CSR Cyber Security Raad

JAAROVERZICHT 2016

Rabobank • foto Jeroen de Bakker

VOORWOORD

Nederland ligt digitaal gezien onder vuur. En hetzelfde geldt voor Europa. Toch is het urgentiegevoel onder politici, bestuurders, ondernemers en burgers nog lang niet altijd hoog genoeg. In 2016 heeft de Cyber Security Raad (CSR) daarom nadrukkelijk ingezet op het op de agenda krijgen van cybersecurity in Nederland, publiek én privaat. Enerzijds door adviezen te geven en onderzoek te laten doen, en anderzijds door onderwerpen voor het belang van cybersecurity in de media te brengen en bij te dragen aan bewustwording, bijvoorbeeld via evenementen, zoals de European Foresight Cyber Security Meeting en de International Cyber Security Summer School.

In de eerste helft van 2016 was Nederland voorzitter van de Europese Unie. Cybersecurity en cybercrime zijn toen aangemerkt als prioritaire thema's voor het Nederlandse voorzitterschap. De raad heeft zich ingezet om belangrijke cybersecurity-onderwerpen bij de Europese Commissie onder de aandacht te brengen en blijft hier ook de komende jaren op inzetten. Zo heeft de CSR een internationale expertmeeting georganiseerd over de thema's Internet of Things en Zorgplichten met twintig invloedrijke internationale organisaties, waaronder het World Economic Forum, Microsoft, Europol, NATO en het Berkman Center for Internet & Society. Het adviesrapport is overhandigd aan de Europese Commissie. Ook heeft de CSR in 2016 de oprichting van gelijksoortige raden in andere EU-lidstaten gestimuleerd, door hen van advies te voorzien.

Op verzoek van de CSR heeft mevrouw Herna Verhagen, CEO PostNL, onafhankelijk onderzoek gedaan naar de stand van zaken in Nederland op het gebied van cybersecurity. Het rapport 'De economische en maatschappelijke noodzaak van meer cybersecurity – Nederland digitaal droge voeten' is in oktober 2016 overhandigd aan minister-president Rutte en de heer De Boer, voorzitter VNO-NCW. Het advies bevatte een belangrijk waarschuwingssignaal: Nederland moet op het terrein van cybersecurity in beweging komen. Digitale aanvallen nemen hand over hand toe. De CSR is evenals Verhagen van mening dat dit vraagt om structurele aandacht van regering, politici, beleidsmakers, bestuurders, toezichthouders, bedrijven en burgers. Iedereen heeft een verantwoordelijkheid in het gezamenlijk beschermen van onze economie, welvaart en maatschappij.

Naar aanleiding van een consultatieronde door de monitoringcommissie corporate governance code verzocht de CSR het onderwerp cybersecurity in de code op te nemen. Dit advies is overgenomen.Tot slot vierde de CSR in 2016 zijn vijfjarig bestaan.

Dit CSR Jaaroverzicht 2016 is te downloaden van www.cybersecurityraad.nl, evenals de diverse documenten die in dit jaaroverzicht aan de orde komen.

1. CYBER SECURITY RAAD

De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet dat bestaat uit vertegenwoordigers van publieke en private organisaties en wetenschap. De minister van Veiligheid en Justitie heeft de CSR in 2011 geïnstalleerd. In dit jaar vierde de CSR daarmee haar vijfjarig bestaan. De installatie van de CSR vloeide direct voort uit de eerste Nationale Cyber Security Strategie die eerder dat jaar door de minister namens het kabinet aan de Tweede Kamer werd aangeboden. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen. Door de unieke samenstelling van de CSR (publiek-privaat-wetenschap) is het mogelijk prioriteiten, knelpunten en incidenten vanuit diverse invalshoeken te benaderen en een integrale visie op kansen en bedreigingen te ontwikkelen. De CSR streeft naar adviezen die theoretisch onderbouwd, richtinggevend en praktisch uitvoerbaar zijn.

Taakstelling

De CSR heeft de volgende taken:

- Het gevraagd en ongevraagd verstrekken van advies aan de regering, publieke en private partijen inzake relevante ontwikkelingen op het gebied van cybersecurity. De raad adviseert het kabinet over de uitvoering en uitwerking van de Nationale Cyber Security Strategie.
- Het voorstellen van prioritaire thema's op het terrein van cybersecurity, onder meer ten behoeve van de afstemming tussen onderzoeksprogramma's van de overheid en waar mogelijk tussen die van wetenschappelijke onderzoekscentra en het bedrijfsleven. Ook draagt de CSR bij aan de Nationale Cyber Security Research Agenda.
- Het bijdragen aan de borging van publiek-private samenwerking in het domein van cybersecurity.
- Het adviseren aan de crisisorganisatie in Nederland tijdens grootschalige incidenten.

