Nieuwe brancheorganisatie Cyberveilig Nederland zoekt toenadering tot verzekeringssector

"WE WILLEN DE MARKT VAN DIENSTVERLENERS IN CYBERSECURITY TRANSPARANTER EN STERKER MAKEN"

Petra Oldengarm (links) en Liesbeth Holterman

Ons land is een brancheorganisatie rijker: Cyberveilig Nederland, een initiatief van acht dienstverleners op het gebied van cybersecurity. Het doel van de nieuwe branchevereniging is de digitale weerbaarheid van de 'BV Nederland' te versterken door de kwaliteit en transparantie binnen de groeiende cybersecuritysector te verhogen. Dat wil men onder meer realiseren door middel van de opzet en invoering van een gedragscode en een keurmerk voor bedrijven die cybersecuritydiensten aanbieden. Daarbij wordt nadrukkelijk toenadering gezocht tot de verzekeringsbranche, zo blijkt uit een interview met Petra Oldengarm en Liesbeth Holterman, respectievelijk directeur en beleidsadviseur bij Cyberveilig Nederland. ✎ Jan van Stigt Thans

Beide vrouwen zijn al een 'heel leven' actief in de wereld van de informatiebeveiliging. Oldengarm heeft een technische informatica-achtergrond en heeft zowel in het publieke en private werkveld functies vervuld op dit specifieke vakgebied, laatstelijk als Director Cybersecurity bij Hoffmann Bedrijfsrecherche. Ook bij Holterman, historica van huis uit, loopt de digitale technologie als een rode draad door haar carrière heen. Zij werkte onder meer bij de overheid in het veiligheidsdomein en laatstelijk als beleidsadviseur bij een tweetal belangenorganisaties: Nederland ICT en FME (de ondernemersorganisatie voor de technologische industrie). Naast hun werk voor Cyberveilig Nederland hebben beide vrouwen, los van elkaar, een eigen adviesbureau op het gebied van cybersecurity.

Nieuwe brancheorganisatie

Cyberveilig Nederland is een brancheorganisatie voor dienstverleners op het gebied van cybersecurity. Dat wil zeggen, organisaties en bedrijven die producten en/of diensten aanbieden op het gebied van digitale veiligheid op de Nederlandse markt. Tot de leden van het eerste uur behoren de initiatiefnemers Computest, FOX-IT, Guardian 360, Hoffmann, Motiv, Northwave, QSight IT en Zerocopter. Oldengarm en Holterman hopen dat het aantal bedrijven dat zich bij de brancheorganisatie aansluit snel groeit. Daarbij zeggen zij nadrukkelijk ook te denken aan verzekeringsbedrijven die cyberverzekeringen en/of andere cyber gerelateerde diensten aanbieden. Immers, cybersecuritydienstverlening richt zich zowel op het voorkomen van incidenten als op schadebeperking nadat een cybercalamiteit heeft plaatsgevonden. "We richten ons met Cyberveilig Nederland voorlopig alleen op bedrijven met personeel, niet op ZZP'ers die op dit vakgebied werkzaam zijn."

Waarom een brancheorganisatie voor dienstverlenende bedrijven op het gebied van cybersecurity? Oldengarm wijst erop dat er weliswaar brancheverenigingen zijn voor de IT-sector, maar dat deze de cybersecuritybranche niet exclusief vertegenwoordigen. "Er zijn wezenlijke verschillen: de IT-sector houdt zich vooral bezig met de technische beveiliging (o.a. firewalls en virusscans), terwijl de cybersecuritybranche zich breder toelegt op onder meer strategische consultancy, risicoanalyses en cyberwetgeving." Holterman vult aan: "De cybersecuritysector is een jonge, dynamische markt die volop in beweging is. Er komen steeds meer bedrijven bij die in aanvulling op hun kernactiviteiten producten en diensten aanbieden op het gebied van cybersecurity."

Doelstellingen

De nieuwe brancheorganisatie heeft als missie de digitale weerbaarheid van de 'BV Nederland' te versterken. Dat is volgens Oldengarm en Holterman nodig, omdat het risico op een cyberincident alleen maar toeneemt. "Enerzijds omdat (cyber)criminelen de laatste jaren actiever zijn geworden en anderzijds vanwege de toenemende verbondenheid tussen machines en systemen (Internet of Things). Het is daarom pure noodzaak dat er bij bedrijven en organisaties meer aandacht komt voor cybersecurity", aldus laatstgenoemde.

