VNO-NCW

FORUM SPECIAL

MAART 2025

# BILDERBERG

**PREPPEN OP HET WERK**
‘Hoe zwarter het scenario, hoe beter’

**GLUREN BIJ DE BUREN**
Finland is al 80 jaar op zijn hoede voor Rusland

**NCTV-BAAS:**
‘Onze economie is heel kwetsbaar’

**HAVEN EN HACKS**
Cyberdreiging zal nooit meer verdwijnen

**STAAT VAN PARAATHEID**

# Iedereen is een potentieel doelwit

# Voorwoord

Sabotageacties om belangrijke kabels in zee te beschadigen of onbruikbaar te maken, cyberaanvallen waarbij statelijke actoren betrokken zijn, oorlogsdreiging op ons continent. Het is inmiddels een realiteit waarmee we ook in Nederland rekening moeten houden en waar we op voorbereid moeten zijn.
Ondernemers zien dit risico ook, blijkt uit een onderzoek dat we onlangs hebben gedaan. Ze noemen sterk fluctuerende energieprijzen, zoals die na de Russische inval in Oekraïne, en cyberaanvallen als de grootste risico's. Ook het risico op langdurige stroomuitval vinden ze reëel. Maar risico's zien en er echt op voorbereid zijn, blijken nog wel verschillende dingen. Niet iedere ondernemer heeft een noodplan en doet (virtuele) oefeningen.

Wij mensen onderschatten de waarschijnlijkheid of de impact van een potentieel gevaar nogal eens. Logisch: we denken dat dingen zullen blijven zoals ze altijd waren. Dat is wel begrijpelijk, maar ook riskant. Dat bleek toen we tijdens de coronapandemie ineens niet meer konden rekenen op de import van noodzakelijke goederen, en toen we genoodzaakt waren de aanvoer van Russisch gas te stoppen. De weerbaarheid van onze samenleving, ons bedrijfsleven en onze economie vergroten is belangrijk, zodat we kunnen omgaan met onvoorziene omstandigheden. Niet voor niets hebben we deze pijler toegevoegd aan onze middellangetermijnvisie. We moeten ook wel, door het steeds grilligere geopolitieke klimaat. De Bilderbergconferentie van dit jaar gaat over het vergroten van die weerbaarheid. In deze speciale uitgave vindt u alvast inspiratie om daar zelf mee aan de slag te gaan. Laat ondernemers, onze premier en een hoge militair u tijdens de conferentie aan het denken zetten: hoe vergroten we onze weerbaarheid? Wat is mijn eigen rol? En hoe zorgen we dat politiek, samenleving en bedrijfsleven voorbereid zijn op wat ons mogelijk te wachten staat? Ik wens u vast veel leesplezier en inspiratie. En misschien tot op de Bilderbergconferentie.

*Ingrid Thijssen*
*Voorzitter VNO-NCW*




## COLOFON

De Bilderberg is een speciale editie van Forum, het opinieblad van ondernemingsorganisatie VNO-NCW. De editie verschijnt ter gelegenheid van de Bilderbergconferentie.

**Redactieadres** Bezuidenhoutseweg 12, 2594 AV Den Haag, telefoon 070 - 3490 165, e-mail forum@vnoncw-mkb.nl

**Redactie** Jiska Vijselaar (hoofdredactie), Şenay Özdemir, Marcia Timmermans (eindredactie), Paul Scheer, Pascal Theunissen (redactie), Anoeska Kruithof (grafische vormgeving)

**Aan dit nummer werkten mee** Linda van Beek, Jessica Maas, Sam Rentmeester, Marion Rhoen, Bas van der Schot, Roy op het Veld, Jeroen Visser, Eduard Voorn

**Concept en basisontwerp** Blue Field Agency, Amsterdam

**Cover** Bas van der Schot

**Drukwerk** Koninklijke Em. de Jong bv, Visweg 8, Postbus 8, 5110 AA Baarle-Nassau

# PROGRAMMA 63STE BILDERBERGCONFERENTIE

## DONDERDAG 10 APRIL 2025

| | |
|---|---|
| **VANAF 17.00 UUR** | Ontvangst/borrel |
| **18.30 UUR** | Opening<br>**Ingrid Thijssen,** voorzitter VNO-NCW |
| **18.40 UUR** | **Dick Schoof,** minister-president |
| **19.00 - 22.00 UUR** | Diner |
| **22.00 - 00.30 UUR** | Borrel |

## VRIJDAG 11 APRIL 2025

| | |
|---|---|
| **VANAF 07.30 UUR** | Ontbijt |
| **09.00 UUR** | Overdenking<br>**Jules Dresmé,** pastoor |
| **09.45 UUR** | Heropening door conferentievoorzitter |
| **09.50 UUR** | **Rob Bauer,** topmilitair |
| **10.35 UUR** | **Michiel Vos,** journalist |
| **11.05 UUR** | Pauze |
| **11.30 UUR** | Parallelsessies met workshops over onder meer: lokale weerbaarheid, cyberweerbaarheid, communicatie (nepnieuws, framing), scenarioplanning, sociale veerkracht, inzet van reservisten |
| **12.30 UUR** | Lunch |
| **13.30 UUR** | **Carola Schouten,** burgemeester Rotterdam |
| **14.00 UUR** | Inspiratiesessie over de verantwoordelijkheid die eenieder heeft in het vergroten van weerbaarheid, met deelnemers vanuit overheid, bedrijfsleven en civil society |
| **14.45 UUR** | Pauze |
| **15.15 UUR** | **Joost Farwerck,** ceo KPN |
| **16.00 UUR** | Slotwoord<br>**Ingrid Thijssen,** voorzitter VNO-NCW |
| **AANSLUITEND** | Borrel |

**Conferentievoorzitter:**
**Diana Matroos**, journalist en presentator voor onder meer BNR Nieuwsradio

De Bilderbergconferentie is alleen toegankelijk op uitnodiging.
Deze uitnodigingen zijn reeds verstuurd. Programma en tijden onder voorbehoud.

# SPREKERS

MARTIJN BEEKMAN

## DICK SCHOOF

Dick Schoof is minister-president. Eerder was hij onder meer secretaris-generaal van het ministerie van Justitie en Veiligheid, hoofddirecteur van de IND, Nationaal Coördinator Terrorismebestrijding en Veiligheid en directeur-generaal van de AIVD.

ROBIN VAN LONKHUIJSEN/ANP

## ROB BAUER

Rob Bauer is topmilitair. Tot januari was hij voorzitter van het Militair Comité van de NAVO en de belangrijkste militair adviseur van de secretaris-generaal. Van 2017 tot 2021 was hij Commandant der Strijdkrachten van de Nederlandse Krijgsmacht.

ROBIN UTRECHT/ANP/HH

## MICHIEL VOS

Michiel Vos is journalist en woont al meer dan twintig jaar in de VS. Vanuit zijn standplaats New York doet hij verslag van de ontwikkelingen in dat land voor onder meer de omroepen RTL en VRT.

CASPER RILA

## CAROLA SCHOUTEN

Carola Schouten is burgemeester van Rotterdam. Ze was minister van Landbouw, Natuur en Voedselkwaliteit in het kabinet Rutte III en minister voor Armoedebestrijding, Participatie en Pensioenen in het kabinet Rutte IV.

GREGOR SERVAIS

## JOOST FARWERCK

Joost Farwerck is ceo van telecombedrijf KPN. Hij werkte er sinds zijn afstuderen in diverse functies, onder meer als managing director KPN Nederland. Hij is ook lid van de Cyber Security Raad, een onafhankelijk adviesorgaan voor kabinet en bedrijfsleven.

