Als expert begrijpen wij het belang van een goede CyberHealth

Specialist Underwriter Cyber Patricia Langermans stond, in verzekeringstechnisch opzicht, aan het begin van de cybermarkt. Inmiddels voelt ze zich er behoorlijk in thuis. Sterker nog, Patricia is van begin tot eind betrokken geweest bij de in mei 2019 gelanceerde cyberpropositie van MS Amlin. Maar wat maakt die Cyberverzekering van MS Amlin anders en hoe draagt Patricia hier aan bij?

Door Chantal Buursema en Cindy van der Helm

Fotografie: Raphaël Drent

Als visual voor de cyberpropositie koos MS Amlin voor een robot met dokterskoffertje. Zo wordt de link gelegd met het MS Amlin First Response Team dat 24/7 klaarstaat voor klanten, de slogan 'Als expert begrijpen wij het belang van een goede CyberHealth' en de verdergaande digitalisering.

Haar laatste werkgever was een makelaar waar zij zich aanvankelijk met brand-, vervolgens met aansprakelijkheids- en de laatste vijf jaar met cyberverzekeringen bezighield. Zodoende weet zij uit eerste hand wat er bij bedrijven speelt. "Opmerkelijk hoe lastig het is om mensen bewust te maken van cyberrisico's. 'Het gebeurt mij niet, want ik heb geen gevoelige informatie' was een veel gehoorde opmerking. Wat mensen zich echter niet realiseren, is dat het criminelen vaak niet om de data gaat, maar om de afhankelijkheid van een bedrijf." Bij MS Amlin is Patricia van begin af aan betrokken geweest bij de ontwikkeling van de cyberpropositie. Hierdoor weet zij als geen ander hoe de MS Amlin Cyberverzekering in elkaar zit.

Ontwikkeling van de cyberpropositie

En nu zet Patricia zich in om makelaars en tussenpersonen – aan de hand van presentaties, simulatiegames en webinars – in zo begrijpelijk mogelijke taal te vertellen welke risico's er op de loer liggen en wat de gevolgen ervan zouden kunnen zijn. Cyber is en blijft een lastig te begrijpen product en daarom zijn haar presentaties doorspekt met voorbeelden. "Ik bezoek makelaars en tussenpersonen en neem ze mee in het hele cyberverhaal. Door hun accountmanagers te trainen, kan ik ze ondersteunen in hun werkzaamheden. Ik schets de mogelijke cyberrisico's, schades en bijpassende oplossingen waarmee makelaars en tussenpersonen op pad kunnen om bestuurders cyberbewust te maken. Dat cyberbewust maken bij de grote corporates gaat steeds beter, maar het MKB blijft achter. Aan het begin van mijn cybercarrière moest ik dit al enorm pushen; het bewust zijn van cyberrisico's was zo laag dat bijna niemand een cyberverzekering nam. Dit is nog steeds iets waar we dagelijks tegenaan lopen, maar gelukkig gaat het langzaamaan de goede kant op. Een cyberverzekering is veel meer dan een 'nice to have'. Het is een essentieel onderdeel van elk continuïteitsplan – voor bedrijven in alle soorten en maten – en dat probeer ik elke dag weer over te brengen. Aangezien ik van begin tot eind betrokken ben geweest bij dit proces, ben ik op de hoogte van alle minuscule ins en outs en kan ik anderen tot in de kleinste details uitleggen wat onze cyberpropositie inhoudt en waarom een bedrijf een cyberverzekering zou moeten afsluiten."

Waar Patricia erg enthousiast over kan worden, is crisismanagement via het MS Amlin First Response Team, een uniek team dat bestaat uit vier partnerpartijen. In haar zoektocht naar geschikte partners heeft zij vooral gekeken welke partijen het best bij MS Amlin passen. "Dat zouden partijen moeten zijn die zowel voor MKB-bedrijven als grote bedrijven werken. Daarnaast dienen ze niet alleen kennis en expertise in huis te hebben, maar ook betrokkenheid te tonen en 24/7 voor ons en onze klanten klaar te staan. Een crisis is zo emotioneel. Het is heel belangrijk dat onze partners mensen ook echt willen helpen, fysiek naar de klanten toe willen gaan, voldoende capaciteit hebben om onze klanten te kunnen bedienen, ook in geval van een cumulatierisico. En bovendien dienen zij ook preventief diensten te willen verlenen. Want wij bieden meerdere diensten aan in het kader van preventie. Voorkomen is nu eenmaal beter dan genezen. Ook voor de organisatie zelf."

