Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 891

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 juli 2022

Met deze brief stuur ik u het Cybersecuritybeeld Nederland 2022 (CSBN2022). Tevens informeer ik u dat de reactie van het kabinet hierop volgt in de nieuwe Nederlandse Cybersecuritystrategie (NLCS) die in oktober aan uw kamer wordt toegestuurd. U ontvangt dan ook de kabinetsreactie op het rapport van de Onderzoeksraad voor Veiligheid (OVV) «Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix». Over deze verzending heb ik de OVV reeds geïnformeerd. Een afschrift hiervan treft u in de bijlage bij deze brief.

Het CSBN2022 biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en tot slot de risico's. De focus ligt daarbij op de nationale veiligheid. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft bij de totstandkoming van het CSBN2022 in samenwerking met partners strategische thema's geïdentificeerd die nu en de komende jaren relevant zijn voor de digitale veiligheid van Nederland:

Risico's vormen de keerzijde van een gedigitaliseerde samenleving.
De Nederlandse samenleving is in hoge mate gedigitaliseerd. COVID-19 heeft dit proces verder versneld. Die afhankelijkheid van digitale processen maakt ons ook kwetsbaar voor uitval en activiteiten van kwaadwillenden.

Digitale ruimte is speelveld voor regionale en mondiale dominantie.
Staten gebruiken de digitale ruimte structureel én intensief voor de behartiging van hun geopolitieke belangen. Cyberaanvallen, bijvoorbeeld voor het vergaren van inlichtingen, zijn het «nieuwe normaal».

Cybercriminaliteit is industrieel schaalbaar, weerbaarheid nog niet.
Zware cybercriminaliteit is schaalbaar geworden en maakt daardoor meer slachtoffers, meer schade en is lucratiever dan ooit. Het schaalbaar maken en houden van de weerbaarheidsketen is een grote uitdaging.

kst-26643-891
ISSN 0921 - 7371
's-Gravenhage 2022

Marktdynamiek compliceert de beheersing van digitale risico's.
Op digitale markten komen vraag en aanbod naar digitale diensten, hardware, software en netwerken samen. Hier is digitale veiligheid meestal niet leidend. Dit compliceert de beheersing van risico's.

Samenhangend en geïntegreerd risicomanagement staat nog in de kinderschoenen.
Digitale risico's hebben nog geen structurele plaats in het bredere risicomanagement binnen en tussen organisaties, sectoren en landen. Risico's zijn vaak niet in beeld, basismaatregelen niet getroffen.

Aanvullend is een overkoepelend thema geïdentificeerd dat de andere thema's raakt:

Beperkingen in digitale autonomie beperken ook digitale weerbaarheid.
Nederland heeft beperkte keuzemogelijkheden om de richting te bepalen van verdere digitalisering – en daarmee van digitale weerbaarheid.

De thema's worden in het CSBN uitgebreid toegelicht. Het CSBN2022 concludeert dat de scheefgroei tussen dreiging en weerbaarheid het risico op ontwrichting vergroot. Om ongestoord te kunnen functioneren, is weerbaarheid van de samenleving tegen digitale dreiging cruciaal. De veiligheid van digitale processen is essentieel in onze sterk gedigitaliseerde maatschappij.

Dit vraagt om een stevige en ambitieuze aanpak om de digitale veiligheid van Nederland te versterken. De strategische en beleidsmatige opvolging van de thema's in het CSBN2022 volgt in de nieuwe Nederlandse Cybersecuritystrategie. Deze strategie is de opvolger van de Nederlandse Cybersecurity Agenda (NCSA) uit 2018. De Nederlandse Cybersecuritystrategie beschrijft integraal en vanuit breed perspectief de visie, doelen en maatregelen op het gebied van cybersecurity die de komende jaren nodig zijn.

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