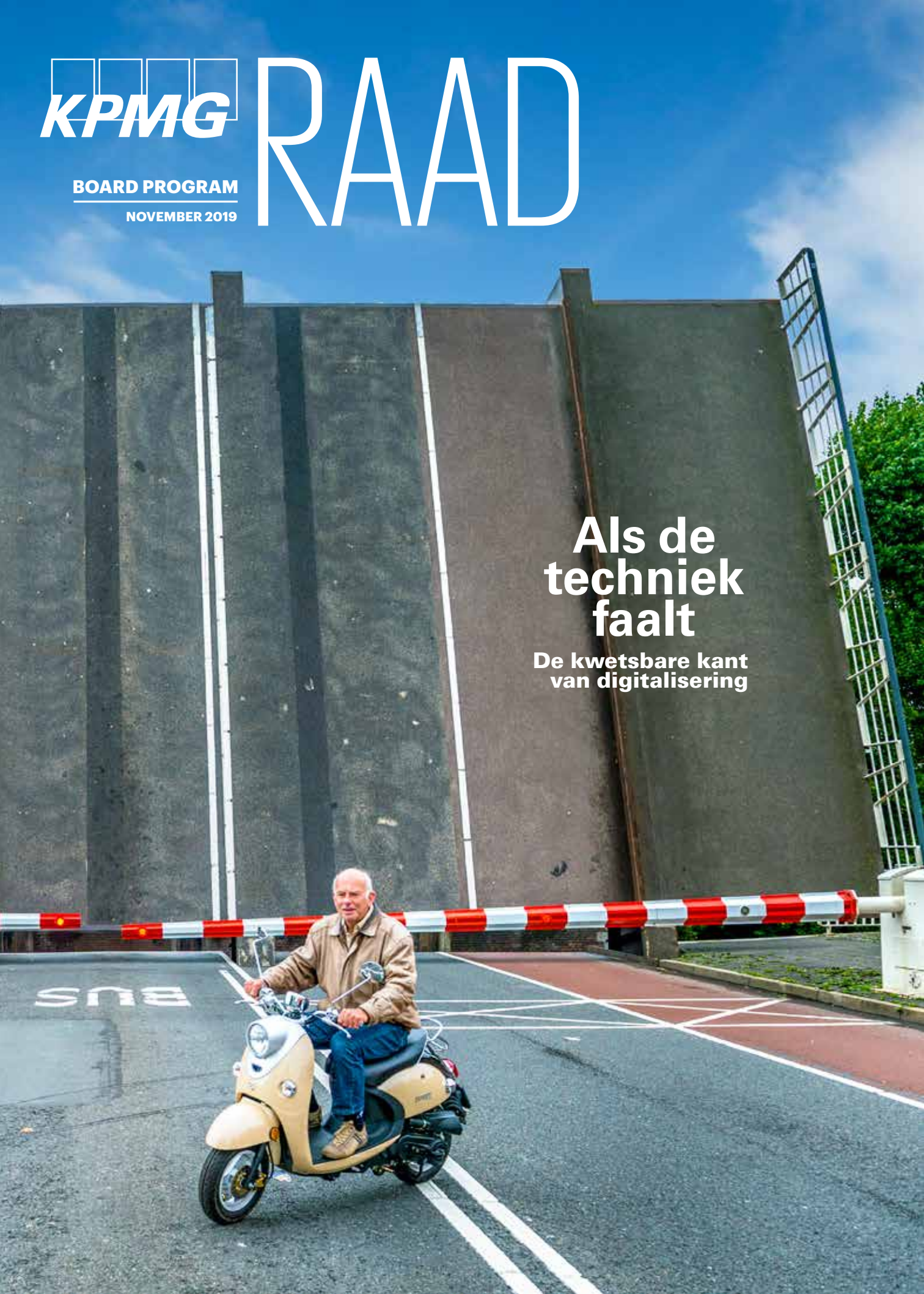
KPMG

RAAD

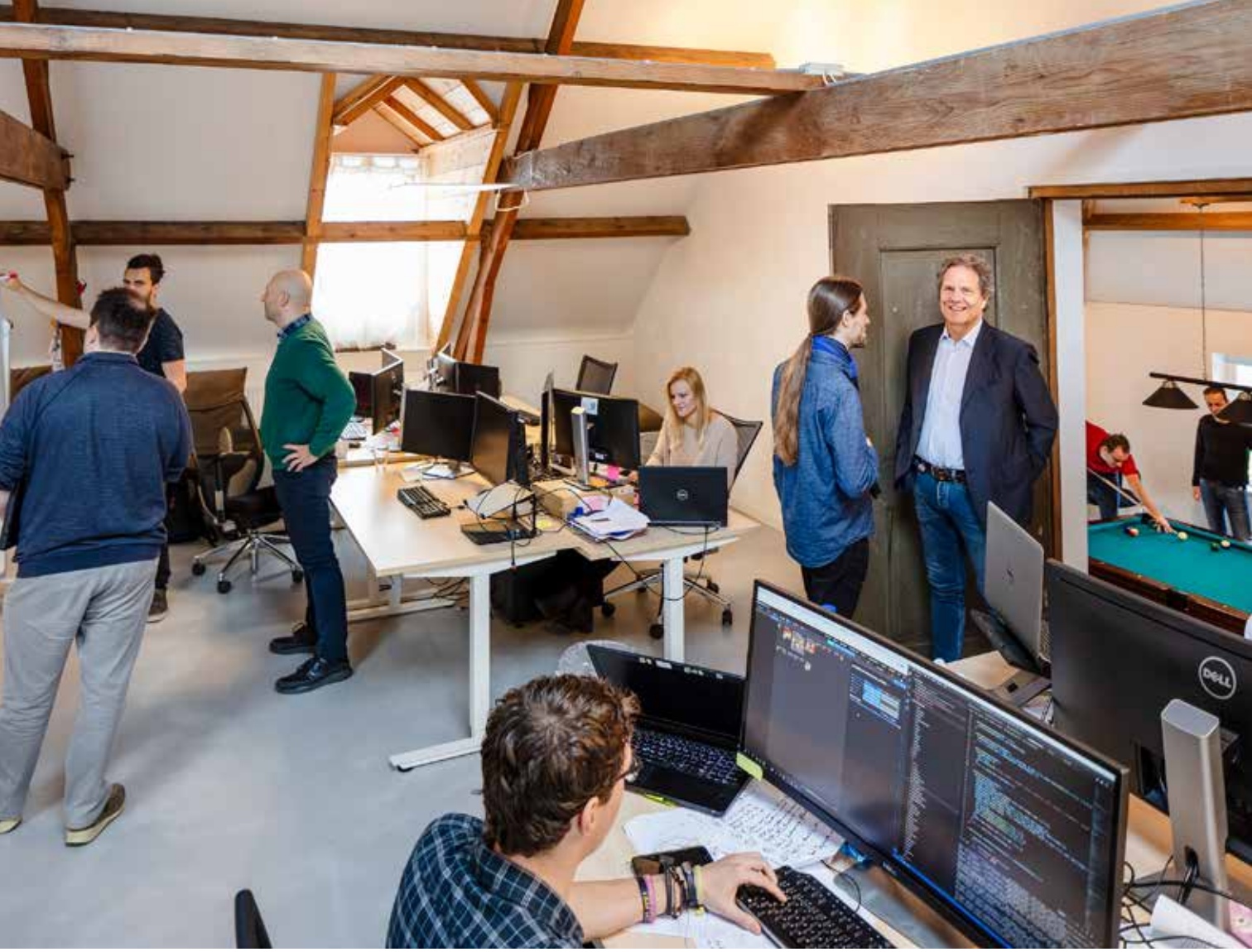
BOARD PROGRAM

NOVEMBER 2019



Als de techniek faalt

De kwetsbare kant van digitalisering



Zien in de duisternis

Als je het over data hebt, denk je al snel aan getallen. Maar tekeningen, foto's, geluidsopnamen, geschreven teksten, facturen, contracten, zelfs etiketten: het zijn óók data. Die gaan echter niet zomaar even samen de computer in voor een fijne analyse. Hoewel, dat gingen ze niet, tot Jan-Kees Buenen er in 2011 met zijn technologiebedrijf SynerScope mee aan de slag ging. Hij bedacht en bouwde met zijn collega's een programma – zie het als een soort MRI-scanner voor data – waarmee je grote hoeveelheden en vele variëteiten aan data, gestructureerd en ongestructureerd, snel en veilig kan verwerken en analyseren. En dat is wel zo fijn, want veel financiële instellingen worstelen met het effectief inzetten van hun data en hebben weinig inzicht in mogelijke onregelmatigheden. SynerScope kan het hele datalandschap inzichtelijk maken – gooi een miljoen contracten in het programma en binnen één dag heb je context en daarmee ook zicht op de kansen en risico's. En daar kun je je beleid of strategie weer op aanpassen.
Voor Buenen voelt het bijna niet als werk. Hij hoort Satya Nadella (Microsoft's ceo) op Inspire 2019 zeggen dat negentig procent van de wereldwijde data jonger is dan twee jaar, en dat 73 procent van alle data nog nooit geanalyseerd is. Ieder jaar valt er meer te ontdekken. Als een ware kaartenmaker zoekt hij naar nieuwe gebieden – nieuwe data – om de wereld weer wat inzichtelijker te maken. En dat is leuk.

Jan-Kees Buenen werkte meer dan twintig jaar werkzaam in de verpakkingsindustrie, toen hij in 2011 SynerScope mede oprichtte als spin-off van de Technische Universiteit Eindhoven. Inmiddels werken 27 mensen aan de ontwikkeling van technologie en producten die grote hoeveelheden data inzichtelijk maken. Samen met KPMG helpt SynerScope onder meer financiële instellingen om zich met meer inzet van data te wapenen tegen financiële criminaliteit en zo ongewenste geldstromen in hun bedrijfsvoering effectiever te kunnen bestrijden.