**TEKST:** ROY OP HET VELD **FOTO'S:** SAM RENTMEESTER

## Wie is Pieter-Jaap Aalbersberg

Pieter-Jaap Aalbersberg (1959) is sinds 2019 Nationaal Coördinator Terrorismebestrijding en Veiligheid. Eerder was hij politiechef in Amsterdam en leidde hij de repatriëringsmissie na de MH17-ramp. Hij specialiseerde zich in intelligence en georganiseerde misdaad. Aalbersberg was lid van EU-commissies en het Executive Committee van Interpol.

PIETER-JAAP AALBERSBERG (NCTV)

# ‘WE KUNNEN RISICO’S NIET UITSLUITEN, MAAR WEL BEHEERSEN’

Hybride oorlogsdreiging en cyberaanvallen zijn aan de orde van de dag. ‘Logistiek gezien is Nederland just in time ingericht. Dat maakt ons kwetsbaar.’ Aldus Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) Pieter-Jaap Aalbersberg.

In januari werd de TU Eindhoven gehackt. Van de ene op de andere dag kon er geen onderwijs meer gegeven worden. Onderzoekswerk lag stil en tentamens moesten een week worden uitgesteld. Was de hack het werk van cybercriminelen die losgeld eisen? Van statelijke actoren (organisaties die gelieerd zijn aan staten) die uit zijn op waardevolle onderzoeksdata of ontwrichting van de Nederlandse economie? Het is niet duidelijk. Feit is dat de dreiging door cyberaanvallen en sabotageacties inmiddels ‘aan de orde van de dag’ zijn, zegt Pieter-Jaap Aalbersberg, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

De vrije wereldhandel, waar Nederland als open economie enorm van heeft geprofiteerd, staat onder druk. ‘De economie, de rechtsorde en de democratie worden bedreigd’, somt Aalbersberg op. ‘De militaire en hybride dreiging is groot. We hebben een open economie en dat heeft ons veel welvaart gebracht. Logistiek gezien is Nederland just in time ingericht, dat wil zeggen dat er weinig voorraden worden aangehouden. ‘Dat is economisch weliswaar efficiënt, maar de coronapandemie en de Oekraïne-oorlog hebben ook aangetoond dat we daardoor kwetsbaar zijn. Als je als onderneming weinig voorraden aanhoudt, dan houdt de bedrijfsvoering snel op als de toelevering verstoord raakt. Dat is een serieus gevaar: dagelijks zijn er sabotageacties en cyberaanvallen.’

Dat blijkt op de dag van het interview. Op de valreep wordt het gesprek een uur verschoven vanwege ‘een spoedgeval’, waar Aalbersberg vervolgens ‘geen mededelingen’ over kan doen.

## LEGERS DIE ELKAAR BEVECHTEN

Waar de NCTV wél graag over praat, is hoe de economie en samenleving van Nederland weerbaarder te maken zijn. Aalbersberg werkt nauw samen met het ministerie van Defensie. ‘Want een weerbaar land verlaagt de kans op een oorlog, dan wel het effect van de verstoringen.’

Oorlog? Voor veel mensen is dat nog een ver-van-mijn-bedshow. En hoewel een klassieke militaire confrontatie, met legers die elkaar bevechten, op Nederlandse bodem onwaarschijnlijk is, brengt hybride oorlogsvoering wel degelijk schade toe. Dan gaat het over de


Pieter-Jaap Aalbersberg: 'Wat doe je als je vijf dagen niet in je systemen kunt?'

sabotage van energie- en telecommunicatiekabels op de zeebodem, langdurige uitval van energie en communicatie, destabilisering van de democratie door beïnvloeding via nepnieuws, digitale spionage en cyberaanvallen.
Aalbersberg: 'Chinese actoren streven naar werelddominantie. Ze doen er alles aan om elke nieuwe westerse technologie te bemachtigen. Veiligheidsdiensten waarschuwen steeds meer voor Chinese en Russische hackers. Het gaat soms om cybercriminelen, maar vaak ook om statelijke actoren. Wij zijn bezorgd dat er een conflict ontstaat aan de oostgrens van de NAVO. Hybride acties kunnen zich dan richten op de logistieke netwerken in Nederland, maar ook op ons energienetwerk. Het doel van dat soort acties is om instabiliteit te creëren. Uiteindelijk heeft Nederland een logistieke kernfunctie.'

## EEN WEEK ZONDER GPS

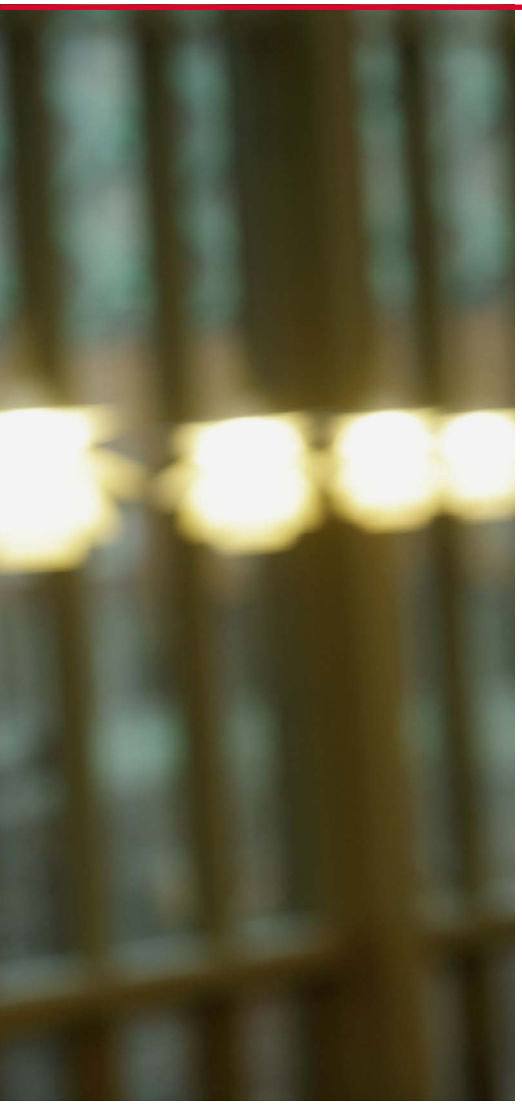
De overheid speelt een belangrijke rol in het weerbaarder maken van de samenleving. Maar het bedrijfsleven kan zelf ook veel doen, benadrukt Aalbersberg. Nederland heeft een kwetsbare stroomvoorziening. Een combinatie van sabotage en cyberaanvallen zou er weleens voor kunnen zorgen dat er langere tijd geen elektriciteit is. Wat doe je dan als bedrijf?
'Daar moet in bestuurskamers over nagedacht worden. Denk na over concrete scenario's. Wat doe je als je vijf dagen niet in je systemen kunt? Wat doe je als het gps-systeem een week uitvalt? Wat is de impact op de bedrijfsvoering en wat zijn je alternatieven?'
Aalbersberg adviseert bedrijven om zulke scenario's uit te werken voor het geval telecom-, internet- of energievoorzieningen ontregeld worden. 'En denk ook na wat je doet als de overheid medewerkers oproept voor publieke taken.'
Het versterken van de weerbaarheid is in ieder geval geen vrijblijvende exercitie, stelt Aalbersberg. 'We moeten versneld gaan investeren', zegt hij. Dat geldt voor de overheid, die de uitgaven aan defensie en cyberveiligheid verhoogt. Maar ook het bedrijfsleven zal moeten accepteren dat het veiligstellen van de eigen continuïteit – want daar komt het op neer – geld kost. 'De potentiële schade is altijd veel groter dan de investering die nodig is om die schade te voorkomen.'
Bedrijven zijn onvoldoende voorbereid op hybride dreigingen. Logistiek op basis van just in time is weliswaar efficiënt. Maar als de toeleveringsketen dagen of weken wordt onderbroken, kan dat de financiële gezondheid van een bedrijf acuut in gevaar brengen. 'Investeren in voorraden kan dan een goed idee zijn. Als je redundantie inbouwt, kun je langer door blijven draaien.'

