Adfiz MAGAZINE

2022 #20

Cybercrime-fighter Ronald Prins:
‘Trek de risico-analyse naar je toe’

Het belang van advies rondom cyberrisico’s
Menno Sombroek, VMD Koster verzekeringen

Wel of geen losgeld betalen bij een hack?
Themadiscussie

CYBER

Aanvankelijk ging Yusuf van Tas Verzekeringen en Risicobeheer de samenwerking met Voogd & Voogd aan om niet afhankelijk te zijn van één volmachtpartij. Maar al gauw bracht hij het gros van zijn verzekeringen onder bij Voogd & Voogd. Niet alleen vanwege de snelheid van acceptatie en het afhandelen van schadedossiers maar zeker ook vanwege het VoordeelPakket.

Het VoordeelPakket is echt appeltje eitje

Yusuf, Tas Verzekeringen en Risicobeheer

"Als ik het vergelijkingssysteem van Voogd & Voogd vergelijk met dat van concurrenten, dan kan ik alleen maar concluderen dat ik weinig concurrentie zie. Het systeem rekent, vergelijkt, is snel en toont zelfs de beste prijs bij een andere pakketsamenstelling. Het is ontzettend makkelijk en de maatschappijkeuze is nog steeds veel ruimer dan bij de concullega's. Daardoor is de klant altijd goed verzekerd zonder teveel te betalen."

"De pakketvergelijker van Voogd & Voogd, het Voordeel-Pakket, dat is echt 'appeltje eitje'! Waarom zou je naar de kruidenier, de slager, de groenteboer en de bakker gaan als je in de supermarkt alles hebt? Het systeem laat meteen de beste opties voor je klant zien. Dat is niet alleen gebruiksvriendelijk maar ook klantvriendelijk. Het is een prachtsysteem", aldus Yusuf.

De waarde van het Voogd & Voogd VoordeelPakket

- Blije klanten die tevreden zijn over de digitale Polismap; in één document zie je welke verzekering je hebt en wat je hiervoor betaalt.
- Eenvoudig en snel berekenen van een totaalpakket waarbij je met weinig vragen de klant al kunt voorzien van een complete offerte.
- Keuze uit verschillende maatschappijen binnen één pakket.
- In één oogopslag overzichtelijk wat verzekerd is en wat de verschillen tussen de maatschappijen zijn.
- Snel oplopende pakketkorting als je kiest voor voornamelijk één partij.

Voogd&Voogd

Voorwoord

Het aantal ondernemers dat getroffen wordt door een cyberaanval groeit schrikbarend. Zo registreerde de politie vorig jaar zo'n 14.000 gevallen van cybercriminaliteit, een toename van een derde in vergelijking met 2020 en een verdriedubbeling in vergelijking met 2019. En ABN AMRO becijferde dat het aantal bedrijven dat afgelopen jaar werd getroffen door een cyberaanval met 45 procent is gestegen. En het zijn echt niet alleen de grootbedrijven die hiermee te maken krijgen: het percentage cyberaanvallen onder zzp'ers lag in februari 2022 op 32 procent; in april 2021 was dit nog 13 procent.

En toch blijven veel bedrijven – met name in het MKB – denken dat cyberveiligheid vooral een issue is voor bedrijven waarin miljoenen omgaan of die met (persoons-)gevoelige informatie werken. Maar cybercriminelen zijn ook niet van gisteren. Die weten dat deze bedrijven inmiddels serieus werk maken van hun cyberveiligheid en in een verhoogde staat van cyberalertheid verkeren. En dat het daardoor meer loont om grotere aantallen kleine bedrijven aan te vallen en genoegen te nemen met een lagere opbrengst per bedrijf.

Hoe je het ook wendt of keert: ondernemend Nederland van groot tot klein moet zijn cyberzaakjes op orde brengen. Goed hang- en sluitwerk, alarminstallaties, sprinklers, enzovoort vinden we namelijk wel logisch, maar onze digitale deuren staan vaak gewoon open. Dat is vragen om moeilijkheden. Want een cyberaanval gaat over veel meer dan gevoelige informatie die mogelijk op straat komt te liggen. Als je IT wordt stilgelegd, ben je lamgeslagen. Letterlijk! En voor wie me niet gelooft: leg eens voor een dag je IT-omgeving plat en probeer dan je bedrijf te runnen. Dat is geen doen. Bedrijven realiseren zich nog te weinig dat ze dagelijks cyberrisico's lopen. Wij moeten die boodschap vertellen, net zo lang en luid als nodig!

Ik wens u veel leesplezier met dit nieuwe Adfiz Magazine.

Roger van der Linden - **voorzitter Adfiz**

COLOFON

2022 **#20**

Meer waarde met Adfiz
Belangenbehartiging Kennis Kwaliteit

Uitgever: Adfiz
Contactgegevens: Stadsring 201, 3817 BA Amersfoort, Postbus 235, 3800 AE Amersfoort, 033 - 46 43 464, info@adfiz.nl

Redactie: Adfiz en Vrhl Content en Creatie, www.vrhl.nl
Eindredactie en coördinatie: Vrhl Content en Creatie
Aan dit nummer werkten mee: Iris Borst, Bas Haring, Sanna Leupen, Eric Kampherbeek, Loraine Bodewes, Myra Langenberg
Cover fotografie: Eric Kampherbeek

Oplage magazine: 1.500 (controlled circulation)
Acquisitie: Elma Media B.V. (Silvèr Snoek: s.snoek@elma.nl)
Grafische vormgeving en druk: Elma Media B.V.

Cyber

'ZE WERDEN INEENS GECONFRONTEERD MET EEN FLINKE REPARATIE'

4

12 **'DE VRAAG IS NIET ÓF JE KLANTEN WORDEN GEHACKT, MAAR WANNEER'**

‘Het restaurant draaide lekker, toen ze ineens geconfronteerd werden met een flinke reparatie’

Tekst Sébastien Wulms
Beeld Loraine Bodewes

Als begin twintigers, midden in de coronapandemie een restaurant overnemen: dat getuigt van lef, geloof in eigen kunnen en ondernemerschap. Dat vond ook Patrick van de Sande van Vzeker uit Best. Vanaf het prille begin hielp hij het jonge stel met het op een goede manier omgaan met de risico’s die bij het ondernemerschap horen.

Toen Van de Sande de jonge ondernemers voor het eerst ontmoette, hadden ze het restaurant al aangekocht; de overdracht zou op een later tijdstip plaatsvinden. “Tijdens het eerste gesprek heb ik van alles met ze doorgenomen: van het verzuim- tot brandrisico en van preventierichtlijnen tot afvalverwerking. Pas in een later stadium hebben we het restaurant daadwerkelijk samen bezocht en kon ik de vorige huurder vragen naar keuringsrapporten en allerhande certificaten om mij een goed beeld te vormen van de onderhoudsstaat.” Dat dit geen overbodige handeling was, bleek al gauw. Van de Sande: “Je ziet regelmatig dat zodra leveranciers, van bijvoorbeeld allerlei systemen, er lucht van krijgen dat een horecazaak is overgenomen ze contact opnemen met de nieuwe eigenaren om nieuwe keuringen uit te voeren. Als je dan kunt aantonen dat een eerdere keuring recent is uitgevoerd en deze nog steeds geldig is, voorkom je onnodige uitgaven.”

Bij de opening van het restaurant eind 2021 golden er voor de horeca nog steeds coronabeperkingen. Daarom richtten de nieuwe eigenaars zich in eerste instantie op het afhalen en laten bezorgen van maaltijden. “Uiteraard heb ik toen gecheckt in hoeverre dat gevolgen had voor hun verzekeringen en – waar nodig – heb ik daar actie op ondernomen.” Eenmaal goed in bedrijf bleek dat er een lek was in de waterleidingen in de vloer. Van de Sande: “Toen de coronabeperkingen net voorbij waren en het restaurant goed draaide, werden de ondernemers ineens geconfronteerd met een flinke reparatie, met als gevolg een tijdelijke sluiting en alle daarmee gemoeide kosten. Ik heb me daar toen goed in verdiept en kwam erachter dat er voor de overname al een melding van de lekkage was gemaakt bij een andere verzekeraar. We zijn nu met de verschillende partijen in overleg om tot een oplossing te komen. Die zaak loopt nog, maar ik heb er alle vertrouwen in dat ook dat goed komt.”


BASTILLE

‘Het gaat om de mindset van mensen’

Tekst Vrhl Content en Creatie
Beeld Eric Kampherbeek

Je kunt nog zulke geavanceerde technologie in huis hebben om hackers buiten de deur te houden, maar als medewerkers binnen de organisatie geen cyberveilig gedrag laten zien, dan is het dweilen met de kraan open. Voor optimale cyberveiligheid is het belangrijk dat mensen zich bewust zijn van de risico’s én dat ze er daadwerkelijk naar handelen om te voorkomen dat cybercriminelen het bedrijf binnendringen. Floor Dijkshoorn is sociaal psycholoog bij Hoffmann; een organisatie gespecialiseerd in o.a. cybersecurity & security risk management. In een team van vijf sociaal psychologen adviseert zij bedrijven hoe gedragsverandering ten opzichte van cybersecurity bij medewerkers aan te pakken. Zij onderzoekt binnen bedrijven waarom mensen bepaald cyberveilig gedrag niet vertonen en hoe dergelijke patronen te doorbreken.

Elke organisatie heeft te maken met informatiebeveiliging om cybercriminelen op afstand te houden. En dat gaat verder dan slimme IT-tools. Dijkshoorn: “Bij cyber-security gaan we uit van drie pijlers; de organisatie (denk aan het juiste beleid/processen), het technisch niveau en de mens. Cyberveiligheid is – in veel gevallen – geregeld op basis van de eerste twee pijlers. Maar wat ik vaak zie, is dat medewerkers niet veilig handelen binnen een organisatie. Daar is veel winst te behalen.” Maar medewerkers stimuleren blijkt in de praktijk vaak lastig. Volgens Dijkshoorn is cyberveilig gedrag meer dan weten hoe te handelen. “Het gaat erom dat mensen het daadwerkelijk gaan doen,” licht ze toe. “Wat ik bij bedrijven constateer, is de heersende gedachte dat als de ‘awareness’ er is, het dan wel goed komt. Toch klopt dat niet, omdat wéten wat te doen niet het einddoel is. Natuurlijk is bewustzijn nodig om uiteindelijk tot verandering van gedrag te komen, maar dat is slechts de eerste stap. Het einddoel is cyberveilig gedrag.”

‘Wéten wat te doen, is niet het einddoel’

Waarom doen we het niet?

“De eerste stap is om te achterhalen waarom mensen iets niet doen. Dat betekent niet gissen of iets zelf invullen, maar in gesprek gaan met medewerkers,” legt Dijkshoorn uit. “Omdat ik met de mensen op de werkvloer in gesprek ga, leer ik het bedrijf en de cultuur goed kennen. Zo zie ik dat het bij de ene organisatie belangrijk is dat er humor zit in de oplossingen die je bedenkt, waar het bij het andere bedrijf juist van belang is dat de oplossingen professionaliteit en zorgvuldigheid uitstralen. Als de redenen zijn verzameld, gebruiken we vanuit Hoffmann het psychologische kader dat stelt dat mensen bepaald gedrag pas gaan vertonen als er sprake is van motivatie, capaciteit en gelegenheid. Doet iemand iets niet omdat hij het niet wil, niet weet, niet in de gelegenheid is om het gedrag te vertonen of een combinatie hiervan? Als ik dit inzichtelijk heb kunnen we kijken naar maatwerkoplossingen en interventies, waarbij je oplossingen aandraagt die zich richten op het verster-

ken van de motivatie, het versterken van de capaciteit of het faciliteren van gelegenheid. Blijven roepen dat personeel die pas moet dragen of moeilijke wachtwoorden moet gebruiken, heeft geen enkele zin als je niet achterhaalt waarom mensen het niet doen."

Motivatie, capaciteit en gelegenheid

Een belangrijke voorwaarde om gedragsverandering tot stand te brengen, is het hebben van voldoende capaciteit. "Ofwel, wéten wat je moet doen," zegt Dijkshoorn. "Medewerkers voeden met kennis op het vlak van cyberveiligheid kan dus worden gezien als een eerste stap naar het veranderen van gedrag. Dit is waar veel bedrijven stoppen: de phishing posters hangen aan de muren en het beleid staat op papier. Zo, nu maar wachten tot de medewerkers het ook gaan doen. Helaas blijkt dit dus niet afdoende. Het gaat er namelijk ook om dat mensen het willen en zich verantwoordelijk voelen voor de borging van cybersecurity. Motivatie is dus essentieel om gedrag te veranderen. Onder motivatie versta ik dat mensen het gedrag willen gaan vertonen. Deze pijler is vaak het lastigst om mee aan de slag te gaan en richt zich op interventies waarmee je mensen als het ware triggert en enthousiasmeert. Dat kan zijn dat je gedragingen die je graag terugziet visueel maakt en bij de ingang ophangt, of het gebruik van een speciaal ontwikkelde app waarbij cyberveilig gedrag in de vorm van een game wordt gestimuleerd. Maar medewerkers motiveren kan ook zitten in voorbeeldgedrag van de leidinggevenden. Onderzoek wijst keer op keer uit dat de invloed van leidinggevenden groot is op medewerkers. Het gedrag dat zij vertonen, zijn de medewerkers geneigd na te doen."
Tot slot dient er voldoende gelegenheid te zijn om het gewenste gedrag te vertonen. Als voorbeeld van wat er mis kan gaan op het gebied van de pijler 'gelegenheid', noemt Dijkshoorn het zichtbaar dragen van een bedrijfspas. "Dat is bij veel organisaties verplicht, maar dat gebeurt nauwelijks. Dan is mijn eerste vraag: 'waarom niet?' Als je die vraag aan medewerkers voorlegt en je hoort terug dat ze dat best willen maar dat ze niets hebben om de pas aan vast te maken – dan worden ze niet in de gelegenheid gesteld het gewenste gedrag te laten zien."

