Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cyberincidenten kunnen maatschappij verlammen

De digitale risico's zijn onverminderd groot en niet fundamenteel veranderd.

Risico's voor de nationale veiligheid zijn vooral spionage en sabotage door andere landen.

Ook bestaat het risico van (grootschalige) uitval door bijvoorbeeld menselijk of technisch falen en cyberaanvallen door criminelen. De digitalisering van onze maatschappij zet door. Digitale veiligheid is een randvoorwaarde geworden voor het functioneren van onze maatschappij.

Digitale risico's staan niet los van andere risico's.

Cyberincidenten kunnen snel en op grote schaal wereldwijd impact hebben op andere domeinen en de maatschappij in het hart raken.

Dit geldt zeker wanneer incidenten zich samen met andere incidenten voordoen. Een grootschalig cyberincident tijdens de huidige COVID-19 pandemie zou grote gevolgen hebben.

Cybersecuritybeeld Nederland 2020

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

Vergroting weerbaarheid belangrijkste instrument maar nog niet overal op orde.

Door vergroting van de digitale weerbaarheid kan zowel de kans op als de impact van cyberincidenten worden verkleind.

Digitale risico's worden soms onderschat. Individuele partijen voelen niet altijd een prikkel om bij te dragen aan digitale veiligheid van de maatschappij. Ook ontbreekt een compleet en scherp beeld van de digitale weerbaarheid van Nederlandse vitale processen.

Wat betekent dit voor u en uw organisatie?

Hulp bij de beantwoording van deze vraag is nieuw in het CSBN. 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 door de NCTV, in samenwerking met het NCSC, opgesteld.

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