## REDUNDANTIE IS JE VERZEKERING

Redundantie – meer voorraden of productiecapaciteit aanhouden dan nodig is – is in feite een verzekeringspremie. 'Dat is misschien duur', zegt Aalbersberg. 'Maar een hek om je bedrijfsterrein zetten en een portier aan de poort is ook kostbaar. Toch doen we dat allemaal.' Behalve een fysiek hek, moeten bedrijven volgens de NCTV dus ook zorgen dat hun digitale hek op orde is, en rekening houden met verstoringen voor het geval dat dat hek het begeeft.
De simpelste en beste tip voor bedrijven is om de software-updates van alle it-systemen tijdig te installeren. 'Als je alle basismaatregelen neemt, is de kans op een hack al een stuk kleiner', aldus Aalbersberg.
Maar kijk ook verder dan de eigen bedrijfspoort, zegt de NCTV. 'Niet alleen individuele bedrijven zijn kwetsbaar. Datacommunicatie is vaak georganiseerd in ecosystemen, met gegevensuitwisseling tussen meerdere bedrijven.' Dat wil zeggen dat de continuïteit van het ene bedrijf mede afhankelijk is van de investeringen in cyberveiligheid van het andere bedrijf. 'Nederland is een logistiek centrum voor Europa. De digitalisering en de integratie van systemen is ver doorgevoerd. Dat zorgt voor extra kwetsbaarheid, want logistieke centra worden in een oorlogssituatie als eerste aangevallen.'

## 'COMPARTIMENTEREN IS VERSTANDIG'

De innige samenwerking tussen bedrijven en de vergaande integratie is volgens Aalbersberg



vanuit het perspectief van veiligheid ‘niet altijd goed’. ‘Sowieso is het verstandig om systemen apart te zetten en te compartimenteren.’ Tegelijkertijd ligt een deel van de oplossing juist wel in de samenwerking. ‘De bedrijven in Brainport Eindhoven doen dit in onderlinge samenwerking. Met name voor het midden- en kleinbedrijf is samenwerking essentieel, omdat die individueel niet de kennis en de capaciteit hebben om alle maatregelen te nemen. Het mkb heeft nog een grote stap te maken.’

De menselijke factor is vaak de zwakke schakel. Een medewerker die in een moment van onoplettendheid op een link in een mail klikt, kan al voldoende zijn voor hackers om binnen te komen. ‘Bewustwording en alertheid zijn essentieel’, meent Aalbersberg.

Van landen als de VS, China en Rusland is bekend dat ze in de systemen van elkaars publieke en private infrastructuur zijn geïnfiltreerd, zonder dat er meteen sabotage wordt gepleegd. Chinese hackers zouden het Amerikaanse mobiele telefonienetwerk plat kunnen leggen op het moment dat China Taiwan inlijft. Door het openbare leven te ontregelen zou de Amerikaanse motivatie worden ‘verpletterd’ om Taiwan te verdedigen, zo tekende tijdschrift *The Economist* op uit de mond van een Amerikaanse cyberveiligheidsfunctionaris.

**‘GA ER MAAR VAN UIT DAT HACKERS AL IN JE SYSTEEM ZITTEN’**

Dus zelfs al zijn alle software-updates keurig geïnstalleerd, zelfs al zijn alle medewerkers op training geweest, dan kan een bedrijf nog steeds kwetsbaar zijn. ‘Ga er maar van uit dat hackers al in je systeem zitten’, waarschuwt Aalbersberg. ‘Zet je bedrijfsgeheimen niet in open systemen.’

## KANTELING IS GAANDE

In januari 2024 zei Aalbersberg: ‘Wat er ook op ons afkomt, we zijn er niet klaar voor. We zijn niet voldoende voorbereid, we zijn niet voldoende weerbaar. […] En dat moet vanaf vandaag veranderen.’

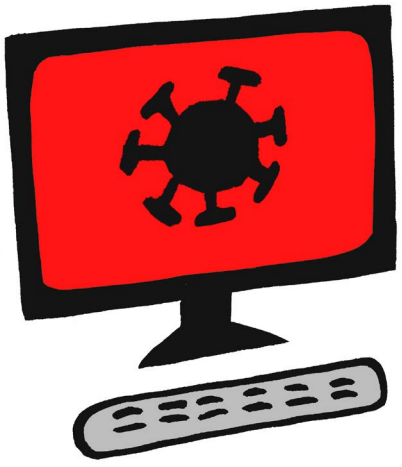
We zijn een jaar verder. Is het gelukt om daar verandering in te brengen? ‘Nog echt niet’, geeft Aalbersberg toe. ‘Maar we hebben wat stapjes gezet in de urgentie. Er is een brief van het kabinet. Er kwam een oproep aan burgers om een noodpakket in huis te halen. Daar werd lacherig over gedaan. Maar er is een kanteling gaande. Ook bedrijven snappen inmiddels dat ze een verantwoordelijkheid hebben. Komend jaar staat in het teken van de hoe-vraag. Samen met VNO-NCW en het ministerie van Economische Zaken wordt dit momenteel met de sectoren uitgewerkt. Hoe gaan we Nederland weerbaarder maken? We kunnen risico’s niet uitsluiten, we kunnen ze wel beheersen.’ ◘

**TEKST:** PASCAL THEUNISSEN **ILLUSTRATIES:** BAS VAN DER SCHOT

STAAT VAN PARAATHEID

# VOORBEREID? JA – MAAR VOORAL OP PAPIER

Twee derde van de Nederlandse ondernemers heeft een noodplan opgesteld voor crises, of is daarmee bezig. Ze wapenen zich vooral tegen cyberaanvallen op grote schaal en problemen met energielevering. Meer dan de helft van de ondernemers oefent niet met scenario's of simulaties om te kijken of het bedrijf is voorbereid op onverwachte gebeurtenissen.



Nederlandse ondernemers zijn zich in groten getale aan het voorbereiden op grote crises. Uit de Bilderberg-enquête van dit jaar blijkt dat twee derde van hen een noodplan heeft opgesteld of daarmee bezig is. Ondernemers wapenen zich vooral tegen cyberaanvallen op grote schaal, en problemen met energielevering.

In totaal beantwoordden 225 ondernemers onze vragen (zie ook kader op pagina 15). Een aantal van hen spraken we nader naar aanleiding van hun antwoorden.

## SABOTAGE DOOR CHINA EN RUSLAND

De noodzaak om je voor te bereiden op onverwachte gebeurtenissen – denk ook aan een pandemie, sabotageacties en een tekort aan grondstoffen – is volgens 96 procent van de respondenten de afgelopen vijf jaar toegenomen. Geopolitieke dreigingen zijn dan ook gestegen, met onder meer de oorlog in Oekraïne die in 2022 uitbrak. En één op de vijf Nederlandse ondernemers wordt jaarlijks getroffen door cybercriminaliteit.

Begin dit jaar werd de TU Eindhoven getroffen door een grote hack die het onderwijs een week stillegde. Er zijn ook meerdere incidenten geweest waarbij datakabels op de bodem van de zee werden beschadigd. Bijna al het internetverkeer loopt via deze kabels. Sabotage door China en Rusland wordt vermoed.

'Nederland heeft zijn zaken goed op orde, maar zonder stroom, water, functionerend betalingsverkeer of goede infrastructuur kan dat snel instorten', zegt Raymond Kouwenberg, eigenaar van schoonmaakbedrijf Klien desgevraagd. 'Dan ontstaat er sociale onrust en gaat iedereen afzonderlijk in de overlevingsstand. De schil van beschaving kan erg dun worden. Ik hoor collega-ondernemers zeggen: 'We zijn zo klein, niemand zal een cyberaanval op ons uitvoeren.' Maar dat is een misvatting. Iedereen is een potentieel doelwit. Nog meer bedrijven moeten een noodplan hebben en zich bewust worden van hun kwetsbaarheid.'

