Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Het CSBN 2024 in vogelvlucht

Oktober 2024

Digitale risico's zijn dynamisch en worden beïnvloed door veel factoren die ook niet-digitaal kunnen zijn. Sinds enkele jaren hebben de turbulente geopolitieke tijden hun weerslag op de digitale dreiging. Nederland is doelwit van cyberaanvallen, of ondervindt de impact van cyberaanvallen die doorwerken binnen het digitale ecosysteem. Daarnaast kunnen storingen leiden tot grootschalige uitval. Digitale risico's zijn complex en in hoge mate met elkaar verbonden. Dat alles kan leiden tot onvoorziene en ontwrichtende effecten. Het risico dat de nationale veiligheid wordt geraakt, kan daardoor toenemen. Om digitale risico's het hoofd te kunnen bieden, is het van belang een brede manier van risicobeheersing aan te nemen. Dit zijn enkele van de conclusies uit het Cybersecurity Beeld Nederland 2024 (CSBN).

Het CSBN 2024 vertaalt zich in de volgende drie hoofdbevindingen:

1. De digitale dreiging tegen Nederland is groot en divers, en cyberaanvallen zijn voornamelijk afkomstig van statelijke en criminele actoren. Cyberaanvallen door statelijke actoren staan niet op zichzelf, maar zijn onderdeel van een bredere gereedschapskist die staten hanteren om hun belangen te behartigen. Criminele actoren voeren op grote schaal aanvallen uit en handelen daarbij opportunistisch. Grootschalige uitval van digitale processen vormt eveneens een dreiging.

2. Digitale risico's vragen om een brede manier van beheersing. Ze zijn dynamisch en worden beïnvloed door vele verschillende factoren. Het bredere digitale ecosysteem, met daarbinnen monoculturen, en de hoge mate van digitalisering zorgen ervoor dat risico's met elkaar verbonden raken.

3. De veiligheid van digitale processen is en blijft essentieel in onze maatschappij en is dus onlosmakelijk verbonden met de nationale veiligheid. Het belang van digitale veiligheid concurreert met andere belangen.

Nieuwe uitdagingen voor digitale veiligheid

Als gevolg van ontwikkelingen in het afgelopen jaar zijn er meerdere nieuwe uitdagingen voor digitale veiligheid geïdentificeerd:

Statelijke actoren intensiveren activiteiten en verbreden capaciteiten

Meerdere statelijke actoren intensiveren hun cyberactiviteiten. Daarnaast verbreedt een aantal landen hun capaciteiten: ze voegen nieuwe methoden toe aan hun bestaande arsenaal, of gebruiken andere, ook niet-digitale, middelen. Op die manier vormen cyberaanvallen een onderdeel van de bredere gereedschapskist. Daar bovenop is de inzet of betrokkenheid van niet-statelijke actoren onderdeel van de verbreding.

Actoren zoeken nieuwe wegen om cyberaanvallen uit te voeren

Kwaadwillenden kiezen vaak de weg van minste weerstand. Zij gaan nog altijd veelal voor aanvalsroutes die relatief eenvoudig en snel toegang bieden. Statelijke en criminele actoren zoeken ook actief naar nieuwe wegen. Zoals het targeten van edge devices, of het toepassen van Living-off-the-Land technieken.

Niet-digitale ontwikkelingen beïnvloeden de digitale veiligheid

Digitale risico's worden beïnvloed door vele, ook niet-digitale, factoren. Dat geldt bijvoorbeeld voor geopolitieke of technologische ontwikkelingen. Ook ontwikkelingen die ogenschijnlijk niks van doen hebben met cybersecurity, kunnen blijvend van invloed zijn op de digitale dreiging of de weerbaarheid. Bijvoorbeeld de grootschalige concentratie van diensten bij de drie grootste cloudaanbieders.

Grootschalige handel in persoonsgevoelige data vormt dreiging voor nationale veiligheid

De grootschaligheid en precisie van de mondiale online datahandel en de wijze waarop online advertentiemarkten functioneren kan de nationale veiligheid op verschillende manieren schaden. Zoals door grootschalige schending van de vertrouwelijkheid van persoonsgevoelige data. Of door misbruik van de opgebouwde datasets en/of gedetailleerde persoonsprofielen.

Digitale veiligheid is randvoorwaardelijk voor vertrouwen in digitale processen

Vertrouwen is noodzakelijk om digitale processen te willen gebruiken. Alleen met vertrouwen kunnen organisaties of individuen omgaan met de vele onzekerheden. Digitale veiligheid is natuurlijk niet de enige randvoorwaarde voor vertrouwen, maar wel een noodzakelijke.

Jaarbeeld

De cyberincidenten in de rapportageperiode van dit CSBN, passen in het dreigingsbeeld. Incidenten, waaronder DDoS aanvallen, (voorbereidingshandelingen voor) sabotage en spionage, kunnen voor een deel worden geplaatst in de context van geopolitieke spanningen en verschuivende internationale machtsverhoudingen. Ransomware-aanvallen haalden opnieuw het nieuws, waarbij regelmatig ook sprake is van datalekken in combinatie met afpersing. Naast cyberaanvallen, zijn er opnieuw tal van voorbeelden van storingen als gevolg van niet moedwillig handelen.

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

Bekijk het CSBN2024 online:
nctv.nl/onderwerpen/cybersecuritybeeld-nederland