congresverslag

CYBERSECURITY EVENT 2017

www.sbo.nl/cybersecurity

Voorwoord

Beste lezer,

Op 10 oktober 2017 vond op het Big Data Value Center in Almere de tweede editie van 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 zodoende 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. Met het Cyber Security Event boden we een podium aan overheden, bedrijven en kennisinstellingen om kennis, producten en diensten met elkaar te delen voor de aanpak van cybercrime en datalekken.

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

Hans van Loon, strategisch adviseur op het terrein van Cyber Security en dagvoorzitter van het Cyber Security Event

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

Opening Cyber Security Event
De tweede editie van het Cyber Security Event werd geopend door Hans van Loon, strategisch adviseur op het terrein van Cyber Security en de dagvoorzitter van dit event. Hij werd vergezelt door Hans van Bragt, projectleider bij het Big Data Value Center waar het Cyber Security Event plaatsvond. Het Big Data Value Center is een uniek open innovatie platform met een fysieke plek in Almere waar verschillende organisaties en partijen experimenteren met (big) data.

Cybercrime en Cyberterrorisme
De eerste presentatie werd verzorgd door Jaap Schekkerman, directeur onderzoek bij het Cyber Research Center – Industrial Control Systems, een onafhankelijk internationaal onderzoekscentrum dat onderzoek verricht naar 'Nation-State sponsort or Rogue Group' cyber aanvallen op industrial control systems / vitale infrastructuur. In zijn presentatie ging hij in op de aard en omvang van cybercrime en cyberterrorisme in Nederland en de rest van de wereld, de risico's en de gevolgen van cybercrime en cyberterrorisme en mogelijke maatregelen om de schade te beperken.

Als we kijken naar de aard en de omvang van cybercrime en cyberterrorisme in Nederland dan zien we dat cyber criminelen en statelijke / rogue group actoren (cyber terrorisme) nog altijd de grootste dreiging vormen en de meeste schade aan richten. Cyber aanvallen worden gebruikt om democratische processen te beïnvloeden en de kwetsbaarheid van het internet of things heeft tot verstorende aanvallen geleid die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven. Daarnaast zien we dat de vitale infrastructuur als ook industriële processen en systemen onvoldoende weerstand kunnen bieden aan serieuze cyberaanvallen en veelal geen getest recovery plan hebben voor het geval ze toch gecompromitteerd zijn. We zien dan ook dat de weerbaarheid van individuen en organisaties ver achter blijft bij de snelle groei van de dreiging. Het aantal serieuze cyber aanvallen neemt exponentieel toe als we kijken naar de afgelopen periode.

In dit digitale tijdperk worden we als industrie, bedrijfsleven en overheid, als ook als individu steeds slimmer, maar ook steeds kwetsbaarder. Cybercrime en cyberterrorisme ligt op de loer en is op wereldwijd niveau een zeer actueel onderwerp. Op papier hebben we in Nederland best wel een aantal zaken geregeld, echter de praktijk is veel weerbarstiger. We worden er regelmatig en op grote schaal mee geconfronteerd, waardoor ook de gevolgen toenemen. Ondanks deze dreigingen wordt er nog veel te weinig gedaan om de digitale weerbaarheid te vergroten, zowel door de overheid, het bedrijfsleven, de industrie als ook particulieren. Daarnaast moeten we accepteren dat we gecompromitteerd kunnen worden, echter hebben we dan maatregelen voorbereid en getest om tegen aanvaardbare kosten weer up en running te komen.

Hoewel de oorzaken en gevolgen van cybercrime en cyberterrorisme inmiddels duidelijk zijn, wordt er niet alleen door de overheid, maar ook door de industrie en het bedrijfsleven veel te weinig maatregelen genomen om vitale data, processen, systemen, netwerken, etc. te beschermen tegen dit soort cyber aanvallen. En ja deze maatregelen kosten zeer veel geld. Echter de kans dat men slachtoffer wordt van een serieuze cyber aanval neemt ook zeer snel toe en hier gaan dus de kosten echt voor de baten uit.

