Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Het CSBN 2023 in vogelvlucht

Juni 2023

Door verwevenheid van processen in het digitale ecosysteem kan iedereen de gevolgen ervaren van een cyberincident, zelfs als deze in eerste instantie ver weg lijken. Daarnaast zetten statelijke actoren cyberaanvallen in om hun geopolitieke doel te bereiken, vormt afpersing een aantrekkelijk verdienmodel voor cybercriminelen en brengen nieuwe technologieën zoals AI nieuwe dreigingen met zich mee. Dat zijn enkele van de conclusies uit het Cybersecuritybeeld Nederland 2023 (CSBN). In het CSBN wordt de oproep aan organisaties gedaan het onverwachte te verwachten.

De hoofdbevindingen

Het CSBN 2023 vertaalt zich in de volgende zes hoofdbevindingen.

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 en voortdurend aan verandering onderhevig.

3. De strategische thema's uit het CSBN 2022 blijven leiden tot complicaties voor het beheersen van digitale risico's.

4. Het verkleinen van de scheefgroei tussen de digitale dreiging en de weerbaarheid blijft een grote opgave.

5. Ondanks groeiende aandacht voor de weerbaarheid van Operationele Technologie (OT) als bouwsteen van vitale processen, is er ruimte voor verbetering.

6. Digitale risico's vragen om een bredere manier van beheersing en moeten worden beschouwd als een integraal onderdeel van de risico's voor de nationale veiligheid. Hierbij kan de invalshoek 'assume breach' (ga ervan uit dat er een cyberincident is) behulpzaam zijn.

Reflectie strategische thema's

In het CSBN 2022 zijn zes strategische thema's benoemd die de komende jaren relevant zijn voor de digitale veiligheid van Nederland. Deze thema's vormden een uitgangspunt voor de doelen van de Nederlandse Cybersecurity Strategie 2022-2028.

De zes thema's zijn:

1. Risico's vormen de keerzijde van een gedigitaliseerde samenleving.
2. Digitale ruimte is speelveld voor regionale en mondiale dominantie.
3. Cybercriminaliteit is industrieel schaalbaar, weerbaarheid nog niet.
4. Marktdynamiek compliceert beheersing digitale risico's.
5. Samenhangend en geïntegreerd risicomanagement staat nog in de kinderschoenen.
6. Beperkingen in digitale autonomie beperken ook digitale weerbaarheid.

Bij de reflectie op deze thema's vallen de volgende veranderingen op:

- De extra eisen voor digitale veiligheid die voortkomen uit nieuwe Europese wet- en regelgeving.
- De verdere verharding van geopolitieke spanningen.
- Het onder druk staan van de verzekerbaarheid van digitale risico's.
- De toenemende onderlinge verwevenheid binnen het bredere ecosysteem.
- De gelegenheidsstructuur die het digitale ecosysteem vormt voor cyberaanvallen.
- Een 'nieuw' inzicht is dat digitale risico's integraal deel uitmaken van een breder en complex risicopalet en enkele andere bijzondere kenmerken hebben. Daardoor vragen digitale risico's om een bredere manier van beheersing dan andere risico's.

Vier risico's voor de nationale veiligheid

Er zijn vier risico's voor de nationale veiligheid. Deze gelden ook voor specifieke sectoren, organisaties en burgers.

1. Ongeautoriseerde inzage in informatie, in het bijzonder door spionage. Denk aan spionage gericht op communicatie binnen de Rijksoverheid of spionage om de ontwikkeling van innovatieve technologieën te achterhalen.

2. Ontoegankelijkheid van (vitale) processen, zoals door (voorbereidingen van) sabotage van de energievoorziening en door cybercriminaliteit.

3. Schending van de digitale ruimte, bijvoorbeeld door misbruik van mondiale ICT-leverancierssketens of internetprotocollen of door sabotage van kabels.

4. Grootschalige uitval: een situatie waarbij één of meer processen zijn verstoord door natuurlijke of technische oorzaken of door niet-moedwillig menselijk handelen.

Dreigingsscenario's

In het CSBN 2023 zijn dreigingsscenario's opgenomen die organisaties kunnen helpen in het maken van keuzes en afwegingen om de weerbaarheid te verhogen. Hierbij wordt gewezen op risico's die voortkomen uit het gegeven dat organisaties onderdeel zijn van een digitaal ecosysteem. Drie fictieve scenario's laten zien hoe een incident niet alleen leidt tot problemen binnen de organisatie, maar kan uitgroeien tot schade voor de maatschappij of andere organisaties in het ecosysteem.

Het CSBN is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Daarbij is nauw samengewerkt met het Nationaal Cyber Security Centrum (NCSC). Het CSBN wordt jaarlijks door de NCTV vastgesteld.

Bekijk het CSBN2023 online:
nctv.nl/onderwerpen/cybersecuritybeeld-nederland