Van de geënquêteerden zegt 74 procent 'maatregelen te hebben genomen' om zich voor te bereiden op nieuwe crises. Want, noteert een van hen: 'Een aanslag via de Noordzee is zo eenvoudig gedaan, dat Rusland hier niet over zal twijfelen.' De meesten (ruim 30 procent) antwoorden dat ze maatregelen hebben genomen op het gebied van cybersecurity. Bijna 20 procent heeft een risicoanalyse uitgevoerd, 11 procent heeft een noodplan opgesteld. Slechts 6 procent heeft geen maatregelen genomen.

Voor het komende jaar wil een derde van de geënquêteerden een noodplan opstellen, een derde de cybersecurity verbeteren en een kwart de 'medewerkers belasten met het vergroten van de weerbaarheid'.

## GEBREK AAN MENSKRACHT

De maatregelen die bedrijven kunnen nemen om beter voorbereid te zijn, zijn zeer divers. Maar voor kleine(re) ondernemingen is dat vaak lastiger, vanwege het gebrek aan financiën of menskracht, of allebei. Dat weet ook Jules Rombouts, hij is mede-oprichter en cto (chief technology officer) van Nature's Principles, een start-up uit Delft. Het bedrijf maakt melkzuur uit onder meer resten van suikerbieten, aardappelen en oud papier en met dat melkzuur kunnen andere bedrijven bioplastics maken.

'We zijn met z'n vieren nu en nog wat stagiairs, adviseurs en freelancers', vertelt Rombouts. 'Wij hebben hier geen boekwerk liggen of een noodplan. De ceo en ik hebben dat wel in ons hoofd. Hoe loodsen we ons bedrijf en medewerkers goed door bijvoorbeeld een nieuwe pandemie? Wat doen we als we gehackt worden? Dat soort scenario's bespreken we.' Ook zat hij om de tafel met een cyberexpert.

## 'WENDBAAR' IS TOVERWOORD

Ook bij het bedrijf van John Martens liggen geen crisis-draaiboeken klaar, maar dat is een bewuste keuze. Niet omdat de armslag er niet zou zijn: de Koninklijke Martens Groep (keramiek, kunststoffen en beton) telt rond de vijfhonderd werknemers.

'Wij zijn niet van de plannen en de deelplannen', stelt Martens. 'Ik ken Duitse bedrijven en die hebben het meteen over *protokollieren*. Daar bedoelen ze mee: alles vastleggen. Als iemand een keer om twee uur 's nachts in een fabriek staat en denkt: wat moet ik nu doen, kan hij het opzoeken. Nou ja, ik geloof daar helemaal niet in. Want op het moment dat je je handboek compleet hebt, is er weer wat veranderd en moet je weer van voren af aan beginnen.'

Volgens Martens is het toverwoord juist 'wendbaar'. 'Dat zie ik hier graag binnen het bedrijf. Dat we continu het vizier houden op wat er gebeurt in onze omgeving, wat dat betekent voor ons, en hoe we daarmee om moeten gaan.

'Dat is een vaardigheid die wij met z'n allen in onze hele maatschappij wat meer zouden mogen hebben. Volgens mij word je vanzelf ook weerbaarder op het moment dat je wendbaarder wordt.'

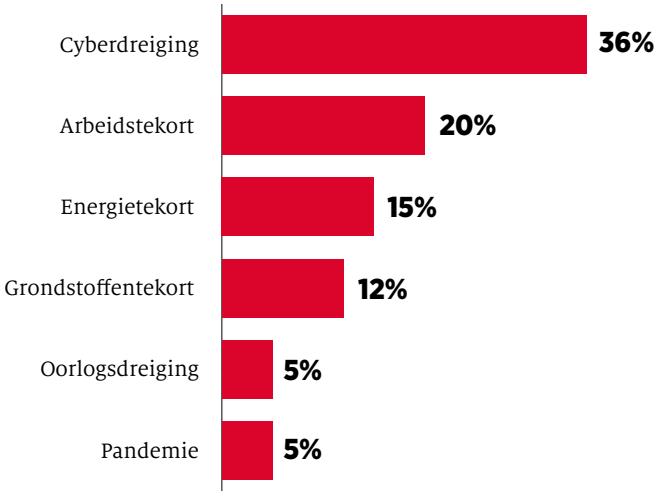
## RISICO'S EVALUEREN

30 procent van de ondernemers zegt dat hun bedrijf 'goed tot zeer goed' is voorbereid op een crisis. 14 procent zegt 'slecht tot zeer slecht' en 54 procent beoordeelt de eigen weerbaarheid als 'neutraal'.

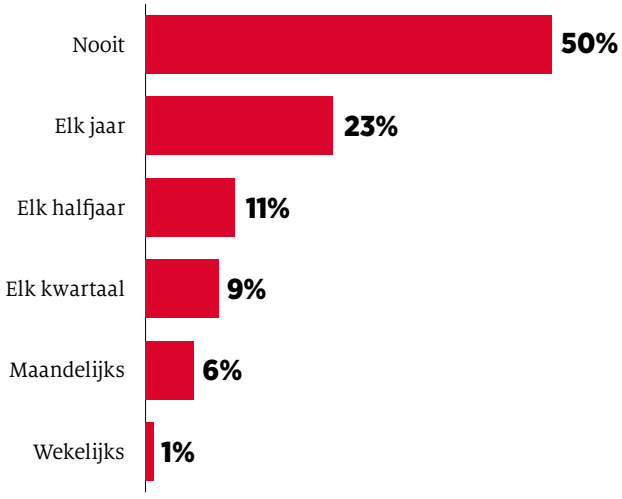
De meeste ondernemers (47 procent) evalueren de risico's die het bedrijf loopt eens

**JE KUNT ALS BEDRIJF DEFENSIE HELPEN MET MACHINES**

**Welke dreiging heeft de meeste impact op uw bedrijf?**




**Hoe vaak voert u simulaties of oefeningen uit om te beoordelen of uw bedrijf weerbaar is?**

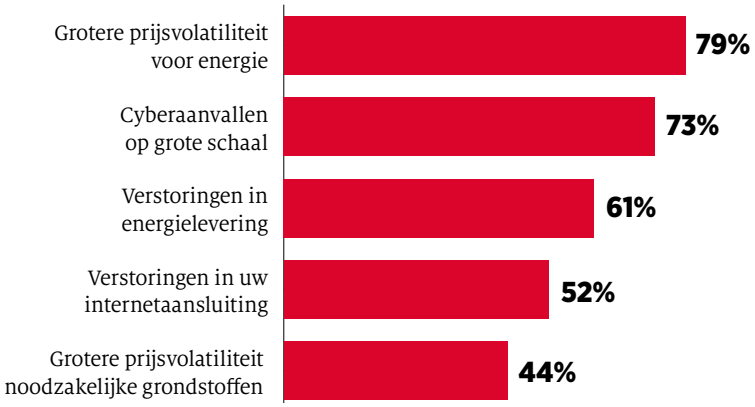



per jaar. Een halfjaarlijkse controle en een kwartaalcontrole komen beide bij een vijfde van de ondervraagden voor.
Belangrijk daarbij is de rol van de techniek. Bij 74 procent speelt technologie een grote tot zeer grote rol bij de weerbaarheid van het bedrijf. Dat maakt het extra belangrijk dat er bijvoorbeeld geen stroomstoringen optreden en dat de online beveiliging klopt. 59 procent van de ondervraagden geeft aan dat hun bedrijf 'goed tot uitstekend' is voorbereid op cyberdreigingen.