“Cybercrime is een realiteit die altijd zal blijven bestaan. Mijn stelling is dat iedere organisatie in de wereld vroeg of laat ‘gecompromitteerd’ wordt. In Nederland ging het in 2016 om een kostenpost van 10 miljard euro. Uit onderzoek blijkt dat 1 op de 5 organisaties slachtoffer is geweest van cyberaanvallen.Cyberterrorisme betreft cyberaanvallen om een bepaald idealogisch doel te bereiken. Wij in het westen hebben een westers denkkader. Op andere delen van de wereld hebben ze andere denkkaders waardoor cyberterrorisme interessant wordt. Het is moeilijk te verklaren waarom iemand wordt aangevallen (waarom wij?) het is moeilijk in te schatten welk doel iemand daarvoor had. Soms willen ze ons schade berokkenen. En soms willen ze ons alleen angst aanjagen, door je even te laten weten dat ze in je systemen zitten en je beveiliging zijn doorgekomen. Dat is heel effectief. Wij doen onderzoek naar aanvallen. We hebben monitoringstools die live wereldwijd zaken bekijken. Nederland staat wereldwijd op nummer 11 van meest aangevallen landen door cyberattacks. De urgentie bij bestuurders en kabinet moet echt omhoog. De digitale weerbaarheid van Nederland blijft achter. Er is sprake van windowdressing: naar buiten toe lijkt het heel wat maar in de praktijk gebeurt er gewoon te weinig. Er is veel te veel papierwerk en wetten. Dat is de verkeerde richting. Je moet kijken waar je bedrijven en overheden echt mee helpt. Dat is niet alleen het voldoen aan de wet.”

Als we ons beter willen beschermen tegen cyber aanvallen, dan wel voorbereid willen zijn voor het geval we toch gecompromitteerd zijn, dan dienen we allereerst een aantal belangrijke vragen te beantwoorden.

- Wat zijn de belangrijkste kroonjuwelen (fysieke infrastructuur / kennis / data / processen / technologie / systemen / netwerken / IP, etc.) welke beschermt dienen te worden?
- Kennen we de type dreigingen waartegen we ons willen beschermen?
- Kennen we de kwetsbaarheden van de fysieke infrastructuur, de organisatie, netwerken, systemen, etc. waartegen we ons willen beschermen?
- Is het topmanagement zich bewust van de dreigingen en de risico’s en bereid serieuze maatregelen te nemen?
- Zijn we bereid en instaat om continu fors te investeren in Cyber Protection & Resilience (voor het IT gedeelte minimaal 10 tot 15% van het IT budget)? Of accepteren we de materiele en immateriële kosten als het fout gaat?
- Hebben we de cyber / security kennis en expertise in huis of moeten we die inhuren om een gedegen cyber security plan / architectuur te ontwikkelen die invulling kan geven aan bovengenoemde vragen?
- Hebben we de kennis en expertise in huis of moeten we die inhuren om de cyber security architectuur te kunnen implementeren en testen om daarna 24 x7 operationeel en actueel te houden?
- En wat als we toch gecompromitteerd worden, hoe kunnen we dan tegen aanvaardbare kosten weer up en running komen?

Cyber Security
De tweede presentatie werd verzorgd door Ben Kokkeler, lector Digitalisering en Sociale Veiligheid bij het Expertisecentrum Veiligheid van de Avans Hogeschool. Hij ging in zijn presentatie in op hoe organisaties de cyber security kunnen organiseren en daarmee kunnen voorkomen dat ze slachtoffer worden van cybercrime en cyberterrorisme.

Ben Kokkeler hield een pleidooi voor het versterken van de digitale infrastructuur. Doel is om organisaties weerbaarder te maken. Hij ziet daarin een rol weggelegd voor de overheid, de wetenschap, het bedrijfsleven (de industrie) en de burger. In zijn presentatie had Ben Kokkeler met name aandacht voor MKB bedrijven. De multinationals hebben de kennis, capaciteit en middelen in huis om zich weerbaar te maken tegen mogelijke cyberaanvallen. MKB bedrijven zijn daarin wat beperkt. Toch zullen ook zij zich digitaal weerbaar moeten maken.

"Ik richt me vandaag op het MKB en dan met name de wat kleinere bedrijven. Waarom? De papieren werkelijkheid verschilt nog al van de werkelijkheid. Op Europese schaal begint het besef te ontstaan dat cijfers met name van bedrijven afkomen. Het is moeilijk verifieerbaar of deze cijfers werkelijk zijn of dat bedrijven deze cijfers opzetten om eigen markten te promoten. Het Rathenau instituut is zich bewust van allerlei bias die er zijn in de cijfers. Daarom gebruik ik graag cijfers van hen. Het digitale grondwater rukt op. Het MKB moet daar zelf voor aan de slag. Cybersafety vereist skills op alle niveaus. We hebben een schreeuwend tekort aan technici. Dit betekent dat we MBO'ers en HBO'ers moeten gaan binnentrekken in de cyberwereld."