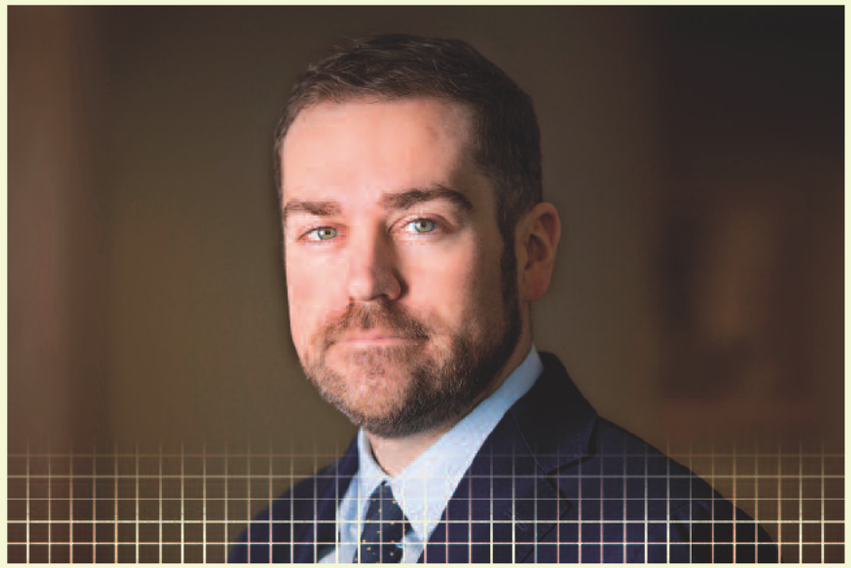
Samenstelling

De CSR heeft een samenstelling met vertegenwoordigers vanuit de wetenschap en private en publieke sectoren. De leden uit de private sectoren nemen hierbij deel namens een bepaalde sector en uitdrukkelijk niet namens hun bedrijf. De CSR bestaat momenteel uit achttien leden: zeven leden uit de private sector, zeven leden uit de publieke sector en vier leden uit de wetenschap.

Werkwijze

De CSR komt vier keer per jaar bijeen in een plenaire vergadering. De leden van de CSR worden ter voorbereiding op deze vergaderingen ondersteund door ondersteuners vanuit hun eigen organisatie. Daarnaast vindt periodiek afstemmingsoverleg plaats tussen alle ondersteuners en de secretaris van de CSR.

Naast de plenaire vergadering heeft de CSR een aantal subcommissies benoemd die zich richten op meer specifieke onderwerpen. In de subcommissies hebben raadsleden zitting en zij hebben een publiek-privaat-wetenschappelijke samenstelling. De subcommissies diepen onderwerpen uit, al



"Nederland neemt cybersecurity serieus en wil daarin vooroplopen met het groepje landen dat er al het beste in is. De Cyber Security Raad speelt hierin een belangrijke strategische rol, door vooruit te kijken naar nieuwe technologieën die op ons afkomen en daarover richtinggevend advies te geven aan kabinet, politiek, bedrijfsleven en (overheids)organisaties."

Klaas Dijkhoff, staatssecretaris van Veiligheid en Justitie

dan niet ondersteund door een werkgroep en/of een wetenschappelijk onderzoek. In het werkprogramma 2016 zijn vijf subcommissies aangekondigd op de onderwerpen Internet of Things, Zorgplichten, Onderwijs, Informatie-uitwisseling cybersecurity en cybercrime, en EU-voorzitterschap.

De CSR levert verschillende type producten op. Zo stelt de raad adviezen en handreikingen op, voeren individuele leden boardroomgesprekken bij (publieke) organisaties en bedrijven, zet de raad onderzoeken uit bij onderzoekers en initieert de raad verschillende activiteiten, zoals in het afgelopen jaar de European Foresight Cyber Security Meeting en de National Cyber Security Summer School.

SAMENSTELLING

PRIVATE SECTOR


Foto: KPN

Dhr. drs. E. Blok (covoorzitter)
Voorzitter Raad van Bestuur en CEO van KPN, lid van CSR namens VNO-NCW


Rita van de Poel

Dhr. R. de Mos
Senior Vice President en General Manager CGI Nederland, lid van CSR namens Nederland-ICT


Mark Engelen

Dhr. M. Krom
CIO PostNL, lid van CSR namens het CIO Platform Nederland


Peter van Es

Mw. T. Netelenbos
Voorzitter ECP


Miranda Koopman

Dhr. J. Nijhuis
CEO Schiphol Group, lid van CSR namen de sector Vervoer


Mark Engelen

Dhr. Ir. B.G.M. Voorhorst
COO TenneT, lid van CSR namens de energie-sector

PUBLIEKE SECTOR

Dhr. drs. H.W.M. Schoof (covoorzitter)
Nationaal Coördinator Terrorismebestrijding en Veiligheid

Dhr. R.A.C. Bertholee
Directeur-Generaal Algemene Inlichtingen en Veiligheidsdienst (AIVD)


Frank Groeliken

Dhr. Mr. G.W. Van der Burg
Lid van het College van procureurs-generaal

Dhr. Drs. J.C. de Groot
directeur Telecommarkt bij het directoraat-generaal Energie, Telecom en Mededinging bij het ministerie van Economische Zaken (waarnemend)


Arenda Oomen

Dhr. drs. H.B. Eenhoorn
Nationaal Commissaris Digitale Overheid


Mark Engelen

Dhr. Dr. S.J.G. Reyn
Directeur Strategie, Beleidsontwikkeling en Innovatie bij het Ministerie van Defensie


