 organisaties die verbonden zijn aan CIO Platform Nederland dient om de awareness van medewerkers ten aanzien van informatieveiligheid te vergroten om zodoende te voorkomen dat organisaties slachtoffer worden van cybercrime. De deelnemers aan het Cyber Security Event hadden ook de mogelijkheid om deze game te spelen, om zelf te ervaren hoe het werkt.

Digitalisering van de overheid

Het Cyber Security Event werd afgesloten met een presentatie van **Bas Eenhoorn**, digicommissaris die door het kabinet is aangesteld om als overheidsbrede regisseur de regie te voeren op de (door)ontwikkeling van de generieke digitale infrastructuur.

Tijdens zijn presentatie ging Bas Eenhoorn in op de digitalisering van de overheid en wat dit betekent voor de burger. Een belangrijke uitdaging voor de overheid is om haar digitale dienstverlening te verbeteren en tegelijkertijd de veiligheid van de gegevens van haar burgers te waarborgen.

Inspiratiesessies

Op het Cyber Security Event konden de deelnemers kiezen uit verschillende inspirerende sessies over actuele cyber security vraagstukken die zij konden volgen. Hieronder worden een aantal sessies die aan bod kwamen op het Cyber Security Event eruit gelicht.

Vitale Infrastructuur, belangrijk doelwit van 'Nation-State' sponsort cyber aanvallen

Cyberaanvallen zijn niet meer alleen het domein van opportunistische criminelen, maar zijn een steeds belangrijker wapen voor overheden in haar streven om de nationale soevereiniteit te verdedigen en om haar macht / kracht te etaleren, aldus **Jaap Schekkerman**, directeur onderzoek bij het Cyber Research Center – Industrial Control Systems, een onafhankelijk internationaal onderzoekscentrum dat onderzoek verricht naar 'Nation-State' sponsort cyber aanvallen op industrial control systems / vitale infrastructuur. Voorbeelden hiervan zijn strategische cyber spionage campagnes, zoals Moonlight Maze (1998) en Titan Rain, tot aan destructieve acties, zoals cyber aanvallen op Iran (Stuxnet), Georgië, Oekraïne (BlackEnergy3) en vele andere landen.Internationale conflicten komen in een nieuwe fase in hun lange geschiedenis waarbij de nucleaire dreiging vervangen wordt door de cyber dreiging. In deze schimmige wereld worden doelen bevochten met bits en bytes in plaats van kogels, malware in plaats van milities en botnets in plaats van bommen. Deze geheime aanvallen vinden grotendeels ongezien plaats voor het publiek. In tegenstelling tot de oorlogen van weleer, produceren deze cyberoorlogen niet direct dramatische beelden van exploderende bommen, verwoeste gebouwen of vluchtende burgers.

Maar de lijst van serieuze slachtoffers wordt met de dag groter en bevat reeds een aantal van de grootste namen in de technologie, financiële diensten, defensie, overheid, staalindustrie, olie & gas en elektriciteit. Dit soort type cyberaanvallen kan het best begrepen worden, niet als een doel op zich zelf, maar als een potentieel krachtig middel om een breed scala van politieke, militaire en economische doelen te bereiken.

Monitoring van verdachte of kwaadaardige gedragingen

Reguliere beveiligingsmaatregelen zoals anti-virussoftware en firewalls blijken steeds vaker onvoldoende bescherming te bieden tegen malware. Want helaas slaan bestaande beveiligingsvoorzieningen lang niet altijd aan als malware uw bedrijf binnen komt. Het aantal dreigingen groeit explosief door de snelle aanwas van soorten en varianten malware. Malafide partijen zitten nu eenmaal niet stil en dataspionage is aan de orde van de dag.

Rickey Gevers, Chief Intelligence Officer bij RedSocks, ging tijdens zijn sessie in op het detecteren en beveiligen van organisaties tegen verdachte of kwaadaardige gedragingen. Belangrijke onderdelen die hierbij aan bod kwamen zij hoe u het gedrag van het uitgaande verkeer monitort op verdachte of kwaadaardige gedragingen, op welke manier u tijdig een waarschuwing ontvangt voor bijvoorbeeld een virusuitbraak en hoe u snel inzicht krijgt in de omvang en de impact van een incident.

Help, wie zit er aan mijn spullen?

Boudewijn van Lith, Security Solution Consultant bij Micro Focus, ging tijdens zijn sessie in op het hoe en waarom van gegevensbescherming. Volgens Boudewijn van Lith zijn mensen hierbij de zwakste schakel. Immers waar mensen werken, daar worden fouten gemaakt. Zoals verkeerd geadresseerde email, gestolen laptops uit de auto of mail doorsturen naar je privé mail adres. De meest risicovolle groep zijn de IT beheerders, die over de toegang beschikken op systeemniveau. Om incidenten en daaruit voortkomende financiële schade, aansprakelijkheidsclaims, boetes en reputatieschade te voorkomen is het belangrijk om te achterhalen wie er nu precies toegang heeft tot welke gegevens, zodat risico's (waar mogelijk en nodig) kunnen worden gereduceerd. Dit kan door middel van identificatie (wie is wie?), toegangsrechten (wie mag wat?), authenticatie (is degene ook wie die zegt dat die is?), aantoonbaar inzicht (wat gebeurd er allemaal?).

Hackers! Do we hug or do we shoot?

Edwin van Andel, Ethical Hacker en adviseur bij Zerocopter ging tijdens zijn sessie in op welke rol hackers kunnen spelen bij het beveiligen van informatie van bedrijven en hun klanten. Zerocopter is een online platform waarmee bedrijven hun online beveiliging kunnen testen, bijvoorbeeld of een database met gevoelige klantgegevens voldoende is beveiligd. Dit geldt ook voor het testen van de beveiliging van online applicaties, interne communicatie of belangrijke bedrijfsbestanden.

Zerocopter biedt drie functionaliteiten aan. Allereerst kunnen bedrijven via Zerocopter hackers inhuren om de beveiliging te testen. Het bedrijf maakt een budget vrij en hackers kunnen gevonden kwetsbaarheden via het platform aan het bedrijf melden. Het tweede onderdeel bestaat uit een verzameling scanners die de beveiliging van een bedrijf analyseren, bijvoorbeeld of software up-to-date is en of er een gevaarlijke opening in een server wordt gevonden. Het derde en laatste onderdeel van Zerocopoter biedt de mogelijkheid om een formulier op de website van het bedrijf te plaatsen waarmee hackers kwetsbaarheden kunnen melden. Deze kwetsbaarheden worden vervolgens door Zerocopter gecontroleerd en doorgestuurd naar het betreffende bedrijf.

Partners Cyber Security Event 2016:

Op zoek naar nog meer verdieping over cyber security voor u of uw collega?

Cursus Cyber Security | start 23 maart 2017

U verdiept zich o.a. in:

- ☐ Imago- en reputatieschade voorkomen voor uw organisatie!
- ☐ Het aantal potentiële dreigingen en kwetsbaarheden reduceren
- ☐ Aansprakelijkheidsclaims, boetes en imagoschade voorkomen
- ☐ Het beveiligingsbewustzijn onder uw medewerkers vergroten

Meer informatie | Bekijk programma | Bekijk docenten | Download brochure