Privacy en Cyber Security
Ton Siedsma, onderzoeker bij Bits of Freedom, verzorgde de derde presentatie van het Cyber Security Event over het belang van privacy van burgers en het beschermen van persoonlijke data en vertrouwelijke informatie. Bits of Freedom is een organisatie die opkomt voor vrijheid en privacy op internet. Dit doet zij via onder andere campagnes, presentaties en het meedenken over (toekomstig) beleid. Bits of Freedom komt op voor twee grondrechten bij je digitale communicatie die onmisbaar zijn voor je vrijheid: privacy en communicatievrijheid. Die rechten zijn in de offline wereld in de loop van eeuwen opgebouwd, omdat ze belangrijk zijn voor je individuele vrijheid, voor een rechtvaardige samenleving en voor een gezond werkende democratie. Met de komst van het internet en andere technologieën hebben we nieuwe mogelijkheden gekregen, en tegelijkertijd geeft het de overheid en het bedrijfsleven ook vergaande controlemogelijkheden. Door de vervagende grenzen tussen publieke, private en privéruimte staat de vrijheid van burgers steeds verder onder druk. Het is maar goed dat daar steeds meer aandacht voor is, want onze wereld is steeds meer een digitale wereld.

"Er zijn veel onbeantwoorde vragen ten aanzien van nieuwe technologie en privacy. Voice-control neemt ook stemmen van mensen op die langslopen en die daar niet om gevraagd hebben. Politie wil telefoons hacken. Dat kan door kwetsbaarheden in de software. Je hebt bekende en onbekende kwetsbaarheden. Bits of Freedom vindt dat een groot probleem omdat je daardoor onbekende kwetsbaarheden bewust kwetsbaar houd in het belang van opsporing. Dan zijn burgers dus onnodig kwetsbaar voor derden. Het is afwachten totdat de eerste schadeclaims bij de politie binnenkomen omdat zij iets hadden moeten melden en dat niet gedaan hebben. Het is toch lullig als je zelfrijdende auto ineens ontspoort."

Ton Siedsma pleit met name voor het slim omgaan met data. *"Bedenk welke data je waarvoor nodig hebt en wat je met die data wil doen. Data die je niet verzameld en opslaat kun je ook niet kwijtraken."*

De Wet op de Inlichtingen- en Veiligheidsdiensten 2017 ook wel aangeduid als de Sleepwet regelt het wettelijk kader voor onder andere de AIVD en MIVD. Deze wet vervangt haar voorganger de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 en is reeds gedeeltelijk in werking getreden. *"Een groot deel van de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten is een verbetering ten opzichte van de oude. Het ding is dat je nu ongericht mag zoeken. Mensen gaan zich anders gedragen als ze het idee hebben dat ze in de gaten gehouden worden. Bits of Freedom is bang dat de vrijheid van burgers op internet afneemt uit angst te worden bekeken."*

Cyber Security Challenge

Na de verschillende presentaties van diverse experts 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 containeroverslagbedrijf in een haven slachtoffer is van een wereldwijde aanval van ramsomware, software die computers gijzelt door alle bestanden te versleutelen. Twee terminals in de haven zijn hierdoor buiten bedrijf. De containerschepen die nu voor de kade liggen kunnen niet geladen en gelost worden. Dit levert ook vertraging op voor het vervolgtraject per binnenvaartschip of vrachtwagen. Daarnaast zijn er schepen naar de haven onderweg waarvan onduidelijk is wanneer zij hun vracht kwijt kunnen. Het gaat om duizenden, met name uit Azië afkomstige containers met kleding, elektronica, chemicaliën, onderdelen en grondstoffen voor fabrieken in Europa, die daardoor ook in de problemen dreigen te komen. Als deze gevolgen van de ransomware-aanval langer aanhouden, dan zullen de containerschepen moeten uitwijken naar terminals van andere bedrijven in de haven of mogelijk zelfs andere havens.

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 aanval van ramsomware 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.

Cyber Security Sessies
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.

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? en wat is zijn of haar rol?), toegangsrechten (wie mag wat?), authenticatie (is degene ook wie die zegt dat die is?), aantoonbaar inzicht (wat gebeurd er allemaal?), context (tijd, locatie, device?).

"Identiteit en logische toegang: dat is de kern. Wat of wie verleen je nou toegang tot systemen? 63% is gerelateerd aan misbruik van login-gegevens. Hackers zoeken naar die "insider threaths". De mens is de zwakke schakel. Cyber Security is het beschermen van de relatie tussen data en personen."