Miranda Koopman

Mw. J. van den Berg
Nationale Politie

WETENSCHAPPELIJKE SECTOR


Miranda Koopman

Mw. Dr. B. Van den Berg
Universitair Hoofddocent eLaw@Leiden


Mark Engelen

Dhr. Prof. Dr. M.J.G. Van Eeten
Hoogleraar Technische Bestuurskunde TU Delft

Dhr. Prof. Dr. B.P.F. Jacobs
Hoogleraar Computerbeveiliging Radboud Universiteit Nijmegen


Miranda Koopman

Mw. Prof. mr. E.M.L. Moerel
Senior Of Counsel Morrison & Foerster LLP, Hoogleraar Universiteit Tilburg

BUREAU CSR


Miranda Koopman

Mw. Drs. E.C. Van den Heuvel
Secretaris

Mw. Drs. A.A. Bakker
adjunct-secretaris

De heer M.N. Bobeldijk
communicatieadviseur

De heer. S.L. van Sommeren
stagiair

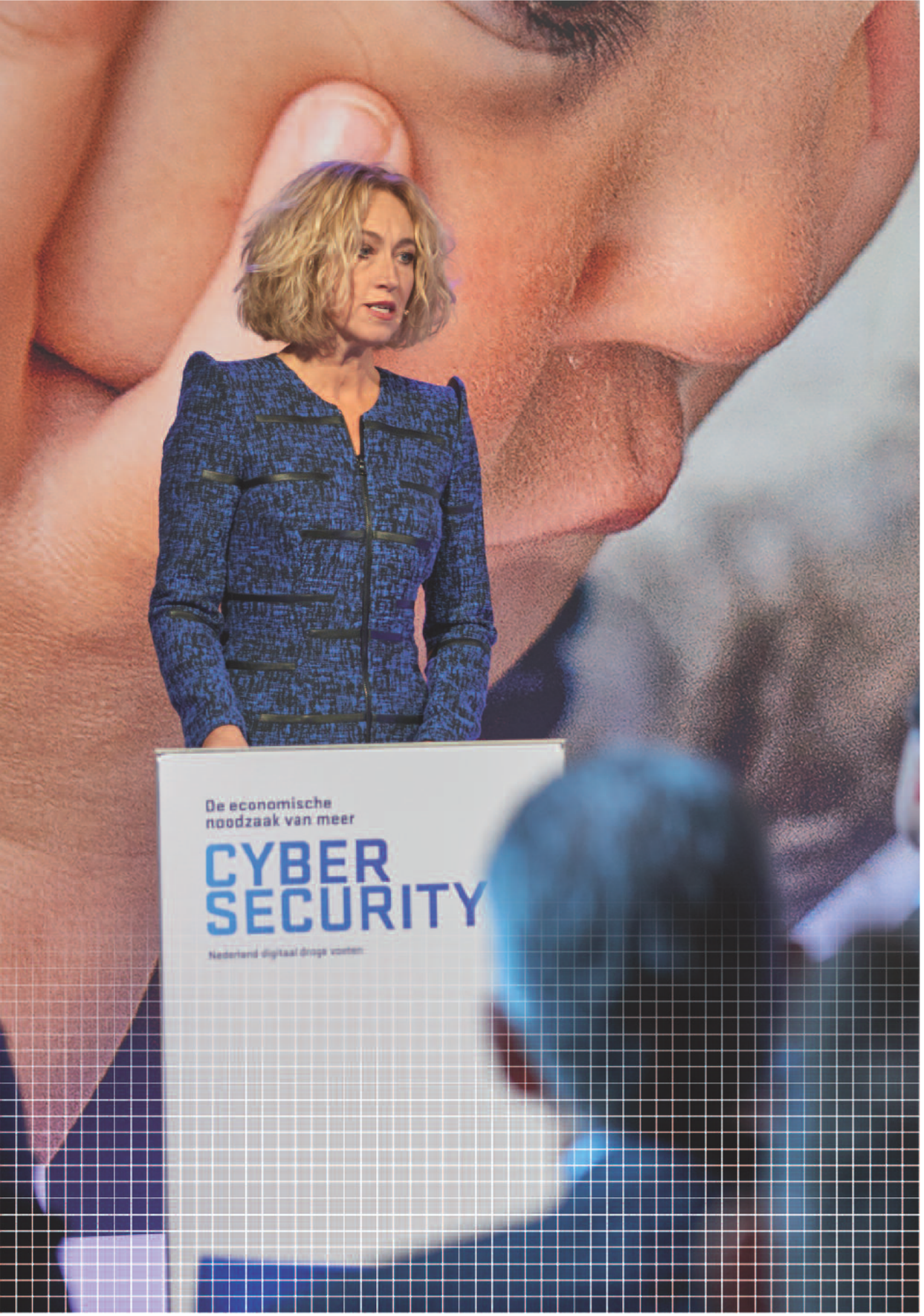
Vertrokken:
Mw. Drs. E.M. Attema
adjunct-secretaris

