Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cybersecuritybeeld Nederland 2026

AI versnelt, verdiept en verbreedt de dreiging

Het Cybersecuritybeeld Nederland (CSBN) 2026 laat zien dat de capaciteiten en activiteiten van statelijke actoren en cybercriminelen toenemen. Hoewel er verschillende maatregelen worden genomen om Nederland tegen deze veranderende cyberdreiging te verdedigen, groeit de digitale weerbaarheid van Nederlandse organisaties en bedrijven niet in hetzelfde tempo mee. Hierdoor ontstaat verdere scheefgroei tussen de cyberdreiging en de digitale weerbaarheid. Dit vormt een ernstig risico voor de nationale veiligheid.

Statelijke actoren

Statelijke actoren zoals China, Rusland, Iran en Noord-Korea vergroten hun cybercapaciteiten.

Ze zetten cyberaanvallen in als onderdeel van hybride en militaire conflictvoering. Nederlandse (overheids) organisaties, bedrijven en burgers zijn geregeld slachtoffer van cyberaanvallen van statelijke actoren.

Cybercriminelen

Cybercriminaliteit is inmiddels uitgegroeid tot een effectief georganiseerd ecosysteem met professionele samenwerkingsverbanden.

Cybercriminelen lijken zich in toenemende mate te richten op het stelen van grote hoeveelheden data, om daarmee bedrijven en organisaties af te persen, om de data te gebruiken voor andere cyberaanvallen of door te verkopen aan andere criminelen of statelijke actoren.

Kunstmatige intelligentie

Cyberactoren gebruiken AI om de snelheid, schaal en efficiëntie van cyberaanvallen te vergroten.

Door het gebruik van AI vinden kwaadwillenden geautomatiseerd steeds sneller en steeds meer onbekende kwetsbaarheden in onze digitale infrastructuur. Ook worden kwetsbaarheden in steeds kortere tijd en door meer actoren misbruikt. Cyberactoren gebruiken AI ook voor het ontwikkelen van malware. Tot slot vervult AI een steeds grotere operationele rol in malware, waarbij malware tijdens de aanval met een AI-model communiceert.

Digitale weerbaarheid

De digitale weerbaarheid van Nederlandse (overheids)organisaties en bedrijven blijft structureel achter bij de cyberdreiging.

Ondanks jarenlange waarschuwingen en concrete cyberincidenten heeft een deel van de Nederlandse (overheids)organisaties en bedrijven de basismaatregelen niet op orde. De digitale weerbaarheid van Nederlandse organisaties en bedrijven is daarnaast onvoldoende voorbereid op technologische ontwikkelingen, zoals AI en quantumcomputers.



Het CSBN is een jaarlijkse publicatie van de NCTV, samengesteld in nauwe samenwerking met verschillende nationale veiligheidsdiensten. Lees het hele CSBN op nctv.nl/csbn