TEKST HILDE DUYX **BEELD** LARS VAN DEN BRINK

KPMG RAAD
BOARD PROGRAM

Inhoud

NR. 9 /
NOVEMBER 2019

Patricia Zorko

Wat vandaag veilig is, hoeft dat morgen niet te zijn, zegt directeur Patricia Zorko van NCTV. Ze ziet cybersecurity vooral als een kans om de digitale voorsprong van Nederland te verzilveren. "Gelukkig slagen we er steeds beter in het gesprek aan te gaan met bedrijven en samen op te trekken."

Verder:

NEDERLAND IS SLECHT VOORBEREID OP DIGITALE RAMP

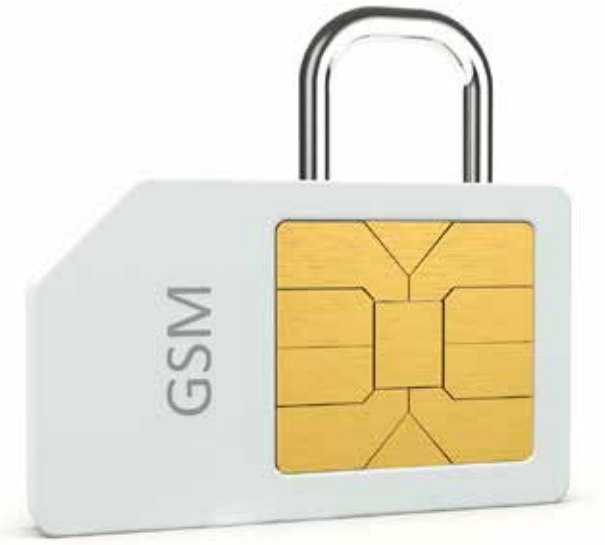
De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) laat er in het rapport 'Voorbereiden op digitale ontwrichting' geen misverstand over bestaan: Nederland is slecht voorbereid op grootschalige digitale ontwrichtingen. Hierbij kunnen cruciale diensten uitvallen, zoals het betalingsverkeer, de elektriciteitsvoorziening of medische zorg.
Naarmate onze afhankelijkheid van digitale systemen groeit, wordt het risico op ontwrichting groter. Zeker als al die systemen ook nog eens aan elkaar gekoppeld zijn. Dat leidt tot onvoorziene gevaren voor de economie, nationale veiligheid en het maatschappelijk leven.
De Wetenschappelijke Raad voor het Regeringsbeleid adviseert daarom een betere voorbereiding op deze 'digitale ontwrichting'. Wat daarvoor nodig is? Onder meer inzicht in afhankelijkheden, een nieuwe benadering van vitale infrastructuur, adequate bevoegdheden om escalatie te voorkomen en inspanningen op het terrein van cyberverzekeringen.

Bron: wrr.nl

48%

48% van de techleiders verwacht dat blockchain de manier waarop ze werken gaat veranderen.

Bron: Technology Industry Innovation Survey, KPMG



TREND: SIM-SWAPPING

Gehackt worden via je 06-nummer. Het kan, en het heeft een naam: sim-swapping. Steeds meer mensen worden slachtoffer van deze relatief nieuwe hackmethode. Met de komst van de e-sim, de nieuwe digitale simkaart, wordt het nog makkelijker: met alleen een wachtwoord kunnen hackers op afstand telefoonnummers overnemen. Volgens verschillende experts is het 06-nummer dan ook een onbekende, maar zeer zwakke plek in de online beveiliging. Tip voor organisaties: zorg voor sterke, unieke wachtwoorden en neem extra beveiligingsmaatregelen, zoals tweestapsverificatie.

Bron: RTL Nieuws

Bouwstenen voor een transparante keten

Kan blockchaintechnologie van waarde kan zijn voor maatschappelijk verantwoord ondernemen? Het antwoord op die vraag staat in een gezamenlijk studierapport van KPMG en de OESO, de Organisatie voor Economische Samenwerking en Ontwikkeling.

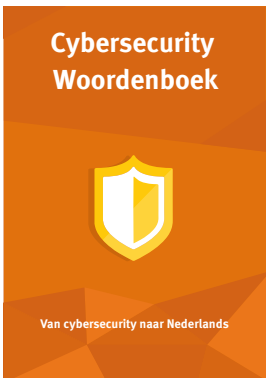
De blockchaintechnologie kan een belangrijke rol spelen bij het inzichtelijker en transparanter maken van de productieketen. De technologie maakt het mogelijk om ontwikkelingen en transacties bij toeleveranciers in de keten wereldwijd nagenoeg 'realtime' te volgen, meer controle uit te oefenen op mogelijke risico's in de keten en deze risico's zoveel mogelijk te beperken.
De blockchain kan bovendien zorgen voor meer transparantie in de activiteiten die in de waardeketen plaatsvinden. Hierdoor kunnen bedrijven hun klanten bijvoorbeeld meer inzicht geven in de herkomst van producten. Dat betekent dat de blockchain een volledig geaggregeerd en transparant beeld kan geven van de volledige toeleveringsketen, één van de eisen van de verplichte 'due diligence' waarmee productiebedrijven te maken hebben. "Productieketens zijn vaak lastig te overzien", constateert Jerwin Tholen van KPMG Sustainability. Tholen: "Maar bedrijven zijn wel verantwoordelijk voor de effecten van hun onderneming op mens en milieu, ook in de toeleveringsketen. In het kader van maatschappelijk verantwoord ondernemen is het dan ook van groot belang dat een onderneming weet wat er in de keten speelt en weet wat de risico's zijn. Due diligence speelt hierbij een belangrijke rol, het in kaart brengen van de risico's van bedrijfsactiviteiten en aangeven hoe met deze risico's wordt omgegaan. Hierbij kan het gaan om mensenrechten, arbeidsomstandigheden, milieu en corruptie."

Lees het volledige rapport op home.kpmg/nl/raad

Wie kent de **Blackhat Hacker?**

Het Cybersecurity Woordenboek draagt bij aan een digitaal veilig Nederland. In het woordenboek staan ruim 600 woorden die voor vakspecialisten vaak gesneden koek zijn, maar voor leken abacadabra.

Wilt u makkelijker meepraten met specialisten? Download het woordenboek gratis via www.cybersecurityalliantie.nl/woordenboek.
Bron: nctv.nl



Pardon?

Blackhat hacker
Iemand die met kwade bedoelingen inbreekt in een computersysteem. De naam 'blackhat' komt uit cowboyfilms waarin slechteriken altijd een zwarte hoed dragen.

Bug bounty
Beloning die iemand krijgt als hij een beveiligingslek in een digitaal systeem heeft gevonden en gemeld. Men krijgt de beloning van de eigenaar van het digitale systeem.

Path Traversal
Aanval via een website, met als doel om bij bestanden en mappen te komen waar men niet bij mag. De aanvaller kan de website manipuleren door bepaalde invoer te sturen. Zo kan hij een pad volgen naar een bestand of map waar hij niet bij mag.

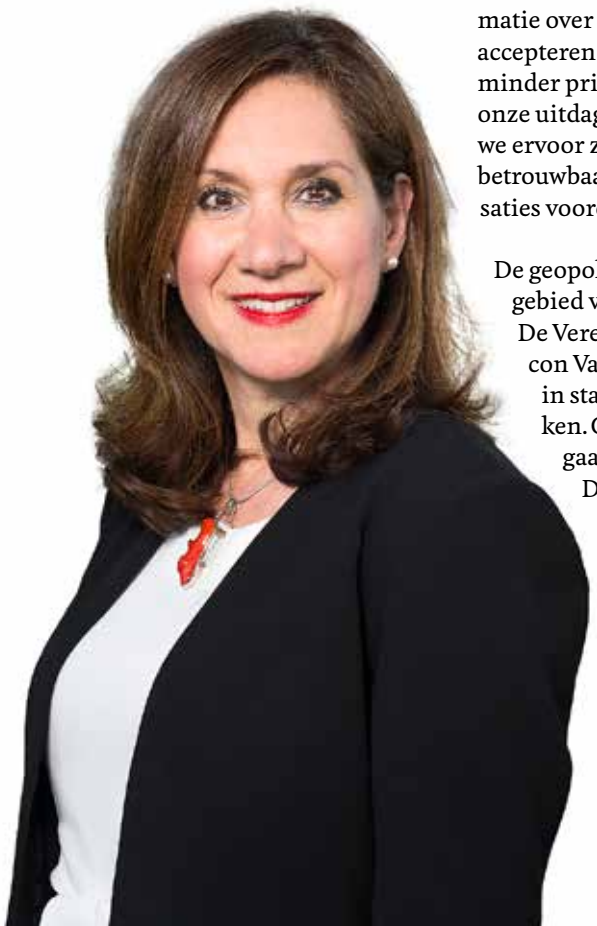
Script kiddie
Iemand die cyberaanvallen doet voor de lol. Of omdat hij wil laten zien dat een site of computernetwerk kwetsbaar is. Vaak zijn het jonge hackers die niet goed snappen wat de gevolgen kunnen zijn van hun acties. Ook weten zij vaak niet heel veel, en gebruiken ze hulpmiddelen van anderen.

Spoofing
Iemand misleiden door te doen alsof je iemand anders bent. Er zijn veel soorten spoofing. Een aanvaller kan zich in een email voordoen als een ander door het afzendadres te vervalsen.

Zó dus!

‘Het individu is Europa’s geheime wapen’

Stephanie Hottenhuis
CEO en voorzitter raad van bestuur KPMG Nederland



Digitale transformatie staat hoog op de agenda in vrijwel iedere organisatie. Nog nooit was het zo makkelijk om klanten te bereiken. Dat moet ook, want diezelfde klant wil snelheid, gemak en veel keus. In ruil daarvoor zijn mensen bereid om informatie over zichzelf prijs te geven. Ze accepteren – bewust – dat er steeds minder privacy is. Op dit snijvlak zit onze uitdaging. Samen met u willen we ervoor zorgen dat veiligheid en betrouwbaarheid van data en organisaties voorop blijven staan.