Teruggetreden in 2016

Dhr. B. Hogendoorn
CEO Hewlett Packard Nederland, lid van CSR namens Nederland ICT

Dhr. Drs. M.E.P. Dierikx
Directeur-generaal Energie, Telecom en Mededinging bij het Ministerie van Economische Zaken, lid van CSR namens het Ministerie van Economische Zaken

Dhr. D.G.T.M. Heerschop
CIO Nationale Politie



2. WERKPROGRAMMA

Op verzoek van de Cyber Security Raad (CSR) heeft mevrouw Herna Verhagen, CEO PostNL, onafhankelijk onderzoek gedaan naar de stand van zaken in Nederland op het gebied van cybersecurity. Zij heeft haar bevindingen en aanbevelingen op 6 oktober 2016 overhandigd aan minister-president Mark Rutte en voorzitter VNO-NCW Hans de Boer.

In het rapport 'De economische en maatschappelijke noodzaak van meer cybersecurity – Nederland digitaal droge voeten' stelt Verhagen dat digitalisering ons land veel economische groei en werkgelegenheid brengt. Cybercriminaliteit bedreigt onze welvaart. Daarom zijn maatregelen en investeringen in de veiligheid op internet noodzakelijk. Het moet net zo vanzelfsprekend zijn om aandacht te hebben voor online dreigingen als voor de beveiliging thuis. Daarom zijn acties en investeringen in cybersecurity noodzakelijk. De CSR onderschrijft in zijn reactie op het rapport de urgentie die spreekt uit het rapport van Verhagen en ziet het als een belangrijk waarschuwingssignaal om Nederland in beweging te krijgen.

Subcommissies

De CSR zette zich in 2016 in op twee belangrijke en grote thema's: het tijdig en effectief inspelen op nieuwe technologische ontwikkelingen; en de rollen en verantwoordelijkheden in het cyberdomein. Beide thema's zijn toekomstgericht, hebben een maatschappelijke en economische relevantie en hangen nauw met elkaar samen. De uitwerking van deze twee thema's vond plaats in subcommissies.

Aan de subcommissievergaderingen nemen een van de voorzitters en een aantal afgevaardigde leden deel. De samenstelling van deze leden is altijd publiek-privaat-wetenschap. Een van de raadsleden is portefeuillehouder. De subcommissie formeert indien nodig een werkgroep met materiedeskundigen, waarbinnen onderwerpen verder inhoudelijk worden uitgediept en uitgewerkt. Ook kan de subcommissie onderzoek uitzetten en daarvoor een begeleidingscommissie inrichten. Het organiseren van dialoog- en reflectiesessies behoort ook tot de mogelijkheden.

Subcommissie Internet of Things

In het werkprogramma 2016 stond het volgende over de subcommissie Internet of Things (IoT) opgenomen:

- *De subcommissie zal een onderzoek laten doen naar de belangrijkste vraagstukken met betrekking tot IoT.*
- *De subcommissie zal een advies opstellen om IoT op verantwoorde wijze te laten landen in onze samenleving.*

Onderzoek Internet of Things (IoT)

Grootschalige adoptie van IoT-toepassingen in onze samenleving is een gegeven: het IoT is geen toekomstmuziek en is er voor een (groot) deel al. Het IoT biedt enerzijds kansen door nieuwe technologische mogelijkheden. Anderzijds brengt het ook bedreigingen met zich mee, bijvoorbeeld op het gebied van cybersecurity. Om de kansen van het IoT te benutten en de bedreigingen te minimaliseren is het van belang hier tijdig op in te spelen. Om deze reden heeft het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), in opdracht van de CSR, een onderzoek uitgevoerd naar het IoT, de impact ervan op de maatschappij en de handelingsperspectieven van relevante stakeholders.

De centrale vraagstelling in dit onderzoek is:
Wat zijn de kansen en bedreigingen van het IoT en hoe kunnen verschillende stakeholders de ontwikkeling van het IoT in Nederland op een positieve manier beïnvloeden?

In april 2016 heeft de subcommisie IoT de nota 'Kansen en risico's van het Internet of Things: handelingsperspectieven' opgesteld. Deze nota is opgenomen in het rapport 'European Foresight Cyber Security Meeting 2016' en is te downloaden vanaf de website van de CSR.

Het WODC-onderzoek en de IoT-nota geven input aan het advies Internet of Things dat in 2017 wordt uitgebracht.

Subcommissie Zorgplichten

In het werkprogramma 2016 stond het volgende over de subcommissie Zorgplichten opgenomen:

- *De subcommissie zal een handreiking opstellen voor bedrijven om de invulling van zorgplichten transparanter te maken.*
- *De subcommissie zal een CSR-advies opstellen om een betere invulling van zorgplichten te stimuleren.*
- *De subcommissie zal een aanzet geven tot harmonisering van de invulling van zorgplichten binnen de Europese Unie. Een uniforme invulling van zorgplichten is noodzakelijk om een 'safe place to do business' te zijn en te blijven.*