Complexiteit

Een positieve benadering is daarbij belangrijk, benadrukt Dijkshoorn. "De insteek die ik gebruik: zeg wat je wel wil zien van mensen en niet wat je niet (meer) wil zien. Daarnaast is het noodzakelijk om ook consequenties te koppelen aan ongewenst gedrag. Het mag best duidelijk worden dat het niet vrijblijvend is en alle betrokkenen een steentje moeten bijdragen. Immers, iedereen kan op een phishing mail klikken en draagt dus verantwoordelijkheid voor cyberveilig gedrag. Toch is het niet zo dat als een klant een van onze programma's gericht op gedragsverandering volgt, alles binnen een bedrijf meteen is veranderd. Dat is te makkelijk. Gedragsverandering is heel complex. Het is niet zo dat als medewerkers het programma doen er een vinkje achter cybersecurity gezet kan worden. Het is vaak een meerjarenplan met verschillende interventies. Gedragsverandering hangt met veel facetten samen en het heeft tijd nodig mensen mee te krijgen. Om dat volledig te realiseren ben je zo een paar jaar verder."

Urgentie

Het lijkt zo logisch, om na te vragen waarom medewerkers bepaald gedrag niet vertonen. Maar bij sommige bedrijven is er vaak onvoldoende bezetting of tijd om dat uit te vragen, zegt Dijkshoorn. "Of medewerkers doen het er een beetje bij, naast hun eigen functie. Terwijl het een onderwerp is waar je dedicated mee aan de slag moet. Ten opzichte van een aantal jaar geleden zie ik wel een grote shift – de meeste mensen die ik spreek zijn op de hoogte van het nut en de noodzaak om cyberveiligheid te verhogen. Die urgentie wordt echt wel gevoeld en gesprekspartners hebben ook meer kennis op dit gebied. Dat is leuk om te merken. De klanten die ik spreek hebben meestal al een beeld van wat er moet gebeuren om zich beter te beschermen, alleen weten ze niet hoe. Redenen waarom organisaties nog niet het gewenste niveau hebben bereikt – dat zit 'm bijvoorbeeld in te weinig budget, te beperkte capaciteit (zowel mensen als middelen) en sommige organisaties zijn groot en werken met complexe systemen waardoor het lang duurt om het te implementeren. Toch zie ik over-all wel een verbetering in het werkveld en dat is een positieve ontwikkeling. Cyberveiligheid staat steeds hoger op de agenda en dat is denk ik heel verstandig."

'Het gaat erom dat mensen zich verantwoordelijk willen voelen voor de borging van cybersecurity'

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

De Verduurzamings-hypotheek

Eenvoudig extra budget regelen voor energiebesparende maatregelen

Een Verduurzamingshypotheek van € 9.000? Bij de WelThuis hypotheek van a.s.r. hoeft uw klant dit alleen maar aan te kruisen op het renteaanbod. Wij bieden dat standaard aan. Heeft uw klant meer budget nodig? Of adviseert u uw klant de DigiThuis hypotheek van a.s.r? Dan vraagt u de Verduurzamingshypotheek tegelijk aan met de hypotheek. Zo regelt u voor uw klant extra budget voor energiebesparende maatregelen tegen extra scherpe rente en aantrekkelijke voorwaarden. Het geld van de Verduurzamingshypotheek staat twee jaar in depot, zonder afslag.

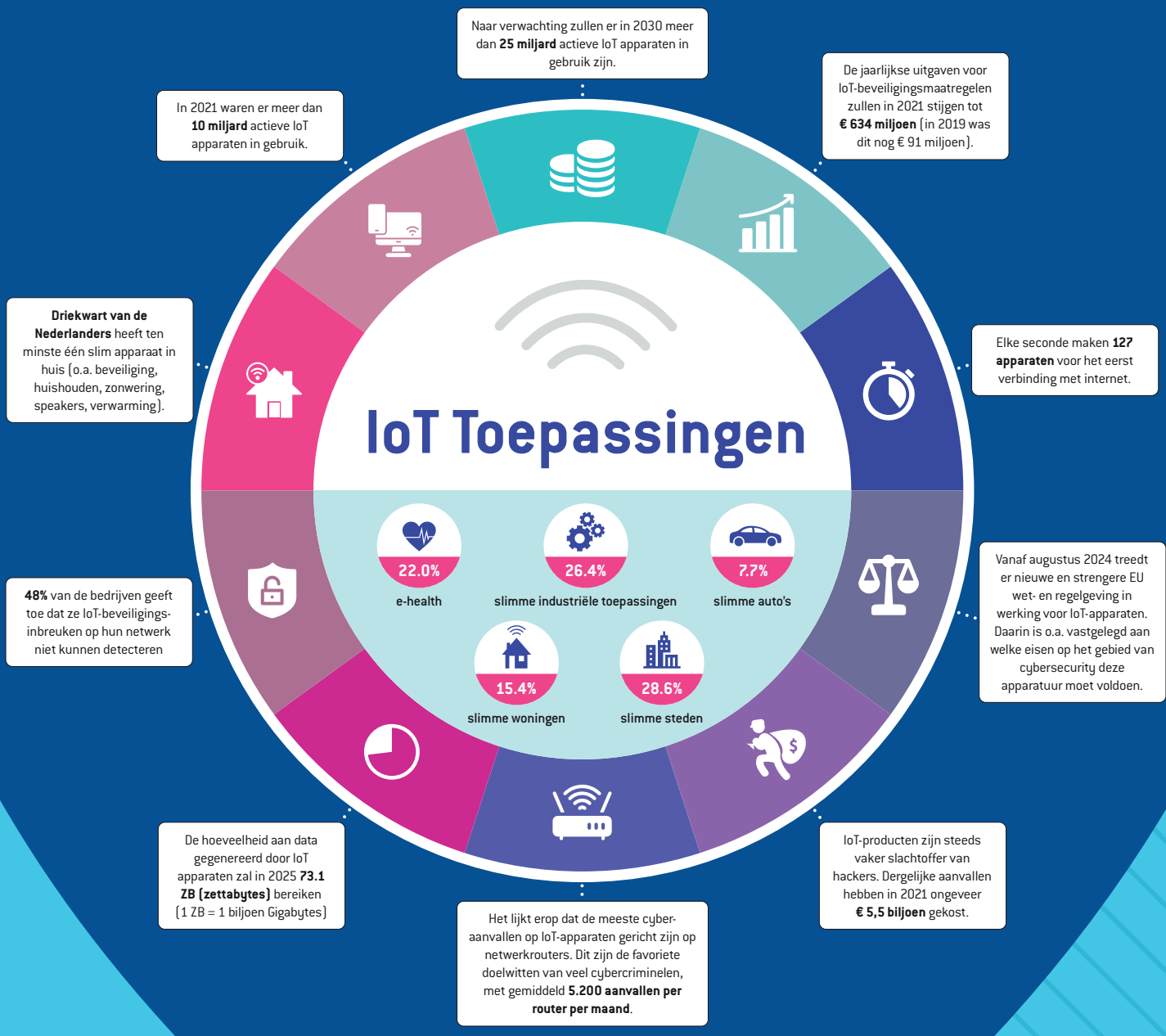
Meer weten over de voorwaarden? **Kijk op asr.nl/verduurzamingshypotheek**

a.s.r. doet het

GROENE LOTUS AWARD 2022

Internet of Things

EEN AANTAL FEITEN BIJ ELKAAR:



Naar verwachting zullen er in 2030 meer dan **25 miljard** actieve IoT apparaten in gebruik zijn.

De jaarlijkse uitgaven voor IoT-beveiligingsmaatregelen zullen in 2021 stijgen tot **€ 634 miljoen** (in 2019 was dit nog € 91 miljoen).

In 2021 waren er meer dan **10 miljard** actieve IoT apparaten in gebruik.

Driekwart van de Nederlanders heeft ten minste één slim apparaat in huis (o.a. beveiliging, huishouden, zonwering, speakers, verwarming).

Elke seconde maken **127 apparaten** voor het eerst verbinding met internet.

48% van de bedrijven geeft toe dat ze IoT-beveiligings-inbreuken op hun netwerk niet kunnen detecteren

Vanaf augustus 2024 treedt er nieuwe en strengere EU wet- en regelgeving in werking voor IoT-apparaten. Daarin is o.a. vastgelegd aan welke eisen op het gebied van cybersecurity deze apparatuur moet voldoen.

De hoeveelheid aan data gegenereerd door IoT apparaten zal in 2025 **73.1 ZB (zettabytes)** bereiken (1 ZB = 1 biljoen Gigabytes)

IoT-producten zijn steeds vaker slachtoffer van hackers. Dergelijke aanvallen hebben in 2021 ongeveer **€ 5,5 biljoen** gekost.

Het lijkt erop dat de meeste cyber-aanvallen op IoT-apparaten gericht zijn op netwerkrouters. Dit zijn de favoriete doelwitten van veel cybercriminelen, met gemiddeld **5.200 aanvallen per router per maand**.

Cyberrisico's loop je niet alleen met je laptop, smartphone en tablet, maar met alle apparaten ('dingen') die via internetverbindingen met andere apparaten of systemen in contact staan en daarmee gegevens uitwisselen. Het zogenaamde Internet of Things. Alledaagse voorwerpen (denk aan slimme tv's, keukenapparatuur, verlichting, auto's, thermostaten, babyfoons, deurbellen, beveiligingscamera's en horloges) zijn verbonden aan het internet en kunnen communiceren met personen en met andere objecten. Veiligheid is bij IoT-producten nog vaak slecht geregeld, én we zijn ons nog vaak nauwelijks bewust hoe verbonden we zijn.


BIG WIN
JACKPOT
PHISHING AWARD
EMPLOYEE OF THE MONTH
W. JANSENS
NOVEMBER 2022

Het belang van advies rondom cyberrisico's

'De vraag is niet óf je klanten worden gehackt, maar wanneer'

Tekst Vrhl Content en Creatie
Beeld Sanna Leupen

We kennen ze allemaal: de horrorverhalen over bedrijfshacks en gegijzelde digitale bestanden, waar de ondernemer of instelling pas weer bij kan nadat een flinke som losgeld is betaald. Veel mkb'ers denken dat zij de dans wel zullen ontspringen, omdat hun bedrijf niet interessant genoeg is. Maar niets is minder waar...

De zwakste schakel

Klinkt angstaanjagend – en dat is het ook. Voorkomen is beter dan genezen en bedrijven moeten hierover geadviseerd worden. Sombroek: "Preventie en awareness zijn het belangrijkst. Medewerkers van je bedrijf zijn de zwakste schakel: als zij op een foute link klikken, hebben criminelen toegang tot je IT-systeem. Medewerkers moeten zich dus heel bewust zijn van hun e-mail- en klikgedrag. Door hier aandacht aan te besteden en preventietrainingen te verzorgen, kun je al 80 tot 90 procent van de schade voorkomen. Ook kun je bijvoorbeeld zelf een nepphishingmailtje rondsturen en kijken wie er binnen je bedrijf op de link klikt. Een mooie manier om het bewustzijn rondom cyberveiligheid te vergroten."

IT-risico's blootleggen

Sombroeks collega Robbert-Paul Verkade is risicomanager. Hij legt uit dat VMD Koster samen met de klant IT-gerelateerde risico's binnen het bedrijf blootlegt, zoals bedrijfsschade en -stilstand. "Ook inventariseren we de herstelkosten. Op basis hiervan adviseren wij welke stappen de klant kan zetten als het gaat om preventie, awareness en bedrijfscontinuïteit.

Eventueel sluiten we een cyberverzekering af, maar dit heeft niet de prioriteit en is ook niet zo makkelijk: veel verzekeraars beperken hun dekking of trekken zich deels terug uit de markt. Het is dus belangrijk je goed in te lezen en scherp te blijven."

> 'Het is belangrijk je goed in te lezen en scherp te blijven'

Impact van een hack

Volgens Verkade is een cyberaanval of hack een groot risico voor bijna elk bedrijf. "Maar het is vaak moeilijk een ondernemer te overtuigen van de noodzaak om snel goede maatregelen te treffen. Ook omdat veel ondernemers denken dat zij niet interessant zijn voor hackers. Dat zijn ze juist wel. Een cyberincident in het mkb komt veel vaker voor dan je denkt. Soms schamen slachtoffers zich, ook als het gaat om de consequenties voor hun imago en betrouwbaarheid. Daarom zijn ze vaak terughoudend om erover te vertellen.

