



CYBER RESILIENCE IN DE BESTUURSKAMER

THE GRAND CONFERENCE IN AMSTERDAM

Marieke Klaver is R&D programmamanager Cyber Security bij TNO.
Zij is te bereiken via marieke.klaver@tno.nl

Op 16 oktober 2012 vond in Amsterdam The Grand Conference plaats. Deze conferentie werd georganiseerd door het Centre for the Protection of National Infrastructure (CPNI.NL) in nauwe samenwerking met de Europese Commissie, de Europese Network and Information Security Agency (ENISA), het Amerikaanse Department of Homeland Security (DHS) en het World Economic Forum (WEF). Het thema was 'Building a Resilient Digital Society'. De internationale conferentie was gericht op de top van het bedrijfsleven, overheden en andere organisaties en trok ruim tweehonderd deelnemers uit tweeëntwintig landen.

The Grand Conference was een activiteit van de gezamenlijke EU - VS werkgroep op het gebied van cyber security en cybercrime. Deze werkgroep richt zich onder andere op informatie-uitwisseling,

kennisdeling en samenwerking op het gebied van veiligheid van Industrial Control

Systems (ICS), procescontrolesystemen, en Smart Grids. Deze procescontrolesystemen spelen in het functioneren van een groot deel van onze vitale infrastructuur, zoals bijvoorbeeld elektriciteitsnetwerken, drinkwater- en waterbeheersystemen en tunnelveiligheid, een belangrijke rol. Daarom is het van groot belang dat de procescontrolesystemen voldoende robuust zijn tegen verstoringen.

De afhankelijkheden tussen (vitale) infrastructuur en de onderlinge connecties en afhankelijkheid tussen organisaties maken dit een gedeelde verantwoordelijkheid, die vraagt om samenwerking tussen landen, tussen overheden en private partijen en tussen leveranciers en gebruikers van deze systemen.

De conferentie was er op gericht om de verschillende aspecten van het creëren van een veilige en robuuste digitale samenleving te belichten. Beginnend bij de kansen die de toenemende

connectiviteit biedt, via mogelijke bedreigingen naar oplossingsrichtingen op het gebied van risicomanagement, organisatorische strategieën en het inzetten van economische prikkels om het doel te bereiken.

Na de opening door organisator Annemarie Zielstra, director van CPNI.NL, schetste Harry

van Dorenmalen, voorzitter van IBM Europa, een positieve toekomstvisie rond de rol van ICT in 2030 en de mogelijkheden die dit de maatschappij gaat bieden. Mikko Hypponen, Chief Research Officer van F-Secure, schetste juist de duistere kant van cyberspace en ging in op de vele spelers die misbruik proberen te maken van de toegenomen connectiviteit van organisaties. Het grootste gevaar ziet hij komen van door staten gesponsorde aanvallen; hij acht het voor

organisaties heel moeilijk om zich te verdedigen tegen "James Bond" gewapend met USB-stick. Mike Maddison (Deloitte), Rod Beckstrom (voormalig CEO van ICANN) en prof. Michel van Eeten (TU Delft) belichtten de eerdere geschetste oplossingsrichtingen. 's Middags vonden er masterclasses plaats op het

gebied van risicomanagement voor ICS en Smart Grids, crisiscommunicatie/reputatiemanagement en ICS Security voor managers. Met name de live hack demo door het gouden Cyberlympics-team van Deloitte maakte veel indruk op de aanwezigen.

Cyber Resilience manifest

Vanwege het grote economische belang van cyber security was het World Economic Forum (WEF) één van de partners van de conferentie. Vanuit het WEF wordt fors ingezet om het onderwerp cyber resilience op de agenda van iedere bestuurskamer te krijgen, aangezien zij zien dat in een "hyperconnected world" een weerbaar cyberdomein van cruciaal belang is voor het functioneren van organisaties. Hiertoe heeft het WEF een manifest ontwikkeld met de titel "Partnering for

Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles

and Guidelines"^[1]. Dit manifest bevat richtlijnen en principes voor de inbedding van cyber resilience tot op het hoogste niveau binnen organisaties. De principes die de WEF heeft gedefinieerd, luiden:

- De organisatie erkent de onderlinge afhankelijkheden in deze hyperconnected wereld en zijn eigen rol

De conferentie was gericht op de top van het bedrijfsleven en trok deelnemers uit 22 landen

Het grootste gevaar komt van door staten gesponsorde aanvallen



Ondertekening Cyber Resilience manifest

om bij te dragen aan een veilige digitale omgeving.

- Het managementteam van de organisatie is zich bewust van haar leidende rol bij het uitdragen en organiseren van cyber resilience.
- De organisatie erkent het belang van het integreren van cyber risicomanagement binnen de algemene risico afwegingen en volgt hierbij de beschreven richtlijnen en principes.
- De organisatie stimuleert zijn afnemers om deze richtlijnen en principes ook te volgen.

Het WEF promoot dit manifest als middel om de dialoog rond cyber resilience binnen organisaties op gang te brengen en om het commitment op bestuurskamer niveau te bestendigen. Tijdens de conferentie toonden bestuurders van Alliander, KPN en TNO dit commitment door publiekelijk het WEF-manifest te ondertekenen.