Harmonisering en invulling van zorgplichten

De groei van onze economie is voor een groot deel afhankelijk van informatie- en communicatietechnologie (ICT). Dat geldt ook voor het functioneren van onze samenleving. De risico's en de kosten van een mogelijke uitval, verstoring, gebrekkig functioneren en verkeerd gebruik van ICT-producten en -diensten nemen dan ook sterk toe. Consumenten kunnen nauwelijks verhaal halen, omdat leveranciers hun verantwoordelijkheid om digitaal veilige producten en diensten te leveren vrijwel uitsluiten. Ook tussen bedrijven onderling is dit gemeengoed. Dit blijkt uit het onderzoek van de Radboud Universiteit en Onderzoekcentrum Onderneming & Recht, naar zorgplichten van bedrijven op het gebied van cybersecurity: 'Towards harmonised duties of care and diligence in cybersecurity'. De CSR heeft opdracht gegeven voor dit onderzoek, zodat aanbevelingen over het harmoniseren van zorgplichten tussen de lidstaten gegeven kunnen worden aan de Europese Commissie. De whitepaper is daarom opgenomen in het rapport 'European Foresight Cyber Security Meeting 2016' dat vorig jaar is aangeboden aan de Europese Commissie.

In de tweede helft van 2016 is gewerkt aan een 'handreiking zorgplichten' voor bedrijven. Ieder bedrijf heeft zorgplichten op het gebied van cybersecurity. In de praktijk blijkt dat veel bedrijven daarvan nauwelijks op de hoogte zijn. Diverse topjuristen, Radboud Universiteit, Openbaar Ministerie, Nederland ICT, CIO Platform

Nederland en Consumentenbond werkten aan de handreiking mee. Met de handreiking kunnen bedrijven invulling geven aan de zorgplichten op het gebied van cybersecurity.

Subcommissie Onderwijs

In het werkprogramma 2016 stond het volgende over de subcommissie Onderwijs opgenomen:

- *De subcommissie zal de voortgang stimuleren van het advies 'Cybersecurity in het onderwijs en bedrijfsleven.*
- *De subcommissie zal een Summer School initiëren.*

Voortgang advies 'Cybersecurity in het onderwijs en bedrijfsleven'

In oktober 2016 hebben de covoorzitters van de CSR, Dick Schoof en Eelco Blok, gesproken met de heer Dekker, staatssecretaris van onderwijs. Naar aanleiding van het CSR-advies heeft Dekker voorgesteld een module cybersecurity op te nemen in de herziening van het vak Informatica. Ook stelde hij voor dat de CSR aansluit bij de 'Leerlabs' die van start gaan in het kader van de uitwerking van het kerncurriculum in het primair onderwijs. Een van de onderwerpen is bijvoorbeeld 'digitale geletterdheid', waar cybersecurity onder valt. De staatssecretaris deelt de urgentie van het onderwerp cybersecurity. Juist vanwege het belang van dit onderwerp wil hij het structureel inbedden in het kerncurriculum, maar dat kost tijd. Op korte termijn is het idee dat leraren die in de leerlabs samenwerken, met dit onderwerp aan de slag gaan binnen het primair en voortgezet onderwijs. De CSR leverde een bijdrage aan de uitvoering van de gemaakte afspraken en blijft dit ook in het komende jaar doen.

National Cyber Security Summer School

De CSR heeft de National Cyber Security Summer School (NCS3) geïnitieerd naar aanleiding van het advies 'Cybersecurity in onderwijs en bedrijfsleven' dat de raad eind vorig jaar heeft gegeven aan de staatssecretaris van Onderwijs, Cultuur en Wetenschap en de staatssecretaris van Veiligheid en Justitie. Deze crash-course maakt studenten bekend met trends en ontwikkelingen in het cyberdomein, en is een stimulans om als cybersecurity-expert aan de slag te gaan. Ook zijn er stageplaatsen aan de NCS3 gekoppeld. De National Cyber Security Summer School werd uitgevoerd door dcypher in samenwerking met CGI, Nederland ICT, TU Delft en TNO en met ondersteuning van Schiphol Group, Universiteit Leiden, Crisisplan, Nationaal Cyber Security Centre, Universiteit Leiden, Logius en NWO.

Sjoerd van der Hucht Fotografie

In totaal volgden 65 studenten van 22 tot en met 26 augustus 2016 de eerste National Cyber Security Summer School (NCS3). Zij kregen les van cybersecurity-experts van hogescholen en universiteiten, uit het bedrijfsleven en van de overheid. Tijdens de CSR-Challenge 2016 streden de studenten met elkaar voor het beste beleidsadvies voor de CSR. Het beleidsadvies over cybersecurity en smart cities won de CSR-Challenge. Op de tweede plaats is het beleidsadvies over smart homes geëindigd. De andere adviezen hadden betrekking op Smart Transportation, Smart Industry, Wearables, E-Health, Augmented and Virtual Reality. De groep 'smart cities' mocht het advies presenteren in de vergadering van de CSR op 29 september 2016.