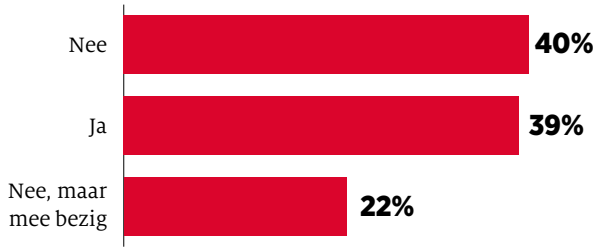
## CYBERDREIGING IS HET GROOTST

Cyberdreiging is ook de dreiging die het meeste invloed zou hebben op de bedrijfsvoeringen, melden de respondenten. Cyber staat met 35 procent op de eerste plaats van disruptieve dreigingen, arbeidstekort met 21 procent op twee en energietekort met 15 procent op de derde plaats. Ook geven veel ondernemers aan – 66 procent – dat zij het voor de weerbaarheid van het bedrijf belangrijk tot zeer belangrijk vinden om hun personeel te trainen en te ontwikkelen.
Wat bij veel bedrijven nog wel ontbreekt, is het daadwerkelijk oefenen met scenario's of simulaties om te kijken of men is voorbereid op onverwachte gebeurtenissen. 51 procent geeft aan dit nooit te oefenen.

**Op welke onverwachte gebeurtenis acht u de kans groot tot heel groot?**




**Heeft u een noodplan of continuïteitsplan voor uw bedrijf?**



## KRITISCH OP OVERHEID

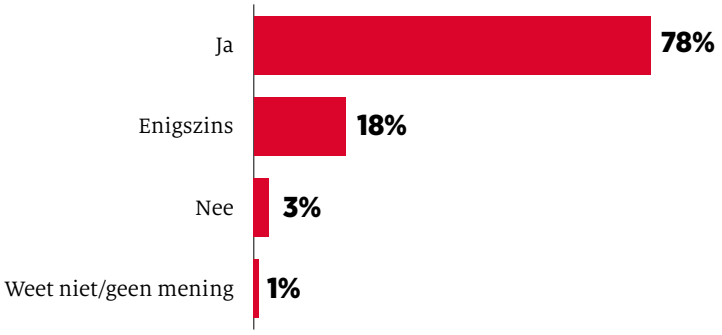
52 procent zegt het ook ‘eens of enigszins eens’ te zijn met de stelling dat bedrijven een verantwoordelijkheid hebben in de voorbereiding van Nederland op onverwachte gebeurtenissen.
John Martens: ‘Ik denk dat de overheid goed kan inschatten waar de risico’s liggen en ons daarover informeren. Maar als Nederland hebben we te lang gedacht: o, het komt allemaal wel goed, de overheid regelt dat wel. Dat kan niet meer. Ik denk dat overheid en bedrijven met elkaar moeten overleggen over wat we van elkaar nodig hebben.’
Ook Kouwenberg pleit voor meer overleg tussen overheid en bedrijfsleven over potentiele risico’s. ‘Door nu al samen te werken, kunnen we ons beter voorbereiden op onvoorziene omstandigheden. Ik denk niet dat er Russische tanks hier de straten binnenrollen. Maar als onze soldaten naar andere gebieden moeten bij een NAVO-conflict, kan dat hier leiden tot capaciteitsproblemen bij Defensie. Als bijvoorbeeld kazernes leeglopen, kunnen bedrijven een waardevolle rol spelen door personeel beschikbaar te stellen, of te helpen met materieel of onderdelen. Zulke gesprekken moeten we tijdig met elkaar voeren.’

# IEDEREEN IS EEN POTENTIEEL DOELWIT

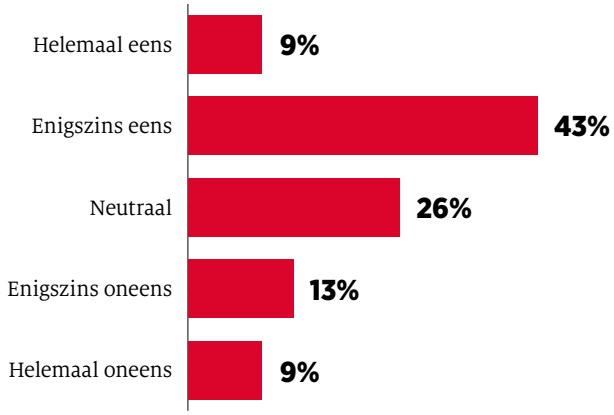
## LESSEN UIT CRISES

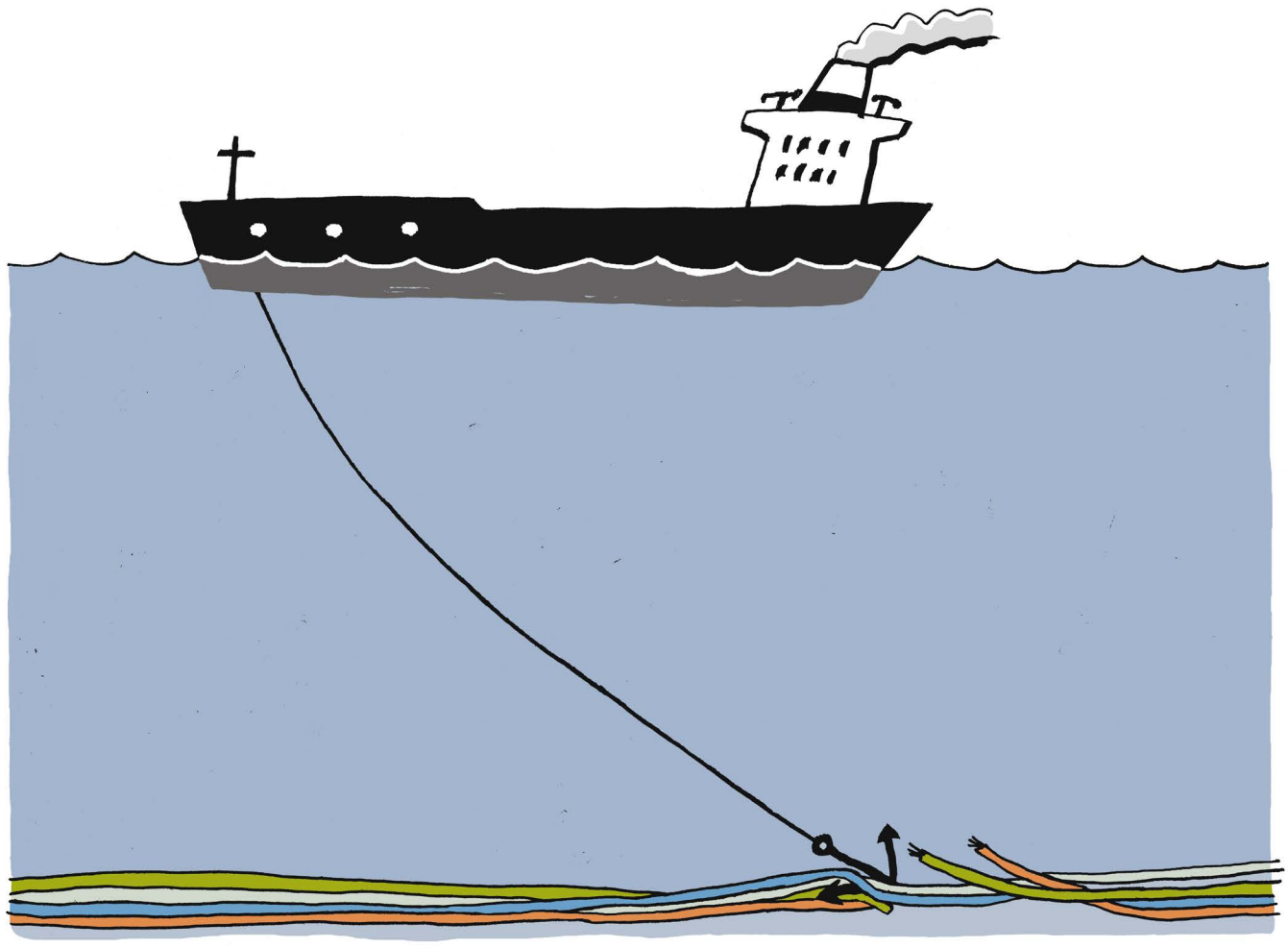
Weerbaarheid is niet alleen vooruitkijken, maar ook lessen trekken uit eerder crises. Ongewild hebben veel bedrijven ervaring opgedaan, bijvoorbeeld tijdens de coronacrisis of de oorlog in Oekraïne. Hoe ga je om met tekort aan personeel of grondstoffen, hoe met geopolitieke dreiging? ‘Ons bedrijf is ouder dan honderd jaar en heeft meerdere crises doorstaan’, schrijft een van de respondenten. ‘In de huidige tijd zijn we sterk afhankelijk van de digitale infrastructuur en dat heeft wel onze focus’.
‘Denken in crisisscenario’s, voorbereiden, trainen en goede crisiscommunicatie’, meldt een ander. Financiële stabiliteit geeft rust, meldt de een, investeringen in cyberveiligheid en thuiswerken ook, meldt een ander. Ook investeren in mentale weerbaarheid van medewerkers biedt houvast. ◘