Boudewijn van Lith noemde een aantal trends op het terrein van cyber security: steeds meer toegang tot verschillende systemen, die steeds eenvoudiger in gebruik moeten zijn, met snel succes en standaard oplossingen. Risicobronnen die hiermee samenhangen zijn onder andere Internet of Things, Cloud, Mobile, Service delivery, netwerken en derde partijen. Het is van belang om tot risicobeheersing rond veranderende bedrijfsmodellen, nieuwe technologieën en toenemende digitalisering en Internet of Things te komen.

"De externen zijn een groot risico, dat zit met name in de proceskant maar ook in strategie. Dat geldt ook voor ketenpartners. Krijgen die allemaal toegang tot de systemen of houd je alles volledig gescheiden? Er moet maar een deur zijn voor logisch toegang. En niet allerlei deurtjes om naar hetzelfde te komen."

Cyber Security op het werk; de mens als zwakste schakel
Sjoerd van der Meulen, Cyber Security Specialist bij DataExpert, ging tijdens zijn sessie in op cyber security op het werk en de rol van de mens hierin. Sjoerd van der Meulen heeft 15 jaar werkervaring bij de politie Amsterdam en is werkzaam bij DataExpert waar hij organisaties adviseert, traint en begeleidt in onder andere internetrechercheren, webtechniek en de linux command line.

Een groot deel van de (juridische) verantwoordelijkheid rondom cybercrime en datalekken ligt in de handen van jouw medewerkers. Sjoerd van der Meulen ging in zijn sessie in op hoe je hen van "onbewust onbekwaam" kunt transformeren naar "bewust bekwaam", waarom alleen techniek niet de oplossing is, hoe je gedrag en de bedrijfscultuur met de juiste training kunt sturen en met welke middelen je dit gedrag kunt borgen.

Volgens Sjoerd van der Meulen is iedereen zeer gevoelig voor hacking, maar kan ook iedereen zelf hacken. Het enige dat daar voor nodig is, is een username en wachtwoord. Het kost een hacker tussen de 2 en 3 minuten om een phishing website op te zetten.

"Bedrijven werken stiekem veel meer via de cloud dan zij zelf denken. Een gemiddeld bedrijf werkt al snel met 1000 unieke applicaties op de cloud. De grootste zijn bijvoorbeeld dropbox, icloud, wetransfer. Bring your own device kan lastig zijn als je op andere devices werkt. DataExpert zorgt voor een online firewall platform die alle gegevens filtert en bij schadelijke gegevens, tegenhoudt."

Gegevensbescherming
Jan Smets, certified Data Protection Officer bij Gemalto en voormalig technical manager bij Motorola Solutions, helpt organisaties bij het implementeren van data security oplossingen. In zijn sessie stond de Algemene Verordening Gegevensbescherming centraal. Oftewel: hoe kan jouw organisatie voldoen aan de Algemene Verordening Gegevensbescherming (General Data Protection Regulation). Om te beginnen moet iedere organisatie een Data Protection Officer aanstellen. Daarnaast moet ieder bedrijf ten alle tijden documentatie aan kunnen leveren wanneer het gaat om persoonsgegevens.

"Zorg dat er security en privacy awareness is. Privacy by design is de toekomst. Prioriteer welke gegevens het beste privacyproof moeten zijn. Doe het stap voor stap maar vergeet niet om parallel daaraan ook al die andere te bekijken. Als je als bedrijf hier niet goed mee omgaat dan ga je vroeg of laat voor de bijl. Vanaf het moment dat is opgemerkt dat er een lek is, heb je 72 uur om het te melden. Maar als de data geanonimiseerd of geëncrypt is, hoef je dat niet te doen. Ofwel, je kan het beste al je persoonsgegevens anonimiseren of encrypten, dan loop je veel minder risico."

Partners Cyber Security Event 2017

Partners Cyber Security Event 2017

Congressen en opleidingen Dataprotectie, AVG, WBP en Privacy

In mei 2018 gaat met de invoering van de Algemene Verordening Gegevensbescherming (AVG) nieuwe wetgeving gelden voor het verwerken van persoonsgegevens. **Is uw organisatie goed voorbereid op deze regelgeving?**

Met onze congressen en opleidingen leert u alles over de nieuwe AVG en dataprotectie om zo imagoschade en forse boetes te voorkomen!

Bekijk ons aanbod:

Cursus de Nieuwe AVG & WBP Overheid

Cursus de Nieuwe AVG & WBP

Opleiding Data Protection voor Financials

Congres Dataprotectie & Privacy

Opleiding Data Protection Officer