We moeten met elkaar cyberweerbaar worden

Preventie ter voorkoming van een cyberincident

Om zelf al de nodige preventiemaatregelen te treffen, kunnen klanten via de website een aantal preventietips lezen. Partner International Security Partners kan daarnaast een risicoanalyse uitvoeren om de kwetsbaarheden in kaart te brengen. Dit gaat overigens verder dan alleen inzicht geven in de weerbaarheid van het bedrijf op het gebied van technologie. Zij kijken ook hoe de processen verlopen en naar de factor mens. Om medewerkers bewust te maken van risico's kunnen zij e-learnings geven. Naast International Security Partners maakt Grant Thornton onderdeel uit van het MS Amlin First Response Team. Grant Thornton kan bijvoorbeeld een phishingmail de organisatie in sturen om te kijken wat er gebeurt en wie er op een link klikt. Veel bedrijven werken met hun eigen ICT-afdeling bij cyberincidenten, maar realiseren zich niet dat security op dit niveau een echte specialiteit is, die van Grant Thornton. En daarmee betekent Grant Thornton enorm veel voor de klant. Grant Thornton en International Security Partners werken bovendien met mystery guests. Door te kijken of die persoon zomaar ergens binnen kan komen, creëren ze bewustwording. Grant Thornton biedt daarnaast ook de preventieve dienstverlening Managed Cyber (security as a service), zoals CyberHunter en CISO (Chief Information Security Officer) as a Service, en een penetratietest (ook wel een pentest genoemd) om kwetsbaarheden in de organisatie op te sporen en de cyberweerbaarheid en privacy te verbeteren. Ook heeft zij ethische hackers in dienst om organisaties te helpen inzicht te verkrijgen in bijvoorbeeld het gebruikte wachtwoordbeleid en de inrichting van de infrastructuur. Met deze dienstverlening ontzorgt Grant Thornton organisaties op alle aspecten van technologie, proces en mens. Advocatenkantoor Kennedy Van der Laan helpt vooraf onder meer met het beoordelen van de afspraken in de verwerkersovereenkomsten, en geeft advies over de inrichting van het gegevensgebruik. En Bex*communicatie geeft vooraf communicatietrainin-

Specialist Underwriter Cyber Patricia Langermans is van begin tot eind betrokken geweest bij de in mei 2019 gelanceerde cyberpropositie van MS Amlin

gen, zoals (mini) masterclasses cybercrisismanagement, crisismediatrainingen en crisissimulaties. Tevens stelt zij een crisiscommunicatieplan op, zodat medewerkers weten wat er van ze verwacht wordt als zich een cyberincident voordoet en wat de gevolgen zouden kunnen zijn. Denk bijvoorbeeld aan reputatieschade. Na een cyberincident kan het lang duren voordat je weer terug op hetzelfde niveau bent als voorheen. De impact van reputatieschade is dan ook enorm.

En dan is er een cyberincident

Als zich dan ondanks alle preventieve maatregelen toch een cyberincident voordoet, zijn de eerste uren cruciaal. "Het is helaas nog steeds de realiteit dat bedrijven vaak eerst zelf het wiel proberen uit te vinden, waardoor de schade alleen maar kan oplopen", aldus Patricia. "Het is dan ook zaak dat verzekerden snel het MS Amlin First Response Team bellen, zelfs als het slechts om een vermoeden gaat. Liever negen keer loos alarm dan één keer niet gebeld. Bij melding komt het MS Amlin First Response Team meteen in actie. Als eerste is dat International Security Partners die 24/7 klaar staat voor alle binnenkomende crisistelefoontjes. Zij is er vooral om de klant te ontzorgen en is gespecialiseerd in crisismanagement. Na het eerste contact zet International Security Partners de andere partijen in beweging, zoals Grant Thornton die zorgt voor de technische ondersteuning en biedt technisch en forensisch onderzoek om de oorzaak van het cyberincident te kunnen achterhalen. Wat Grant Thornton doet, is echt een vak apart en overstijgt alles wat een gewone ICT-partner kan en doet.

Om het cirkeltje rond te maken, komen we bij advocatenkantoor Kennedy Van der Laan voor de juridische ondersteuning, zoals het melden van een datalek bij de Autoriteit Persoonsgegevens, en communicatiebureau Bex*communicatie voor crisiscommunicatie en communicatie aan alle stakeholders."

