CASE

Digitale ontwrichting kan veelheid aan oorzaken hebben

Dit jaar zal de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) een *policy* brief uitbrengen over de rol en verantwoordelijkheid van de overheid bij digitale ontwrichting. Dan gaat het over een situatie waarbij sprake is van grootschalige digitale verstoring, een cyberramp.

De grote stroomstoring bij Schiphol, april 2018, werd onder meer veroorzaakt door een verkeerd afgestelde noodaggregaat. De *check-in* systemen vielen uit, vluchten moesten worden geannuleerd en duizenden reizigers bleven aan de grond. En meer recent de stroomstoring van enorme proporties waardoor tientallen miljoenen huishoudens zonder stroom kwamen te zitten in Argentinië, Uruguay en Paraguay.

Met enige regelmaat worden we geconfronteerd met verstoringen als gevolg van DDoS-aanvallen op banken waardoor (een deel van de) betaalsystemen uitvalt.

Black-out

Maar wat nu als straatlantaarns, verkeerslichten, wegbewijzering, bruggen, sluizen, een deel van het elektriciteitsnetwerk - en daarmee telefonie en internet - worden gehackt en platgelegd? Of 'op zwart' gaan tijdens een zware storm en springtij? Dan kan het boek *Black-out* van Marc Elsberg (dit gaat over de chaos die ontstaat in Europa na een grote stroomuitval) zomaar realiteit worden...

De WRR constateert dat met het belang, de verdere verspreiding en verwevenheid van digitale technologie ook de risico's toenemen - en de complexiteit. Bovendien kan een veelheid aan oorzaken een digitale verstoring in gang zetten. Van terroristen en hackers tot natuurrampen en technische problemen: allemaal kunnen ze een digitale ontwrichting in gang zetten en daarmee de samenleving potentieel enorm ontregelen en schade toebrengen, zo geeft de WRR aan.

Het op 28 maart jl. aan de Tweede Kamer aangeboden rapport van de Algemene Rekenkamer 'Digitale dijkverzwaring: cybersecurity en vitale waterwerken' onderschrijft dat spionage, sabotage, terrorisme en criminaliteit zich hebben verplaatst naar de digitale wereld. Daarmee is ook de automatisering van waterkeringen een risicofactor.

Miljoenen mensen zijn voor hun veiligheid afhankelijk van de betrouwbaarheid van die waterwerken. Ook de economische en ecologische belangen ervan zijn groot.

Het keren en beheren van water is daarom door de overheid als vitale sector aangemerkt. Uitval kan leiden tot maatschappelijke ontwrichting en raakt ook andere vitale sectoren, zoals de distributie van elektriciteit, aldus de Algemene Rekenkamer.

Real-time detectie

Mogelijk dat een representatief voorbeeld uit de praktijk hierbij handvatten kan bieden om een cyberramp te voorkomen: de Olympische Spelen. Al sinds 1989 maken het Internationaal Olympisch Comité (IOC) en het Internationaal Paralympisch Comité (IPC) gebruik van de kennis, ervaring en diensten van internationaal IT-partner Atos. De implementatie en het operationeel houden van de IT voor de Olympische Spelen is het best te vergelijken met een onderneming met 200.000 werknemers en 4,8 miljard klanten die 24/7 operationeel is. En die zich ook nog eens elke twee jaar (de cyclus van de Zomer- én de Winterspelen) naar een ander land verplaatst. Kortom: alle ingrediënten aanwezig voor digitale ontwrichting.

De Olympische Zomerspelen in Rio de Janeiro, in 2016, toonden meer dan 400 potentieel kwaadaardige *events* per seconde. Tijdens de openingsceremonie van de Olympische Winterspelen in Pyeongchang, in 2018, werd het duizendkoppige securityteam geconfronteerd met een cyberaanval.

Mede dankzij de Security Operations Centers, waar specialisten van Atos 24/7 veiligheidsrisico's monitoren en prescriptieve data-analyse toepassen, worden dit soort cyberdreigingen *real-time* gedetecteerd en via een snelle, geautomatiseerde response geneutraliseerd. Het veiligheidssysteem filtert vooraf technische storingen en eventuele menselijke fouten eruit, zodat het securityteam zich kan toeleggen op feitelijke incidenten. Het is immers cruciaal dat alle systemen blijven draaien.

‘The Green Games’

De Olympische Zomerspelen van 2020 in Tokyo worden al ‘The Green Games’ genoemd. Japan bouwt een CO_2-neutraal Olympisch Stadion dat alleen natuurlijke energiebronnen zoals zonne-energie en windenergie gebruikt. Het regenwater wordt gebruikt voor de bewatering van de sportvelden en de rioleringen en waterstof zal worden ingezet voor de verwarming, de spelersbussen en de Olympische vlam.

Atos levert daaraan een bijdrage door het inzetten van de cloud voor de kritische toepassingen, zoals het accreditatiesysteem en het vrijwilligersportaal. Ook wordt het Technology Operations Center (TOC), het Atos controle- en commandocentrum voor de monitoring en besturing van de IT-systemen in Tokyo, op afstand ondersteund door het permanent in Barcelona ingerichte Technical Technology Operations Center (TTOC).

Het werken vanuit de cloud impliceert dat er niet iedere keer weer een volledige infrastructuur voor de Spelen opgezet dient te worden. Het stelt het IT-team in staat flexibeler te reageren wanneer capaciteit op- of afgeschaald moet worden naar gelang de nieuwe vraag en behoeften. Dat impliceert ook dat er minder Atos medewerkers naar Tokyo hoeven af te reizen, wat bijdraagt aan minder CO_2-uitstoot.

Valentijn van der Meijden is expert Cyber Security bij Atos.
Voor meer informatie: valentijn.vandermeijden@atos.net