CSR Cyber Security Raad

WERKPROGRAMMA 2018-2019

De CSR Meerjarenstrategie bevat een duidelijke focus waarmee de raad in de komende vier jaar aan de slag gaat. Het streven van de raad is om gemiddeld drie adviezen per jaar te publiceren. De raad beschikt over een gevarieerd repertoire aan werkwijzen ('klassieke' adviezen, handreikingen, gesprekken en bijeenkomsten) die afgewogen worden ingezet. Ook voeren individuele leden boardroomgesprekken bij (publieke) organisaties en initieert de raad verschillende activiteiten die de impact van zijn adviezen helpen te vergroten, zoals de National Cyber Security Summer School (NCS3).

Op basis van de CSR Meerjarenstrategie 2018-2021 is de agendering voor de periode 2018-2019 bepaald. De onderwerpen volgen uit de strategische thema's zoals beschreven in de meerjarenstrategie. Dit zijn:

1. Regie en sturing
2. Groeiende (digitale) afhankelijkheid
3. Handhaving en toezicht
4. Nieuwe technologieën

Specifieke onderwerpen

Aan de hand van de strategische thema's gaat de raad in de komende twee jaar met een vijftal specifieke onderwerpen aan de slag. De onderwerpen zijn gerelateerd aan de strategische thema's regie en sturing, groeiende (digitale) afhankelijkheid en nieuwe technologieën. Alle onderwerpen dragen bij aan het versterken van de cybersecurity van Nederland en vormen de leidraad voor de agendering van de raad. De onderwerpen worden al dan niet uitgediept in subcommissies.

De onderwerpen waartoe de raad in de periode 2018 - 2019 verschillende producten en adviezen voor zal ontwikkelen, zijn:

1. Nationale Cyber Security Agenda (NCSA)
2. Nieuwe technologieën
3. Meldplicht Datalekken
4. Industrial Automation & Control Systems (IACS)
5. Evaluatie rapport Verhagen:
   'De economische en maatschappelijke noodzaak van meer cybersecurity - Nederland digitaal droge voeten'

Daarnaast houdt de raad scherp oog voor de actualiteit. Het cyberlandschap is continu in beweging. Het is een permanente ratrace en dat dwingt ons om continu alert en voorbereid te zijn op alle mogelijke scenario's. Dat geldt uiteraard ook voor ons als raad. De actualiteit bepaalt onze agenda, dus is net als de meerjarenstrategie ook het werkplan een levend document dat we waar nodig aanvullen en aanpassen aan actuele ontwikkelingen.

1. Nationale Cyber Security Agenda (NCSA)

Het kabinet heeft in het regeerakkoord 'Vertrouwen in de toekomst' aangekondigd te willen komen tot een ambitieuze cybersecurity-agenda, die onder andere moet leiden tot standaarden voor IoT-apparaten, software-aansprakelijkheid, versterken van het Nationaal Cyber Security Centrum (NCSC), stimuleren van cybersecurity-onderzoek en het verbeteren van voorlichtingscampagnes. Dit wordt vertaald naar de Nederlandse Cybersecurity Agenda (NCSA) onder verantwoordelijkheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in samenwerking met verschillende partijen. De NCSA kan worden gezien als een update van de laatste Cyber Security Strategie II uit 2013. De NCSA moet ertoe bijdragen dat Nederland een veilig, open en welvarende samenleving blijft en dat we als land in de voorhoede blijven als het gaat om digitalisering. De agenda verschijnt in het voorjaar van 2018 en de CSR zal bij het vaststellen van de NCSA een adviserende rol hebben. De raad gaat zich inzetten om de verschillende agenda's, zoals de Cybersecurity Strategie 2.0: van bekwaam naar bewust van het ministerie van Justitie en Veiligheid, de Digitale Agenda: vernieuwen, vertrouwen en versnellen van het ministerie van Economische Zaken en Klimaat en de Defensie Cyber Strategie van het ministerie van Defensie, te clusteren en te komen tot een integrale visie voor de NCSA.

2. Nieuwe technologieën

In de aankomende jaren zullen veel nieuwe technologieën en datastromen worden ingezet, zoals robotica, biometrie, Internet of Things, kustmatige intelligentie, kwantum computing en big data. De mogelijke inzet van nieuwe technologieën en datastromen kan positief bijdragen aan de digitale weerbaarheid van Nederland en het verzilveren van kansen voor een digitaal veilige economie. De raad laat hiertoe wetenschappelijk onderzoek uitvoeren naar de mogelijke inzet van nieuwe technologieën als het gaat om cybersecurity. Op basis van het rapport zal de raad een advies uitbrengen over hoe het niveau van cybersecurity verhoogd kan worden door de inzet van nieuwe technologieën.

