Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1045

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 juli 2023

Hierbij bied ik u het Cybersecuritybeeld Nederland 2023 (CSBN 2023) aan. Het CSBN 2023 biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en digitale risico's. De focus ligt daarbij op de nationale veiligheid. Daarnaast heeft het CSBN 2023 tot doel om te reflecteren op de strategische thema's die in het CSBN 2022 zijn toegelicht (Kamerstuk 26 643, nr. 891).

De veiligheid van digitale processen is en blijft essentieel in onze sterk gedigitaliseerde maatschappij en is dus onlosmakelijk verbonden met de nationale veiligheid. In het CSBN 2023 wordt geconcludeerd dat de digitale dreiging voor Nederland onverminderd groot is. 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. Bij verdere escalatie van de oorlog kan de digitale dreiging abrupt veranderen en kunnen Nederlandse belangen worden geraakt.

De NCTV heeft bij de totstandkoming van het CSBN 2022 in samenwerking met partners strategische thema's geïdentificeerd die ieder op zich en in samenhang complicaties vormen voor risicobeheersing. Het betreft de volgende strategische thema's:

- 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.

Deze thema's leiden nog onverkort tot complicaties voor risicobeheersing. Wel zijn enkele veranderingen ten opzichte van vorig jaar opgevallen:

kst-26643-1045
ISSN 0921 - 7371
's-Gravenhage 2023

Extra eisen voor digitale veiligheid, maar het kost tijd voor deze effect hebben.

Een belangrijke verandering die de digitale weerbaarheid de komende jaren kan vergroten, zijn de extra eisen voor digitale veiligheid. De bewustwording over en verdere uitwerking en implementatie van dat alles, vergt wel de nodige doorlooptijd.

Verzekerbaarheid digitale risico's onder druk

De verzekerbaarheid van digitale risico's staat onder druk om uiteenlopende redenen. Deze redenen kunnen er uiteindelijk toe leiden dat financieel gezonde organisaties ten onder gaan aan de schade die zij lijden door cyberincidenten.

Onderdeel zijn van een breder ecosysteem compliceert risicobeheersing

Onderdeel zijn van een breder ecosysteem heeft voordelen, zoals het profiteren van schaalvoordelen en specialistische kennis, waaronder op het terrein van cybersecurity. Onderdeel zijn van een breder ecosysteem compliceert tegelijkertijd ook risicobeheersing. Zo bestaat lang niet altijd inzicht in afhankelijkheden en kwetsbaarheden in het bredere ecosysteem.

Het digitale ecosysteem vormt een gelegenheidsstructuur voor cyberaanvallen

Cybercriminelen zijn afhankelijk van een malafide digitaal ecosysteem. Deze afhankelijkheid geldt ook voor legale diensten, bijvoorbeeld webhosting of het afnemen van communicatiediensten als VPN. Deze afhankelijkheid biedt kansen voor het verhogen van digitale weerbaarheid tegen cybercriminelen én tegen andere kwaadwillenden.

Daarnaast wordt in het CSBN 2023 geconcludeerd dat het verkleinen van de in het CSBN 2022 benoemde scheefgroei tussen de digitale dreiging en de weerbaarheid een grote opgave blijft. Ook wordt gewezen op de bijzondere kenmerken van digitale risico's. Die vragen om een bredere manier van beheersing dan bij 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 gaat het CSBN 2023 in op operationele technologie (OT). OT speelt een centrale rol in het aansturen, monitoren en beheren van fysieke processen binnen (vitale) organisaties. De veiligheid van de OT is van vitaal belang, maar kent belangrijke uitdagingen. Ondanks groeiende aandacht voor de weerbaarheid van OT, is er ruimte voor verbetering.

Bovenstaande inzichten worden uitgebreid toegelicht in het CSBN 2023. De strategische en beleidsmatige opvolging van het CSBN 2023 volgt in de Voortgangsrapportage op de Nederlandse Cybersecuritystrategie die aan uw Kamer is toegezegd voor het najaar van 2023. In deze voortgangsrapportage wordt u geïnformeerd over de eventuele bijstelling van de Nederlandse Cybersecuritystrategie en de voortgang.

Om in te kunnen spelen op trends, actuele dreigingen en risico's, worden de acties uit de Nederlandse Cybersecuritystrategie in de loop van de tijd

uitgewerkt, aangepast of versterkt. Het actieplan kan daarom jaarlijks op punten worden geactualiseerd, waardoor adequaat ingespeeld kan worden op de snelle ontwikkelingen in relatie tot digitale veiligheid.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius