Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cyberaanvallen tasten zenuwstelsel maatschappij aan

De digitale dreiging blijft zich ontwikkelen.

Aanvallen van statelijke actoren en cybercriminelen kunnen organisaties en ketens langdurig schaden.

Ze nemen de tijd om netwerken van slachtoffers binnen te komen en brengen daar vaak langere tijd ongezien in door. Ook cybercriminelen kunnen zorgen voor ontwrichting van de maatschappij. Ze zijn vaak net zo vaardig als statelijke actoren, richten zich ook op vitale processen en werken nauw samen met staten.

Digitale en fysieke wereld zijn onscheidbaar.

Digitale processen vormen het zenuwstelsel van de maatschappij.

Ze zijn onmisbaar voor het ongestoord functioneren van de samenleving.
Het niet naar behoren werken van digitale processen heeft een grote impact. Organisaties kunnen hun werk niet doen, persoonsgegevens komen op straat te liggen en voorzieningen kunnen uitvallen.

Cybersecuritybeeld Nederland 2021

Het CSBN biedt inzicht in digitale dreigingen, belangen en weerbaarheid. Het accent ligt daarbij op de nationale veiligheid.

De weerbaarheid is nog onvoldoende.

Ondanks positieve ontwikkelingen blijkt uit de cyberincidenten die Nederland hebben geraakt dat de weerbaarheid nog niet voldoende is.

Basismaatregelen worden niet voldoende genomen, zoals het gebruik van sterke wachtwoorden en het tijdig patchen van kwetsbaarheden. Daarnaast bestaan er grote verschillen in mate van weerbaarheid tussen bedrijven en organisaties.

Wat betekent dit voor u en uw organisatie?

Gebruik de drie dreigingsscenario's en beantwoord de kernvragen. Ga na of het scenario zich bij uw organisatie kan voordoen, welke voorbereidingen u heeft getroffen en wat u doet als het onverhoopt misgaat.

Het CSBN is een jaarlijkse publicatie van de NCTV en is opgesteld door de NCTV en het NCSC.

Lees het hele CSBN op ***nctv.nl***