



Democratische processen worden beïnvloed

Digitale aanvallen worden gebruikt om democratische processen te beïnvloeden.

In meerdere landen zijn democratische processen beïnvloed met cyberaanvallen.

In Nederland zijn maatregelen genomen rond de Tweede Kamerverkiezingen.



Digitale weerbaarheid blijft achter

Weerbaarheid van individuen en organisaties blijft achter bij de groei van de dreiging.

Daardoor nemen risico's toe als er geen extra maatregelen worden genomen.



Kwetsbaarheid internet of things

De kwetsbaarheid van het internet of things heeft tot versturende aanvallen geleid die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven.

Steeds meer apparaten worden op het internet met elkaar verbonden. Dat brengt kansen maar ook risico's met zich mee.



Beroepscriminelen en landen grootste dreiging

Beroepscriminelen en statelijke actoren vormen nog altijd de grootste dreiging en richten de meeste schade aan.

Beroepscriminelen zijn uit op financieel gewin. Landen houden zich bezig met digitale spionage, sabotage en beïnvloeding. Meer dan 100 landen spioneren wereldwijd met digitale middelen en willen waardevolle informatie van overheden en bedrijven verkrijgen.



Cybersecuritybeeld Nederland 2017



Het Cybersecuritybeeld Nederland 2017 geeft inzicht in belangen, dreigingen en weerbaarheid op het gebied van cybersecurity.

Sterke afhankelijkheid infrastructuur-diensten

Verder blijkt dat Nederland, voor de digitale infrastructuur, sterk afhankelijk is van een klein aantal buitenlandse dienstverleners.

De maatschappelijke gevolgen kunnen bij een verstoring groot zijn.



Het CSBN komt tot stand door samenwerking van het Nationaal Cyber Security Centrum met publieke en private partners en is een jaarlijkse publicatie van de NCTV.

Lees het hele CSBN op www.nctv.nl