De vraag is niet óf je als ondernemer wordt gehackt, maar wanneer. Iedere organisatie verzekert zijn pand en inventaris, maar het risico van een cyberincident is wellicht groter dan het risico op een brand. Bovendien kan de impact van een hack veel groter zijn. Het is dus vooral belangrijk geld te steken in awareness en preventie."

Ondernemers overtuigen

Sombroek vertelt hoe je een ondernemer zover krijgt dat hij inderdaad aandacht besteedt aan IT-risico's: "Stel open vragen en laat de ondernemer zelf nadenken wat de risico's voor zijn bedrijf zijn. Trigger hem met voorbeelden als: 'Weet je hoeveel procent van jouw medewerkers hun zakelijke laptop of telefoon gebruiken voor andere apps, zoals spelletjes? En hoeveel medewerkers hun mail lezen op hun mobiele telefoon?' Dit zijn namelijk ook risico's. Een veelgehoorde tegenwerping is: 'Mijn IT-provider heeft alles goed geregeld'. Maar als je de samenwerkingsovereenkomsten goed leest, zal in de praktijk blijken dat de IT-provider zich vrijwaart of de aansprakelijkheid fors beperkt, waardoor je alsnog flink in de problemen kunt komen. Bovendien is een IT-bedrijf iets heel anders dan een cybersecurity-onderneming. Maak je klanten weerbaarder en spoor ze aan hun bedrijfscalamiteitenplan op orde te hebben. Veel ondernemers weten niet wat ze moeten doen als zich een hack voordoet – en wat het kost om het probleem op te lossen. Laat staan de schade die het bedrijf ondervindt vanwege het mislopen van omzet. Door alvast een plan klaar te hebben liggen, bespaar je kostbare tijd als zich een cyberincident voordoet."

'Door alvast een plan klaar te hebben liggen, bespaar je kostbare tijd als zich een cyberincident voordoet'

Preventie: hulp van experts

Om de preventie bij hun klanten goed op poten te zetten, werkt VMD Koster samen met Naq Cyber. Mede-oprichter en CEO Nadia Kadhim legt uit: "We helpen het mkb bij het nemen van cyberbeveiligingsmaatregelen. Om de betreffende bedrijven te beschermen, maar ook omdat dit wordt gedicteerd door de overheid, klanten of verzekeraars. Dit is vaak ontzettend complex voor ondernemers: de materie is ingewikkeld en het is erg overweldigend en tijdrovend. Wat moet je precies doen? Waar moet je beginnen? En wat kost dat? Met alleen een anti-virusprogramma kom je er niet. Bovendien is de markt ingericht op bedrijven die flinke budgetten te besteden hebben."

Financiële en reputatieschade

Het mkb wordt volgens Kadhim vaak over het hoofd gezien. "Ten onrechte, daarom richten wij ons op deze

doelgroep met een eenvoudig te gebruiken platform waarmee ze inzicht krijgen in hun netwerk en het beveiligen hiervan. Wij voeren scans uit op hun website en in de cloud en brengen zo in kaart waar de beveiliging beter kan. Hiervoor maken we een actieplan, inclusief instructiefilmpjes, gidsen en advies. Daarnaast kunnen we medewerkers trainen in het veilig gebruik van e-mail en internet om zo het bedrijf van binnenuit te beschermen: een menselijke firewall tegen cybercriminelen. Door te zorgen voor goede preventiemaatregelen, kan een ondernemer met een gerust hart ondernemen, zonder bang te hoeven zijn voor een hack of ransomware-aanval. Die kunnen uiteraard nog steeds voorkomen, maar de uiteindelijke schade zal veel kleiner zijn dan als je niets doet. Niet alleen financieel, maar ook wat betreft je bedrijfsreputatie."

Noodzaak

Ook Kadhim merkt dat er bij ondernemers vaak weerstand bestaat om met cyberzaken bezig te zijn. "Het kan lastig zijn om ondernemers te overtuigen van de noodzaak ervan. Maar het mkb is steeds vaker het doelwit van cybercriminelen, omdat grote bedrijven en ziekenhuizen hun preventie steeds beter op orde hebben. Bovendien kunnen ook MKB-bedrijven miljoenen omzet maken, dus is er veel te halen. Ik stel ondernemers altijd de vraag: 'Weet je wat je moet doen als je gehackt wordt?' En: 'Weet je bij wie je de hack moet melden en hoe je op een inzageverzoek moet reageren?' De meeste ondernemers hebben geen idee. Dat triggert vaak wel. Bovendien is het zó zonde om je niet op preventie te richten: je wordt hoe dan ook een keer gehackt en preventie is zóveel goedkoper dan achteraf het probleem proberen op te lossen."

Nieuwe wetten

"Wat ook belangrijk is, is dat er in Europa nieuwe wetten over cybersecurity in aantocht zijn, met veel meer controle op het naleven hiervan," vervolgt Kadhim. "Wil je hier straks aan voldoen, dan moet je nu alvast stappen gaan zetten. Je kunt het je straks helemaal niet meer veroorloven om geen cybersecuritymaatregelen te nemen. Dat kun je niet goedpraten tegenover de overheid, je klanten én je medewerkers. Met tegenwerpingen als 'ik heb er geen zin in' of 'het is te duur' kom je straks niet meer weg. Je moet kunnen uitleggen wat jij doet om hun gegevens veilig te stellen, anders verlies je je geloofwaardigheid en zet je je goede reputatie op het spel. Wereldwijd heeft 60 procent van de mkb'ers die een datalek of cyberaanval hebben meegemaakt, als gevolg daarvan klanten verloren. Die zijn overgestapt naar een partij die hun privacy wél serieus neemt."

Oplettendheid creëren

Als financieel adviseur doe je er volgens Kadhim goed aan om je te realiseren dat cybersecurity geen apart adviesonderdeel is: "Het in kaart brengen van de cyberrisico's is vaak een ondergeschoven kindje, maar moet juist bovenaan het prioriteitenlijstje staan. Ook bij de adviseur: financiële gegevens van jouw klanten moeten goed beschermd zijn. Zorg er zelf ook voor dat jouw medewerkers zich bewust zijn van de gevaren en valkuilen. Bijvoorbeeld door ambassadeurs binnen je bedrijf aan te stellen die dit regelmatig intern aankaarten. Door tips te geven over de kenmerken van phishingmailtjes en het regelmatig vernieuwen van wachtwoorden. Praat erover en zet het regelmatig op de agenda. Dit hoeft niet saai of negatief te zijn, je kunt er ook een spelletje van maken: is deze mail echt of niet? De medewerker die de meeste phishingmails herkent kun je bijvoorbeeld belonen met een cadeaukaart. Hiermee creëer je oplettendheid. En ook goed om te weten: voor het aanvragen van advies rondom cybersecurity kun je bij de Rijksdienst voor Ondernemend Nederland (RVO) subsidie aanvragen. Voordelig voor jou én je klanten."

'Een cyberincident in het mkb komt veel vaker voor dan je denkt'

Vanuit het oogpunt van de verzekeraar

Hoe gaan verzekeraars om met advies rondom cyberrisico's? Jules Brader, manager Productmanagement en Marketing bij De Goudse, legt uit: "We merken dat veel financieel adviseurs het lastig vinden om het belang van cybersecurity tussen de oren bij hun klanten te krijgen. Vaak krijgen zij meteen de reactie dat de ICT-dienstverlener van de ondernemer alles heeft geregeld, terwijl dit in heel veel gevallen de risico's niet voldoende afdekt. Om adviseurs te ondersteunen en bewust te maken van cyberrisico's, organiseren we – samen met cybersecurity professional Promax – per branche presentaties, webinars, trainingen en opleidingen. Daarnaast hebben financieel adviseurs op de website van De Goudse toegang tot de cyber toolkit. Hierin hebben we veel informatie verzameld over het risico van een cyberaanval en over onze verzekering. En om adviseurs een beter beeld te geven, zijn hier ook voorbeelden per branche te vinden. Ten slotte geeft de nieuwsbrief van Erkend MKB-adviseurs (EMA) veel informatie."

Alertheid is geboden

Brader vervolgt: "Als extra ondersteuning hebben we de app Boris ontwikkeld; een interactieve risico-inventarisatietool die alle bedrijfs- en ondernemersrisico's in kaart brengt – dus ook cyberrisico's. Zeker geen overbodige luxe: de digitalisering neemt alleen maar toe en hierdoor stijgt het risico op een cyberincident. De bewustwording bij de kleine ondernemer groeit langzaam en dat betekent dat de behoefte naar een cyberverzekering zal groeien. Tegelijkertijd verandert het risico met de tijd. Dat vraagt om continue alertheid."

Cybercriminaliteit

Telefonische hulplijn Cyberwacht helpt gehackte particulieren

Phishing e-mails, geïnfecteerde harde schijven en identiteitsfraude. Cybercriminaliteit is de afgelopen tien jaar fors gegroeid. En daarmee ook het aantal slachtoffers van cybercriminaliteit. Alle reden voor Nationale-Nederlanden om haar klanten bij te staan met preventie, service en verzekeringsoplossingen.

Nog dit jaar is de Cyberservice van Nationale-Nederlanden onderdeel van haar Inboedelverzekeringen Standaard en Maatwerk. Bestaande klanten met een inboedelverzekering krijgen de Cyberservice er vanaf hun prolongatiedatum bij, te beginnen op 1 januari 2023. Iedereen die te maken krijgt met cyberincidenten kan contact opnemen met de Cyberwacht, 070 513 5550. De Cyberwacht is van maandag tot en met vrijdag van 9.00 tot 20.00 uur bereikbaar en op zaterdag van 9.00 tot 15.00 uur.

Het aantal slachtoffers van online criminaliteit is sinds 2012 met ruim 22 procent toegenomen. In 2021 was liefst 17 procent van de bevolking van 15 jaar en ouder slachtoffer van één of meer online delicten. Dat blijkt uit de Cybersecuritymonitor 2021 van het Centraal Bureau voor de Statistiek (CBS). "Mensen denken vaak dat ze met een firewall of antivirussoftware beschermd zijn", zegt Arjan Nollen, directeur Marketing & Verkoop, Schade Intermediair, bij Nationale-Nederlanden. "Maar cybercriminelen zijn vindingrijk. Met valse e-mails die afkomstig lijken te zijn van betrouwbare organisaties maken ze bijvoorbeeld listig gebruik van de goedgelovigheid en onoplettendheid van mensen, en proberen ze inloggegevens en andere persoonlijke informatie te stelen."

Zakelijke markt

Nationale-Nederlanden voelt een grote urgentie om daar iets tegen te doen. Een verzekeringsdekking is misschien niet het eerste waar je aan denkt als je wordt geconfronteerd met cybercriminaliteit. Maar wat doe je als je bijvoorbeeld op een link hebt geklikt waardoor je laptop is gehackt, met alle mogelijke grote gevolgen van dien? Arjan: 'Voor onze zakelijke klanten is Nationale-Nederlanden samen met adviseurs een paar jaar geleden van start gegaan met PerfectDay, een cybersecurity-bedrijf voor het MKB. Met deze service hebben we inmiddels veel ervaring opgedaan: we weten met welke cyberrisico's onze klanten te maken krijgen en hoe wij hen kunnen helpen, zowel preventief als op het moment dat ze daadwerkelijk met cybercriminaliteit worden geconfronteerd.'

Particuliere markt

Deze ervaring zet Nationale-Nederlanden nu in voor haar particuliere klanten. "Uit eigen onderzoek (*bron: Motivaction B7219, in opdracht van NN, februari 2021*) weten we dat cyber-

criminaliteit een onderwerp is dat onder hen sterk leeft", aldus Arjan. "Mensen beseffen dat ze, ondanks een bepaalde mate van alertheid, gemakkelijk slachtoffer kunnen worden van online criminaliteit. Bovendien zijn er veel cyberrisico's waarvan zij zich nog niet of onvoldoende bewust zijn. Denk aan identiteitsfraude, waarbij criminelen jouw persoonlijke gegevens gebruiken om transacties te doen. Tegen deze risico's willen wij onze klanten zo goed mogelijk beschermen. Bovendien willen we hen helpen als ze daadwerkelijk met cybercriminaliteit te maken krijgen. Onze cyberpropositie, genaamd Cyberservice, biedt onze klanten preventie, service en dekking. Daarmee spelen we niet alleen in op een herkenbaar probleem, maar ontzorgen we ook onze particuliere klanten."

Aanvulling op inboedelverzekering

Nationale-Nederlanden voegt deze Cyberservice, die bestaat uit cyberpreventie, cyberdekking én cyberhulp, toe aan haar inboedelverzekeringen. "Uit ons eerdergenoemde onderzoek bleek dat veel klanten cyber een logische aanvulling op onze inboedelverzekering vinden", legt Arjan uit. "Dat kunnen wij ons goed voorstellen. Cybercriminaliteit komt helaas veel voor. De kans is dan ook groot dat onze klanten ermee te maken krijgen; groter zelfs dan de kans op brand-, inbraak- of waterschade.