De geopolitieke concurrentie op het gebied van digitalisering is enorm. De Verenigde Staten hebben Silicon Valley, en zijn als geen ander in staat om kapitaal aan te trekken. China loopt voorop als het gaat om Artificial Intelligence. De extreem planmatige aanpak, veel financiering vanuit de overheid en weinig wetgeving omtrent privacy versterken deze positie.

Blijft Europa achter? In mijn visie niet. Europa is een geweldige plek om te leven. In onze eeuwenoude democratieën hechten we veel waarde aan individuele vrijheid. Juist die aandacht voor het individu is ons geheime wapen. We moeten respect voor privacy omarmen en technologisch waarborgen, in onze instituties, producten en diensten. Daar zit onze kracht en maakt onze samenleving juist zo prettig.

Digitale veiligheid kent vele aspecten, u leest erover in dit nummer. Haroon Sheikh vergelijkt de digitale transformatie met de opkomst van de autoindustrie halverwege de vorige eeuw. Hij trekt lessen uit het verleden, maar benadrukt in zijn betoog dat wij mensen zijn. Met alle beperkingen van dien. Patricia Zorko weet hoe Nederland ervoor staat op het gebied van digitale veiligheid en geeft inkijk in de Cyber Security Agenda. We laten ook zien dat cybersecurity niet alleen een issue mag zijn voorde afdeling ICT. Van werkvloer tot boardroom, iedereen moet zijn steentje bijdragen.

KPMG gaat graag met u in gesprek. We delen onze ervaringen en dilemma’s en gaan met u op zoek naar oplossingen. Ook dat is samenwerken.
Op home.kpmg/nl/raad vindt u alle informatie over onze programmering. Wellicht tot ziens op één van onze events.

Hacken voor het goede doel

We zien hier studenten aan het werk tijdens Cal Hacks 5.0, een hackathon in Berkeley, Californië. Het doel van dit soort hackathons is om met technologie oplossingen te creëren voor een betere wereld. Voor de ruim 2.200 deelnemers van 50 universiteiten uit 5 landen lonkt een relatief nieuw beroep, dat van ethical hacker. Zo'n ethical hacker denkt en doet als een 'echte hacker', met één wezenlijk verschil: de kennis en kunde wordt niet gebruikt om bedrijven schade te berokkenen of om veel geld te verdienen, maar juist om IT-omgevingen veiliger te maken.

BESTUURDER, KEN JE BEPERKINGEN

‘We moeten niet ‘naar’ technologie kijken, maar ‘door’ technologie.’ Haroon Sheikh, als filosoof, bestuurskundige en politicoloog verbonden aan de WRR, adviseert organisaties over de impact van digitale ontwikkelingen. Zijn advies aan bestuurders: ‘Verzamel mensen om je heen die je schaduw adresseren. Juist in deze tijd moeten leiders kwetsbaar kunnen zijn.’

TEKST SARAH LEERS **BEELD** FRANK RUITER

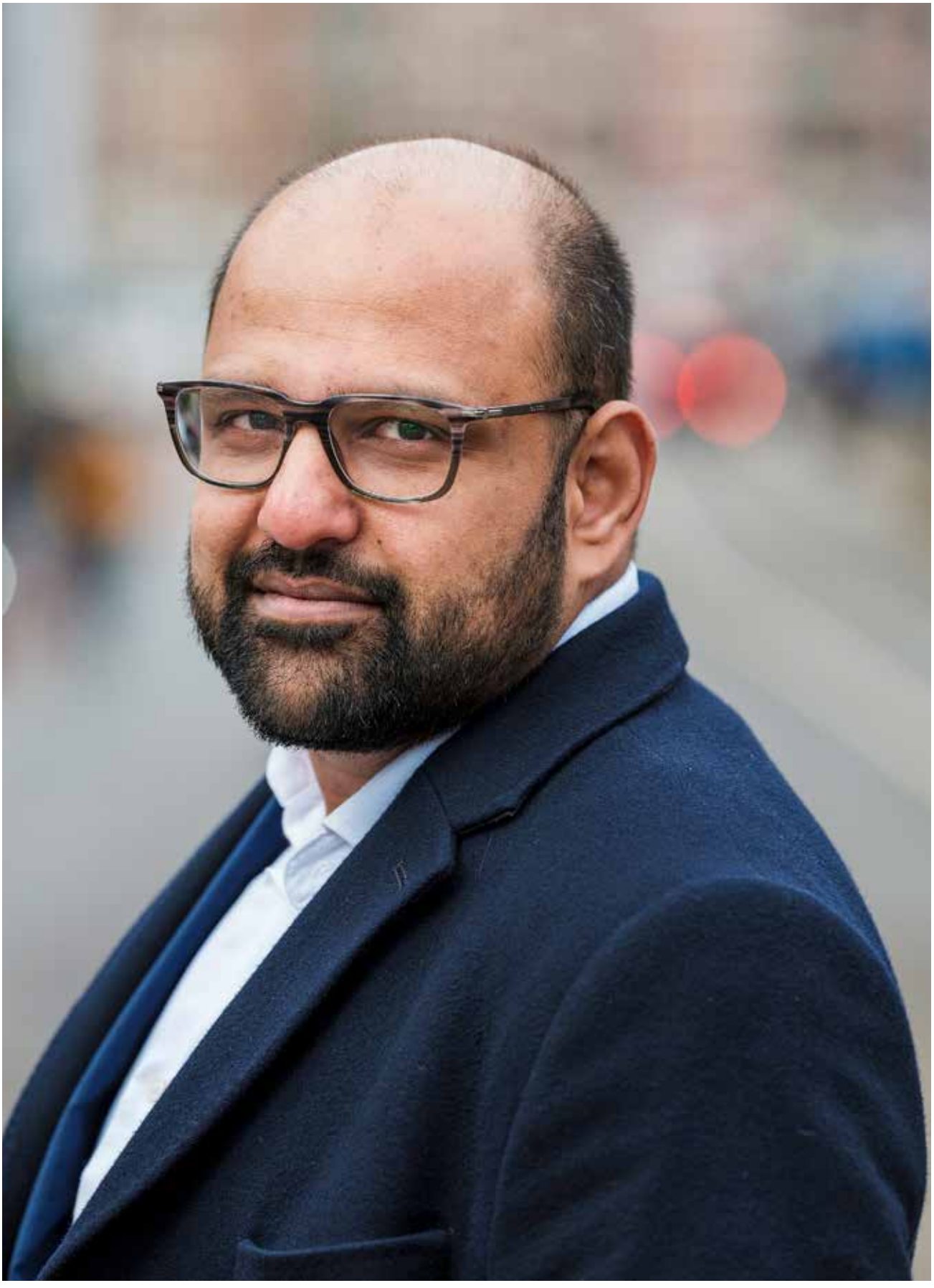
De huidige digitale transformatie is verbazingwekkend goed te vergelijken met de opkomst van de auto-industrie halverwege de vorige eeuw. Zo dachten mensen destijds dat een auto een soort koets was, maar dan zonder paarden. En zo denken wij nu dat een zelfrijdende auto een gewone auto is, maar dan zonder chauffeur. Wetenschapper Haroon Sheikh onderbouwt zijn betoog graag met verwijzingen naar verleden. Niet alleen om daar lessen uit te trekken voor de toekomst, maar ook om te benadrukken dat wij te allen tijde mens zijn. Met alle beperkingen van dien.

Als het over digitale transformatie gaat, wordt vaak gesproken in termen van kansen of bedreigingen. Is dat eigenlijk wel zinvol?

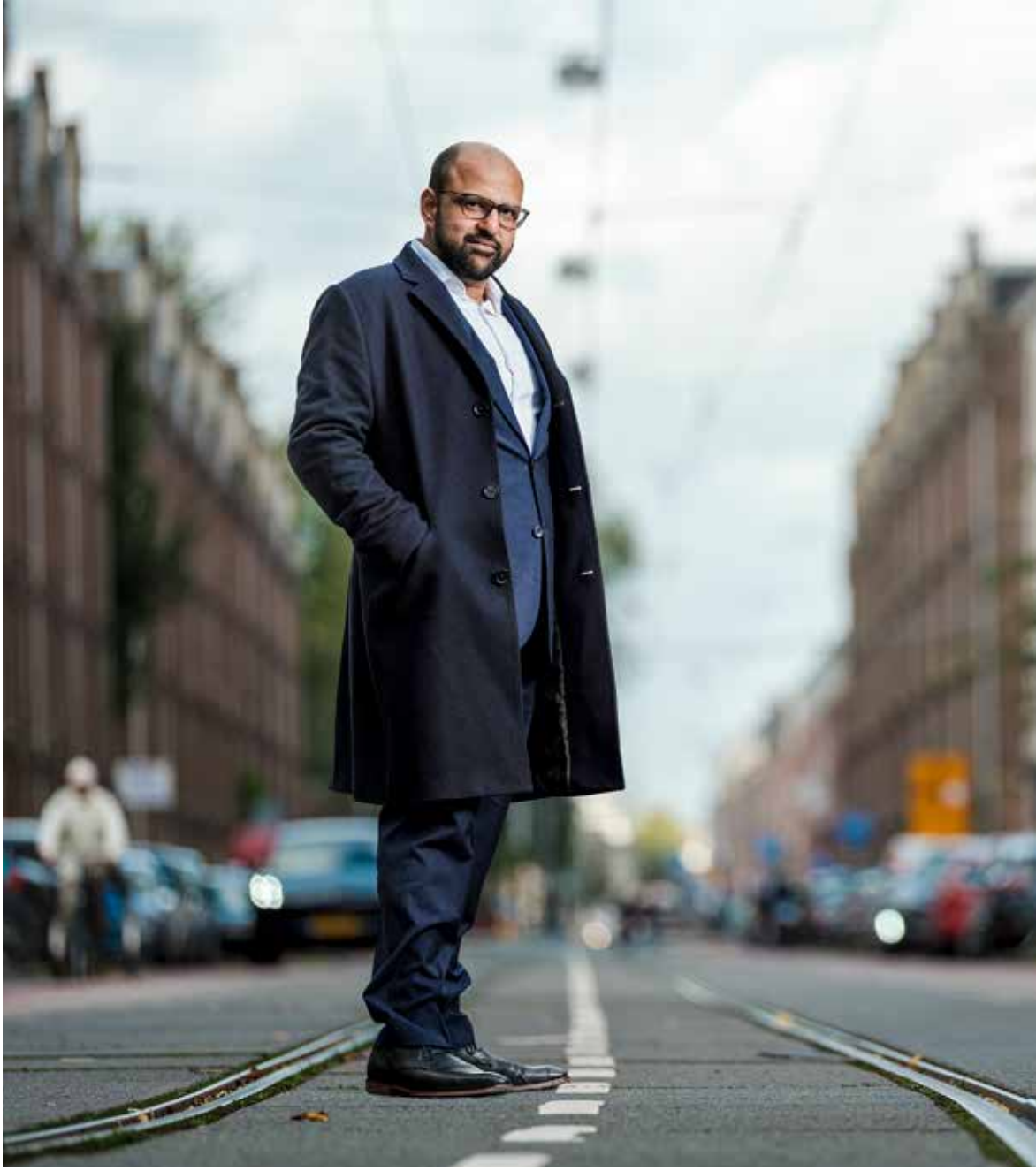
“Als er een nieuwe techniek op de markt komt, zijn we geneigd onszelf af te scheiden van die techniek. We zien het als iets buiten onszelf en gaan vervolgens besluiten: zijn we ervoor of zijn we ertegen; willen we het hebben of willen we het niet hebben? Deze zienswijze is eigenlijk te beperkt, ze maakt ons blind voor de mogelijkheden die technologie ons kan bieden. Feit is namelijk dat we nog niet weten hoe de technologie onze omgeving en maatschappij zal veranderen.

