Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Het CSBN 2025 in vogelvlucht

November 2025

Het digitale dreigingslandschap wordt steeds diverser en onvoorspelbaarder. Er is een grote verscheidenheid aan aanvallen door statelijke actoren, cybercriminelen, en andere kwaadwillenden. Daarnaast vertaalt geopolitieke onvoorspelbaarheid zich naar het digitale domein. Cyberprogramma's worden opgezet door statelijke actoren of uitgebreid met inzet van niet-statelijke actoren of private organisaties. Ook kunnen veranderende geopolitieke verhoudingen ervoor zorgen dat digitale afhankelijkheden risicovol worden, terwijl ze dat eerder niet waren. Verder kunnen kwaadwillenden generatieve AI inzetten, wat betekent dat aanvallen eenvoudiger en op grotere schaal zijn in te zetten. Deze ontwikkelingen vinden gelijktijdig en in samenhang met elkaar plaats, waaruit voortvloeit dat het dreigingslandschap in toenemende mate complex wordt. Dit illustreert dat er continu aandacht moet blijven voor de weerbaarheid en de ontwikkelende dreiging en dat de basisprincipes van belang blijven – ondanks de toegenomen complexiteit. De diversiteit, onvoorspelbaarheid en het toenemende belang van digitale veiligheid maakt dat het steeds minder enkel een vraagstuk is voor technische experts, maar juist ook voor bestuurders.

Statelijke cybercapaciteiten nemen toe en vermengen met niet-statelijke organisaties

Landen zijn meer en meer bereid hun macht te gebruiken om hun geopolitieke belangen te behartigen, en vergroten daarbij hun cybercapaciteiten. Statelijke actoren zetten cyberaanvallen in om hun politieke, militaire en/of economische doelen te bereiken en zijn in staat om hun belangen te behartigen zonder dat ze de juridische drempel van gewapend conflict over gaan. Sommige statelijke actoren maken vernuftig gebruik van bedrijven en organisaties of zogeheten staatsgesteunde groeperingen. Staatsgesteunde groeperingen zijn bijvoorbeeld cybercriminelen of hacktivisten die officieel geen onderdeel uitmaken van een staat. Deze groepen worden vaak echter wel gedoogd, gesteund of aangestuurd door statelijke actoren. Deze vermenging van statelijke cybercapaciteiten met niet-statelijke organisaties leidt tot verdere complexiteit en een onvoorspelbaar dreigingsbeeld.

Dreiging telecomsector reëel, ook Nederland doelwit

Er is al jaren terecht aandacht voor de weerbaarheid van de vitale infrastructuur; de continuïteit van een vitaal proces als telecommunicatie is immers van groot belang voor het functioneren van onze samenleving. Incidenten in de Amerikaanse telecomsector laten zien dat de sector interessant is voor actoren en dat de dreiging zich manifesteert. Ook in Nederland waren enkele kleine internet service- en hosting providers doelwit van kwaadwillenden. Alhoewel grote incidenten in Nederland tot nu toe zijn uitgebleven en de weerbaarheid binnen de sector robuust is, vormt de sector doorlopend een interessant doelwit voor kwaadwillenden. Het doorlopend op orde houden van de digitale weerbaarheid in vitale sectoren is dan ook van groot belang.

Geopolitieke ontwikkelingen leggen afhankelijkheden nadrukkelijk bloot

Europa, en daarmee Nederland, is voor vele verschillende digitale processen en diensten afhankelijk van aanbieders uit veelal niet-Europese landen. Zo zijn publieke organisaties in allerlei sectoren in toenemende mate afhankelijk van diensten van enkele grote technologiebedrijven in de VS.

In de huidige geopolitieke context moeten we er rekening mee houden dat landen scherper hun eigen belangen afwegen, waardoor Nederland geconfronteerd kan worden met afhankelijkheden die als drukmiddel kunnen worden ingezet. Juist die geopolitieke ontwikkelingen kunnen er voor zorgen dat de afhankelijkheid van digitale diensten en processen uit andere landen risicovol is of kan worden.

Generatieve AI versterkt bestaande dreigingen voor digitale veiligheid

In de afgelopen jaren is de ontwikkeling van generatieve AI in een versnelling gekomen. De technologie achter generatieve AI vormt geen dreiging op zichzelf, maar door specifieke toepassingen van de techniek en intenties van de actor die het inzet kunnen hier wel dreigingen uit voortvloeien. Generatieve AI kan op verschillende manieren worden ingezet: zowel als ondersteuning voor kwaadaardige activiteiten, als ter verdediging tegen dreigingen.

Daarnaast vormt generatieve AI op zichzelf een mogelijk doelwit. Hierbij gaat het om aanvallen die gericht zijn op het verstoren of misleiden van AI-systemen.

Jaarbeeld

Hoewel nuances veranderen, hebben er geen grote verschuivingen plaatsgevonden in het dreigingsbeeld. Er is sprake van een grote verscheidenheid aan typen incidenten, oorzaken, aanvallers, en mate van impact. Zowel statelijke actoren als cybercriminelen voeren cyberaanvallen uit op Nederlandse doelen en/of raken Nederlandse belangen. Daarbij zijn edge devices blijvend interessant voor kwaadwillende actoren. Ook blijft er sprake van DDoS-aanvallen. Daarnaast zijn er met regelmaat cybersecurityincidenten bij toeleveranciers/dienstverleners die leiden tot datalekken bij afnemers. Naast incidenten die veroorzaakt zijn door cyberaanvallen, zijn er opnieuw tal van voorbeelden van storingen als gevolg van niet moedwillig handelen, zoals door softwarefouten.

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 CSBN 2025 online:
nctv.nl/onderwerpen/cybersecuritybeeld-nederland