Cyberwacht

De cyberservice is voortgekomen uit de Cyberwacht, die Nationale-Nederlanden al eerder ontwikkelde. "Dit is een op zichzelf staande betrouwbare helpdesk voor particuliere klanten die te maken hebben met cyberincidenten", vertelt Arjan. "Maar klanten kunnen juist ook bellen als ze preventieve maatregelen willen nemen, bijvoorbeeld als er nog geen incident heeft plaatsgevonden of als ze een verdachte e-mail hebben ontvangen. Bij de Cyberwacht werkt een team van experts. Als geen ander kennen zij de bedreigingen die rondgaan op internet en weten zij hoe te handelen. Daardoor kunnen zij onze klanten kwalitatief hoogwaardige ondersteuning bieden. Ze helpen telefonisch en kijken zo nodig op afstand mee. Het mooie is dat een helpdeskmedewerker een incident, zoals het klikken op een valse link of een vals e-mailadres, dikwijls snel kan oplossen, doordat dit incident zich in een korte periode heel veel voordoet."

Dé helpdesk

Kwalitatief hoogwaardige cyberservice om klanten te ontzorgen. Dát is waar het Nationale-Nederlanden om gaat. "En we houden deze dienstverlening niet alleen voor onszelf", benadrukt Arjan. "We stellen onze Cyberwacht ook open voor klanten van andere grote verzekeraars. Daardoor ontwikkelen we schaalgrootte, wat nodig is om onze kwaliteit te waarborgen. Daarmee zijn we met onze Cyberwacht dé helpdesk op het gebied van cybercriminaliteit geworden."

Schadedekking

Zoals gezegd biedt de cyberpropositie van Nationale-Nederlanden naast service ook een dekking voor schades als gevolg van online criminaliteit. "Daarbij kun je denken aan schade bij diefstal van geld van de rekening van de klant als gevolg van een phishing e-mail", aldus Arjan. "Of aan de vervanging van een laptop die door een cyberincident is getroffen, als het niet mogelijk is om de malware te verwijderen of als de kosten van herstel van de laptop niet in verhouding staan tot vervanging ervan."

Samen Bereik Jij Meer

De Cyberservice past volgens Arjan naadloos bij de campagne *Samen Bereik Jij Meer.* "Onze propositie is in nauwe samenspraak met het intermediair tot stand gekomen. We bundelen onze deskundigheid, zodat we met gezamenlijke moderne oplossingen klaarstaan voor onze klanten. Dat doen we vanuit de wetenschap dat onze klanten veel waarde hechten aan kwaliteit. En dat is precies waar Nationale Nederlanden voor staat: ultieme zekerheid en kwalitatief hoogwaardige dienstverlening."

Nationale-Nederlanden ■

Cybercrime-fighter Ronald Prins: ‘Trek de risico-analyse naar je toe’

Tekst Vrhl Content en Creatie
Beeld Eric Kampherbeek

Nederland is wereldwijd koploper als het gaat om IT: we doen ontzéttend veel online. Hierdoor valt er bij ons veel te halen. Aan kennis, maar ook aan geld: door complete systemen stil te leggen en zo een bedrijf te gijzelen. Een duistere business. Ronald Prins – expert op het gebied van online beveiliging – vertelt over de risico’s en hoe je die het beste kunt managen.

U bent mede-oprichter en -eigenaar van cybersecuritybedrijf Hunt & Hackett. Wat doen jullie?

“In bepaalde sectoren houden we digitale bedreigingen buiten de deur. Zoals spionage in organisaties waar waardevolle kennis is opgeslagen of belangrijke research wordt gedaan. Of hackers die bestanden proberen te stelen of de productie stilleggen om vervolgens losgeld te vragen. Dit soort dreigingen komt bij steeds meer bedrijven voor, ook in het mkb. Het is dus belangrijk om hier alert op te zijn en op voorhand maatregelen te treffen. Want er is overal wel wat te halen en als hackers ergens een opening zien, slaan ze toe.”

Hoe bewaken jullie dan precies?

“Door middel van detectie: we kijken mee met wat er gebeurt in een netwerk of in de cloud. Simpel gezegd: we kijken of hier inbrekers zijn en jagen die weg. We verzamelen gegevens die over het netwerk naar buiten gaan. Door op een slimme manier naar deze verzamelde data te kijken, kunnen we patronen ontdekken en zien of er een hacker actief is. Als er bijvoorbeeld midden in de nacht veel dataverkeer is terwijl een bedrijf is gesloten, kan dat betekenen dat er een back-up wordt gemaakt of dat een hacker informatie wegsluist. Maar hackers weten ook dat we dit zo doen, dus die proberen hier weer op een slimme manier mee om te gaan. Bijvoorbeeld door over een heel lange periode steeds kleine beetjes informatie te stelen. We proberen elkaar steeds te slim af te zijn. Dit doen we ook door in de buitenste ring van het systeem honeypots neer te zetten: lokdoosjes die gewilde informatie lijken te bevatten. Een relatief makkelijke manier om te zien of hackers jou in het vizier hebben, al binnen zijn en waar ze naar op zoek zijn. Op basis hiervan kun je je beveiliging verbeteren.”

‘Van je 1.000 medewerkers hoeft er maar één op een foute link te klikken en daar ga je’

Een spannend kat-en-muisspel dus. Werken jullie ook samen met hackers?

“Ja, we werken met zogenoemde red teams en blue teams, waarbij een red team een netwerk aanvalt en een blue team dit verdedigt. Je kan bijvoorbeeld als bedrijf een red team inhuren om te testen hoe veilig je netwerk is en of je medewerkers in een speciaal opgesteld phishing-mailtje trappen. Op deze manier kun je kijken waar de verdediging beter kan. Hierbij is het trouwens niet alleen belangrijk dat medewerkers niet op een link in zo’n mailtje klikken, maar vooral dat ze het binnenkrijgen ervan melden bij een security officer. Die kan vervolgens de andere medewerkers waarschuwen en onderzoeken of iemand anders wel op de link heeft geklikt. Het is belangrijk dit te blijven doen, want iedere maand worden er door kwaadwillende criminelen nieuwe trucjes bedacht om ergens binnen te komen. En een keer lukt het ze.”

Waarom is cybersecurity zo belangrijk?

"In de eerste plaats moet je je natuurlijk houden aan de AVG-wetgeving en persoonsgegevens veilig stellen. Maar het gaat ook om de continuïteit van je bedrijf. Als je systeem wordt lamgelegd, sta je met je rug tegen de muur. In 2016 lagen de terminals in de Rotterdamse havens drie weken plat. Reken maar uit wat dat kost. Als je als winkelier op een drukke zaterdag je pinautomaat niet kunt gebruiken, loop je al veel omzet mis. En als je als groot bedrijf in de aanloop naar kerst vijf dagen geen transacties kan doen, kan dat je faillissement betekenen. Die ransomwarejongens weten dat. Ook als er intellectueel eigendom op het spel staat. Gaat iemand met een slimme innovatie van jou aan de haal, dan is jouw bedrijf over een paar jaar misschien niet meer zo relevant – en dus niet meer zoveel waard. Veel directeuren en managers vinden security vooral irritant: het maakt het werken soms lastiger. Maar je zult wel moeten: iedereen komt een keer aan de beurt. Hoe eerder je een hacker op het spoor bent, hoe kleiner de uiteindelijke schade. Vergelijk het met je huis: je kunt nog zoveel sloten op je deur zetten en kiezen voor dubbel glas, maar je gaat pas echt gerust slapen als je een alarmsysteem hebt geïnstalleerd, dat doorschakelt naar de meldkamer van de politie. Een goed slot is een tijdvertrager, maar een hacker heeft alle tijd. Als hij maar lang genoeg tegen het netwerk aanduwt, komt hij binnen en steelt hij wat hij wil hebben. Natuurlijk is awareness en preventie belangrijk, maar van je 1.000 medewerkers hoeft er maar één op een foute link te klikken en daar ga je."

'Cyberrisico's zijn een wezenlijk onderdeel van alle risico's die een ondernemer loopt'

Hoe kan een bedrijf zelf beveiligingsmaatregelen treffen?

"Veel ondernemers denken: 'Dat kan onze IT'er er wel even bij doen', maar dat is een slecht idee. Zo zien we regelmatig dat bedrijven zich veilig wanen met een firewall, speciale computer en een awareness-training waarbij medewerkers leren niet op foute links te klikken, maar dat is echt niet genoeg. Ook zien we regelmatig dat bedrijven vertrouwen op apparaatjes die ze hebben aangeschaft om cybercriminelen buiten de deur te houden en vervolgens toch worden gehackt. Je moet je richten op detectie, net als op het gebruik van moeilijke wachtwoorden en tweefactorauthenticatie. Hetzelfde geldt voor het maken van back-ups. De meeste bedrijven doen dat keurig en denken zo veilig te zijn: 'Worden we gehackt, dan zetten we toch gewoon de back-up terug?' Maar ze hebben niet getest of dat ook werkelijk goed gaat. Of hackers hebben zich heel langzaam slim toegang verschaft tot die back-upbestanden en ze gewist. Je moet niet alleen naar apparatuur en software kijken, maar alle bedrijfsrisico's in kaart brengen en elk hoekje van je netwerk altijd in de gaten houden."

Hoe kunnen financieel adviseurs hier op anticiperen?

"Je kunt een cyberverzekering aanbieden, maar dat wordt steeds moeilijker: de premies zijn flink gestegen en de voorwaarden streng. Ik vind het jammer dat verzekeringsmaatschappijen niet intensiever samenwerken met cyberbedrijven. Bijvoorbeeld door een lagere premie aan te bieden als je samenwerkt met een goed aangeschreven cybersecuritybedrijf. Die kan niet beloven dat je nooit gehackt wordt, maar de schade altijd beperken.
Het belangrijkste is het voorkomen dat je in een hacksituatie terechtkomt. Als financieel adviseur zou je je moeten richten op de IT-controle, vooral bij zeer liquide bedrijven: die zijn erg interessant voor de ransomwarejongens. Zeker als duidelijk is waar zij hun geld mee verdienen en er computers en machines mee gemoeid zijn. Computers zijn misschien een klein schakeltje in het geheel, maar dat schakeltje moet goed afgedekt zijn. Maak als adviseur berekeningen: overleeft een bedrijf het als het twee weken plat ligt? Of als het een week niet kan factureren? Trek die risico-analyse naar je toe. Cyberrisico's zijn een wezenlijk onderdeel van alle risico's die een ondernemer loopt. Je hoeft niet zelf te snappen hoe alles in elkaar zit, maar je kunt wel adviseren om red teams in te schakelen of een gespecialiseerd bedrijf een dreigingsanalyse laten maken. En vergeet ook vooral de veiligheid van je eigen onderneming niet. Er ligt gevoelige data bij financieel adviseurs: ook jouw werk kan stil komen te liggen als je hier niet bij kunt."

WIJ ZIJN Nh1816

WE HEBBEN KENNIS VAN ZAKEN EN KENNEN DE MARKT

Sander van Mourik, accountmanager

Wij zijn Nh1816. Een deskundige, betrokken en nuchtere Westfriese particuliere schadeverzekeraar. Die klantgericht samenwerkt met lokale financieel adviseurs.

Vanuit een coöperatieve samenwerking maken we het verschil.

#klantgericht #wijzijnNh

www.Nh1816.nl/wijzijnNh

Nh1816 Verzekeringen

DISCUSSIE

Moet je als ransomware-slachtoffer losgeld betalen of niet?

Het is een vraag die al vele jaren voor verhitte discussies zorgt. Voor de getroffenen van een dergelijke cyberaanval is het vaak de snelste en goedkoopste manier om de organisatie overeind te houden. Keerzijde ervan is dat het criminele verdienmodel ermee ondersteund, beloond en gestimuleerd wordt. Is, in het geval van ransomware, een wettelijk verbod op losgeldbetalingen gewenst?

Zwaard van Damocles

"Het betalen van losgeld na een ransomware-aanval is in de meest letterlijke zin asociaal. Het is namelijk gedrag dat niet in het belang van de samenleving is. Door losgeld te betalen kan een organisatie op korte termijn uit de problemen geholpen worden. De cyberaanvallen nemen echter toe omdat de criminele kas wordt gespekt. De afgelopen jaren werd er veel losgeld betaald. De ransomware-activiteit nam toe. Men spreekt zelfs over een ransomware-epidemie. Misschien moeten we toe naar een verbod op losgeldbetalingen.

De cybersecurityindustrie staat op haar achterste benen als je zegt dat je losgeldbetaling moet verbieden. De industrie zegt dan dat sommige organisaties niet anders kunnen dan losgeld betalen en met de rug tegen de muur staan. En dat als je het verbiedt organisaties stiekem zullen gaan betalen. Ik vind deze argumenten niet getuigen van veel besef van de maatschappelijke opgave die we hebben om ransomware te voorkomen. Deze retoriek slaat alleen op de korte termijn problematiek die cybersecuritydienstverleners bij hun klanten tegenkomen.