Technologieën staan niet los van ons, want we gebruiken ze als verlengstuk. We kijken nu ‘naar’ technologie, maar we zouden ‘door’ technologie moeten kijken. Zoals door een bril. Je zou kunnen zeggen: een bril is een apparaat waardoor je ogen anders functioneren, niet meer dan dat. Maar het punt is dat die bril je in een nieuwe ruimte brengt, in een andere dimensie met nieuwe mogelijkheden.

We moeten onszelf dus niet de vraag stellen of we bepaalde technologieën willen of niet. De vraag zou veel meer moeten zijn: in wat voor soort ruimte brengt de technologie ons en hoe zorgen we ervoor dat die ruimte zo humaan mogelijk is. Want een nieuwe ruimte biedt ons veel mogelijkheden, maar is nog niet door de samenleving eigengemaakt. We hebben er nog geen normen voor. We moeten met elkaar



Haroon Sheikh brengt in De opkomst van het Oosten de veranderde geopolitieke en economische verhoudingen op het Euraziatische continent in kaart.



afspreken wat de regels zijn binnen die nieuwe ruimte, waardoor we er allemaal, burgers, overheid en bedrijven, van kunnen profiteren.
We zijn tegenwoordig van mening dat we digitalisering gewoon moeten omarmen. Maar stel je voor dat we de auto gewoon omarmd hadden. In de jaren zestig liepen mensen in San Francisco rond met gasmaskers, omdat ze dachten: dat hoort nu eenmaal bij die auto. De auto zou een nieuwe wereld creëren van ongelukken, onveiligheid en allerlei gezondheidsrisico's. Dus wat we hebben gedaan is afspraken maken en structuren bouwen: een rijbewijs, verkeersregels, maximumsnelheden, kentekens, een jaarlijkse keuring. Een heel palet waardoor de maatschappij zich die nieuwe ruimte eigen heeft kunnen maken. We realiseren ons nu dat we dit met digitalisering ook moeten doen."

'Techniek valt niet te begrijpen vanuit oude logica'

Hoe vertaal je als bestuurder deze zienswijze naar je organisatie?
"Vaak zie je dat organisaties digitalisering beschouwen als een aanvulling op bestaande processen: we blijven doen wat we altijd deden en we zetten er een laagje bovenop. Ik denk dat dit niet de juiste manier is. Techniek creëert een nieuwe ruimte en die heeft zijn eigen regels, zijn eigen logica. Die valt dus niet te begrijpen

Haroon Sheikh is wetenschappelijk medewerker bij de Wetenschappelijke Raad voor het Regeringsbeleid. Hij studeerde bestuurskunde, politicologie en filosofie in Leiden en Oxford. Hij promoveerde als filosoof op een onderzoek naar de invloed van oude tradities op moderne samenlevingen. Als hoofdonderzoeker van opkomende markten was hij werkzaam bij investeringsmaatschappijen Cyrte en Dasym. Van 2015 tot 2018 leidde hij Freedomlab Thinktank, een denktank die zich bezighoudt met de impact van nieuwe technologie en veranderende mondiale verhoudingen.

Haroon Sheikh schreef De Opkomst van het Oosten: Eurazië en de nieuwe wereldorde en Embedding Technopolis. Hij schrijft opiniërende artikelen voor NRC Handelsblad en het Financieele Dagblad. Aan de VU geeft hij les bij de master Filosofie van Cultuur en Bestuur en bij Politics, Philosophy and Economics (PPE).

vanuit de oude logica. De nieuwe ruimte zal alles beïnvloeden, van productieprocessen tot de omgang met de klant. We moeten ons die nieuwe logica dus toe-eigenen en haar in het hele bedrijfsproces proberen op te nemen.
We zijn geneigd om technologie te begrijpen vanuit zaken die we uit het verleden al kenden. Toen de auto in het straatbeeld verscheen, werd hij aangekondigd als *the horseless carriage*: het is een koets, we gaan hem op dezelfde manier gebruiken, maar dan zonder paard. We konden niet overzien wat een revolutie de auto zou veroorzaken. Nog steeds kijken we op deze manier naar nieuwe technologieën. We beschouwen de zelfrijdende auto bijvoorbeeld als een auto, maar dan zonder chauffeur. Maar misschien blijkt het in de toekomst een ander voortuig te zijn, dat heel anders gebruikt wordt dan de auto nu. Net zoals een auto geen koets was.

We moeten ons dus niet langer bezighouden met het optimaliseren van het verleden, het sneller, efficiënter, goedkoper maken van onze praktijken. In plaats daarvan moeten we proberen ons een beeld te vormen van de nieuwe praktijken. Op die manier kunnen we gevoeliger worden voor de mogelijkheden die nieuwe technologie met zich meebrengt."

Wat vraagt dat van bestuurders? Welke eigenschappen zijn essentieel?
"Enerzijds moet je als bestuurder openstaan voor en durven experimenteren met een nieuwe werkelijkheid, met een nieuwe ruimte die je nog niet kent. Aan de andere kant moet je je goed bewust zijn van de mogelijke risico's en beslissingen nemen voor de lange termijn. Ik realiseer me dat dat tegengestelde dynamieken zijn.

Ik denk dat het ontzettend belangrijk is dat je als bestuurder je eigen schaduw adresseert. Zorg dat je iets tegenover je kwaliteiten zet. Je kan bijvoorbeeld een heel inspirerend, charismatisch persoon zijn. Maar tegelijkertijd kan dat charisma ervoor zorgen dat je ongeduldig bent en onvoldoende aandacht hebt voor structuur. Zorg dan dat er iemand naast je staat die de structuur bewaakt en die je terechtwijst als je te ver afdwaalt. Om succesvol te anticiperen op ontwikkelingen in de toekomst, moet je de mensen om je heen verzamelen die je confronteren met je blinde vlekken.
In het verlengde daarvan: zorg dat er plekken zijn waar je de rol van bestuurder ook even kunt loslaten. Bijvoorbeeld bij een groep oude vrienden, die jou niet zozeer kennen als de CEO maar met wie je in de studiebanken zat. Die tegen je kunnen zeggen: dat wat je daarnet zei, is gewoon heel dom. Mooi vind ik altijd hoe de Romeinen dat deden. Als een strijder een slag gewonnen had, werd hij gevierd en gelauwerd. Tegelijkertijd stond er dan een slaaf naast hem, die hem eraan herinnerde dat hij een mens was. Nederigheid, je beperkingen kennen, dat vonden ze heel belangrijk. Juist in tijden van succes en voorspoed.
Als bestuurder word je geacht overal een antwoord op te hebben. Je probeert alle risico's in te dammen, want voor je het weet veroorzaak je een schandaal of controverse en dan zitten de media er bovenop. Juist daarom is het belangrijk dat er ook plekken zijn waar je je kwetsbaarheid kunt tonen, waar je die last even naast je neer kunt leggen."

‘Zorg dat er plekken zijn waar je je rol als bestuurder even los kunt laten’

Wat betekent dit voor de machtsverhoudingen binnen en tussen organisaties?
"De manier waarop veel markten zijn ingericht wordt zo langzamerhand onhoudbaar. Dat zit hem in de monopoliepositie. Er is een soort mondiale consolidatie bezig waarin een paar spelers heel dominant zijn. Dat fenomeen kennen we al lang. De opkomst van nieuwe technologieën ging vrijwel altijd gepaard met gigantische superbedrijven. Toen de auto-industrie opkwam, had je de *big three* van Detroit: General Motors, Ford en Chrysler. Die drie domineerden de wereldmarkt van auto's, met alle negatieve gevolgen van dien. General Motors kocht op zeker moment alle tramlijnen op. Niet omdat ze het tramvervoer wilden verbeteren, maar omdat ze de vervoersmaatschappijen failliet wilden laten gaan, zodat mensen gedwongen werden een auto te kopen.
In deze fase zitten we nu ook met digitale technologie. Er zijn een paar bedrijven heel groot en machtig geworden. Dat brengt ons nu wel op een keerpunt. We zien dat overheden steeds meer gaan ingrijpen. Zelfs in Amerika, waar al een paar flinke boetes aan grote techbedrijven werden opgelegd. Politieke partijen zoeken naar manieren om grote monopolies op te breken en anders te reguleren. Dat is een noodzakelijke stap.
Maar ook binnen bedrijven zou een verschuiving moeten plaatsvinden. Medewerkers zijn vaak de eersten die in de gaten hebben of het bedrijf de juiste bijdrage levert of niet. Kijk naar giganten als Google, Amazon en Microsoft. Op veel projecten van deze bedrijven zijn het juist de werknemers die zich organiseren om in opstand te komen. Zo heeft Google bijvoorbeeld een project om autonome drones, autonome wapens voor het Amerikaanse leger, stopgezet doordat werknemers in opstand kwamen. Die weerstand zal voor een bestuurder behoorlijk uitdagend zijn, maar is tegelijkertijd een goede manier om je draagvlak te versterken. Ben je nog met de juiste dingen bezig? Van wat jou nu de juiste businesscase lijkt, kunnen jouw medewerkers morgen zeggen dat het een verkeerde impact heeft. Werknemers zijn misschien wel de hedendaagse variant van de Romeinse slaaf: herinner je dat je een mens bent." ■

MIJN INSPIRATIE

Als partner Customer & Brand Advisory bij KPMG, is **Nienke Wichers Hoeth** onder meer verantwoordelijk voor de dienstverlening op het gebied van Digital Banking en Fintech. Door wie of wat laat zij zich inspireren? Over functionele simpelheid en woeste wildernis.

