WAT VANDAAG VEILIG IS, *HOEFT DAT MORGEN NIET TE ZIJN*

TEKST SASKIA KLAASSEN **BEELD** JACQUELINE DE HAAS

Een sombere boodschap? Het is maar hoe je het meest recente cybersecuritybeeld bekijkt, vindt directeur Patricia Zorko van NCTV. Ze ziet cybersecurity vooral als een kans om de digitale voorsprong van Nederland te verzilveren. "Gelukkig slagen we er steeds beter in het gesprek aan te gaan met bedrijven en samen op te trekken."

Nederland is een populair doelwit voor cybercriminelen: zijn wij vaker slachtoffer dan de ons omringende landen?

"De precieze cijfers ken ik niet, maar onze indruk is dat Nederland hier meer dan gemiddeld last van heeft. Dat heeft te maken met de goede kwaliteit van onze digitale snelweg en onze hoge connectiviteit: internetbankieren en online winkelen zijn hier bijvoorbeeld heel normaal. Nederlanders kennen weinig schroom om de digitale snelweg op te gaan. Maar dat heeft ook zijn keerzijde. Uit cijfers van CBS blijkt dat 1,2 miljoen Nederlanders slachtoffer waren van cybercriminaliteit, het gaat hierbij vooral om vermogenscriminaliteit. Maar we weten dat ook bedrijven vaker doelwit zijn. Uit ons jaarlijkse Alert Online trendonderzoek Nationaal Cybersecurity Bewustzijnsonderzoek 2019 blijkt dat 48 procent van werkend Nederland weleens te maken gehad met een cyberincident op de werkvloer."

In het recente Cybersecuritybeeld Nederland worden spionage en sabotage door landen als grootste dreiging gezien voor de maatschappij.

"Vaak is het lastig om te duiden wie een aanval uitvoert, een land of een criminele organisatie. We hebben zelf de afgelopen jaren ook flink geïnvesteerd in de capaciteit van inlichtingendiensten. Hierdoor is er ook meer zicht gekomen op de rol die landen als Rusland en China spelen bij incidenten. Statelijke actoren worden in het Cybersecuritybeeld 2019 dan ook de grootste bedreiging genoemd op het gebied van cyberveiligheid in relatie tot de nationale veiligheid.
Daarbij wordt niet alleen de overheid slachtoffer, maar ook bedrijven. In het algemeen lopen bedrijven het risico om slachtoffer te worden van spionage-aanvallen gericht op het verkrijgen van intellectueel eigendom. Voor bedrijven in de vitale infrastructuur geldt dat zij zelfs doelwit kunnen worden van digitale sabotage."

Heb je een beeld hoe bewust men op het niveau van de boardroom is van de risico's?

"Ik spreek regelmatig ceo's, onder meer via de Cybersecurity Raad die bestaat uit vertegenwoordigers uit overheid, bedrijfsleven en wetenschap. Deze organiseert regelmatig zogeheten boardroomgesprekken om organisaties te wijzen op het belang van cybersecurity. Het bewustzijn van de risico's is heel verschillend. Laatst sprak ik een ceo van een hoogtechnologisch bedrijf die het budget voor cyberveiligheid de afgelopen paar jaar had vervijfvoudigd. Maar er zijn ook bedrijven die zich nauwelijks bewust zijn van de gevaren.
Soms is het een probleem dat we niet altijd dezelfde taal spreken. Om die reden ontwikkelde Cyberveilig Nederland met steun van de Cybersecurity Alliantie van de NCTV het Cybersecurity Woordenboek. Een woordenboek dat de technische professional verbindt met andere professionals, die steeds meer met cybersecurity te maken krijgen. Hoe dan ook zullen risico's de komende jaren niet minder worden. Iedere board zal daarom moeten bepalen hoe hiermee om te gaan. De kunst is cyberveiligheid onderdeel te laten worden van het normale risk management, zodat de risico's in beeld zijn, worden afgewogen en waar nodig zijn afgedekt."

Stel, je zit in de board van een onderneming met een flinke achterstand, wat zou je als eerste aanpakken?

"Bedrijven kunnen eigenlijk dezelfde aanpak volgen die wij voor Nederland toepassen voor de nationale veiligheid. Eerst bepalen wat je kroonjuwelen zijn. Welke belangen wil je in elk geval beschermen? Wat zijn de dreigingen? Welk risico wil je lopen? En wat zijn de maatregelen die dan in elk geval genomen moeten worden om je weerbaarheid tegen de dreiging te vergroten? Het gaat steeds om de afweging van de belangen tegenover de acceptabele risico's? Zodat als je toch geraakt wordt je weer snel *up and running* bent. Een proces dat iedereen zou moeten doorlopen en waarmee je helaas nooit klaar bent. De technologische veranderingen gaan zo snel. Wat vandaag veilig is, hoeft dit morgen niet meer te zijn.
Als NCTV ligt onze focus in de eerste plaats op de vitale infrastructuur omdat hier het effect op de samenleving het meest ontwrichtend is. Als de energie uitvalt of sluizen doen het niet meer, dan hebben we in het hele land een groot probleem. Maar ook zet de rijksoverheid bewustwordingscampagne's in zoals 'Alert Online' en 'Eerst checken dan klikken' om veilig online gedrag bij burgers te stimuleren. En het Digital Trust Center van het ministerie van Economische Zaken en Klimaat helpt ondernemers met veilig digitaal ondernemen."

In een ander interview adviseer je om tien procent van ICT-budget te reserveren voor cyberveiligheid. In hoeverre gebeurt dit bij bedrijven?