We moeten zo snel mogelijk naar een situatie toe waarin organisaties geen losgeld hoeven betalen omdat ze een adequaat niveau van cybersecurity hebben. De markt gaat dat niet zelf oplossen omdat er een verschil is tussen de korte termijn problematiek en het lange termijnbelang van de samenleving. De overheid kan daarin sturen door niet betalen goedkoper te maken (door bijvoorbeeld ondersteuning) en het betalen van losgeld duurder (door bijvoorbeeld een belasting). Ik denk dat het goed is als een verbod op losgeld betalingen voorlopig als een zwaard van Damocles boven de markt blijft hangen."

mr. dr. ir. Bernold Nieuwesteeg
Centre for the Law & Economics of Cyber Security
directeur

Grote impact

"Door de jaren heen is ransomware een verfijnd verdienmodel geworden voor criminelen. De aanvallen die gepaard gaan met ransomware worden ook steeds complexer en meer geraffineerd. Waarbij eerst enkele systemen werden versleuteld zijn het nu volledige netwerken. Daarnaast wordt op verschillende manieren afgeperst; data publicatie, verstoren van diensten, en actief benaderen van het slachtoffer of klanten.
Ik ben van mening dat je niet zou moeten betalen, echter ligt het in de praktijk allemaal niet zo simpel. Bij Responders.NU helpen wij juist bedrijven die met de rug tegen de muur staan en de keuze moeten maken tussen betalen of faillissement. We zien bedrijven waarbij kritische bedrijfsdata die jarenlang is opgebouwd volledig is versleuteld inclusief backups. Bij veel bedrijven lijkt er nog onvoldoende besef dat elke sector vandaag de dag interessant kan zijn voor een ransomware aanval. Daarnaast zien wij ook steeds meer vitale- en zorgsectoren aangevallen worden, iets wat in de beginjaren zelfs door de aanvallers werd vermeden. Als een arts niet bij de data van een patiënt kan, dan kan dit grote gevolgen hebben, in zo'n geval wil je weer snel bij de data kunnen en is betalen soms de enige reële optie. Daarnaast is het ook nog zo dat als je betaalt niet direct alles weer hetzelfde is als voor de aanval.
De primaire bedrijfsprocessen kunnen vaak snel hersteld worden maar een aanval heeft vaak een grote impact. Bedrijven zijn doorgaans weken tot maanden bezig met herstel en implementeren van maatregelen om herhaling te voorkomen en weerbaar te zijn.
Bedrijven moeten zelf kunnen blijven afwegen om wel of niet te betalen. Met eventuele wetgeving of sancties zal het probleem niet worden opgelost maar eerder verlegd. De oplossing ligt naar mijn mening in sterke (internationale) samenwerking tussen opsporingsinstanties, crypto betaalplatformen en private bedrijven uit de IT-security sector."

Rickey Gevers
Responders.NU
Voorzitter

Victim-blaming

“We willen natuurlijk allemaal graag het criminele verdienmodel doorbreken. Misdaad mag niet lonen. Door het betalen van losgeld strafbaar te maken wordt de verantwoordelijkheid voor het doorbreken van dit verdienmodel in mijn ogen onevenredig veel bij het slachtoffer neergelegd. Sowieso doen we in ons vakgebied al veel aan victim-blaming. Want als een organisatie geraakt wordt door een cyberincident, dan staan de kranten vol over hoe slecht het daar dan met de beveiliging was gesteld. Natuurlijk hebben organisaties een verantwoordelijkheid als het gaat om het op orde brengen en houden van hun cybersecurity. Maar we moeten hen ook helpen als ze geraakt worden door een aanval om de juiste stappen te zetten. Om het criminele verdienmodel te doorbreken moeten we in mijn ogen het ecosysteem veranderen en vanuit een systemisch perspectief naar deze uitdaging kijken. En vooral ook goed samenwerken in de strijd tegen deze vorm van criminaliteit. De politie moet bijvoorbeeld meer capaciteit steken in opsporing en het verstoren van de werkwijze van criminelen. Én organisaties moeten hun weerbaarheid verhogen. Én ze moeten aangifte doen als ze slachtoffer zijn geworden. Én we moeten stimuleren dat slachtoffers minder snel geneigd zijn om losgeld te betalen. Én …? We dachten hier een tijdje geleden al eens over na met experts uit de wetenschap en de cybersecuritysector. Eén van de ideeën die toen ontstond is het onderzoeken van een ‘anti-ransomware fonds’ dat onder voorwaarden organisaties ondersteunt die geen losgeld betalen. Ook denk ik dat we een verplichting om losgeld te betalen beter kunnen vervangen door een verplichting tot het delen van informatie over een ransomware incident met de overheid en de cybersecuritysector. Met die informatie kunnen nieuwe slachtoffers worden voorkomen. En ook dat helpt om het verdienmodel te doorbreken.”

Petra Oldengarm
Cyberveilig Nederland
directeur

Forensisch onderzoek

“Een verbod op losgeldbetaling bij ransomware is de abortus van cybersecurity. Iedereen wenst een wereld waarin losgeld niet nodig is. Tegelijkertijd is de realiteit dat er slachtoffers vallen. Niemand zou betalen als er alternatieven waren. Ik ben pertinent tegen de criminalisering van hulp aan het slachtoffer en dit past ook helemaal niet in de Nederlandse rechtstraditie. Als we die kant op gaan, zal hulp duurder en slechter worden. Bovendien verliezen we dan zicht op ransomware en daarmee de ontwikkeling voor mogelijke oplossingen. Daarnaast is het recht op de inzet van het uiterste middel (losgeldbetaling) een vorm van zelfbeschikking. Wij mogen niet aan een ondernemer vragen zijn of haar bedrijfsmatige levenswerk op te offeren voor het grotere goed terwijl wij collectief niet in staat zijn om onze samenleving te vrijwaren van deze vorm van criminaliteit.

Een ontwikkeling die mij zorgen baart, is dat steeds vaker forensisch onderzoek uitblijft. Als er een wettelijke eis komt, of een voorwaarde voor verzekeringsuitkering, dan graag verplicht forensisch onderzoek naar de oorzaken zodat wij deze inzichten met elkaar kunnen delen. Daar worden we allemaal veiliger van. Ook zou de AP een constructieve rol kunnen spelen door geen boete op te leggen bij bijvoorbeeld een datalek, maar een onderneming te verplichten om bijvoorbeeld de aanbevelingen op te volgen die uit dat forensische onderzoek voortkomen.”

Inge Bryan
FOX-IT
directeur

ASN AUTOSCHADE

Autoschade?

Bij ASN Autoschade staan u en uw berijder centraal, wij ontzorgen en verrassen. ASN Autoschade heeft een landelijk dekkend netwerk van autoschadeherstelbedrijven. Bij alle ASN Autoschade vestigingen staan kwaliteit, efficiëntie en klanttevredenheid hoog in het vaandel. Wij zijn een gewaardeerd partner voor verzekeraars, volmachten, leasemaatschappijen, fleetowners en dealerorganisaties.
Wij doen er alles aan om u en uw berijders tevreden te stellen, want schade is al vervelend genoeg.
Bekijk onze scores op asnautoschade.tevreden.nl

Tevreden klanten
Onafhankelijk en transparant klanttevredenheidsonderzoek

Landelijk netwerk
Franchiseketen met zelfstandige ondernemers

Autoschade
Vakkundige medewerkers en modern gereedschap

Vervangend vervoer
ASN Autoschade houdt uw klanten mobiel met vervangend vervoer en haal- en brengservice

Klant contact center
24/7 bereikbaar

Polis check
Dekking verificatie via webservice voor procesvoordeel en tijdwinst

Meer weten? Bel 020 - 44 88 020

BOVAG ERKEND SCHADEHERSTEL · GROEN GEDAAN! · DEKRA · Quick Repair. · Tevreden.nl

www.asnautoschade.nl

Maak van de computer een wasmachine

Tekst: Bas Haring
Beeld: Heidi de Gier

Ik neem aan dat u ongeveer weet hoe een wasmachine werkt. Het is een grote bak waar water in kan stromen, met onderin een elektrische spiraal om dat water op te warmen. In de bak draait een trommel met gaatjes waar de was in gaat. Het zit natuurlijk ietsje ingewikkelder in elkaar, maar dit is in essentie wat een wasmachine is. En hoe dan ook is een wasmachine – naar ik aanneem – geen magisch apparaat voor u.

Dat is voor velen met computers net iets anders. Die lijken wél een beetje magisch. Je kunt er teksten op schrijven, maar ze kunnen ook rekenen, je kunt er spelletjes op doen, en ze zijn tegenwoordig zelfs slim. Rara hoe kan dat?

Ik ga hier niet de computer demystificeren; voor de uitleg van hoe een computer werkt heb ik meer tekst nodig. Maar ik heb wel de ruimte om te zeggen dat het magische van computers een consequentie heeft: u bent er eerder bang van. U bent niet bang voor wasmachines; u weet immers wat voor apparaten het zijn. Maar computers zijn vanwege hun ondoorgrondelijkheid voor velen wel een beetje angstaanjagend: Zijn ze wel te vertrouwen? Kunnen anderen geen misbruik van ze maken? En is het veilig om gegevens aan ze toe te vertrouwen?

Er is een oplossing voor deze angst: maak van de computer een wasmachine. In metaforische zin. Verdiep je eens in dat apparaat. Sloop er eentje uit elkaar, of doe een cursus programmeren. U gaat niet leren de computer compleet te doorgronden. Maar dat hoeft ook niet. U zult wel beter gaan nadenken over de veiligheid van computers, hun risico's en nadelen. Zonder overdreven angst.

Bas Haring

Bas Haring is filosoof en informaticus. Aan de universiteit van Leiden is hij bijzonder hoogleraar publiek begrip van wetenschap en oprichter van het masterprogramma media technologie van LIACS. Hij is daarnaast schrijver. Hij schreef onder meer *Kaas en de evolutietheorie*, *Voor een echt succesvol leven*, *Waarom cola duurder is dan melk* en *Why Biodiversity Loss is Not a Disaster*. Op televisie presenteerde hij voor de RVU de programma's *Stof*, *Haring* en *Wisebits*. Hij schrijft ook columns voor onder meer de Volkskrant.

Werken aan digitale weerbaarheid

Tekst Sébastien Wulms
Beeld Shutterstock

Tijdens de coronacrisis heeft digitalisering in het dagelijkse leven een enorme versnelling doorgemaakt. Daardoor is de afhankelijkheid van digitale processen nog meer toegenomen, net zoals het aantal gerichte cyberaanvallen op organisaties. Uit cijfers blijkt dat bijna 7 op de 10 ondernemers in Nederland al eens te maken heeft gehad met een cybersecurityincident, zoals een hack of een datalek. En dat aantal is nog steeds groeiende.

Als risicomanager van zijn klanten is de financieel adviseur bij uitstek de persoon die een belangrijke rol kan spelen bij het in beweging brengen van ondernemers door ze bewuster te maken van cyberrisico's en te adviseren over hoe met deze risico's om te gaan. Zélf bewust zijn van de cyberrisico's die de adviseur loopt én maatregelen treffen om deze risico's te voorkomen of te verkleinen, zijn daarbij cruciaal. Als de branchevereniging van onafhankelijk financieel adviseurs ondersteunt Adfiz haar leden daar volop bij vanuit de gedachte *practice what you preach*.

Wet- en regelgeving

Voor financieel adviseurs is het niet alleen belangrijk dát ze hun digitale weerbaarheid op orde brengen, maar ook dat ze deze op zo'n manier inrichten, vormgeven en onderhouden dat dit in lijn is met de vereisten die wet- en regelgevers hieraan stellen:

- Zo stelt de AVG informatiebeveiligingseisen op het gebied van het beveiligen van persoonsgegevens, het inschakelen van verwerkers en de omgang met datalekken.
- Verwacht de AFM dat de wijze waarop wordt omgegaan met informatiebeveiliging en digitale weerbaarheid wordt vastgelegd in beleid, dat daarnaar gehandeld wordt en dat het beleid up-to-date wordt gehouden.
- En ook op Europees niveau wordt met de verordening DORA gewerkt aan het vergroten van de digitale weerbaarheid van ondernemingen in de financiële sector.

5-stappenplan

Er zijn dus nogal wat instanties betrokken bij het digitaal weerbaarder maken van bedrijven in de financiële sector. Om ondernemers wegwijs te maken door de vele informatiedocumenten, checklisten en hulpmiddelen die beschikbaar worden gesteld om de eigen digitale weerbaarheid en informatiebeveiliging op het goede niveau te brengen, heeft Adfiz het kennisportaal Digitale weerbaarheid ontwikkelt. Hierin wordt aan de hand van een 5-stappenplan uitgelegd hoe advieskantoren hun informatiebeveiliging structureel op orde houden en hoe ze dat kunnen doen zodat ze ook meteen compliant zijn. Daarvoor wordt per stap aangegeven hoe de AFM kijkt naar de benodigde maatregelen, welke tools kunnen helpen om de stappen goed te doorlopen en waar meer informatie kan worden gevonden.

Proportionaliteit

De eisen op het gebied van digitale weerbaarheid die aan ondernemers in de financiële sector worden gesteld, zijn omvangrijk en vragen om een flinke investering in tijd en geld. Daarbij is het goed om te weten dat adviseurs deze naar proportionaliteit mogen toepassen, dus rekening houdend met de aard, complexiteit en omvang van de onderneming.