**Is de noodzaak om weerbaar te zijn/voorbereid te zijn op onverwachte gebeurtenissen toegenomen de afgelopen vijf jaar?**




**Bedrijven zijn verantwoordelijk voor de voorbereiding van Nederland op onverwachte gebeurtenissen**





CONCRETE TIPS OM JE VOOR TE BEREIDEN OP EEN CRISIS? OP PAGINA 32 STAAN ER TIEN.


## OVER DEZE ENQUÊTE

Elk jaar houdt VNO-NCW een enquête over het thema van de Bilderberg-conferentie. Dit jaar is dat 'weerbaarheid'. De enquête werd digitaal verspreid onder ondernemers, die van 25 november 2024 tot en met 25 januari dit jaar konden reageren. 225 mensen vulden de vragenlijst in. Deelname was anoniem. De geïnterviewden in dit artikel gaven aan benaderd te mogen worden. De respondenten zijn actief in zakelijke dienstverlening (28 procent), industrie (20 procent), handel, transport en opslag (13 procent), bouw (10 procent) en it (9 procent) en overig (20 procent).

**TEKST:** JEROEN VISSER **FOTO:** LAURI HEINO/LEHTIKUVA/AFP/ANP

FINLAND

# ALTIJD KLAAR VOOR HET ERGSTE

Al tachtig jaar is Finland op zijn hoede voor buurland Rusland. Overheid én bedrijfsleven werken samen voor wat ze de ‘totale verdediging’ van het land noemen. Belangrijke ondernemers gaan drie weken op weerbaarheidscursus. ‘We moeten continu kijken of we ergens een zwakke plek hebben’.

**Reservisten tijdens schietoefeningen bij de zuidoostelijke grens met Rusland (maart 2022)**

Elke zes weken zit Olli-Pekka Piipponen van S-Bank aan een grote tafel met collega's van alle grote Finse financiële instellingen. De gesprekken, georganiseerd door de Finse overheid maar voorgezeten door iemand uit het bedrijfsleven, gaan over veiligheidsdreigingen en hoe die te lijf te gaan. Alle scenario's komen op tafel, van cyberaanvallen tot het uitbreken van een oorlog. 'Eigenlijk is de vraag elke keer: wat kunnen we doen om normaal te functioneren in abnormale tijden?' aldus Piipponen.

De 42-jarige Fin is directeur operationele risicobeheersing bij S-Bank, waar 3,3 van de 5,5 miljoen Finnen klant zijn. Hij en zijn team moeten ervoor zorgen dat de bank altijd kan blijven functioneren, ook in een crisis. Klanten moeten toegang houden tot hun bezittingen en transacties kunnen doen. 'Als dat wegvalt, begint alles te ontrafelen', zegt Piipponen.

Er is waarschijnlijk geen land ter wereld dat zo grondig is voorbereid op crises en oorlog als Finland. Zo kan het land in oorlogstijd 300 duizend militairen mobiliseren en telt het 900 duizend reservisten. Daarnaast kan het land meer mensen een schuilplaats bieden dan er inwoners zijn; hoeveel precies, dat is geheim. Zeker is dat tientallen gemeentegebouwen, zoals bijvoorbeeld een zwembad in Helsinki dat half in een rots is gebouwd, ook fungeren als schuilkelder. Ook de private sector doet mee: elk nieuw gebouw van meer dan 1.500 vierkante meter moet een schuilkelder bevatten. In totaal kunnen naar schatting alleen al in Helsinki 850 duizend mensen schuilen, anderhalf keer zoveel als het aantal inwoners.

ANP/EPA/FINNISH BORDER GUARD


Een Fins patrouilleschip in de Finse Golf nadat daar pijpleidingen en telecomkabels zijn beschadigd (oktober 2023)

## 1.300 KILOMETER RUSSISCHE GRENS

De reden voor de grondige Finse voorbereiding is buurland Rusland. De laatste oorlog die Finland uitvocht, tijdens de Tweede Wereldoorlog, was met Moskou. In de Winteroorlog vochten Finse soldaten in witte pakken en op ski's tegen het Rode Leger. Ze verloren. Tien procent van het grondgebied ging over in Russische handen. Om een herhaling te voorkomen bouwde de Finse overheid na de oorlog, samen met de private sector, een omvangrijk weerbaarheidsapparaat, een systeem van 'totale verdediging'. De Fins-Russische grens is immers meer dan 1.300 kilometer lang en het land ligt vrij geïsoleerd. 'Veel legerofficieren, die op relatief jonge leeftijd met pensioen moesten, hielpen bij de opbouw van dit apparaat', vertelt Markku Rajamäki, beleidshoofd bij de Finse industriefederatie EK. 'Ook de rest van de samenleving kreeg hier een belangrijke taak in.' Militaire schermutselingen bleven sindsdien uit.

## ECONOMISCHE DEFENSIE

Economische defensie is een van de pijlers van Finlands totale verdediging. Bedrijven die handelen in essentiële goederen voor de samenleving, zoals farmaceuten, apotheken en importeurs van medicijnen, moeten altijd voor een paar maanden normaal gebruik aan antibiotica op de plank hebben. Oliebedrijven moeten drie maanden benzinevooraad achter de hand hebben, zodat de samenleving vooruitkan.

De spil in het systeem is de nationale weerbaarheidsorganisatie Nesa. Die is aanjager van de bedrijfsoverleggen, organiseert crisisoefeningen en regelt dat er genoeg noodvoorraden zijn. Soms betaalt de organisatie bedrijven voor de opslagcapaciteit. Het komt ook voor dat er op vrijwillige basis afspraken worden gemaakt.

## KUNST AFKIJKEN

De Finse methode maakt furore in Europa, zeker nu de dreiging uit Rusland toeneemt. Niet voor niets vroeg de Europese Raad de Finse oud-president Sauli Niinistö vorig jaar om een rapport met tips voor een Europese weerbaarheidsstrategie. Een van de aanbevelingen: in tijden van crisis moeten burgers zich 72 uur kunnen redden. Iedereen moet dus een noodpakket hebben met blikken soep en bonen, flessen water, noodzakelijke medicijnen en een radio op batterijen. Als het aan Niinistö ligt, gaan bedrijven zich ook beter voorbereiden op het ergste. Dat betekent meer reserve-voorraden aanhou-

den, de ict-beveiliging beter op orde hebben en met gelijksoortige bedrijven overleggen over wat er beter kan.

