Nieuwsbrief

December 2024, Nummer 2

Deze nieuwsbrief geeft een overzicht van het werk van de Cyber Security Raad (de raad) in de afgelopen maanden.

Kennismaking en dialoog met de minister van Justitie en Veiligheid

Op 28 november jl. bracht de nieuwe minister van Justitie en Veiligheid, David van Weel, een bezoek aan de raad voor een eerste kennismaking en een dialoog over een aantal belangrijke cybersecurity-onderwerpen. Maatschappelijke weerbaarheid is een topprioriteit in zijn beleid en heeft een belangrijke digitale component. In het gesprek kwamen kansen en risico´s m.b.t. specifieke cybersecurityonderwerpen ter sprake, mede gezien nieuwe technologische ontwikkelingen. De huidige geopolitieke situatie leidt tot nog hogere digitale dreigingen en meer risicovolle afhankelijkheden. Extra aandacht voor cyberweerbaarheid is daarom essentieel, waarbij in de dialoog uitgebreid werd ingegaan op onze digitale infrastructuur, vanuit een nationaal en EU-perspectief. De unieke samenstelling van de raad zorgt ervoor dat standpunten uit diverse sectoren kunnen worden meegenomen. Dit zal ook in de toekomst leiden tot breedgedragen adviezen over bovenstaande onderwerpen. Die adviezen zullen gericht zijn aan het kabinet in het algemeen, en aan minister van Weel in het bijzonder, in zijn rol als eigenaar van de raad.

Follow-up CSR-advies ‘Verkleinen van de weerbaarheidskloof’

Eind november 2024 ontving de raad van de minister van Economische Zaken een beleidsreactie op het CSR Advies 'Verkleinen van de Cyberweerbaarheidskloof' dat de raad in juni van dit jaar heeft gepubliceerd en persoonlijk is overhandigd aan zijn voorgangster Micky Adriaansens. Deze reactie werd mede namens de minister van Justitie en Veiligheid gestuurd, aan wie het advies eveneens gericht was. In de brief is uitgebreid aangegeven welke stappen er in publiek-private samenwerking gezet of voorgenomen zijn om de negen gerichte adviezen van de raad zo goed mogelijk in te vullen. Ook wordt vermeld dat het ministerie van EZ samen met het ministerie van JenV en het Digital Trust Center (DTC) in het Actieprogramma Veilig Ondernemen 2023-2026 structureel samenwerken met de politie en het bedrijfsleven om de cyberweerbaarheid van het mkb te verhogen. De raad zal de verdere ontwikkelingen blijven volgen.

Reactie van de CSR op het Cybersecuritybeeld Nederland (CSBN) 2024

Op 28 oktober jl. verscheen het CSBN 2024. Het document schetst een overkoepelend beeld van het huidige cybersecurity-speelveld in ‘turbulente tijden’. In zijn reactie op het CSBN onderschrijft de raad de geschetste toepassingen van artificiële intelligentie (AI), de symbiose tussen cybercriminelen en statelijke actoren en de arbeidsmarktproblematiek (zie ook de CSR Signaalbrief hierover). De raad geeft aan dat de diverse typen digitale dreigingen in een breder perspectief passen, waarin de veranderende wereldorde ook kansen biedt voor veilige digitalisering in de EU, en in Nederland in het bijzonder.

Voorgenomen CSR advies over digitale communicatie-infrastructuur

In de raadsvergadering van juni 2024 besloot de raad een subcommissie in te stellen die zich zal richten op de securityrisico's van de digitale communicatie-infrastructuur van Nederland (SECCOM). In de loop van 2025 wil SECCOM de regering adviseren over het huidige beeld – op macroniveau – en het advies voorzien van mogelijke maatregelen. De eerste concrete stappen zijn inmiddels gezet. Er is een charter ontworpen dat de aanleiding, werkwijze en tijdlijn weergeeft. Vervolgens is op 19 november een workshop georganiseerd met experts uit het telecom- en internetveld. Hierin zijn de strategische aanbevelingen vanuit de EU over dit onderwerp ingebracht en gewogen. Dit is richtinggevend voor het vervolg, waarbij een extern onderzoek wordt ingezet als opmaat naar een uiteindelijk advies.

AI-ontwikkelingen in relatie tot cybersecurity

De raad buigt zich momenteel over artificiële intelligentie (AI) als technologie in de context van cybersecurity. Vooral de waarborging van de authenticiteit van informatie baart zorgen. Binnen een paar jaar zijn 'echt' en 'niet-echt' niet meer van elkaar te onderscheiden. De kwaliteit van AI-toepassingen gaat omhoog en de impact ervan wordt almaar groter. AI kan structuren aantasten, waardoor het belang van incident response steeds prominenter wordt. Bestuurders lopen op het gebied van AI tegen allerlei dilemma' s aan en de vraagstukken zijn taai. Voor nu is al wel duidelijk dat er behoefte is aan informatie. Informatie waarin de relatie met de bestuurlijke dynamiek duidelijk wordt uitgelegd en die praktisch relevant is. De raad verkent op dit moment of een bijdrage op dit vlak mogelijk is, met focus op de inzet van AI bij cybersecurity-toepassingen enerzijds en het waarborgen van de cybersecurity van AI-toepassingen anderzijds.

Namens de raad wensen wij u fijne feestdagen toe en een gezond, digitaal inspirerend en veilig 2025!

© loops7 / Getty Images

CYBER SECURITY RAAD
p/a Nationaal Coördinator Terrorismebestrijding en Veiligheid
Korte Voorhout 7 | 2511 CW I Den Haag
Postbus 20011 I 2500 EA I Den Haag

Telefoon: 070 751 5333 (secretariaat)
E-mail: info@cybersecurityraad.nl

www.cybersecurityraad.nl