Meer informatie:
www.adfiz.nl/dossiers/digitale-weerbaarheid

'De adviseur is bij uitstek de persoon die ondernemers kan helpen met cybersecurity aan de slag te gaan'

5-Stappenplan

Stap 1: risico's inventariseren

Welke risico's loopt de onderneming? Daarbij is het goed voor de ondernemer om zich te realiseren dat de dreiging kan komen vanuit:

- Intern (nalatigheid medewerker)
- Extern (verwerker, toeleverancier)
- Digitaal (hack, ransomware)
- Fysiek (ongeautoriseerde toegang computersystemen op werkvloer, natuurrampen, stroomuitval).

Stap 2: maatregelen treffen

Als inzichtelijk is welke risico's de onderneming loopt op het gebied van informatiebeveiliging, wordt vanzelf ook duidelijk óf er al maatregelen zijn getroffen en zo ja, welke maatregelen dat dan zijn. De maatregelen voor informatiebeveiliging zijn onder te verdelen in vier gebieden:

- Technisch (antivirussoftware, firewalls, encryptie)
- Mens en cultuur (bewustwordingsprogramma's, trainingen, waar melden)
- Processen (beschikbaarheid, integriteit en vertrouwelijkheid van systemen waarborgen)
- Fysiek (gebouwen, apparatuur).

Stap 3: verantwoordelijken aanwijzen

Vastleggen wie verantwoordelijk is voor het treffen, uitvoeren en onderhouden van de maatregelen. Niet alleen intern, maar ook in het geval dat er bepaalde (kritische) diensten en activiteiten zijn uitbesteed.

Stap 4: implementatie

Zijn de informatiebeveiligingsrisico's binnen de onderneming geïnventariseerd, de juiste maatregelen bepaald om ze te (helpen) voorkomen en verantwoordelijken aangewezen? Dan is het belangrijk om ervoor te zorgen dat de wijze waarop de onderneming met informatiebeveiliging wil omgaan, wordt ingevoerd en nageleefd.

Stap 5: schriftelijke vastlegging

In het informatiebeveilingsbeleid legt de onderneming vast hoe de organisatie met een samenhangend geheel van maatregelen, procedures en processen de informatiebeveiligingsrisico's beheerst. Het informatiebeveiligingsbeleid moet actueel gehouden worden door dreigingen en risico's periodiek te evalueren.

Lindenhaeghe

Laatste kans!

PE SEH 2022

Boek nu jouw PE SEH-training
en haal jouw punten voor 2022.

**Verschillende
combinaties mogelijk.**

Autoruitschade?

Bij A•Glas Autoruitschade staan u en uw berijder centraal, wij nemen graag alle zorgen uit handen. A•Glas Autoruitschade heeft een landelijk dekkend netwerk. Bij alle A•Glas Autoruitschade vestigingen staan kwalitatief hoogstaand en veilig herstel van autoruitschade, met een focus op efficiëntie, hoog in het vaandel. De klant staat bij ons altijd centraal, en geniet van een volledige ontzorging. A•Glas is een gewaardeerd partner voor verzekeraars, volmachten, leasemaatschappijen, fleetowners, tussenpersonen en dealerorganisaties.

Klantcontactcenter
24/7 online en telefonisch bereikbaar

Reparatie
Autoruitschade snel en veilig hersteld

Ontzorgen
A•Glas regelt alles met uw verzekering

Tevreden klanten
Onafhankelijk en transparant klanttevredenheidsonderzoek

Landelijk netwerk
Franchiseketen met zelfstandige ondernemers

Autoruitschade
Vakkundige medewerkers met modern gereedschap

Tevreden.nl

Wilt u meer weten? Bel ons op: 020 – 44 88 022

www.aglas.nl

Hoe is het geregeld in jouw droomland?

Zorgverzekering in het buitenland niet vanzelfsprekend

De charme van werken en wonen in het buitenland is natuurlijk de uitdaging. Het land en misschien wel het leren van een andere taal, maar een gezonde dosis realisme is ook belangrijk. De zorgverzekering - en ook andere verzekeringen - zoals wij die in Nederland hebben, is niet zo vanzelfsprekend in andere landen.

Als je gaat emigreren zijn je verzekeringen niet het eerste waar je bij stilstaat. Kijken waar de dichtstbijzijnde school is of de beste route naar de supermarkt gaan vaak voor; de verzekering blijft een sluitpost.

Maar hoe zit het eigenlijk? Als je gaat emigreren, schrijf je je uit in Nederland. Zodra je dat doet, vervalt je recht op een zorgverzekering in Nederland. Wat gebeurt er dan als je in het buitenland ziek wordt? Of stel dat je moeder in Nederland overlijdt: wie betaalt dan je vliegticket? Dat zijn zaken waar je liever niet over na wilt denken, maar die wel kunnen gebeuren.

OOM Verzekeringen verkoopt niet alleen alle verzekeringen die je als emigrant of expat nodig kunt hebben, maar wil ook graag bewustwording creëren bij mensen met emigratieplannen. Nederland is een uniek land, alles is hier tot in de puntjes geregeld. Dat er zoveel regeltjes zijn, is vaak ook een reden om te vertrekken. Maar wij horen maar al te vaak: 'In het buitenland is niets geregeld.' In Nederland leven we in een verzorgingsstaat. We kennen de AOW, de werkloosheidswet, we hebben overal een potje voor. Maar in het buitenland is dat niet overal zo.

Niet alleen het landschap wordt anders

We horen vaak dat Nederlanders in het buitenland bijvoorbeeld op een lokaal contract werken en dan een ziektekostenverzekering hebben bij hun werkgever maar dat deze niet afdoende is. Bij andere verzekeraars zit er vaak een maximering op de vergoeding, wij betalen kostprijs oftewel wat het kost. Ook het ziekenhuis kies jij, wij geven je die keuzevrijheid. Omdat we heel goed weten dat verblijf in een openbaar ziekenhuis in sommige landen niet hetzelfde is als in Nederland. Een goede nazorg is minstens zo belangrijk als de behandeling zelf.

Besteed tijd aan het checken van je verzekering, al is het maar een uurtje. Je neemt jezelf en je gezondheid altijd overal mee naartoe. Besef wat dat voor consequenties heeft. Steek je kop niet in het zand. Wat wordt er niet beter op en hoe kun je dat invullen? Goede voorlichting is het halve werk.

Wil je meer weten?
Check dan www.oomverzekeringen.nl ■

‘De kennis die Jan heeft van de paardensport is enorm waardevol’

Tekst Sébastien Wulms
Beeld Loraine Bodewes

Nederlandse springpaarden gooien al jaren hoge ogen op (inter)nationale concoursen. Maar voordat een paard dat niveau (mogelijk) bereikt, gaat er een intensieve, meerjarige training aan vooraf. Leon Kuijpers, van Stal Krabbebos in Breda, is een van die specialisten die paarden traint tot een carrière als springpaard. Zijn adviseur Jan Timmermans, van Timmermans Verzekeringen uit Oosterhout, zorgt ervoor dat de risico’s die daarbij komen kijken goed gemanaged worden.

Paardeneigenaren, zowel nationaal als internationaal, weten Kuijpers te vinden als het gaat om hun paard de basisbeginselen aan te leren van het springen. Rond het vierde levensjaar vertrouwen zij hun paard toe aan Kuijpers die vervolgens een intensief twee à driejarig opleidingstraject start. Kuijpers: “Wat ik het paard aanleer, is vertrouwd te raken met een hindernisparcours. Ik zorg ervoor dat als een paard mijn stal verlaat, het weet wat er van hem verwacht wordt tijdens een springwedstrijd. Dat betekent zeker niet dat een paard dan klaar is met zijn opleiding: ik leid het op tot een bepaald niveau en daarna is het aan de ruiter om er verder mee aan de slag te gaan.” Kuijpers heeft zo continu vijftien à twintig paarden onder zijn hoede.

Passie voor paarden

Op het vlak van risicomanagement wordt hij daarbij ondersteund door Timmermans, zelf ook een paarden-

liefhebber in hart en nieren: “De passie voor paarden heb ik meegekregen van mijn vader. Op mijn vierde kreeg ik mijn eerste pony en in de twintig jaar daarna ging er vrijwel geen dag voorbij zonder dat ik in het zadel te vinden was. Ik was in die tijd vrij fanatiek bezig met de paardensport en deed mee aan wedstrijden in zowel het binnen- als buitenland. Maar op een gegeven moment verwaterde dat een beetje: ik was klaar met mijn studie, kreeg een baan en verhuisde verder van de stal vandaan. Maar de interesse voor paarden is nooit verdwenen: mijn kinderen rijden nu paard en samen met een aantal bevriende ondernemers investeer ik in paarden als belegging.”
Die passie voor paarden is volgens Timmermans cruciaal voor een adviseur die hippische ondernemers adviseert over risico’s: “De wereld van de paardenhouderij is toch een beetje een apart wereldje met zijn eigen gebruiken en eigenaardigheden. Het is ons kent ons en veel gebeurt op basis van vertrouwen. Om een voorbeeld te geven: de opdracht om een paard op te leiden, wordt vaak mondeling gegeven; er staat niets op papier. Vanuit risico-oogpunt is dat niet zo handig. Want wat als er iets gebeurt met een paard van enkele tienduizenden euro’s dat Leon onder zijn hoede heeft? Dat zijn risico’s waarvan ik tegen Leon zeg: ‘die moet je niet willen lopen’.” Om dergelijke aansprakelijkheidsrisico’s beter te managen heeft Timmermans, samen met een jurist, standaardcontracten laten opstellen voor het trainen en verzorgen van de paarden en de vergoeding die daarvoor staat.

Toewijding

Ook voor Kuijpers is het een pre dat Timmermans de paardenwereld kent. “Jan weet hoe het er in de praktijk in een stal en tijdens wedstrijden aan toe gaat en hoe paarden soms kunnen reageren. En hij kan dat ook nog eens goed uitleggen, richting verzekeraars bijvoorbeeld. Zo heb ik een paar jaar geleden tijdens een wedstrijd een open beenbreuk opgelopen als gevolg van een trap van een paard van een ander. Dankzij Jan heeft me dat financieel geen nadeel opgeleverd.”

‘Ik heb de andere partij toen aansprakelijk gesteld voor de inkomensderving’

Timmermans herinnert zich het voorval ook nog goed: “Leon heeft een goede naam in de paardensport. Klanten komen naar hem toe vanwege zijn reputatie. Als hij het paard niet kan trainen, kan dat ertoe leiden dat ze het paard weghalen. Dat was ook het geval toen Leon met die breuk zat; bijna de helft van de paarden is toen weggehaald. Ik heb de andere partij toen aansprakelijk gesteld voor de inkomensderving, maar diens verzekeraar beweerde dat Leon onvoorzichtig was geweest en dat het zijn eigen schuld was. Maar ik ken Leon; hij is nooit onvoorzichtig in het bijzijn van paarden.” Door de omstandigheden – zoals waar Kuijpers zich exact bevond tijdens het ongeluk en hoe groot het paard was – minutieus in kaart te brengen, kon Timmermans aantonen dat Kuijpers zich aan alle veiligheidsvoorschriften had gehouden en geen schuld had aan het ongeval. De verzekeraar moest alsnog over de brug komen. Kuijpers: “De kennis die Jan heeft van de paardensport en de toewijding waarmee hij zich in deze zaak beet, is enorm waardevol.”

Madelon Moorlag, Afdeling Vermogensbeheer
Klaverblad Verzekeringen

'De groene intermediair moet de standaard worden'

In 2050 beleggen we bij Klaverblad volledig klimaatneutraal. Dat is geen wens, maar een belofte. En om dat te realiseren is er hard gewerkt aan een duurzaam beleggingsbeleid met concrete tussendoelstellingen voor 2030. Onze manager Vermogensbeheer Madelon Moorlag legt uit wat klimaatneutraal beleggen en duurzaam vermogensbeheer inhoudt.

Madelon startte in 2018 de afdeling Vermogensbeheer op binnen Klaverblad. In datzelfde jaar ondertekende de verzekeringsbranche ook het IMVO-convenant (zie kader). Alle pijlen waren gericht op het opzetten van en invulling geven aan duurzaam beleggingsbeleid. Een extra motivatie om vanuit Klaverblad een goed voorbeeld te geven. Inmiddels is de tweede versie van het beleid ingevuld, gepubliceerd in juni 2022, en weten we wat ons te doen staat.

Waarom is duurzaam beleggen belangrijk?

"We beheren bij Klaverblad honderden miljoenen euro"s aan vermogen. Daarmee kunnen we altijd direct uitkeren aan onze verzekerden. Dat is het belangrijkste doel van ons vermogensbeheer: mensen helpen op het moment dat dat nodig is. Als coöperatie beleggen we ook een deel van het vermogen. En dat doen we zo duurzaam mogelijk. Een positieve bijdrage leveren aan de maatschappij begint bij jezelf en het handelen naar je overtuigingen. Daar zijn we ons erg van bewust en daarbij zetten we de mens centraal. Welzijn en goede leefomstandigheden zijn volgens ons de voorwaarden voor een prettig en onbezorgd leven.