Satya Nadella (de CEO van Microsoft)

"Microsoft was een grote logge tanker toen Satya Nadella het roer overnam. Door te luisteren naar wat de klant wil en met een heldere strategie, leidde hij Microsoft de nieuwe wereld in. Met veel succes. Het mooie is dat hij de focus niet alleen op technologie legt, maar juist ook op cultuur, strategie en de behoefte van de klant. En dat doet hij op een rustige manier, met positieve keuzes voor samenwerken en transparantie. Ik werk zelf veel aan digitale transformaties van grote organisaties en ervaar de complexiteit hiervan. Ik heb bewondering voor hoe hij het hele bedrijf heeft gekeerd."

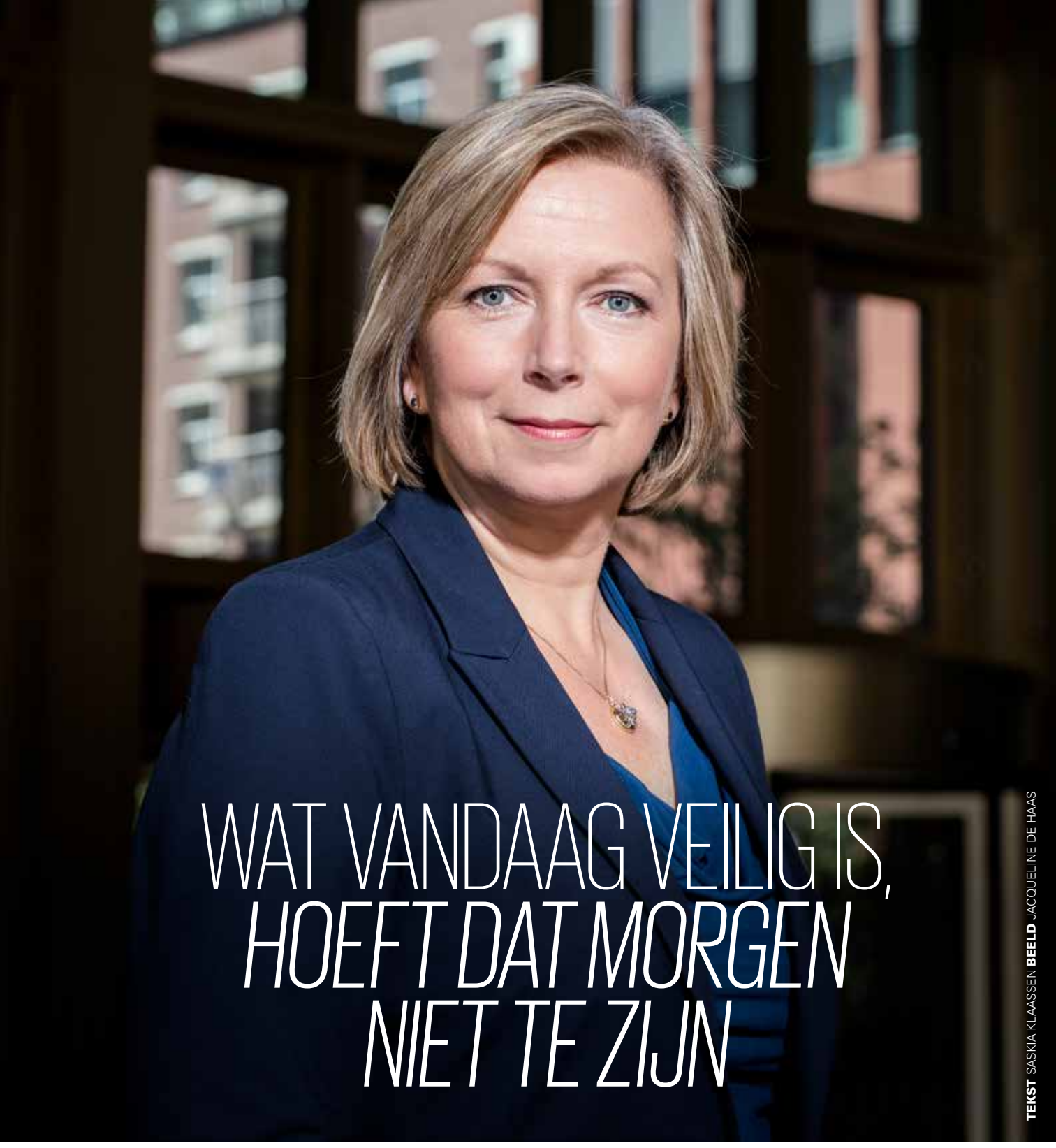
Schotland en Patagonië

"Als ik mijn hoofd echt wil leegmaken, zoek ik de woeste natuur op. En die vind je in Schotland, en ook in Patagonië waar de natuur alles bepaalt en de wind overheerst. Daar weet ik weer, 'het is leuk wat we allemaal doen, maar we zijn maar heel klein in het grote geheel.' Tegelijkertijd kom ik dan op de beste ideeën. Laat mij daar maar een tijdje rondlopen."

Dutch design

"Ik heb veel in het buitenland gewerkt en heb daar gezien hoe goed Nederland het als klein land doet. Dutch design symboliseert dat voor mij. Gebruiksvoorwerpen die uitblinken in een combinatie van gebruiksgemak en mooiheid. Hiermee tonen de ontwerpers aan in staat te zijn naar de kern van het probleem te kijken en het niet te complex te maken. Dutch design gaat voor mij om de kunst van het weglaten en functionele simpelheid. Heel inspirerend."

TEKST HILDE DUYX **BEELD** ISTOCK, DROOG DESIGN, MICROSOFT



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

TEKST SASKIA KLAASSEN **BEELD** JACQUELINE DE HAAS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Patricia Zorko

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

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

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

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

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

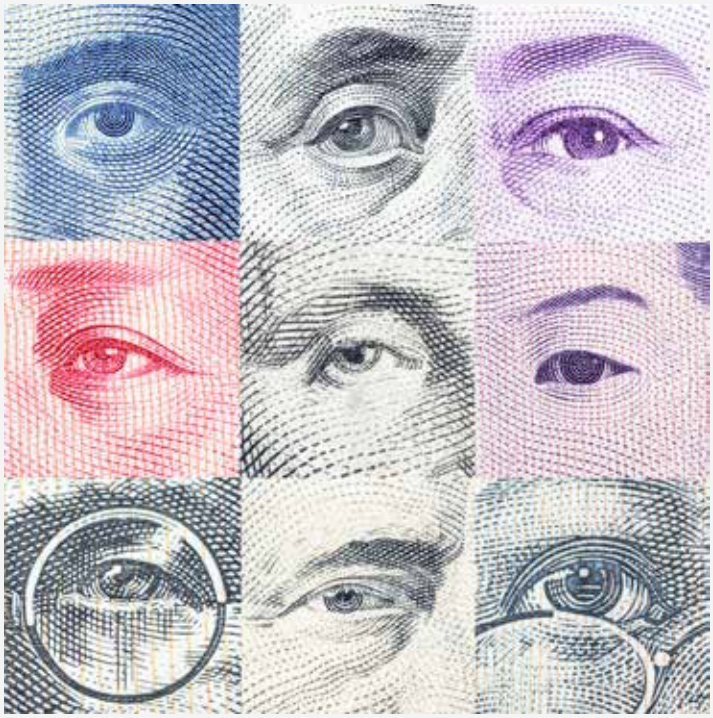
De NCTV stelt somber dat de weerbaarheid van bedrijven nog steeds onvoldoende is. Zijn er ook lichtpuntjes?

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

Dutch Transformation Forum

Tijdens het Dutch Transformation Forum (DTF) op 20 november buigen deelnemers uit het bedrijfsleven en de publieke sector zich over de vraag hoe Nederland zich het beste kan positioneren in een wereld die een veelomvattende transformatie doormaakt. Én welk leiderschap daarbij hoort. Het thema dit jaar: economische, geopolitieke en digitale veiligheid.

De Amerikaanse strateeg Robert Kaplan noemt het de terugkeer van Marco Polo's wereld; China's president Xi Jinping noemt het zijn Nieuwe Zijderoutestrategie. Hoe je het ook noemt: het is duidelijk dat de geopolitieke context van Europa's veiligheid en verdienvermogen radicaal aan het veranderen is. Het Euraziatisch continent – dat enorme speelveld van macht en handel dat spant van Brussel tot Beijing – bruist van nieuwe verbindingen, net zoals het deed in de tijd van de Venetiaanse handelsreiziger Marco Polo. Tegelijkertijd wordt Europa geconfronteerd met de terugkeer van een machtspolitiek die het lang niet heeft gekend. Het Dutch Transformation Forum 2019 bespreekt dit nieuwe speelveld van Europa's geopolitiek, veiligheid en verdienvermogen – vol risico's en kansen voor bedrijfsleven, overheid en wetenschap.