In zijn rapport over de Europese weerbaarheidsstrategie schrijft Niinistö, geen verrassing, dat overheden en bedrijven in Europa beter moeten samenwerken. Ze moeten vaker informatie uitwisselen over dreiging en crisisaanpak en zo vertrouwen opbouwen. Dat gaat niet alleen over 'kritieke' bedrijven als banken of elektriciteitsleveranciers. 'Als jij als kleine ict-firma diensten levert aan zo'n groot bedrijf, moet jij aan dezelfde basisvoorwaarden voor cyberveiligheid voldoen', zegt Rajamäki van de industriefederatie.

## CONTINU ALERT

In 27 sectoren, zoals banken en ict, overleggen Finse bedrijven zelf over dreigingen en maatregelen. In het bankenoverleg staat cyberdreiging vaak op de agenda, volgens Piipponen van S-Bank is dat ook het grootste risico voor zijn bank. De aanvallen kunnen van alle kanten komen, van hackersgroepen tot criminele bendes die ransomware proberen te installeren, tot vijandelijke mogendheden die de verdediging testen.

S-Bank heeft de afgelopen jaren geïnvesteerd in menskracht en technologie om die dreigingen het hoofd te bieden. Piipponen: 'Het is een race tussen ons en de slechteriken. We moeten continu kijken of we ergens een zwakke plek hebben.'

De banken helpen elkaar om risico's en kwetsbaarheden beter te begrijpen. Maar ze geven elkaar geen inzage in wat ze doen tegen specifieke dreigingen. Dat mag ook niet volgens de concurrentie-afspraken, zegt Piipponen. 'Het gaat er meer om gevaren te benoemen en te kijken wat we collectief kunnen doen om deze het hoofd te bieden.'

## KABELBREUKEN

Ook de recente kabelbreuken in de Oostzee, waarbij de autoriteiten sabotage vermoeden, kwamen op de agenda bij het overleg van de financiële instellingen. Op Eerste Kerstdag enterde de Finse politie de olietanker Eagle S, nadat die vermoedelijk met zijn anker een stroomkabel had vernield tussen Finland en Estland, en vier datakabels. Het schip maakt waarschijnlijk deel uit van de vloot die Rusland helpt sancties te omzeilen. Een maand eerder raakten twee glasvezelkabels op de bodem van de Oostzee beschadigd, toen een Chinees vrachtschip in de buurt voer.

Banken opereren op basis van dataverkeer. Het wegvallen van kabels kan voor grote problemen zorgen, stelt Piipponen, helemaal als je zo geïsoleerd ligt als Finland. 'Dit maakt ons kwetsbaar. Hopelijk gaat Nesa dit bespreken met de kabelbedrijven. Wellicht moeten er extra kabels komen.'

## SPANNING DOOR NAVO-LIDMAATSCHAP

De sectoroverleggen zijn extra relevant nu de verhoudingen tussen Finland en Rusland zijn verslechterd. Na de Russische invasie in Oekraïne werden de Finnen in april 2023 lid van het westerse militaire bondgenootschap NAVO, een historische stap. De grens is al meer

**DE KABEL-BREU-KEN IN DE OOSTZEE STON-DEN OP DE AGENDA**

ANP/LAURI HEINO/LEHTIKUVA/AFP

Finland telt 900 duizend reservisten, onder meer in de Kareliabrigade, die hier bezig is met een oefening

dan een jaar gesloten, nadat de Russen honderden migranten richting Finland stuurden om in Finland asiel aan te vragen en het land zo extra te belasten.

De oorlog heeft ook de crisisvoorbereidingen beïnvloed. 'Voor 2022 werkten we vooral met scenario's als een grote brand of werknemers die massaal ziek werden, zoals tijdens corona. Nu is het uitbreken van een oorlog een prominent scenario', aldus Piipponen.

De overheid biedt werknemers uit de private sector ook trainingen aan. Zo kent Finland een Defensie-universiteit met crisis- en veiligheidstrainingen. Die nodigt een paar keer per jaar vijftig topbestuurders uit de publieke en private sector uit voor een 3,5 week durende veiligheidstraining. Er zijn simulaties om hun crisisvaardigheden te testen en ze zijn drie dagen op een militaire basis om hun kennis over het Finse leger bij te spijkeren.

## GEEN GEKLAAG OVER TRAINING

Ruim drie weken uit de roulatie, dat is nogal wat voor een ceo. Maar volgens Rajamäki van de Finse industrie-federatie is klagen zeldzaam. 'Het is toch een teken dat je blijkbaar op een kritieke post zit.' Een van de eisen is overigens dat je nog minimaal tien dienstjaren voor je hebt, anders heeft de opfriscursus, die na vijf jaar komt, geen zin.

S-Bank-medewerker Piipponen ging nog niet naar de prominentencursus. Maar aan een informatiedag voor bedrijven mocht hij wel meedoen. Hij sprak mensen uit andere vakgebieden, 'heel nuttig'. 'Iemand die materiaal importeert voor laboratoria legde me uit waarom dat belangrijk was in tijden van crisis: als de laboratoria niet werken, functioneren de ziekenhuizen ook niet. Grappig om te zien hoe iedereen zijn aandeel heeft in de grote machine.'

Al die overleggen, de decennia-oude infrastructuur, de samenwerking met bedrijven: het contrast met Nederland is groot. Waar moeten we beginnen, als we onze weerbaarheid willen vergroten? Een speciale organisatie zoals Nesa helpt al heel veel, zegt Piipponen. 'Maar stap één is het gesprek aangaan. Zet de juiste partijen bij elkaar en stel de vraag: wat kunnen we doen als het misgaat?'

## BETERE DATABEVEILIGING

Volgens Rajamäki kunnen bedrijven verwachten dat in de nabije toekomst de eisen voor de beveiliging van data en leveringszekerheid strenger worden. Maar het is ook een kwestie van mentaliteit. Net zoals burgers zich moeten voorbereiden met hun noodpakketten, moeten bedrijven, van de zorg tot ict en voedselproductie, bereid zijn met de overheid mee te denken over wat nodig is om de samenleving te beschermen.

Dat betekent dat je als werkgever personeel vrijmaakt om over weerbaarheid na te denken, je informatie uitwisselt met de overheid over voorraden en risico's. Je moet zelfs bereid zijn om op cursus te gaan. 'Dat vergt wel wat van ondernemers', zegt Rajamäki. 'Het betekent dat je niet allen in termen van efficiëntie en winst kunt denken.' ◘

# RAMPEN-WERK

EEN REGIO LOOPT ONDER WATER, EEN BUG LEGT SOFTWARE VAN JE LUCHTHAVEN PLAT. HOE BEREID JE JE DAAR OP VOOR ALS BEDRIJF? VIJF CRISISMANAGERS VERTELLEN. 'OEFENEN, OEFENEN, OEFENEN: DAT IS MIJN STOKPAARDJE.'

# JAN POL

**Initiatiefnemer samenwerkingsverband Infra Capacity Alliance**

## ‘VIND MAAR EENS SNEL VIJFTIG BRUGGEN’

‘Ken je de Mandelabrug over de A12? Die stond op instorten en moest twee jaar geleden rond kerst snel vervangen worden. Dat is het werk van Janson Bridging, een van de deelnemers van Infra Capacity Alliance. En vier jaar geleden, tijdens de overstroming in het Ahrdal in Duitsland, waren ineens vijftig bruggen nodig. Vind die maar eens; dat is toch wat anders dan een mondkapje.