Het IMVO-convenant

De verzekeringssector heeft met haar beleggingen in bedrijven een belangrijke rol in het voorkomen en terugdringen van schade aan het milieu en schending van mensenrechten. Verzekeraars, de overheid en vakbonden hebben in het IMVO-convenant (Convenant internationaal verantwoord beleggen in de verzekeringssector) vastgelegd hoe als sector aan de slag te gaan met verantwoord beleggen. Vroeger werkten we met de zogeheten 'Code Duurzaam Beleggen'. Deze is opgegaan in het IMVO-convenant.

Het een is vaak van invloed op het ander. Zo hebben leefomstandigheden zoals toegang tot schoon drinkwater een grote invloed op het welzijn van mensen.
Duurzaam en verantwoord beleggen zien we als een vanzelfsprekendheid. Op de langere termijn kunnen die duurzame keuzes bovendien tot financieel voordeel leiden, daar zijn we van overtuigd."

Wat zijn dan duurzame keuzes?

"Het spreekt denk ik voor zich dat we niet beleggen in bedrijven of landen die (inter) nationale principes schenden op het gebied van duurzaamheid. Maar duurzaam beleggen omvat meer dan dat. Onze negatieve impact op mens en milieu proberen we zoveel mogelijk te voorkomen. Maar we kijken ook naar hoe we ons actief kunnen inzetten voor een pósitieve impact. Dat bereiken we door onder andere te investeren in duurzame bedrijven en ons aan te sluiten bij grotere platforms die duurzaamheid op de voor ons belangrijke en specifieke thema's omarmen."

'Welzijn en goede leefomstandigheden zijn belangrijke voorwaarden'

In welke bedrijven wordt er geïnvesteerd?

"Niet zo lang geleden hebben we onze aandelenportefeuille opnieuw ingericht. Met een blik op de toekomst en focus op het terugdringen van

onze Carbon Footprint. Zo bestaat nu minstens 5 procent van onze aandelen uit een 'green pocket'. Dat zijn bedrijven die duidelijk bijdragen aan de energietransitie. Daarnaast investeren we in bedrijven waar een strenge selectie op is gedaan ten aanzien van onze duurzaamheidscriteria. We hebben zelf niet de omvang om direct een financiële impact te maken. Daarom willen we ook laten zien waarom we bepaalde – soms moeilijke - keuzes heel bewust maken."

Transparantie voorop dus?

"We vinden het belangrijk om onze duurzaamheidsinspanningen te delen en zichtbaar te maken, ja. Dat het niet blijft bij het schrijven van beleid, maar dat iedereen kan zien wat we doen en waar we staan. Transparant, met een duidelijke toelichting op alle thema's én in normale, voor iedereen begrijpelijke taal. Daarom ontwikkelen we nu een dashboard dat in de toekomst voor iedereen is in te zien.

'We zetten ons actief in voor een pósitieve impact.'

Van doelen naar actieplan, hoe gaat dat?

"Onze nieuwe versie van het duurzame beleggingsbeleid is net gepubliceerd en voor 95 procent geïmplementeerd. Voor het einde van 2022 zijn ook alle actieplannen met onze ambities tot 2030 klaar. Dan hebben we mooie mijlpalen om naartoe te werken. Wij richten ons in ons beleggingsbeleid hoofdzakelijk op vijf duurzame thema's. Stuk voor stuk thema's die aansluiten bij de SDG's (Sustainable Development Goals of Duurzame Ontwikkelingsdoelen) die zijn opgesteld door de Verenigde Naties om van de wereld een betere plek te maken in 2030. De vijf meest relevante thema's waar we een verschil kunnen maken, zijn Klimaat, Biodiversiteit, Water, Circulariteit en Gezondheid.'

Wat moet er gebeuren om deze doelen te halen?

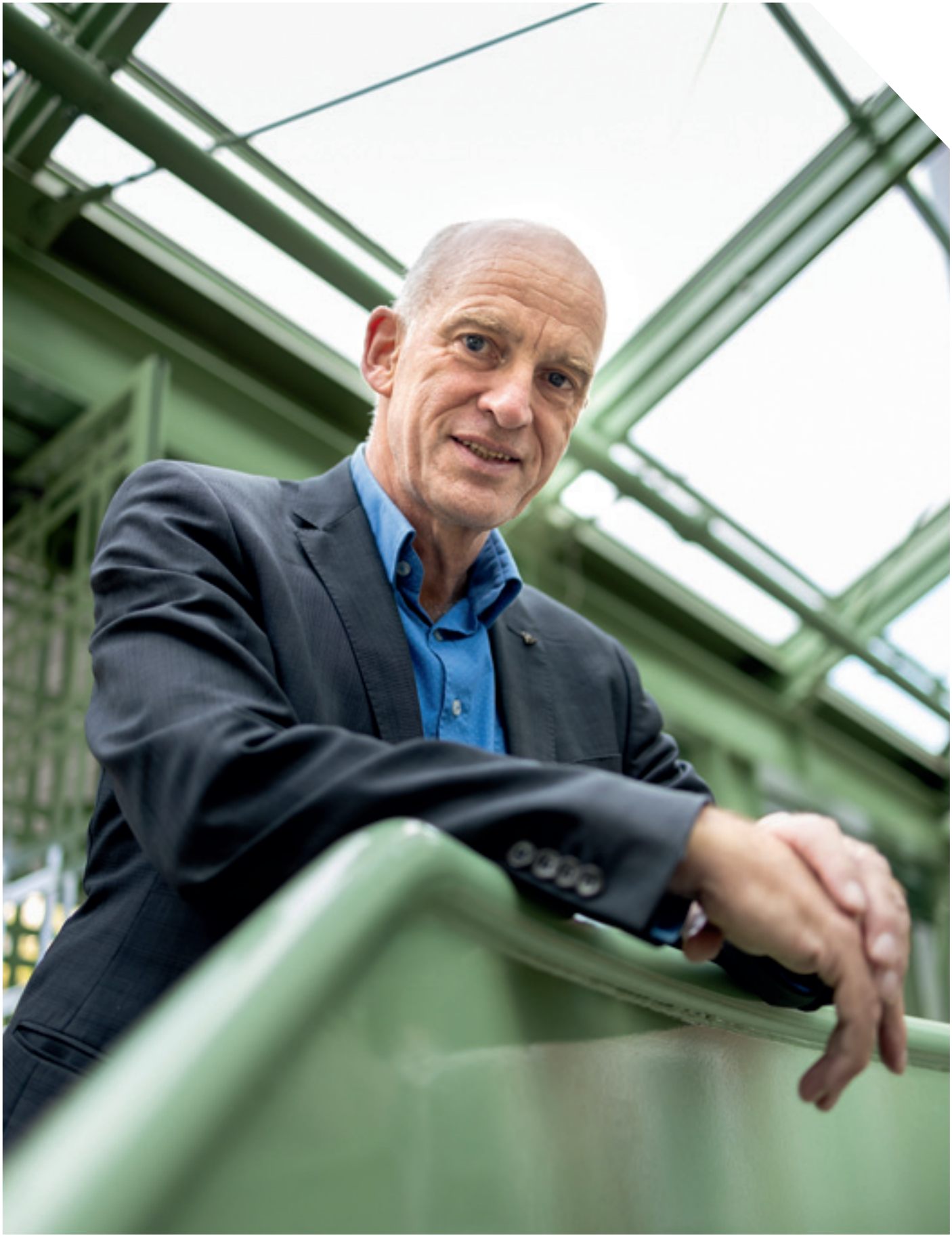
"Dat verschilt per thema. Onze belangrijkste doelstelling is duidelijk: volledig klimaatneutraal beleggen. Liever vandaag nog dan morgen, maar uiterlijk in 2050. Een tussendoel is om in 2030 de 'carbon footprint' van onze beleggingen alvast met 50 procent verminderd te hebben ten

opzichte van 2020. Hetzelfde geldt voor de afvalproductie van bedrijven waarin we investeren. Kijk je naar biodiversiteit, dan willen we in 2030 niet meer bijdragen aan ontbossing. Zo werken we voor elk van de vijf thema's concrete doelstellingen uit.'

Welke rol speelt samenwerken tot slot?

"Verzekeren is vertrouwen. Zoals verbinden een belangrijke waarde is in de omgang met onze verzekerden, geldt dat ook voor onze omgang met vermogensbeheerders. Daar willen we echt een band mee opbouwen. En zo hopen we ook dat de verzekeringsadviseurs waarmee we samenwerken steeds meer onze duurzame principes uitdragen. Dat helpt toekomstige verzekerden bewuster kiezen.'

Klaverblad Verzekeringen ■



‘Je hebt pas oog voor alle risico’s als je ook oog hebt voor cyberrisico’s’

Tekst Sébastien Wulms
Beeld Eric Kampherbeek

Nederland kent meerdere overheidsinstellingen die zich bezighouden met cybersecurity. Een van die instellingen is het Digital Trust Center (DTC), een onderdeel van het ministerie van Economische Zaken en Klimaat. Michel Verhagen, hoofd van het DTC, vertelt met welke doelstellingen het DTC is opgericht en hoe belangrijk de hulp van de diverse branches is om die doelen te bereiken.

“Dat het cruciaal is dat vitale organisaties, zoals banken, energieleveranciers, telecomproviders en de overheid hun cybersecurity op orde hebben, snapt iedereen. Een hack bij een energieleverancier, waardoor grote delen van Nederland zonder stroom komen te zitten, of bij een bank, waardoor het niet meer mogelijk is om geld over te maken, kunnen tot grote onrust leiden en de maatschappij ontwrichten. Dergelijke vitale organisaties helpen digitaal weerbaarder te worden is het domein van mijn collega’s van het Nationaal Cyber Security Centrum (NCSC).”

Achilleshiel

“Ongeveer vijf jaar geleden heeft de overheid besloten dat niet alleen vitale organisaties aandacht en hulp behoeven op het vlak van cybersecurity, maar dat dit net zo goed geldt voor niet-vitale organisaties. Onze sterke economische positie steunt immers voor een belangrijk deel op de hoge mate van digitalisering in Nederland, maar dat is tegelijkertijd ook onze achilleshiel. Daarom is het zo belangrijk dat ondernemers, en dat geldt overigens ook voor burgers, digitaal weerbaar zijn en hun digitale veiligheid op orde hebben. Want: van zzp’er tot grootbedrijf; ze lopen stuk voor stuk het risico slachtoffer te worden van een cyberaanval. Dat besef is er nog onvoldoende. ”

“Om die digitale weerbaarheid van de circa twee miljoen bedrijven te vergroten, werken we langs twee hoofdlijnen. Enerzijds is dat door ondernemers informatie en advies aan te bieden waar ze direct zelf mee aan de slag kunnen. De vijf basisprincipes van veilig digitaal ondernemen – die ondernemers als gids kunnen gebruiken om de basale, digitale veiligheidsmaatregelen van hun onderneming op orde te krijgen – zijn daar een goed voorbeeld van. De andere lijn is het stimuleren van samenwerkingsverbanden: we stellen subsidies beschikbaar voor bedrijven om samen te werken in de keten, regio of branche. Op die manier kunnen organisaties van elkaar leren en elkaar inspireren en helpen om veiliger digitaal te werken.”

> ‘Van zzp’er tot grootbedrijf; ze lopen stuk voor stuk het risico slachtoffer te worden van een cyberaanval’

Aan de slag

“Die twee miljoen bedrijven bereiken en overtuigen om hun cyberveiligheid op orde te brengen, lukt ons overigens niet in ons eentje. Daarom trekken we samen op met bijvoorbeeld regionale organisaties als de Rotterdamse haven of Brainport Eindhoven. En we werken intensief samen met brancheorganisaties als Adfiz om bedrijven zo goed en zo breed mogelijk te bereiken. En dat werpt z’n vruchten af. Steeds meer bedrijven gaan aan de slag met cyberveiligheid. Of dat nu is omdat het moet van de regelgever, omdat een bedrijf het verlangt van een toeleverancier, het uit eigenbelang is, of omdat financieel adviseurs hun klanten er steeds beter van kunnen overtuigen dat ze pas oog hebben voor alle risico’s als ze ook oog hebben voor cyberrisico’s.”

WIE IS...

Harry Berkelouw is een geboren Rotterdammer. Hij deed de meao waar hij stageliep bij een verzekeraar; dat werk greep hem meteen. Na de meao werkte hij bij verzekeraar Stad Rotterdam waar hij zich bezighield met de transportverzekeringen. In de avonduren behaalde hij het assurantie B en A diploma, branche varia diploma en het GA-diploma. Voorts vanuit de eigen organisatie diverse (internationale) opleidingen. Kwam vervolgens bij Kuehne + Nagel terecht binnen de kleinere Nacora multinational. Hij hield zich als Regional Director Benelux, naast de reguliere bedrijfsmatige verzekeringen, vooral bezig met transport- en transportaansprakelijkheidsverzekeringen. De focus met name op de logistieke dienstverleners. Inmiddels werkt hij er al 32 jaar met veel plezier.