De kersverse directeur van Cyberveilig Nederland noemt desgevraagd drie doelstellingen van de nieuwe brancheorganisatie. Als eerste wijst zij op het verhogen van het niveau van de cybersecuritymarkt. "Het is niet alleen een jonge, maar ook een hele diverse markt. Door middel van bijvoorbeeld de invoering van een gedragscode en/of keurmerk denken we de markt van dienstverleners op cybersecuritygebied naar een hoger niveau te brengen en te versterken. Tegelijkertijd kunnen we hierdoor voor (potentiële)

> "We willen onze kennis en ervaring inzetten om de digitale weerbaarheid van Nederland te vergroten"

opdrachtgevers de markt transparanter maken", wat meteen onze tweede doelstelling is aldus Oldengarm. Als derde doelstelling noemt zij het risicobewustzijn en het kennisniveau binnen de 'BV Nederland' te vergroten. Cyberveilig Nederland wil hierin fungeren als gesprekspartner voor zowel de overheid als andere organisaties op cybersecuritygebied. "We willen onze kennis en ervaring inzetten om de digitale weerbaarheid van Nederland te vergroten, bijvoorbeeld door bij te dragen aan nieuwe wet- en regelgeving en de opzet van risicoanalyses en risicomodellen."

Risico's

Welke risico's lopen bedrijven op cybergebied? Volgens Holterman verschilt dat sterk per bedrijf. Voor de één is dat systeemuitval, zoals bijvoorbeeld voor nutsbedrijven (water, gas, elektra). Voor een ander is dat een hack van de (persoons)gegevens van klanten of ransomware, een risico waarvan elk bedrijf en individu het slachtoffer kan worden. Net als bij het omzeilen van fysieke beveiliging, geldt ook bij cybercriminaliteit dat criminelen voor de makkelijkste weg kiezen. Het bedrijf met de slechtste beveiliging heeft de grootste kans om slachtoffer te worden van hun activiteiten."

Oldengarm onderscheidt ruwweg drie risicotypen. Allereerst, de beschikbaarheid van data. Wat betekent het voor een bedrijf als het geen toegang meer heeft tot zijn bedrijfsinformatie en systemen? Daarnaast, de integriteit van de data. Zijn de gegevens volledig en juist? Als laatste, de vertrouwelijkheid van de data. Het risico dat anderen dan geautoriseerde personen toegang tot het systeem verkrijgen. "Organisaties dienen zich af te vragen welke risico's zij lopen, of zij weerbaar genoeg zijn en zo niet, welke maatregelen er nodig zijn om een en ander te verbeteren", aldus de directeur van Cyberveilig Nederland. Ze geeft nadrukkelijk aan zich ook zorgen te maken om de (vaak kleinere) toeleveranciers in de keten, vooral bij vitale sectoren. "Zij kunnen een risico vormen voor de andere partijen in de keten. Een keten is nu eenmaal zo sterk als zijn zwakste schakel."

Zekerheid en meedenken

Wat kan ondernemend Nederland in het algemeen en de verzekeringsbranche in het bijzonder verwachten van Cyberveilig Nederland? Oldengarm steekt van wal: "Veel. In de eerste plaats extra zekerheid bij de aanschaf van een product of dienst. Bij een bedrijf dat bij onze vereniging is aangesloten kun je vanwege de gedragscode en het keurmerk ervan uitgaan dat het met de kwaliteit goed zit en je verzekerd bent van de juiste risicoanalyse en verbetermaatregelen." Holterman noemt dat laatste van cruciaal belang. "De revenuen van je investeringen in cyberveiligheid moeten gerechtvaardigd zijn en in verhouding staan tot het risico. Je zou je anders bij wijze van spreken failliet kunnen investeren."

Een andere meerwaarde zien de beide vrouwen in het meedenken over wetgeving met betrekking tot cyberveiligheid, maar ook over risicomodellen, preventie en risico-inspecties. "We verwachten dat dit vooral voor de verzekeringsbranche van belang kan zijn bij het bepalen van premies en voorwaarden van de cyberpolissen die ze op de markt (willen) brengen. Ook denken we aan een benchmark op grond waarvan bedrijven kunnen vergelijken hoe ze er qua cybersecurity voorstaan. Op basis daarvan kunnen ze gericht aanvullende maatregelen treffen."

Volwassen sector

Tot slot, wanneer zijn jullie bij Cyberveilig Nederland tevreden? "Op de lange termijn als de markt voor cyberdienstverleners mede door onze inspanningen daadwerkelijk op een transparante en kwaliteitsvolle manier tot volwassenheid is gegroeid", antwoordt Holterman. "Op de korte termijn willen we een zo breed mogelijke vertegenwoordiging realiseren met cyberdienstverleners die zich bij ons aansluiten, ook vanuit de verzekeringsbranche. We zitten immers in elkaars keten en hebben elkaar nodig."

Oldengarm voegt daaraan toe: "Daarnaast willen we snel komen met een gedragscode en keurmerk en een substantiële bijdrage leveren aan de kennis en het risicobewustzijn op cybergebied bij zowel de overheid als ondernemend Nederland. Hierdoor worden niet alleen de bedreigingen gezien, maar ook de kansen die cybersecurity ontegenzeggelijk biedt." <