Subcommissie Informatie-uitwisseling cybersecurity en cybercrime

In het werkprogramma 2016 stond het volgende over de subcommissie Informatie-uitwisseling cybersecurity en cybercrime opgenomen:

- *De subcommissie zal een bijdrage leveren aan het creëren van een veilige setting om informatie tussen overheid en bedrijfsleven uit te wisselen.*
- *De subcommissie zal nagaan of de informatieverstrekking door het NCSC kan worden verbreed.*
- *De subcommissie zal een bijdrage leveren aan de invulling van het Landelijk Servicepunt E-crime.*

Werkgroep Informatie-uitwisseling cybersecurity en cybercrime

In oktober 2016 is de subcommissie 'Informatie-uitwisseling cybersecurity en cybercrime' gestart. Het doel van deze subcommissie is: het stimuleren van de informatievoorziening tussen publieke en private partijen en onderling door het zoveel mogelijk laten wegnemen van barrières en het vergemakkelijken van het doen van meldingen/aangifte van cyberdelicten.

De resultaten die deze subcommissie wil bereiken zijn:

- Inzicht op hoofdlijnen in de benodigde informatievoorziening bij publieke en private partijen binnen en buiten de vitale sectoren.
- Inzicht in de belangrijkste obstakels die er in deze informatievoorziening zijn.
- Het stimuleren van coalities op deelgebieden.
- Een richtinggevend advies over informatie-uitwisseling.

In november 2016 is een publiek-privaat samengestelde werkgroep geformeerd om te komen tot een inventarisatie en overzicht van initiatieven op het gebied van cybersecurity in Nederland. De 'kaart' van Nederlandse initiatieven is in samenwerking met cybersecurity- en cybercrime-experts tot stand gekomen. Het is niet uitputtend, maar bevat wel organisaties en activiteiten die als zichtbaar en betrouwbaar zijn aangemerkt en voldoende bereik hebben. De CSR heeft als wens dat dit overzicht door een organisatie actueel wordt gehouden, zodat bestaande en nieuwe initiatieven elkaar weten te vinden en elkaar kunnen versterken. De vele cybersecurity- en cybercrime-initiatieven laten zien dat het 'cybersecurity-landschap' een flinke versnippering kent.

4. INTERNATIONAAL

In het werkprogramma 2016 stond het volgende over de subcommissie EU-voorzitterschap opgenomen:

- *De subcommissie zal samenwerking zoeken met andere Cyber Security Raden in Europa en lidstaten stimuleren een dergelijke raad op te richten als die er nog niet is.*
- *De subcommissie zal een bijeenkomst organiseren aan de vooravond van hoogambtelijke bijeenkomst met invloedrijke personen, waarin relevante onderwerpen, zoals zorgplichten, Internet of Things en publiek-private samenwerking aan de orde komen.*
- *De subcommissie zal in januari 2016 het tweede nummer van het CSR Magazine uitgeven, met als thema 'Cybersecurity in de EU'.*

Stimuleren oprichting Cyber Security Raden binnen de EU

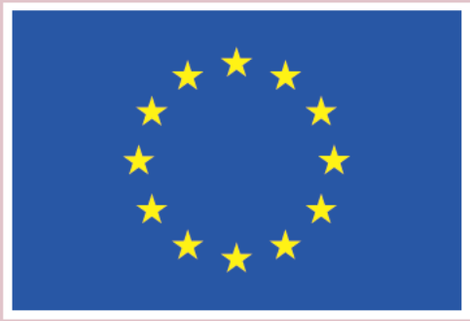
In het kader van het EU-voorzitterschap en kennisdeling tussen de EU-lidstaten, stimuleert de Cyber Security Raad (CSR) de oprichting van gelijksoortige raden met publiek-privaat-wetenschappelijke samenstelling in andere EU-landen. Verschillende lezingen zijn gegeven door de secretaris van de raad.

De CSR is benaderd door het Deense Nationaal Cyber Security Centrum met de vraag kennis en ervaring te delen voor de oprichting van een Deense Cyber Security Raad. De secretaris heeft in een aantal sessies met verschillende Deense stakeholders presentaties gegeven over de opzet en aanpak van de Nederlandse CSR. De Denen hebben besloten om in eerste instantie voor een jaar een raad op te richten en daarna te evalueren.

Ook vanuit België is de vraag gesteld om kennis en ervaring te delen met de Belgische Cyber Security Raad. Deze raad is in zijn geheel samengesteld uit private partijen en wil graag de publieke sector erbij betrekken. De secretaris van de CSR heeft een vergadering bijgewoond en kennis en ervaring gedeeld over de Nederlandse werkwijze.