"Dat percentage is een richtlijn. Ik zou graag zien dat de vrijblijvendheid om maatregelen te nemen verdween, maar we kunnen organisaties vaak niet verplichten. Probleem is dat de meeste bedrijven onderdeel zijn van een keten. Door deze afhankelijkheden kunnen ook andere bedrijven slachtoffer worden. Vandaar dat we steeds vaker afspraken maken met hele ketens, bijvoorbeeld in de *supply chain* rondom Schiphol of de haven van Rotterdam. Een andere vraag die elk bedrijf zich

'Als de energie uitvalt of sluizen doen het niet meer, dan hebben we in het hele land een groot probleem'

moet stellen is: moeten alle processen gedigitaliseerd zijn. En zo ja, moeten alle systemen met elkaar verbonden zijn of kunnen we deze beter onderbrengen in compartimenten? Volgens ons Alert Online trendonderzoek 'Nationaal Cybersecurity Bewustzijnsonderzoek 2019' neemt het bewustzijn over deze verknooptheid bij bedrijven gelukkig toe."

Over verknooptheid van systemen gesproken: een aanval op een energiecentrale in Oekraïne legde in 2018 de primaire processen van Maersk plat in de Rotterdamse haven...

"Dit is een goed voorbeeld van de cascade-effecten die kunnen ontstaan als gevolg van de toegenomen ketenafhankelijkheid. Beide bedrijven gebruikten hetzelfde boekhoudprogramma. De aanval, die wordt toegeschreven aan Rusland, was primair gericht op het verstoren van de openbare orde in Oekraïne. Maar het effect was veel groter, 64 landen werden uiteindelijk door de aanval getroffen."

De Wetenschappelijke Raad van de Regering (WRR) waarschuwt dat we er met preventie alleen niet zijn. We moeten ook investeren in crisisbeheersing. Heeft de overheid een crisisplan? En hoe zit dat met bedrijven?

"Een nationaal crisisplan is er en wordt op dit moment geactualiseerd. Ook bereiden we een grootschalige cyberoefening voor die in 2020 plaatsvindt. Waarin we met alle betrokkenen, dus ook bedrijven, alle rollen en taken oefenen die bij een digitale ontwrichting met maatschappelijke gevolgen horen. Pas dan kom je er namelijk achter welke problemen er zijn en op welke punten het meevalt. De overheid kan ondersteunen met een oefen- en testprogramma op nationaal niveau, maar bedrijven hebben hierin ook een eigen verantwoordelijkheid om klaar te zijn voor digitale uitval. De beste manier is om het een keer te ervaren. Er zijn goede simulaties beschikbaar, onderwerp de systemen bijvoorbeeld eens aan een penetratietest of boots de situatie na waarbij het bedrijf na een cyberaanval op zwart gaat. Wat doe je dan, als Raad van Bestuur? Het liefst zag ik dat de cyberoefening een verplicht onderdeel wordt, zoals de brandoefening. Maar voorlopig gaat deze verplichting alleen gelden voor organisaties in de vitale infrastructuur."

Patricia Zorko

Patricia Zorko werkte ruim dertig jaar bij de politie. Ze had diverse functies, waaronder districtschef, hoofd regionale recherche en politiechef van de Landelijke Eenheid. In die laatste functie gaf ze onder andere leiding aan het strafrechtelijk onderzoek naar de aanslag op vlucht MH17.
In 2015 maakte Patricia Zorko de overstap naar plaatsvervangend Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

De WRR stelt ook dat digitale ontwrichting onvermijdelijk een keer komt?

"Samen met publiek-private partijen zijn we bezig met een reactie op de WRR, die eerder dit jaar met een rapport kwam. Feit is: we moeten ons voorbereiden op zo'n scenario. Natuurlijk is dat een taak van de overheid, daar zijn we ook mee bezig, samen met publieke en private partners. Maar ook bedrijven en burgers moeten zich binnen de eigen organisatie voorbereiden. Wat zijn je terugvalopties als de elektriciteit uitvalt? Of het water en de telefoonverbinding? Het ergste scenario voor een bedrijf is dat er problemen zijn en je kunt elkaar niet meer bereiken. Wat moet er in zo'n geval in elk geval doorgaan en hoe zorg ik daarvoor?"

Als politiechef zocht je naar slimme allianties met private partijen. Wie zijn nu de partijen die je werk kunnen verlichten?

"We werken samen met bedrijven uit de vitale infrastructuur, maar ook met technologiebedrijven en wetenschappers. En soms met wellicht minder voor de hand liggende partners als ethische hackers. Zolang ze natuurlijk de regels respecteren van *coordinated vulnerability disclosure*. Dat betekent: niet zomaar inbreken bij bedrijven, netjes melden als je kwetsbaarheden hebt gevonden en het niet zomaar openbaar maken. Je ziet dat steeds meer bedrijven op hun website deze hackers uitnodigen om eventuele kwetsbaarheden te delen. Soms staat hier ook een beloning tegenover, ook al zijn de meesten niet uit op geld maar gaat het om de eer."

De NCTV stelt somber dat de weerbaarheid van bedrijven nog steeds onvoldoende is. Zijn er ook lichtpuntjes?

"Als overheid en bedrijfsleven kijken we steeds meer gezamenlijk naar economische- en veiligheidsbelangen van digitalisering. Twee begrippen die vaak lastig te verenigen waren. Voor veel bedrijven betekent veiligheid dat er ook geen geld meer verdiend kan worden. De focus ligt op economische voorspoed en voorop blijven lopen. Het is lastig om die groei in samenhang te zien met cyberveiligheid. Voor mij is het soms hard werken om me in het standpunt van bedrijven te verplaatsen. Maar we slagen er beiden steeds beter in het gesprek aan te gaan en samen op te trekken." ■