Digitale spionage op de loer

Een belangrijk thema binnen deze context is cybersecurity. Veel leiders in zowel de particuliere als de publieke sector begrijpen volledig het belang hiervan voor hun bedrijfsresultaten en doelstellingen. De inzet is hoog. Er is risico op onderbreking van vitale diensten na aanvallen door kwaadwillende groepen, maar ook digitale spionage of diefstal van intellectueel eigendom liggen op de loer. Volgens een wereldwijd onderzoek van Harvey Nash en KPMG, gehouden onder meer dan 3.500 Chief Information Officers (CIO's) in meer dan 100 landen, heeft 32 procent de afgelopen twee jaar een grote cyberaanval meegemaakt. In 2014 was dat 22 procent.

Handel niet uit angst

In het DTF-paper, dat KPMG samen met Instituut Clingendael schreef, is één van de vragen: wat is de beste houding ten opzichte van de opkomende dreigingen? Handelen uit angst is waarschijnlijk niet de beste optie, evenals het loskoppelen van de kabels – het zou innovatie verstikken en economieën verlammen.
Wél haalbaar is het om deze bedreigingen deel uit te maken van de *business as usual*. Dat begint met het herkennen van wat er op het spel staat - de 'kroonjuwelen' - en analyseren welke partijen nauwlettend in de gaten moeten worden gehouden. Dat gebeurt deels al, want volgens hetzelfde onderzoek van Harvey Nash en KPMG vinden gelukkig steeds meer CIO's dat ze goed voorbereid zijn op aanvallen: 26 procent, vergeleken met 21 procent in 2017.

Experts schatten dat commerciële spionage 55 miljard euro aan economische groei en tot 289.000 banen in de EU in gevaar kan brengen.

Het volledige DTF-paper is vanaf 20 november te lezen op kpmg.nl/topics

CYBER IN DE BOARD ROOM

Cybersecurity mag niet alleen een issue zijn voor de afdeling ICT. Van werkvloer tot boardroom, iedereen moet zijn steentje bijdragen.

BOARDROOM

Een aanval op clouddiensten van Google. Een datalek bij de concurrent waardoor de klantgegevens op straat liggen. Het zijn vaak incidenten waardoor cyber security ineens op de agenda van de boardroom belandt. Waar staan wíj eigenlijk op het gebied van cybersecurity? En investeren we – vergeleken met andere bedrijven – genoeg?

Terechte vragen, want te vaak gaan bestuurders en commissarissen uit van een schijnzekerheid. 'Bij ons gebeurt nooit wat' gaat voorbij aan de blinde vlekken en zwaktes die elk bedrijf heeft. Een Cyber Maturity Assessment geeft inzicht in hoe een organisatie omgaat met gevoelige gegevens en hoe het staat met onder andere de governance, de processen rondom riskmanagement en informatietechnologie. Het maakt de kwetsbaarheid voor cyberdreigingen zichtbaar en de kwaliteit van de voorbereidingen daarop.

Het kennisniveau in boardrooms is nog steeds wisselvallig, de verschillen zijn groot. Zeker niet alle boardleden kennen de ins en outs van de technologieën als blockchain en Artificial Intelligence. Laat staan dat ze bekend zijn met de betreffende cyberrisico's. De informatietechnologie en de bijbehorende processen worden vaak nog gezien als een IT-issue, terwijl deze het hele bedrijf aangaan. Eens per kwartaal zou cybersecurity daarom minimaal op de agenda van de boardroom moeten staan.

Het managen van cyberrisico's is namelijk geen momentopname, maar een doorlopend proces. De technologie verandert zo snel en dat geldt ook voor de regelgeving op het gebied van privacy en toezicht. In het meest ideale geval is cyberveiligheid onderdeel van het businessproces en is er sprake van *security by design*. Cybersecurity is dan standaard bij de ontwikkeling van nieuwe producten en diensten.

WERKVLOER

Elke organisatie is uniek en heeft andere vragen. Soms is er vooral behoefte aan specifieke oplossingen voor concrete vraagstukken. Denk bijvoorbeeld aan het in kaart brengen van risico's van het gebruik van clouddiensten. Andere bedrijven willen advies over de strategie. Goed om dan eerst het niveau van aanvaardbare en tolereerbare risico's te bepalen. Een organisatie krijgt dan zicht op de 'kroonjuwelen' en de belangrijkste cyberdreigingen.

De meeste cyberrisico's komen nog steeds voort uit menselijk handelen. Personeel maakt een fout bij het installeren van een app, de helpdesk lekt door onoplettendheid privacygevoelige informatie. KPMG biedt tools en diensten om de awareness in organisaties structureel te verhogen en te verankeren in de organisatiestructuur. Hierbij kijken we ook hoe het personeel scoort op risicobewustzijn. Soms is ook een stukje social engineering nodig. Een ethical hack laat medewerkers inzien en ervaren dat zij, naast alle securitymaatregelen, veelal de zwakke schakel zijn. Ondanks het strenge wachtwoordbeleid komt een ongenode gast toch in de systemen. Met een aantal klikken verder is hij in de inbox van een boardmember. Hoe snel werd het probleem ontdekt en hoe adequaat was de reactie? Maar ook: hoe kon het (technisch gezien) zover komen? Er is geen betere wake-up call.

STRATEGIE

Bij KPMG streven we naar voortuitgang die goed is voor de maatschappij. Digitalisering heeft de samenleving veel gebracht, maar levert ook problemen op. Met onze oplossingen kunnen klanten de nieuwste technologie gebruiken terwijl ze het vertrouwen houden in hun zakelijke omgeving.

Een cybersecurity-strategie vormt vaak het sluitstuk van een adviestraject. In een strategische *roadmap* schetsen we een duidelijk beeld van waar de organisatie over één tot twee jaar staat, en welke trajecten prioriteit hebben. Dit alles met het doel om de cyberrisico's structureel verminderen. Belangrijk hierbij is om cybersecurity een structureel onderdeel van het business proces te maken. Welke risico's moeten als eerste worden aangepakt? Hoe vergroten we de awareness van de medewerkers?

KPMG ontwikkelt cybersecurity strategieën en *roadmaps* voor elk type organisatie en elke soort industrie. We maken gebruik van internationale standaarden van informatiebeveiliging, de ervaringen van onze nationale en internationale specialisten en leading practices op het gebied van cyber security. Wanneer een strategie effectief wordt doorgevoerd, leidt dit tot positief rendement op cyberinvesteringen, de klantervaring, de merkreputatie en de naleving van wet- en regelgeving.

Met medewerking van Ton Diemont

TEKST SASKIA KLAASSEN **BEELD** ISTOCK

Veranderingen in de belastingfunctie volgens Unilever

'IK VOORZIE EEN GROTE VERANDERING VAN ROLLEN'

Loek Helderman van KPMG wisselde op het hoofdkantoor van Unilever in Londen van gedachten over (de toekomst) van belastingen met de CFO van Unilever, Graeme Pitkethly en EVP Global Tax & Treasury, Janine Juggins. RAAD was erbij.

Janine Juggins
Executive Vice President Global Tax & Treasury Unilever

Graeme Pitkethly
Chief Financial Officer Unilever

Loek Helderman
Loek Helderman is Tax Partner bij KPMG Meijburg. Tot 2010 werkte hij bij Unilever, als VP Tax en als lid van het Global Tax Leadership Team.

Loek Helderman: Kunnen jullie beschrijven hoe de huidige belastingfunctie georganiseerd is binnen Unilever?
Janine Juggins: "De belastingfunctie is bij ons een wereldwijde functie in die zin dat alle belastingprofessionals rapporteren aan de Global Head of Tax. Op managementniveau maken wereldwijd circa 85 mensen deel uit van het fiscale team. En dan op junior- tot managementniveau zijn dat er nog eens circa 175. We zijn zeer gedecentraliseerd, dus onze belastingprofessionals bevinden zich veelal in de landen waar we met onze bedrijfsonderdelen actief zijn. Wanneer we geen fiscale vertegenwoordiging ter plaatse hebben, is het land gewoonweg niet groot genoeg. We hebben ook een corporate team dat gevestigd is op een paar locaties: Londen, Rotterdam, New York en Singapore. Maar afgezien daarvan is de belastingfunctie op die plekken gevestigd waar onze bedrijfsonderdelen actief zijn. In de meeste van onze grote landen hebben we tax compliance – de aangifte vennootschapsbelasting - uitbesteed aan een van de Big Four."

Wat zijn naar jullie idee vandaag de dag de grootste uitdagingen voor een belastingfunctie zoals die van Unilever?
Janine: "Wij zijn fervent voorstander van het BEPS-initiatief van de OESO om de internationale belastingheffing te hervormen, zodat winsten daar worden belast waar sprake is van waardecreatie. We willen zeker weten dat we op de juiste plaats het juiste bedrag aan belasting betalen en laten ons leiden door onze belastingbeginselen bij het maken van moeilijke afwegingen. We willen graag soortgelijke verbeteringen zien om dubbele belastingheffing te voorkomen en om bedrijven meer investeringszekerheid te bieden. We hebben wereldwijd te maken met een aantal belastingcontroles en deze nemen veel tijd en middelen in beslag. Zowel belastingautoriteiten als belastingbetalers zouden er baat bij hebben als deze onzekerheden worden weggenomen."
Graeme Pitkethly: "Drie belangrijke factoren veranderen het belastinglandschap. De eerste is technologie, omdat technologie inmiddels een wezenlijk instrument van belastingautoriteiten, overheden en bedrijven is als het gaat om wijzigingen in de manier van zakendoen. De tweede is dat er een substantiële verschuiving plaatsvindt van waardecreatie met bijvoorbeeld vaste activa naar waardecreatie met intellectuele eigendommen; ik denk dat vooral de vraag waar de waarde van die laatstgenoemde component zich bevindt interessant is. De derde factor is economisch nationalisme, dat leidt tot een nieuwe, contradictoire wereldorde onder invloed van het politieke klimaat in elk land."
Janine: "Ik zou nog een andere factor willen toevoegen. In de afgelopen jaren is enorm veel vertrouwen verloren gegaan. Om dat vertrouwen terug te winnen gaan belastingautoriteiten er niet langer van uit dat belastingbetalers te goeder trouw hebben gehandeld en hun best hebben gedaan om aan de regels te voldoen. Elke aangifte wordt gecheckt. Transparantie is het nieuwe toverwoord. Deze vier factoren bij elkaar gaan het belastingklimaat van de toekomst bepalen. Uiteindelijk is zelfs een scenario denkbaar waarin de belastingautoriteiten de aangifteformulieren invullen en de belastingbetaler deze controleert. Volledig omgekeerde rollen, dat heeft de toekomst voor ons in petto."