High-level meeting cybersecurity

Op 12 en 13 mei 2016 organiseerden de NCTV en het Nationaal Cyber Security Centrum een high-level meeting cybersecurity in Amsterdam, passend binnen het EU-voorzitterschap van Nederland. Deelnemers aan de bijeenkomst waren ambtenaren (directeuren-generaal) die verantwoordelijk zijn voor cyberveiligheid, CEO's en leden van de raad van bestuur van organisaties die zich bezighouden met veiligheid, ICT en vitale infrastructuur. De 'High Level Meeting' bestond uit plenaire en interactieve focussessies waarbij de discussie ging over onderwerpen als standaardisatie van hard- en software, responsible disclosure en educatie, om zo in te kunnen spelen op ontwikkelingen als Internet of Things, interconnectiviteit en toenemende complexiteit en afhankelijkheid van ICT-producten en -diensten. Publiek-private samenwerking is daarbij essentieel voor een breed en effectief antwoord op huidige en toekomstige cyberdreigingen. Bureau CSR gaf tijdens deze high-level meeting een workshop, gericht op trends, disruptieve technologieën, publiek-private samenwerking en de werkwijze van de Nederlandse CSR. In samenwerking met de Belgische en Deense CSR (io) werden lessons learned gepresenteerd over de oprichting en het functioneren van zo'n raad. Tijdens de discussie bleek dat lidstaten interesse hebben in een CSR en onderlinge samenwerking op strategisch niveau via deze raden, maar dat publiek-private samenwerking in veel EU-landen nog in de kinderschoenen staat.






Europese Toekomstverkenning Cybersecurity

Op initiatief van de CSR werd op 11 mei 2016 in Haarlem de eerste European Foresight Cyber Security georganiseerd. Binnen de EU wordt onderkend dat er behoefte is aan toekomstgericht, strategisch advies over nieuwe technologische ontwikkelingen en bijbehorende cybersecurity risico's. Deze Europese Toekomstverkenning Cybersecurity komt aan deze behoefte tegemoet. Meer dan twintig internationale en invloedrijke deskundigen op het gebied van cybersecurity en IT uit de publieke, private en wetenschappelijke sector discussieerden over de thema's Internet of Things en harmonisering van zorgplichten binnen de EU. Op basis van deze discussie werd een rapport met aanbevelingen geschreven. Covoorzitter van de Cyber Security Raad, Dick Schoof, heeft op 21 september 2016 het EU-rapport 'European Foresight Cyber Security 2016' overhandigd aan Michael Hager, chef-kabinet van EU-commissaris Günther Oettinger, Digital Economy & Society.

Doorontwikkeling Europees beleid

Commissaris Oettinger heeft tijdens de overhandiging de intentie uitgesproken om samen met de CSR te willen werken aan een tweede European Foresight Cyber Security (toekomstverkenning cybersecurity). Verder heeft de CSR commissaris Oettinger en ENISA (European Union Agency for Network and Information Security) informatie verstrekt over het concept en de uitwerking van de eerste National Cyber Security Summer School in Nederland. Ook heeft de CSR informatie verstrekt over de Nederlandse cybersecurity-aanpak en de publiek-private samenwerking die ons land op dit vlak kent. De Europese Commissie gebruikt deze informatie om de kennis over publiek-private samenwerking in de lidstaten te verhogen. De aanbevelingen in het rapport 'European Foresight Cyber Security 2016' zullen als belangrijke input worden gebruikt voor de verdere doorontwikkeling van Europees beleid.

Deelnemers toekomstverkenning

Belgian Cyber Security Council, CSIS Security Group, CSO Confidential Ltd., Energinet DK, European Union Agency for Network and Information Security (ENISA), Directorate General for Communications Networks, Content & Technology (DG CONNECT, European Commission), Europol, European Cyber Security Group (ECSG), Harvard University, International Federation for Information Processing (IFIP), Internet Society, NATO Communications and Information Agency, Microsoft, Radboud University, Royal Philips, Symantec, World Economic Forum USA en de Nederlandse CSR.




Speciale EU-uitgave CSR Magazine

In januari 2016 is de tweede editie van het CSR Magazine verschenen. Het is een speciale EU-uitgave waarin diverse auteurs ingaan op cybersecurity-onderwerpen die spelen binnen de EU en welke rol de CSR kan spelen.
In de tweede editie van het CSR Magazine legt Staatssecretaris Klaas Dijkhoff van Veiligheid en Justitie uit welke ambities Nederland heeft als het gaat om cybersecurity tijdens het EU-voorzitterschap in de eerste helft van 2016. Jos Nijhuis, CEO Schiphol Group en lid CSR, benadrukt het belang van publiek-private samenwerking. Nicolas Castellon, cybersecurity-onderzoeker, gaat in op de governance van cyberspace. Paul Timmers, directeur Directoraat-Generaal Connect EU, gaat in op de barrières die geslecht moeten worden om te komen tot één Europese digitale markt. Lokke Moerel, Senior of councel bij Morrison & Foerster LLP en lid CSR, schetst belangrijke Amerikaanse cyberontwikkelingen die hun weg zullen vinden naar Europa. Andreas Swab, rapporteur NIB-richtlijn (Netwerk- en Informatiebeveiliging) voor het Europees Parlement gaat in op die richtlijn en Steve Purser van ENISA vertelt hoe zijn organisatie EU-lidstaten helpt om deze richtlijn te implementeren. Wil van Gemert, adjunct-directeur Operatiën bij Europol, gaat in op cybercrime en strategische samenwerking om dit een halt toe te roepen. Alexander Seger van het Cybercrime Convention Committee Programme Office licht de Boedpast-conventie toe.
Naast deze auteurs zijn er nog diverse andere auteurs die een belangrijk Europees onderwerp bespreken. Het magazine is te downloaden van de website van de CSR.

