Ministerie van Justitie en Veiligheid

Minister van Justitie en Veiligheid

Ministerie van Justitie en Veiligheid

Datum
3 juli 2023

Ons kenmerk
4754845

nota

Cybersecuritybeeld Nederland 2023

1. Aanleiding

Het Cybersecuritybeeld Nederland 2023 (CSBN2023) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de digitale weerbaarheid en digitale risico's. De focus van het CSBN2023 ligt op de nationale veiligheid

2. Geadviseerd besluit

Aan de minister wordt gevraagd:

- Kennis te nemen van het Cybersecuritybeeld Nederland 2023.
- In te stemmen met de verzending van de Aanbiedingsbrief Cybersecuritybeeld Nederland inclusief het CSBN2023 aan de Tweede Kamer.

3. Kernpunten

1. De veiligheid van digitale processen is en blijft essentieel in onze sterk gedigitaliseerde maatschappij en is dus onlosmakelijk verbonden met de nationale veiligheid.
2. De digitale dreiging voor Nederland is onverminderd groot. Wel is die dreiging voortdurend aan verandering onderhevig. Zo is er sprake van geopolitieke verharding, met de Russische oorlog tegen Oekraïne als prominent voorbeeld. Die oorlog heeft daarnaast (mede) geleid tot een opleving van hacktivisme: het uit ideologische overwegingen uitvoeren van cyberaanvallen. Bij verdere escalatie van de oorlog kan de digitale dreiging abrupt veranderen en kunnen Nederlandse belangen worden geraakt.
3. De in het CSBN 2022 benoemde strategische thema's leiden nog onverkort tot complicaties voor risicobeheersing. Het betreft de volgende strategische thema's:
    - Risico's vormen de keerzijde van een gedigitaliseerde samenleving.
    - Digitale ruimte is speelveld voor regionale en mondiale dominantie.
    - Cybercriminaliteit is industrieel schaalbaar, weerbaarheid nog niet.
    - Marktdynamiek compliceert beheersing digitale risico's.
    - Samenhangend en geïntegreerd risicomanagement staat nog in de kinderschoenen.
    - Beperkingen in digitale autonomie beperken ook digitale weerbaarheid.

Enkele veranderingen ten opzichte van vorig jaar zijn opgevallen:
- de extra eisen voor digitale veiligheid die onder andere voortkomen uit nieuwe Europese wet- en regelgeving;
- het onder druk staan van de verzekerbaarheid van digitale risico's;
- de steeds verder toenemende onderlinge verwevenheid binnen een breder – niet alleen digitaal - ecosysteem;
- de gelegenheidsstructuur die het digitale ecosysteem vormt voor cyberaanvallen.

4. Het verkleinen van de in het CSBN 2022 benoemde scheefgroei tussen de digitale dreiging en de weerbaarheid blijft een grote opgave. De aard van de digitale risico's voor de nationale veiligheid is niet fundamenteel gewijzigd.
5. Operationele technologie (OT) is een kwetsbare bouwsteen voor vitale processen. OT speelt een centrale rol in het aansturen, monitoren en beheren van fysieke processen binnen (vitale) organisaties. De veiligheid van OT is van vitaal belang, maar kent belangrijke uitdagingen. Ondanks groeiende aandacht voor de weerbaarheid van OT, is er ruimte voor verbetering.
6. Bijzondere kenmerken van digitale risico's vragen een bredere manier van beheersing dan andere risico's. Zo maken digitale risico's onderdeel uit van een breder, dynamisch én complex risicopalet en is de digitale ruimte een uiterst complex systeem dat zich lastig laat doorgronden. Bij een bredere manier van beheersing valt te denken aan een benadering waarin digitale risico's worden beschouwd als een integraal onderdeel van de risico's voor de nationale veiligheid. Verder kan de invalshoek van 'assume breach' (ga ervan uit dat er een cyberincident is) behulpzaam zijn.

4. Toelichting

4.1 Politieke context
Het CSBN2023 vormt een van de elementen voor de mogelijke bijstelling van het actieplan bij de Nederlandse Cybersecuritystrategie. Gedurende de looptijd van de Nederlandse Cybersecuritystrategie bestaat de mogelijkheid om het actieplan te herijken om op deze manier in te kunnen spelen op de snelle ontwikkelingen in het cybersecurityveld. Aan de Kamer is toegezegd dat zij jaarlijks worden geïnformeerd over de voortgang van de strategie en het bijbehorende actieplan.

4.2 Krachtenveld
Het CSBN is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Daarbij is nauw samengewerkt met het Nationaal Cyber Security Centrum (NCSC). Ook is samengewerkt met onder andere de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de politie. Het CSBN kent verder een uitgebreid validatietraject, waarbij de concepttekst voorgelegd wordt aan externe partners ter commentaar. Na het verwerken van het verzamelde commentaar wordt de definitieve tekst opgemaakt en door de NCTV vastgesteld.

4.4 Ontwikkelingen hiervoor

Het CSBN is een jaarlijks terugkerende analyse die sinds 2012 wordt gepubliceerd.

5. Informatie die niet openbaar gemaakt kan worden

5.1 Toelichting

De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.