In het slotgedeelte van The Grand Conference onderstreepte Mark Dierikx, directeur-generaal van het Ministerie van Economische Zaken, Landbouw en Innovatie, het belang dat zijn ministerie hecht aan een goede en betrouwbare cyberinfrastructuur. De conferentie werd afgesloten met een speech van Eurocommissaris mevrouw Kroes.

Zij constateerde dat er een toename is in zowel aantal als ernst van cyberincidenten. De EU is daarom bezig haar inspanningen op het gebied van digitale veiligheid te versterken door het uitbrengen van

een Europese Cyber Security Strategie.

De strategie beschrijft de noodzaak van internationale samenwerking tussen de EU landen. De ICT infrastructuur en de aanvallen daarop houden zich immers niet aan landsgrenzen.

De Europese Commissie streeft daarom naar een versterking van het niveau van digitale bescherming in alle EU landen. Daarnaast ziet zij samenwerking met de verschillende partijen uit de vitale infrastructuur als



Eurocommissaris mevrouw Kroes

essentieel. Het gaat hierbij bijvoorbeeld over transport, energievoorziening, gezondheidszorg en de financiële sectoren. Publieke en private partijen binnen deze sectoren moeten gezamenlijk optrekken, waarbij ieder zijn verantwoordelijkheid neemt. De verantwoordelijkheid voor cyber security ligt volgens de Eurocommissaris niet alleen bij bedrijven en overheden, maar ook bij iedere ICT gebruiker. Er zijn simpele maatregelen die iedereen afzonderlijk zelf kan nemen. Europa heeft daarom oktober als European Cyber Security Month ingesteld om de thuisgebruikers in de veiligheidsdiscussie te betrekken. Tenslotte noemde mevrouw Kroes internationale samenwerking met landen buiten de EU als essentieel onderdeel: "It's time to give cyber-security the attention it deserves. Let's be strategic, let's work together, and let's ensure we protect our infrastructure, and our citizens, in the digital age".

Als invulling van deze oproep tot samenwerking vond één van de hoofdbestanddelen van de conferentie 's avonds plaats. Een select gezelschap

Publieke en private partijen moeten gezamenlijk optrekken

van rond de veertig topbestuurders ging tijdens een walking dinner aan

de hand van een drietal toekomst-scenario's concreet met elkaar aan de slag, om ook op bestuurskamer niveau het cyber security netwerk te bouwen en input te leveren voor de WEF-bijeenkomsten in december (Dublin en Washington) en januari (jaarlijkse conferentie wereldleiders in Davos). Duidelijk werd dat het tonen van leiderschap in de top van de organisaties cruciaal is om de digitale weerbaarheid van onze maatschappij verder te verhogen. De overheid moet daarbij de private sector faciliteren, stimuleren en belemmeringen wegnemen. Deze conferentie is een eerste opstap naar structurele discussies tussen publieke en private partijen over cyber resilience en de weg om dat te bereiken.

De conferentie kan met recht een succes genoemd worden wanneer deze vervolgacties concreet worden opgepakt en leiden tot meer commitment voor cyber resilience in de bestuurskamer. Eén succes is al binnen: namens de Europese Commissie gaf mevrouw Kroes haar steun aan de organisatie van een vervolg conferentie in 2013, The Grand Conference 2013.

U en uw organisatie zijn aan zet

Ook u en uw organisatie kunnen nu al aan de slag. Op de Cyber Resilience website van CPNI.NL ^[2] kunt u meer informatie vinden over cyber resilience. Daar vindt u onder andere een verzameling met bewustwordingsmateriaal, een database met verschillende incidenten en een C-suite executive checklist op basis van de WEF-principes. Door het invullen van de vragenlijst krijgt u een overzicht van het cyber resilience volwassenheidsniveau van uw organisatie en hoe dit zich verhoudt tot andere organisaties. Bij een interactieve sessie met de deelnemers aan de conferentie, bleken de aanwezige organisaties bovengemiddeld te scoren daar waar het gaat om hun eigen volwassenheid. Daar waar het ging om zicht op de hele toeleveringsketen bleek dit beduidend minder goed geregeld. Gebruik de tools om te bepalen waar uw organisatie staat en (indien nodig) uw eigen digitale weerbaarheid te vergroten. ●

(Dit artikel is eerder verschenen in het managementblad Beveiliging)

Referenties



1. World Economic Forum, Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines, on-line:
http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.



2. Meer over cyber resilience:
www.cyber-resilience.org



INTERNATIONAL MANAGEMENT FORUM

cursussen ♦ trainingen post-HBO opleidingen

Identity Management & Access Control

9-delige schriftelijke cursus over het beheren, beveiligen en controleren van digitale identiteiten en toegangsrechten. De cursus is geschreven door André Koot. André is redacteur van het vakblad Informatiebeveiliging van het Platform voor Informatiebeveiliging (PvIB).



Informatiebeveiliging



In deze schriftelijke cursus leert u vorm en inhoud te geven aan de informatiebeveiliging binnen uw organisatie. De cursus biedt concrete handvatten voor het opstellen van een informatiebeveiligingsbeleid op strategisch en tactisch niveau en de daadwerkelijk te treffen maatregelen op operationeel niveau.

CISA

CISA staat voor Certified Information Systems Auditor en is een titel van ISACA. De 4-daagse Nederlandstalige CISA training leidt op voor het wereldwijd erkende CISA certificaat van ISACA.



Meer informatie en inschrijven?
www.imf-online.com/partner/pvib

**Leden van het PvIB
ontvangen € 200,- korting**