5. OVERIGE ADVIEZEN EN ACTIVITEITEN

De Cyber Security Raad (CSR) voerde een aantal overige activiteiten uit, die niet vallen onder een subcommissie. Zo is er op verzoek van derden advies gegeven, hebben raadsleden hun medewerking verleend aan evenementen en is de media benaderd om diverse onderwerpen voor het voetlicht te brengen.

Adviezen

Op verzoek van de Koninklijke Nederlandse Beroepsorganisatie van Accounts (NBA) heeft de CSR gereageerd op haar 'public management letter cyber security'. De CSR gaf vier belangrijke signalen af:

1. Cybersecurity is een onderwerp voor de bestuurskamer;
2. Stel vast welke kroonjuwelen een bedrijf heeft;
3. Neem maatregelen tegen zwakke schakels, bijvoorbeeld in de keten;
4. Wees in staat te incasseren en te reageren op cyberincidenten.

Tijdens de consultatieronde voor een nieuwe Corporate Governance Code vraagt de CSR aandacht voor het onderwerp cybersecurity in de boardroom. Het is noodzaak dat het niveau van digitale veiligheid in het bedrijfsleven en in Nederland in het algemeen omhoog gaat. Daarom verzocht de CSR de Monitoring Commissie Corporate Governance Code om het onderwerp cybersecurity op te nemen in de beginselen en best practises van de nieuwe Corporate Governance Code. Dit advies werd overgenomen en in de code wordt nu gewezen op de noodzakelijke beheersing van risico's op het gebied van cybersecurity. Paragraaf 1.5.1 lid iii luidt nu als volgt: 'de toepassing van informatie- en communicatietechnologie van de vennootschap, in het bijzonder de beheersing van risico's op het gebied van cybersecurity'.

Activiteiten

Het SC Congres werd in april 2016 georganiseerd door SC Magazine UK. Bart Hogendoorn, lid van de CSR nam plaats in een panel. De discussie stond in het teken van 'EU Data Protection regulation, Cybercrime, attacks on critical infrastructure/IoT en cyberwarfare'.

In april 2016 voegde de Elsevier een bijlage toe over bedrijfscontinuïteit. De CSR werkte hieraan mee. De bijlage bevatte interviews van Lokke Moerel, hoogleraar aan de Tilburg University, Gerrit van der Burg, lid van het College van procureurs-generaal en lid van CSR namens Openbaar Ministerie, Michel van Eeten, Hoogleraar Technische Bestuurskunde TU Delft en lid van CSR, Ben Voorhorst, COO TenneT, lid van CSR namens de Vitale Infrastructuur en Marcel Krom, CIO PostNL, lid van CSR namens CIO Platform. Lokke Moerel gaat in haar verhaal in op de juridische gevolgen van datalekken, deelt haar internationale ervaring en legt uit dat bedrijven zorgplichten hebben op het gebied van cybersecurity. Gerrit van der Burg gaat in op de rol van het OM bij het bestrijden van cybercrime en Michel van Eeten legt de economische mechanismen rondom cybersecurity uit. Tot slot gaan Ben Voorhorst en Marcel Krom in op ketenveiligheid.

De CSR was in september 2016 kennispartner van NRC Live 'CyberinSecurity'. Eelco Blok, covoorzitter van de CSR, Lokke Moerel, Bibi van den Berg en Ben Voorhorst adresseerden de onderwerpen 'urgentie van cybersecurity', IoT, ketenveiligheid en zorgplichten.

Een aantal keer benaderde de CSR de media om bewustwording te creëren rondom belangrijke onderwerpen. Zo is er veel aandacht besteed aan het onderwerp 'cybersecurity in de keten'. De raad constateert dat maar weinig bedrijven en overheden zicht hebben op de digitale ketens waar zij afhankelijk van zijn en riep alle bedrijven, overheden en sectoren op te onderzoeken van welke digitale ketens zij deel uitmaken, welke risico's zij lopen en welke cyberveiligheidsmaatregelen zij zouden moeten treffen.

Ook hebben de media aandacht besteed aan de reactie van de CSR op het Cybersecurity Beeld Nederland 2016. De raad stelt dat cyberveiligheid een normaal onderdeel is van al ons dagelijks handelen, net zoals we op onze fysieke veiligheid letten. Publieke en private partijen moeten daar veel meer op inzetten en op investeren.

Verder stonden de media uitgebreid stil bij het onafhankelijke adviesrapport van mevrouw Verhagen, dat zij op verzoek van de CSR heeft opgesteld, en de reactie van de raad daarop. De CSR onderschrijft de urgentie die spreekt uit het rapport van Verhagen en het advies aan regering, politici, beleidsmakers, bestuurders, toezichthouders, bedrijven en burgers om structureel aandacht te geven aan cybersecurity. Ook is structurele financiering nodig. De CSR ziet het adviesrapport Verhagen als een belangrijk waarschuwingssignaal om Nederland op het terrein van cybersecurity in beweging te krijgen. Een brede en nationale aanpak is nodig om Nederland in alle lagen van de economie en maatschappij op een hoger niveau van cybersecurity te krijgen. Cybersecurity is randvoorwaarde voor een welvarend digitaal Nederland.