CYBER VEILIGHEID IN EEN DIGITALE WERELD

IN GESPREK MET

WILMA VAN DIJK,

DIRECTEUR SAFETY, SECURITY &

ENVIRONMENT BIJ SCHIPHOL

BW
BANK|WERELD

Veiligheid in al zijn facetten staat op luchthaven Schiphol natuurlijk op nummer één. Spil daarin is Wilma van Dijk, directeur Safety, Security & Environment bij Schiphol. Ook is Van Dijk voorzitter van de Commissie Vitale Infrastructuur (CVI) van VNO NCW, en op dit moment zit haar termijn van vier jaar er bijna op. Goed moment voor de brede visie van Van Dijk op een cyberveilig Nederland.

"De CVI behartigt de sector-overstijgende belangen van de private vitale sectoren en bedrijven inzake nationale veiligheid en vitale infrastructuur. Ook formuleert de CVI het VNO-NCW beleid hierin", zo omschrijft Van Dijk de commissie waarvan ze binnenkort afscheid neemt.
"We vormen een netwerk voor intersectorale uitwisseling van kennis, informatie, ervaringen en best practices. We volgen kritisch het relevante overheidsbeleid en (inter)nationale wet- en regelgeving en spreken ons hierover uit. Ook fungeren we als klankbord voor de overheid. In de huidige coronacrisis zijn we onder meer ook klankbord en 'doorgeefluik' van informatie. Een centrale 'hub' voor informatiedeling tussen de vitale aanbieders. We behartigen hun belangen en zijn een linking pin met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Dat leidde onder meer tot de 'Verklaring van vitaal belang'."

NIET OVERAL EVEN HOOG OP DE AGENDA

Voor haar rol als directeur bij Schiphol was Van Dijk ruim vier jaar directeur Cybersecurity bij de NCTV. Op de vraag of Nederland cyberveilig is en waar de sterke punten en verbeterpunten liggen, antwoord Van Dijk: "Nederland heeft een sterke cultuur van vrijwillige samenwerking en kennisdelen voor een gedeeld resultaat. De afgelopen tien jaar zijn veel goede stappen gezet in publiek-private samenwerking en kennisdeling voor een cyberveilig Nederland. De vitale sectoren nemen allerlei extra maatregelen. Dit in nauwe samenwerking met de vakdepartementen en toezichthouders. Maar cybersecurity staat niet bij alle Nederlandse – publieke en private – organisaties even hoog op de agenda. Hier is zeker verbetering en versnelling mogelijk. Ook valt er winst behalen door samen te oefenen en leren."

ROL OVERHEID CYBERVEILIG NL

Van Dijk: "In mijn ogen is de rol van de overheid het ondersteunen en adviseren van vitale bedrijven, en in het bijzonder het delen van betrouwbare informatie over dreigingen - met bijbehorend handelingsperspectief. Dan kunnen bedrijven maatregelen treffen en investeren in preventie. Ook zou de overheid een regierol kunnen pakken bij de realisatie van één loket, waar bedrijven terechtkunnen voor informatie en vragen over cyberveiligheid. Juist bij bedrijven in de vitale infrastructuur, waaronder Schiphol, staat cybersecurity zeer hoog op de agenda. Samen en in nauw overleg met vakdepartementen en toezichthouders zijn ze volop bezig met de invulling van hun wettelijke zorgplicht. Belangrijk om hierbij op te merken, is dat honderd procent veiligheid niet bestaat. Cyberincidenten zullen er altijd zijn."
"En over een meer sturende rol voor de overheid: ik onderschrijf het achterliggende doel dat cybersecurity alle aandacht verdient. Cybersecurity is randvoorwaardelijk voor digitalisering én voor de nationale veiligheid. Wel is er al een zeer uitgebreid stelsel van sectorale toezichthouders. Een extra autoriteit – dus een nieuwe toezichtslaag – lijkt mij niet nodig. Het zou zelfs afbreuk kunnen doen aan de publiek-private samenwerking die onder meer is gebaseerd op vertrouwen, kennisuitwisseling en leren van incidenten in een open cultuur. Binnen de luchtvaart geldt al heel lang dat het meest wordt geleerd van vooral veel kleine dingen die fout gaan. En dat je door het open delen van kennis hierover, grotere incidenten tijdig kunt voorkomen. Een actieve meldingscultuur is onontbeerlijk. Zit de toezichthouder aan tafel als incidenten worden besproken, dan is de kans groot dat er minder gemeld wordt en dat het lerend vermogen drastisch afneemt."

PERMANENTE AANDACHT

De samenleving wordt toenemend digitaal afhankelijk, ziet ook van Dijk: "Digitale infrastructuur is inmiddels volledig verweven met processen die cruciaal zijn voor de samenleving, de economie en de democratische rechtstaat. Voor veel processen bestaat geen analoog alternatief meer. De aandacht voor digitale continuïteit en het voorkomen van digitale ontwrichting is echter nog niet overal even groot. Permanente aandacht voor het zo klein mogelijk houden van cyberrisico's is onlosmakelijk verbonden met de verdergaande digitalisering. Dit vraagt om een proactieve en bewuste houding van overheid, bedrijfs-

>>

leven en burgers. En om een proactieve publiek-private samenwerking waarin preventie, kennisdeling en van elkaar leren centraal staan."

Nederland moet zich beschermen tegen cybercriminelen die vaak ook grensoverschrijdend werken. Van Dijk: "Los van onze eigen verantwoordelijkheid als bedrijfsleven, zijn we hierin echt afhankelijk van de informatie die de overheid ons geeft. Informatiedeling over cyberdreigingen, zeker over statelijke actoren, is noodzakelijk om de cyberveiligheid op niveau te kunnen houden en te versterken. Juridische obstakels die informatiedeling belemmeren, zouden moeten worden geslecht. Voorwaarde is dan natuurlijk dat de overheid de juiste specialisatie in huis heeft om dit goed te doen. Ook bepleit de CVI een versteviging van de internationale samenwerking."