3. Meldplicht Datalekken

Sinds 1 januari 2016 geldt de Meldplicht Datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). In Nederland zijn de gegevens over individueel gemelde datalekken vertrouwelijk. Wel kan de AP in het algemeen informatie geven over het aantal meldingen binnen specifieke sector(en).

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Deze privacywetgeving geldt in de hele Europese Unie (EU) en vervangt de Wet bescherming persoonsgegevens (Wbp). De AVG zorgt onder meer voor versterking en uitbreiding van privacyrechten, meer verantwoordelijkheden voor organisaties, dezelfde bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.
De raad wil wetenschappelijk onderzoek laten uitvoeren naar het effect van openbaar melden van datalekken binnen de kaders en mogelijkheden van de Meldplicht Datalekken en de AVG. Het openbaar maken van meldingen van datalekken kan mogelijk een positieve bijdrage leveren aan cybersecurity. Er kan bijvoorbeeld informatie beschikbaar komen over de beleidseffecten van bepaalde maatregelen. Bij het openbaar maken van meldingen kan echter ook het grondrecht privacy in geding komen.

4. Industrial Automation & Control Systems (IACS)

Steeds meer fysieke objecten worden aan de digitale infrastructuur gekoppeld. Hierbij gaat vooral aandacht uit naar ICT en Industrial Automation & Control Systems (IACS) heeft nauwelijks prioriteit, terwijl IACS voornamelijk ingezet wordt om de infrastructuur van Nederland te bedienen. In het kader van de bescherming van onze vitale infrastructuur speelt IACS daarmee een essentiële rol. De levensduur van industriële controlesystemen, zoals ICS/SCADA, is vele malen langer dan IT. Waar IT-apparatuur normaliter binnen drie tot vijf jaar wordt afgeschreven is het gebruikelijk dat IACS-apparatuur vijftien tot twintig jaar actief blijft functioneren. Bij de ontwikkeling van IACS wordt er beredeneerd vanuit functionaliteitsoogpunt en niet vanuit cybersecurity. Een doelbewuste verstoring van vitale sectoren kan door sabotage, het uitbuiten van de kwetsbaarheden in IACS, leiden tot economische schade en maatschappelijke ontwrichting.
De raad wil wetenschappelijk onderzoek laten uitvoeren naar de belangrijkste problematiek bij IACS als het gaat om cybersecurity en een advies voor een aanpak hiertoe uitbrengen.

5. Evaluatie rapport Verhagen

Op verzoek van de CSR heeft mevrouw mr. drs. Herna Verhagen, CEO PostNL, onafhankelijk onderzoek gedaan naar de stand van zaken in Nederland op het gebied van cybersecurity. Het adviesrapport ‘De economische en maatschappelijke noodzaak van meer cybersecurity - Nederland digitaal droge voeten’ is op 6 oktober 2016 gepresenteerd en overhandigd aan minister-president drs. Mark Rutte en voorzitter VNO-NCW drs. Hans de Boer. De adviezen uit het rapport gaan over de rol van de overheid, de rol van de private sector, de samenwerking tussen beide én digitale vaardigheden.
De CSR wil graag inzicht krijgen in hoeverre de adviezen van Verhagen zijn opgevolgd en de voortgang van de adviezen uit het rapport stimuleren om de impact ervan te vergroten.

RESULTATEN

Nationale Cyber Security Agenda (NCSA)

De raad zal:

- een advies opstellen om vanuit een integrale visie de koers van de NCSA te bepalen.

Nieuwe technologieën

De raad zal:

- op basis van onderzoek een advies opstellen over de inzet van nieuwe technologieën ten behoeve van cybersecurity.

Meldplicht Datalekken

De raad zal:

- op basis van onderzoek advies opstellen over het al dan niet openbaar melden van datalekken in Nederland.

Industrial Automation & Control Systems (IACS)

De raad zal:

- op basis van onderzoek advies opstellen over de aanpak van de belangrijkste problematiek bij IACS als het gaat om cybersecurity.

Evaluatie rapport Verhagen

De raad zal:

- de impact van het rapport Verhagen op hoofdlijnen evalueren.

CSR Cyber Security Raad