Integrale samenwerking

"Effectieve risicoanalyse, preventieve maatregelen en crisisbeheersing zijn essentieel om de naam en reputatie van een bedrijf te beschermen en continuïteit te waarborgen", vervolgt Patricia. "Dankzij onze samenwerking met International Security Partners, Grant Thornton, Kennedy Van der Laan en Bex*communicatie kunnen wij crisismanagement, technische ondersteuning, forensisch onderzoek, juridisch advies, en crisiscommunicatie via een en hetzelfde telefoonnummer aanbieden. Iedereen kent elkaar goed en we werken als één team samen. We schakelen elkaar waar nodig in en weten dat we van elkaar op aan kunnen."

Eén totaalpakket zorgt voor rust en gemak

Gerenommeerde partners dus die expliciete kennis hebben. "Dat MS Amlin First Response Team is belangrijker dan die zak geld", volgens Patricia. Daar worden klanten echt mee geholpen en ontzorgd. Voor inzet van dat MS Amlin First Response Team geldt voor de eerste 72 uur dan ook geen eigen risico. Zo wordt de drempel om te bellen bij een vermeend cyberincident weggehaald. En er geldt bovendien een inlooptermijn van twee jaar. "Omdat we weten dat hackers gemiddeld 11 maanden in een systeem zitten voordat dat wordt ontdekt, zorgen wij voor inloop. Als je vandaag een verzekering afsluit en morgen openbaart zich schade die al eerder is begonnen, dan is er wel dekking. Zowel voor de eigen schade als voor de aansprakelijkheidsschade.

Daarnaast geldt er voor bedrijfsschade een wachttijd van acht uur. Maar wordt die periode van acht uur overschreden, dan is er vanaf de eerste minuut dekking. Verzekerden zijn bovendien niet afhankelijk van het moment waarop ze de schade bij ons melden. Het tijdstip van melding bij het MS Amlin First Response Team is ook direct ons tijdstip van melding."

De cyberpropositie van MS Amlin bestaat uit één totaalpakket. "Wij hebben er bewust voor gekozen om geen modules te gebruiken. Deze modules maken het alleen maar lastiger voor de klant om te kiezen waar ze zich wel of niet voor willen verzekeren. Het product 'cyber' is al zo abstract. Daarom hebben we gekozen voor een totaalpakket waarin alle rubrieken, inclusief de dienstverlening van het MS Amlin First Response Team, verzekerd zijn. Er zijn bovendien slechts twee sublimieten: voor telefoonhacking en computerfraude gelden beperkte dekkingen. Door bewust voor een totaalpakket te kiezen wordt het eindklanten gemakkelijker gemaakt om het product af te nemen.

De polisvoorwaarden zijn overigens toegespitst op de drie pijlers beschikbaarheid, integriteit en vertrouwelijkheid, oftewel: het BIV-model. Met een risicoanalyse volgens het BIV-model kan continuïteit worden gewaarborgd. Het gewenste niveau van beveiliging wordt op basis hiervan bepaald. Het is een continu proces waarbij gekeken wordt naar de technologie (IT), processen en niet te vergeten: de menselijke factor. De mens blijft namelijk altijd de zwakste schakel!"

Kennisdeling als einddoel

En zo werkt Patricia dag in dag uit om – via makelaars en tussenpersonen – MKB-bedrijven bewuster te maken van alle gevaren die op de loer liggen. Omdat zij – vanuit haar achtergrond als makelaar – weet hoe het werkt in de distributieketen kan zij makelaars en tussenpersonen als geen ander ondersteunen. In oktober, de Cyber Security Maand, werd er bovendien elke week in samenwerking met het MS Amlin First Response Team een artikel gepubliceerd via e-mailings, de MS Amlin website en LinkedIn om het bewustzijn van cyberveiligheid te verhogen. Ook is er begin juli het webinar 'Ransomware? Geen schijn van kans!' georganiseerd. Een interactieve online bijeenkomst waarbij de deelnemers, onder begeleiding van het MS Amlin First Response Team, aan de slag gingen met een realistische case. Veel kennis werd vergaard over ransomware, wat dat voor schade kan opleveren en welke preventieve maatregelen ingezet kunnen worden. Een wijze les voor iedereen.

Onder leiding van Patricia en in goede samenwerking met de hele markt probeert MS Amlin bewustzijn te creëren en te verhogen onder ondernemers. "Kennisdeling. Daar draait het om", besluit Patricia. "Want we moeten met elkaar cyberweerbaar worden." <