‘Hou je vast aan waar je goed in bent’

Tekst Vrhl Content en Creatie
Beeld Eric Kampherbeek

Ruim 7 miljoen relaties worden geholpen door Adfiz-leden. Wie zijn deze mannen en vrouwen die dagelijks alles op alles zetten om hun klanten zo goed mogelijk te bedienen? Elk nummer laat een lid het achterste van zijn tong zien in de rubriek Spiegel. Dit keer Harry Berkelouw (63) Regional Director Benelux bij Nacora International Insurence Brokers in Rotterdam.

Je werkt al 32 jaar bij Nacora. Nooit de behoefte gehad verder te kijken?

“Ik hoor mensen vaak zeggen: ‘Goh, wat een prestatie om ergens zo lang te werken.’ Maar ik heb het leukste beroep dat er is. Het voelt niet als een prestatie, omdat ik het hier ontzettend naar mijn zin heb, en daardoor ook nooit de neiging gehad om op zoek te gaan naar een andere baan. Dat we een internationaal kantoor zijn met wereldwijd 85.0000 medewerkers, maakt het heel leuk en afwisselend – zo ben ik regelmatig in het buitenland om klanten op te zoeken. Dit jaar bestaat Nacora vijftig jaar en er komt een groot feest in Hamburg om dat te vieren. Ik kijk er nu al naar uit.”

Wat is jouw drijfveer?

“Met Nacora richten wij ons heel sterk op een specifiek stuk dienstverlening; namelijk de vervoerders en expediteurs in de transportsector. Het leuke is dat we ook echt de taal van onze klanten spreken. Wat transportverzekeringen behelzen, kun je uit een boekje leren, maar er helemaal inzitten dat kost vele jaren. Je hebt praktijkervaring nodig om goede adviezen te kunnen geven. Ik merk dat ik het heel leuk vind om die kennis over te dragen aan jonge mensen op kantoor. Denk bijvoorbeeld aan het delen van productinformatie, maar ik neem medewerkers ook vaak mee naar nieuwe prospects. Dan evalueren we hoe een gesprek verloopt, wat de knelpunten zijn en hoe ze daarmee kunnen omgaan. Als ik dan zie dat ze daar zelf een bepaalde routine in ontwikkelen en ze zich steeds verder in het vak verdiepen – dat is heel leuk om te zien.”

Welke karaktereigenschap zit je soms in de weg?

“Ik ben een harde werker en ga door totdat iets is opgelost – ook in de avonduren. In mijn jonger jaren verwachtte ik dat ook van anderen. Dan kon ik echt zeggen: ‘niet zeuren, schouders eronder.’ Of als mensen een snotneus hadden, dan riep ik standaard ‘daar ga je niet dood aan, doorgaan.’ Die felheid en scherpe randjes zijn er wel af, gelukkig. Als je ouder wordt, word je meestal ook wat zachter.”

‘Als je ouder wordt, word je meestal ook wat zachter; de felheid en scherpe randjes zijn er van af’

Waar verbaas je je over?

“Als ik naar onze branche kijk, dan zie ik op dit moment regelmatig overnames. Assurantiekantoren die klein zijn begonnen, middelgroot worden en tegen de klippen op willen blijven groeien. Ik zie dat de gehele implementatie van overgenomen kantoren een hele lastige oefening blijkt in de praktijk, waarbij ontevredenheid van zowel personeel als klanten op de loer liggen. Ik begrijp de keuze om te willen groeien, maar doe dat dan wel beheerst en ken je grenzen. Hou je vast aan waar je goed in bent. Kleinere kantoren zijn vaak flexibeler, meer dedicated en kunnen vaak betere support bieden. Door die overnameslag zie ik een mogelijke vervlakking in ons vakgebied ontstaan en dat vind ik een zorgelijke ontwikkeling. Iets vergelijkbaars zien we bij verzekeraars. Ga op dit moment maar eens een collectief vrachtwagenpark van een vervoersbedrijf op de markt aanbieden. Hoeveel verzekeraars hebben hier nog mogelijkheden? Ook hier zijn overnames van de afgelopen jaren in verzekeraarsland de oorzaak van een voor ons als maar krimpende marktplatform.”

Van wie heb je veel geleerd?

“Van mijn moeder. Zij had als zelfstandige een eigen confectiezaak met allemaal dames in dienst. Ze ontwierp en maakte kleding en verkocht dat aan grote warenhuizen als Schreuder. Doordat het zo goed liep, nam ze een personal assistent aan die veel uit handen nam voor haar. Delegeren is een kunst. Mensen die niet kunnen loslaten, lopen tegen een muur aan. Dan ben je alleen nog met de randzaken en dagelijkse problemen bezig en verlies je de focus. Laat je niet weghouden van je missie, dat leerde zij mij. Geef mensen het vertrouwen dat ze het werk kunnen doen.”

Samen bereik jij meer

Als adviseur weet jij wat jouw klanten drijft en bezighoudt. Je ziet ook welke risico's er spelen en wat er op hen afkomt. Zoals cybercrime, duurzaamheid, bedrijfscontinuïteit en nieuwe pensioenwetgeving.

Jij wilt je klanten in deze uitdagende tijd zo goed en zo breed mogelijk adviseren. Wij helpen je daar graag bij. Dat begint met een goede onderlinge relatie waarin we elkaar inspireren, scherp houden en aanvullen. Daarom vragen we regelmatig om jouw feedback. Organiseren we sessies waarin we samen stilstaan bij trends en ontwikkelingen. En staan onze experts voor je klaar als er bij jouw klant bijzondere risico's spelen. Of complexe vragen.

Jij hebt de adviesvaardigheden en diepgaande kennis van je klant. Wij versterken je op basis van data en analyses, praktische ondersteuning en vernieuwende producten en diensten. Zodat jij je klant nóg verder kunt helpen.

Samen bereik jij meer!

Bekijk hoe we dat doen op adviseur.nn.nl

nationale nederlanden

Uitgelicht

12 JANUARI 2023: ADFIZ NIEUWJAARSBIJEENKOMST

Op de 2e donderdag van januari opent Adfiz traditiegetrouw het verzekeringsbranchejaar met de Adfiz Nieuwjaarsbijeenkomst (NJB). Het thema van de NJB 2023, dat dit jaar op 12 januari plaats heeft in Fort Voordorp in Groenekan, is Duurzame samenwerking. Samen gaan we op zoek naar wat er nodig is om nog beter met elkaar samen te werken, welke technologieën ons daarbij kunnen helpen en welke valkuilen we moeten zien te vermijden. Tijdens de NJB worden ook de winnaars bekendgemaakt van het vernieuwde Adfiz Prestatie Onderzoek. De NJB is hét netwerkevenement voor Adfiz-leden, aanbieders, ministeries, toezichthouders en andere stakeholders.

JAN DE LANGE: 55 JAAR IN HET VAK

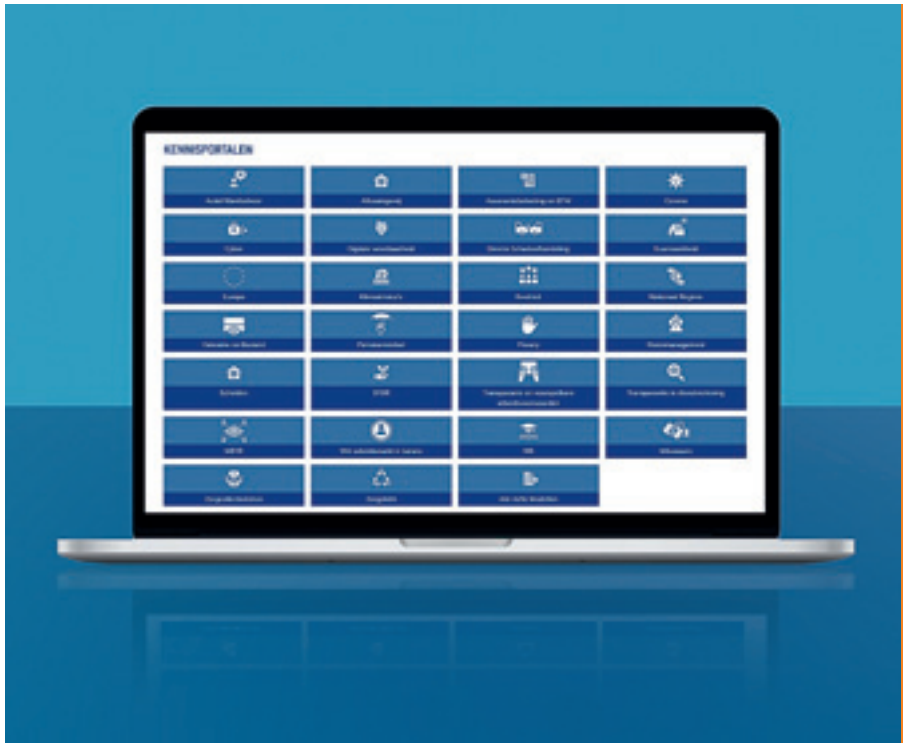
Jan de Lange, van Assurantiekantoor J.C. de Lange uit Heemskerk, zit dit jaar al 55 jaar in het verzekeringsvak. Op 23-jarige leeftijd trad hij in dienst bij het kantoor dat zijn vader 16 jaar eerder, in 1952, had opgericht. In 1979 voegde zijn jongere broer Harry zich bij het bedrijf, dat zij nu – samen met twee medewerkers – nog steeds bestieren. Namens alle leden, bestuur en verenigingsbureau van harte gefeliciteerd met dit jubileum.

ENGELSE ADVIES IN CIJFERS VERSCHENEN

De jaarlijkse Adfiz-uitgave Advies in Cijfers biedt inzicht in de omvang, het belang en de impact van onafhankelijk financieel advies in Nederland. Dit beeld helpt adviseurs, aanbieders, ministeries, toezichthouders en andere stakeholders, de juiste keuzes te maken om zo bij te dragen aan het verbeteren van de financiële fitheid in Nederland. Omdat deze informatie ook waardevol kan zijn voor buitenlandse partijen, bijvoorbeeld in de Europese lobby, heeft Adfiz de uitgave 2022-2023 ook dit jaar naar het Engels laten vertalen. *The intermediary market in The Netherlands 2022-2023* is te downloaden via adfiz.nl/intermediarymarketnl of te bestellen door een e-mail te sturen naar info@adfiz.nl.

MEERWAARDE MET ADFIZ-EVENEMENTEN

- 12 januari: Adfiz Nieuwjaarsbijeenkomst
- 21 maart: Politieke safari



NIEUWE KENNISPORTALEN OP ADFIZ.NL

De afgelopen paar maanden zagen twee nieuwe kennisportalen het levenslicht op de Adfiz website. In september werd het kennisportaal Transparante en voorspelbare arbeidsvoorwaarden geïntroduceerd. Dit kennisportaal bundelt en duidt alle nieuwe regels die gelden sinds de *Wet Transparante en voorspelbare arbeidsvoorwaarden* op 1 augustus van kracht werd. Het kennisportaal Digitale weerbaarheid, dat medio oktober werd gepubliceerd, informeert adviseurs over de eisen die aan kantoren gesteld worden en hoe ze daaraan kunnen voldoen. Het portaal wijst adviseurs de weg langs de vele informatiedocumenten, checklisten en hulpmiddelen die beschikbaar worden gesteld om de eigen digitale weerbaarheid en informatiebeveiliging op het goede niveau te brengen.

Goed advies is belangrijk

Voor alle financiële producten, maar zeker voor rechtsbijstandverzekeringen. Vooral in deze onzekere tijden. Een juridisch conflict is nooit te voorzien, dus het is van belang om dit risico goed in te schatten en te zorgen voor een rechtsbijstandverzekering die aansluit op de behoefte van uw klant. Dat kan met de nieuwe particuliere verzekeringen van ARAG. Daarmee biedt u iedereen een passende verzekering.

ARAG Rechtsbijstand Basis Verzekerd
Tegen een aantrekkelijke premie verzekerd voor veelvoorkomende conflicten.

ARAG Rechtsbijstand Uitgebreid Verzekerd
Uitgebreide dekking en keuzevrijheid in de onderdelen waarvoor de klant verzekerd wil zijn.

ARAG Rechtsbijstand Excellent Verzekerd
De rechtsbijstandverzekering met de meest complete dekking en door de Consumentenbond beoordeelt met een 7,9.

In top 3 van **beste rechtsbijstandverzekeringen**
Consumentenbond 2022

Meer weten over de particuliere rechtsbijstandverzekeringen van ARAG?
Kijk dan op **www.arag.nl/intermediair**.

ARAG juridisch probleemoplossers

Cyber Compact

Extra zekerheid: cyberdekking standaard meeverzekerd op de inboedelverzekering.

INTRODUCTIE DEC. '22

Cyber Compact, met:

- **Cyberhulplijn**, voor hulp bij cyberincident.
- **Cyberrisico online tool**, voor inzicht in je cyberveiligheid.
- **Schade door hacking** is verzekerd.

www.ansvar-idea.nl

www.turien.nl

Ansvar idéa VERZEKERINGEN

TURIEN&CO ASSURADEUREN