DIGITALE ONTWRICHTING

Op de vraag voor welke opgave Nederland staat bij het digitaal veilig houden van vitale diensten als watervoorziening, telecom, elektriciteit en ook bankdiensten, antwoordt Van Dijk: "Opgave is om cybersecurity altijd hoog op de agenda te houden. Proactieve publiek-private kennisdeling blijft nodig voor de juiste preventie-investeringen."

In 2019 pleitte de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) voor een betere voorbereiding op een digitale ontwrichting; onder meer middels adequate bevoegdheden om escalatie te voorkomen en inspanningen op cyberverzekeringen. Van Dijk onderschrijft het belang van voorbereiding: "De CVI benadrukt al langer het belang van een structurele, gezamenlijke oefenagenda. Samen scenario's oefenen geeft inzicht in de gezamenlijke doelen en welke ondersteunende processen en technieken belangrijk zijn. Ook wordt de weerbaarheid van het geheel getoetst. Belangrijke verbeteringen komen zo aan het licht. Net zo relevant – en vaak onderbelicht – zijn een goede evaluatie van bestaande incidenten en een follow up."

"Bij calamiteiten is het natuurlijk extra belangrijk dat vitale diensten beschikbaar blijven, vervolgt Van Dijk. "Naast de interactie georganiseerd op basis van calamiteitenplannen is er ook extra afstemming en informatie-uitwisseling. Het gemeenschappelijk maatschappelijk belang staat voorop. En als het gaat om financiële instellingen: die worden het meest van alle sectoren aangevallen. Door de snelle digitalisering groeit hun aanvalsoppervlak. Dat risico hebben financiële instellingen in het algemeen al lang geleden onderkend. Hun cyber resilience is dus ook navenant. Wat ik krachtig blijf vinden in de financiële sector, is de open samenwerking op cyber security. Bij Schiphol hebben we daar veelvuldig baat bij gehad, in contacten met meerdere banken. Ik denk dat veel financiële instellingen al een belangrijke maatschappelijke bijdrage leveren door het delen van hun kennis en ervaring en significant te investeren in cyber security."

WIN/WIN-SITUATIE

Een nauwe publiek-private samenwerking is dé sleutel bij het digitaal veilig houden van de vitale diensten, benadrukt Van Dijk: "Schiphol heeft ervaren dat daarmee veel winst te behalen is, als partijen uitgaan van vertrouwen, elkaars rol en verantwoordelijkheden erkennen, kennis delen en gezamenlijk veiligheidsprojecten uitvoeren. Bedrijven staan hiervoor open; een win/win-situatie. Binnen het NCSC wordt intensief publiek-privaat samengewerkt. De overheid speelt hier een belangrijke rol in. De betrokken overheidsinstanties moeten dan wel beschikken over de juiste (IT en OT) kennis en expertise. De CVI pleit daarom voor investeringen in meer kennis en expertise bij de overheid waar nodig."
"Voor de vitale infrastructuur is er een goed werkend stelsel van toezicht en handhaving, belegd bij de sectorale toezichthouders (AT, DNB en ILT). Daarnaast kan het ministerie van Justitie en Veiligheid escaleren naar vakdepartementen en toezichthouders als men vindt dat vitale be-

BW
BANK|WERELD

drijven onvoldoende gehoor geven aan de adviezen. Toezichthouders kunnen op hun beurt eventueel de betrokken bedrijven aanwijzingen geven, dan wel maatregelen afdwingen. Het toezicht is zo in mijn ogen voldoende en adequaat ingericht."

LESSONS LEARNED IN CORONACRISIS?

Op de vraag of er al 'lessons learned' zijn inzake de continuïteit van de vitale sectoren in deze coronacrisis, antwoordt Van Dijk: "Veel issues komen nu scherper naar voren. Zo ook de noodzaak tot digitale veiligheid, in deze tijd van versnelde digitale afhankelijkheid. Het proactief signaleren en oplossen van cyberkwetsbaarheden is essentieel. Daartoe moeten alle bedrijven en organisaties toegang krijgen tot relevante (operationele) cyberinformatie. En voor de vitale sectoren zijn trusted channels nodig, voor het delen van geclassificeerde informatie. Ook zouden we - in publiek-privaat samenwerkingsverband - meer inzicht moeten verkrijgen in de ketenafhankelijkheden in de kritische ICT-processen, om beter te kunnen sturen op de continuïteit van de vitale ICT-ketens. En, nogmaals, we moeten ook nu van elkaar leren door te oefenen." —

Als directeur Safety, Security & Environment bij **Schiphol** is **Wilma van Dijk** verantwoordelijk voor het beleid en de uitvoering op aviation security, access control, cybersecurity (CISO van Schiphol) en company security. Dit bevat meer de dagelijkse 24-uurs security-operatie, contractbeheer, contacten met (inter)nationale overheidsinstanties, particuliere beveiligingsbedrijven en technische ontwikkelingsbedrijven. Ook is Van Dijk verantwoordelijk voor het beleid in Safety & Environment op de luchthaven, en voor de luchthavenbrandweer. Verder is Van Dijk verantwoordelijk voor Seamless Flow, het innovatieve programma dat middels biometrie moet zorgen voor een veilige, zorgeloze en papierloze passage op de luchthaven. Verder is Van Dijk vanaf 1 juni ook algemeen directeur van Lelystad Airport.