En als het gaat om de belastingfunctie als zodanig en de mensen van de belastingafdeling, worden er specifieke eisen gesteld aan de vaardigheden van fiscalisten?
Janine: "Dat is zoals je weet een heet hangijzer binnen een belastingafdeling. We proberen ons de toekomst voor te stellen: hoe ziet de belastingafdeling er over vijf jaar uit? Wat voor soort dingen doen ze dan misschien anders vergeleken met nu? En welk type vaardigheden vereist dat? Is het eenvoudiger om een IT'er belastingvaardigheden bij te brengen of is het eenvoudiger om een belastingspecialist bij te scholen op het gebied van IT? We buigen ons over al dit soort vragen. Je moet weten wat er gebeurt binnen een bedrijfsonderdeel om financiële en fiscale taken naar behoren te kunnen uit-

TEKST JOKE VAN ROOYEN **BEELD** HOLLADSE HOOGTE, UNILEVER

In 1884 begint Lever & Co met het produceren van zeep onder de merknaam Sunlight. Unilevers visie – mensen helpen er goed uit te zien, zich goed te voelen en meer uit het leven te halen – loopt als een rode draad door de hele geschiedenis.

Het in 2010 gelanceerde *Unilever Sustainable Living Plan* omschrijft drie doelen voor 2020:
→ Meer dan een miljard mensen helpen hun gezondheid en welzijn te verbeteren
→ De milieu-impact van de productie en het gebruik van onze producten halveren
→ De levensstandaard van duizenden mensen in onze toeleveringsketen verbeteren

voeren. Daarnaast moeten we allemaal veel meer oog hebben voor technologie, misschien niet als specialisten maar in ieder geval door zich bewust te zijn van de ontwikkelingen op het vlak van technologie."

Graeme: "Als je vijf jaar vooruitkijkt, misschien zeven of tien jaar, dan denk ik dat functionele scheidslijnen over het algemeen vervagen. Ik denk dat het bedrijf in de toekomst mogelijk geen strikt gescheiden afdelingen HR, Finance, Audit of Tax zal hebben. Uiteraard zal een zekere mate van expertise noodzakelijk blijven, maar in grote lijnen wordt zakendoen gestuurd door technologie, door data, door de activiteit van een bedrijfsonderdeel. Door dingen te benaderen vanuit de invalshoek van consumenten, medewerkers en klanten kun je veel beter verbanden leggen zonder dat dit ingewikkelde organogrammen vereist. Nog iets dat we hebben geleerd is dat je wel uitstekende functies kunt hebben, maar de kunst bij het vervullen van deze functies is om goed samen te werken tussen afdelingen en bedrijfsonderdelen. Dit brengt onvermijdelijk met zich mee dat het onderscheid tussen wat een financieel directeur doet vergeleken met wat een directeur personeelszaken of een logistiek directeur doet, vervaagt."

Janine: "Ja, ook technologische vaardigheden zijn vandaag de dag zonder meer een pre wanneer we potentiële kandidaten beoordelen. Maar waar we ons nu al op richten, is het toepassen van belastingtechnologie in de praktijk. Om het minder ontmoedigend en toegankelijker te maken hebben we een aantal kleine projecten op het gebied van belastingtechnologie geïmplementeerd, waarbij mensen zich afvroegen hoe technologie kan helpen om knelpunten in bestaande processen weg te nemen. Dankzij deze interessante en nuttige projecten kregen onze mensen meer oog voor de mogelijke toepassingen van technologie."

Een van de grootste uitdagingen voor (Nederlandse) bedrijven is om terreinen in kaart te brengen waar de belastingfunctie en risicomanagement kunnen worden verbeterd door het gebruik van technologie. Bent u het ermee eens dat dit een insteek is om werk te maken van technologie?

Janine: "De juiste business case vinden en de financiering verkrijgen is een grote sta-in-de-weg, vooral bij grotere projecten. Maar een van de grote innovaties die we vorig jaar binnen Unilever hebben beproefd is de totstandbrenging

'Strikt gescheiden afdelingen HR, Finance en Tax verdwijnen mogelijk'

→ Graeme Pitkethly, Chief Financial Officer Unilever
Pitkethly trad in 2002 in dienst van Unilever en was eerder Executive Vice President en General Manager van Unilever UK en Ireland. Daarvoor bekleedde hij een aantal financiële en commerciële functies binnen Unilever, waaronder Senior Vice President of Finance for Global Markets, Global Head of M&A, Head of Treasury, Pensions and Tax en Chief Financial Officer van Unilever Indonesia. Graeme heeft binnen en buiten het bedrijf zijn sporen verdiend met, voorafgaand aan zijn dienstverband bij Unilever, diverse senior financiële functies in de telecommunicatiesector en bij PricewaterhouseCoopers.

→ Janine Juggins, Executive Vice President Global Tax & Treasury Unilever
Juggins trad in 2013 in dienst van Unilever als SVP Global Tax. Ze maakte de overstap van Rio Tinto, waar ze actief was als Global Head of Tax. In juli 2018 werd Juggins in aanvulling op haar fiscale taken benoemd tot Group Treasurer van Unilever. Ze beschikt over ruim 25 jaar ervaring met internationale belastingaangelegenheden, daar ze tevens als Head of Tax werkzaam was voor het in de FTSE 250 opgenomen ingenieursbureau APV, en als VP of Tax-Trading verbonden aan Enron Europe. Ze is voorzitter van de Tax Committee van de Britse werkgeversorganisatie CBI.

→ Loek Helderman
Loek Helderman is partner International Tax, Transfer Pricing, Value Chain Management bij KPMG Meijburg & Co Belastingadviseurs. Tot 2010 werkte hij bij Unilever, als lid van het Unilever Tax Leadership Team.

van een 'digifund' voor kleine projecten waardoor mensen naar financiering kunnen dingen zonder de uitdaging een ultieme business case te moeten presenteren. Dit maakte het makkelijker om van start te gaan en dat is echt belangrijk."
Graeme: "Grootschalige IT-problemen vormen vandaag de dag een veel kleiner risico dan in het verleden. Er zijn momenteel talloze technologieën voorhanden, en je kunt de plank nauwelijks echt misslaan wat technologie betreft. Maar bij het ontwerpen van RPA's (Robotic Process Automation) bijvoorbeeld, zijn twee aspecten van belang: allereerst moet je toegang hebben tot wat de robot doet en je moet er controle over kunnen uitoefenen. Daarnaast moet je nagaan of dataretentie binnen je bedrijf ethisch verantwoord is. Dit is een interessant gegeven voor bedrijven. Ook relevant voor de Big4 trouwens."

Hoe ziet u de rol van de Big Four? Wat verwacht u van ze?
Janine: "Het is belangrijk om met vele adviseurs te spreken om een goed beeld van de nieuwste ontwikkelingen te krijgen. Het was goed om samen te werken met adviseurs, met name wanneer ze beschikken over specifieke technologie die we kunnen toepassen op onze eigen systemen en data. Wat RPA's en het wegnemen van knelpunten in onze huidige processen betreft, zodra je de eerste stappen hebt gezet en wat vertrouwen hebt gekweekt, is het van belang om een stapje terug te doen en de automatisering van het proces eerst ter hand te nemen zodra je je hebt afgevraagd – mogelijk met de hulp van een adviseur – of de zaak van meet af aan anders benaderd kan worden; dus het anders inrichten van je proces."

Terug naar de belastingfunctie als zodanig. Tijdens de EMA Tax Summit in Rome vorig jaar discussieerde een panel over de omvang en inhoud de belastingfunctie. De sprekers schatten dat over drie tot vijf jaar twintig procent van de mensen data analisten en technologiedeskundigen zullen zijn, met een belastingachtergrond. Ziet u dit gebeuren over drie tot vijf jaar?
Janine: "Het routinewerk zal worden geautomatiseerd, maar je hebt nog altijd iemand nodig die met de belastingautoriteiten in een land samenwerkt, die de cultuur begrijpt, de context, en hoe cruciaal het is de belastingcontrole naar behoren uit te voeren. Tijd die wordt bespaard door de routine te automatiseren kan ook worden besteed aan taken die meer waarde toevoegen. Maar ik voorzie wel dat wat de vaardigheden betreft je mensen nodig hebt die beter in staat zijn om systemen te beheren of die in ieder geval begrijpen hoe gegevens worden verwerkt binnen het systeem en hoe je de gegevens kunt gebruiken. Met andere woorden: je hebt iemand nodig die enerzijds beschikt over de specifieke IT-kennis om de gegevens te extraheren en te verwerken, en anderzijds weet waar hij of zij naar op zoek is."

Belastingautoriteiten ontwikkelen momenteel andere manieren om belasting te heffen, met gebruikmaking van technologie. Wat vindt u van deze ontwikkeling?

Janine: "Wat transactiebelastingen betreft gaan we naar een situatie waar bedrijven hun belastingaangifte niet langer zelf invullen maar deze reeds ingevuld ontvangen, met mogelijk een omkering van de bewijslast dus. Bij directe belastingen moeten we afwachten of de ontwikkeling van de digitale economie veranderingen in het internationale belastingsysteem met zich meebrengt."

Wil Unilever een voortrekkersrol vervullen als het gaat om transparantie?
Janine: "Sinds de invoering van onze belastingbeginselen in 2013, delen we elk jaar meer informatie; informatie waarvan we denken dat deze de potentiële doelgroep van pas zal komen en die ingaat op de voornaamste probleemgebieden. We hebben een pagina op onze website 'What Matters To You – Tax" onder 'Duurzaamheid' op onze website. Britse bedrijven zijn tegenwoordig verplicht tekst en uitleg te geven over hun strategie inzake belastingen, en deze pagina is mede daaraan gewijd. Ook valt er te lezen hoe onze governance wordt bepaald door onze belastingbeginselen, wat deze inhouden, een paar voorbeelden van hoe ze worden toegepast, en hoe we tegenover fiscale stimuleringsmaatregelen staan. We zijn dus heel open."

Unilever staat al jarenlang bovenaan de Dow Jones Sustainability Index. Is dat een bewust streven?
Graeme: "Ons bedrijfsmodel is gebaseerd op een doelbewuste benadering waarbij alle belanghebbenden worden betrokken. Verantwoorde, duurzame, consistente en winstgevende groei is niet alleen het juiste om te doen, maar levert ook voordelen op voor onze consumenten, leveranciers, klanten, werknemers en onze aandeelhouders. De Dow Jones Sustainability Index erkent onze prestaties op tal van gebieden en de transparante wijze waarop we over onze prestaties communiceren." ■

Investeren in de aanpak van cybercrime

'ER ZIT EEN GRENS AAN INVESTEREN'

Investeren in de weerbaarheid van je organisatie is goed, stelt John Hermans, partner bij KPMG. Maar er zit een grens aan, want de kosten rijzen intussen de pan uit. Hoe houd je het betaalbaar? "Misschien is het tijd voor een fundamenteel andere aanpak van cybercrime."

TEKST LEONIE HAGE BEELD ARON VELLEKOOP LEÓN

Cybersecurity-specialist John Hermans zag de laatste jaren de weerbaarheid van organisaties flink toenemen. Dat is volgens hem niet in de laatste plaats te danken aan bestuurders en commissarissen, want cybercrime staat inmiddels in heel veel boardrooms op de agenda. Hermans: "Waar een paar jaar geleden bijna geen enkele bestuurder of commissaris iets van dit onderwerp wist, is tegenwoordig het overgrote deel zich bewust van de risico's. Er is aandacht voor het inrichten van cybersecurity maatregelen, er lopen weerbaarheidsonderzoeken (al dan niet door derde partijen) om de effectiviteit van deze maatregelen te testen en bestuur laat zich goed informeren over waar ze staan met betrekking tot cybersecurity."

John Hermans is partner binnen KPMG Advisory en is verantwoordelijk voor de KPMG dienstverlening op het gebied van informatiebeveiliging. Daarnaast is hij verantwoordelijk voor de EMEA Cyber Security dienstverlening van KPMG. Ook is hij lid van de Raad van Advies van Cyber Security Academy in Den Haag.

Risico aanvaarden

De toegenomen bewustwording is een goede zaak, maar brengt tegelijkertijd nieuwe uitdagingen met zich mee. Want door de extra aandacht, nemen ook de investeringen toe. Tot hoever moet je gaan wetende dat al deze investeringen het risico op een cyberincident niet tot nul reduceren. Bedrijven doen er goed aan om tien procent van het ICT-budget te reserveren voor maatregelen tegen cybercrime, adviseerde Herna Verhagen een aantal jaar geleden. Hermans sluit zich daarbij aan, maar plaatst ook een kanttekening. "Het kan ook te veel worden. Je moet je afvragen tot wanneer het de organisatie daadwerkelijk nog wat

Cyber in de audit

De rol van accountants in de strijd tegen cybercrime is in Nederland nog redelijk onontgonnen terrein. "Maar wél relevant", zegt John Hermans. "Incidenten met cybersecurity in je organisatie kunnen gevolgen hebben voor de jaarrekening. Denk alleen aan boetes vanwege de AVG, of de enorme boetes van Facebook en Britisch Airways vanwege datalekken. Of als je intellectueel eigendom wordt weggehackt. Immers, dat staat als waarde op de balans. Ook een veranderend businessmodel als gevolg van nieuwe technologieën hebben invloed. Bestuurders en commissarissen doen er goed aan om de taakverdeling bespreekbaar te maken. Wat hoort bij internal audit, waar speelt de accountant een rol?"

oplevert. Honderd procent beveiliging bestaat niet, nergens. Dus ergens moet je stoppen met investeren en het risico aanvaarden."
Maar er valt zeker nog winst te behalen, weet Hermans. "Het kan allemaal misschien nog wel slimmer, bijvoorbeeld door de krachten te bundelen. "We zien dat nu al gebeuren in de energiesector, en ook bij kleinere banken en verzekeraars. Het is een logische stap: deze organisaties hebben dezelfde soort systemen en dezelfde aanvallers. Zij gaan uit van gelijke aanvalscenario's die ze monitoren. Om dat via één concept te doen, wellicht zelfs met een onafhankelijke partij voor de hele sector, is veel efficiënter."

Terug de business in

Ondertussen liggen er ook kansen in de organisaties zelf. Hermans ziet een toename in investeringen in de tweede lijn en niet in de eerste lijn. Heel veel organisaties hebben een speciale afdeling voor cybersecurity, en die groeien de laatste jaren flink. " In mijn ogen kan er, zoals ook bij andere processen gebeurt, veel terug de business in. Een simpel voorbeeld: dubbel betaalde facturen zijn onwenselijk in iedere organisatie. Dan kun je iemand inzetten die dat controleert. Beter zou het zijn, als je in het systeem kunt invoeren dat die factuur überhaupt niet dubbel betaald wordt. Ook bij cybersecurity kun je simpele controles terugbrengen in de eerste lijn. Denk bijvoorbeeld aan achteraf controles die door de tweede lijn wordt gedaan ten aanzien van toegangsrechten. Dit kun je natuurlijk ook meteen in de eerste lijn laten afhandelen door gebruik te maken van slimme analytics oplossingen."

War for talent

Zowel het bundelen van de krachten als processen terug de business inbrengen leiden volgens Hermans tot een bijkomend voordeel: de *war for talent* zal afnemen of in ieder geval niet verder groeien. "Ik ken organisaties waar drie of vierhonderd mensen werken op de afdeling cybersecurity. Er is op dit moment een grote gekte gaande als het gaat om cyberspecialisten. De salarissen zijn heel erg hoog, wat niet bijdraagt aan de totale kosten. Als sectoren meer samen optrekken en binnen organisaties door digitalisering activiteiten in de eerste lijn worden geborgd, zal je nu eenmaal minder capaciteit van de echte cybersecurity specialisten nodig hebben." ■

KPMG RAAD *BOARD PROGRAM*

AGENDA

KPMG organiseert regelmatig bijeenkomsten en rondetafel-sessies. We zien u komend jaar graag op één van onze events.

MAART

> Wat? Bijeenkomst voor raad van commissarissen
Thema: Cyber - hebben we genoeg zicht op de kansen en bedreigingen op het gebied van digitale veiligheid (cyber)? Hoe wordt cyber gebruikt in geopolitiek? Europa lijkt achter te liggen op het gebied van cybersecurity, cyberwarfare en belangrijke technologieën die daarvoor nodig zijn. Het bewustwordingsproces, ook in de samenleving, over de cyberaspecten van onze veiligheid komt pas net op gang. Hoe gaan we die inhaalslag maken?

> Wat? Rondetafel voor president raad van commissarissen
Thema: Balancing between Business (as Usual) and Societal Expectations

> Wat? Bijeenkomst op 27 maart voor senior finance professionals van gevestigde organisaties die in de top van de finance-functie werken en die leiding geven in finance en transformatie-uitdagingen van hun organisatie
Thema: Next gen Finance

APRIL

> Wat? Bijeenkomst voor raad van commissarissen
Thema: Digitaal leiderschap, wat heb je nodig om succesvol leiding te geven in deze digitale transformatie?

> Wat? Rondetafel voor president raad van commissarissen
Thema: Balancing between Business (as Usual) and Societal Expectations

MEI

> Wat? Bijeenkomst voor raad van commissarissen
Thema: ethische dilemma's binnen algoritmen

> Wat? CFO-Forum voor chief financial operators
Thema: Strategy in the Convergence of Change

JUNI

> Wat? Bijeenkomst op 19 juni voor senior finance professionals van gevestigde organisaties die in de top van de finance-functie werken en die leiding geven in finance en transformatie-uitdagingen van hun organisatie
Thema: Next gen Finance

AUGUSTUS

> Wat? Zomersessie op 31 augustus voor raad van commissarissen

OKTOBER

> Wat? Bijeenkomst op 9 oktober voor senior finance professionals van gevestigde organisaties die in de top van de finance-functie werken en die leiding geven in finance en transformatie-uitdagingen van hun organisatie
Thema: Next gen Finance

Altijd actueel

Wilt u per e-mail op de hoogte worden gehouden van alle evenementen, nieuwsbrieven en andere uitingen, dan kunt u dit aangeven via ons preference center via home.kpmg/nl/raad

Heeft u vragen of wilt u meer informatie, stuur dan een mail naar Raad@KPMG.nl.

RAAD magazine is een speciale uitgave van KPMG, verschijnt twee keer per jaar en helpt commissarissen, toezichthouders en bestuurders bij het nog beter invullen van hun rol. RAAD biedt inspiratie, inzicht en persoonlijke ervaringen op terreinen als audit & assurance, business conduct, boardroom dynamics & soft skills, innovatie en internationalisering.

Uitgever
KPMG N.V.
Realisatie
KPMG Brand, Reputation & Management
Concept, vormgeving en redactie
Maters & Hermsen Journalistiek
Lithografie
Studio Boon
Drukwerk
Reijnen Media

Redactieadres
KPMG N.V.
Brand, Reputation & Management
Postbus 74555
1070 DC Amsterdam
E-mail: raad@kpmg.nl

Adreswijziging
Wilt u dit magazine liever op een ander (zoals uw privé)adres ontvangen? Of wenst u het magazine niet meer te ontvangen? Stuur ons dan een e-mail: raad@kpmg.nl.

MIX
Papier van verantwoorde herkomst
FSC® C017135
FSC www.fsc.org

Cyber Security draait om technologie en mensen

People-driven progress

Meer weten over Cyber Security?
Kijk op kpmg.nl

KPMG