‘Zo is het balletje gaan rollen, en hebben we in 2022 samen met Bredenoord, MTD en Daiwa House Modular Europe een samenwerkingsverband opgericht voor tijdelijke, grondgebonden infrastructuur: ICA. We zijn nu met vijftien bedrijven, allemaal actief in noodwatersystemen, tijdelijke woningen, aggregaten, verhuurbedrijven. We hebben contact met veiligheidsregio’s, waterschappen, gemeenten en Defensie. Juist die samenwerking tussen overheid en bedrijfsleven is ten tijde van rampspoed cruciaal. En al onze bedrijven zijn gewend om snel te handelen; dat zit in hun dna.

‘Onze overheid maakt met haar oproep over samenwerking met het bedrijfsleven en weerbaarheid veel los. Maar wie zet het vast? Ambtenaren vinden het nog heel spannend om met het bedrijfsleven aan tafel te gaan. Maar áls het misgaat, hebben we elkaar keihard nodig. Dan wil je weten wie er aggregaten op voorraad heeft en de mensen om ze te bedienen.

‘Een crisis verloopt in fases. Denk aan een enorme overstroming. In de eerste 24 uur is noodhulp nodig. Dan ga je redden, evacueren en schuilen. De medische zorg wordt opgeschaald. Daarna zijn de basisbehoeften nodig: dak, bed, bad, brood en breedband. Daarna komt herstel van de infrastructuur, en komen onze bedrijven in beeld.

‘Vorig jaar hebben we met het waterschap Brabantse Delta een dreigende dijkdoorbraak geoefend. Op basis van de behoeften van de overheid hebben we materieel klaargezet en uitgerold. En onze leden hebben veel ervaring, en denken mee. Wat is straks nog meer nodig? Een goede voorbereiding is cruciaal. Als er geen crisis is, moeten bedrijfsleven en overheid elkaar leren kennen en de samenwerking passend maken. Het is niet de vraag of die ongekende crisis komt, maar wanneer.’

**‘HOE DONKERDER HET SCENARIO, HOE LEUKER’**

# MAAIKE AANSORGH-BOK

**Crisismanager bij netbeheerder Alliander**

‘Het afgelopen jaar hebben we veel gefocust op cyberdreigingen. Een concrete oefening was ook gebaseerd op de serie *Black-out* van de EO. Stel je voor dat een cyberaanval van een ander land een grote energie-uitval in Nederland veroorzaakt. Dat soort scenario’s werken we helemaal uit: wat gebeurt er als de stroom langdurig uitvalt? Niet een paar uur, maar meerdere dagen? Wat zijn andere gevolgen? Welke dienstverlening kan dan niet meer doorgaan? Hoe kunnen we ons net zo snel mogelijk herstellen?

‘Dagenlang zonder energie, het is geen ondenkbaar scenario. Nog in juli vorig jaar zorgde een verkeerde update door het beveiligingsbedrijf CrowdStrike wereldwijd voor problemen. Zo zie je hoe alles met elkaar verbonden is en hoe tricky het kan worden. De Russische inval in Oekraine en de coronacrisis hebben ons geleerd om nog breder te kijken en te handelen.

‘We zijn getraind in het bedenken van de zwartste scenario’s. Hoe donkerder, hoe leuker. Maar dat is mijn persoonlijke afwijking als crisismanager. We hebben bij Alliander een *all-hazards approach*: we leren onze crisiscollega’s een besluitvormingsproces aan, zodat we met alle soorten crises kunnen omgaan.

‘Oefenen, oefenen, oefenen, dat is mijn stokpaardje. Door herhaling krijgen we het besluitvormingsproces goed in de vingers. Ons team bestaat uit vijf mensen die zich dagelijks bezighouden met crisismanagement. We zitten in de meldkamer, in het hart van ons bedrijf. We investeren in een professionele crisisorganisatie, met fulltime crisismanagers.

‘De oproep van Defensie, dat Nederlanders beter voorbereid moeten zijn op rampen, vind ik heel goed. Er zijn dreigingen in de wereld en die kunnen dichterbij komen, zowel fysiek als digitaal. We zijn zo gewend dat alles werkt. Dat merk je al aan de reacties bij een willekeurige stroomstoring. Het gaat om bewustwording. Dat geldt ook voor het bedrijfsleven. Heb je een noodvoorziening geregeld, een uitwijklocatie? Bedrijven die met een vitaal proces werken, hebben dat wel goed geregeld. Maar kleinere bedrijven?’

# THOMAS MULDER

**Executive Director HR en voorzitter van het crisismanagementteam VodafoneZiggo**

## ‘WE ZIJN IN NEDERLAND GEWEND DAT ALLES WERKT’

‘Soms is een crisis voorspelbaar. Een aannemer beschadigt per ongeluk een kabel, waardoor in een gebied de connectiviteit wegvalt. We hebben een draaiboek om dat op te lossen. Maar soms is niet duidelijk wat er gaat gebeuren. Zie de overstromingen in Limburg of de coronapandemie.

‘Dat vraagt om een andere manier van crisismanagement en het volgen van een robuust crisisproces. We kijken altijd naar de gevolgen: voor klanten, medewerkers en de maatschappij. Wat kan er nog meer gebeuren? Wat als het drie dagen duurt om een storing op te lossen? Hebben we dan rekening gehouden met de rusttijden van onze mensen?

‘Wanneer je goed nadenkt over de impact, kom je op creatieve oplossingen. Bij de wateroverlast in Limburg vermoedden we dat modems weleens konden gaan drijven. We hebben daar toen meteen onze busjes met monteurs naartoe gestuurd. Zodra het water ging zakken, konden de monteurs mensen weer aansluiten.

‘Na de corona-uitbraak in Wuhan werd daar een speciaal ziekenhuis gebouwd. Ik dacht: wat als dat in Nederland gebeurt en er in dat ziekenhuis een storing optreedt? Hoe sturen we dan een monteur? Hoe komen we aan beschermingsmateriaal? We hebben meteen een draaiboek gemaakt.

‘In onze samenleving, die zo afhankelijk is van ketens, is voorbereiding cruciaal. Bedrijven moeten verder kijken dan hun eigen responsplannen en meer samenwerken. Wat als er geen eten meer wordt aangevoerd uit de Rotterdamse haven? Hoelang houden we dat dan vol? Over dit soort gevolgen moet je goed nadenken.

‘We zijn in Nederland gewend dat alles werkt. Onze energievoorziening is de beste ter wereld, onze mobiele netwerken behoren tot de top vijf wereldwijd. Niet gek dat we daarop vertrouwen. Mensen vinden crisisscenario’s dan ook vaak sensationeel, maar het is bloedserieus. Daarom nodigden we eerder een ziekenhuisdirecteur uit om voor onze zeventig *senior leaders* te spreken. Wat als in zijn ziekenhuis alle mobiele verbindingen uitvallen? Daarmee lieten we zien wat voor verantwoordelijkheid we hebben.’

‘WE ZIEN DREIGINGEN VERANDEREN EN DICHTERBIJ KOMEN’

# SARAH OLIEROOK

**Manager havenveiligheid, Havenbedrijf Rotterdam**

‘We noemen onszelf de verkeersleiding van de haven. De haven is met drieduizend bedrijven dé hub. Hier komen vitale sectoren samen, zoals telecom, energie en scheepvaart. We werken daarom nauw samen met Defensie, de NCTV, inlichtingendiensten en bedrijven. Die samenwerking is cruciaal, want de haven heeft impact op de hele keten. Als er iets misgaat, ontstaat er vaak een domino-effect.

‘Mijn team is verantwoordelijk voor zowel safety als security in de haven. We oefenen met grote waterverontreiniging, branden, maar ook met langdurige stroomstoringen. Stel er is lange tijd geen elektriciteit of de communicatie valt uit. Wat doe je dan? Onze piketmensen gaan dan naar vooraf afgesproken locaties.

‘Oefeningen zijn belangrijk, maar we weten dat een crisis in de praktijk anders is. Onze oefeningen zijn vaak gericht op het proces. En we kijken naar scenario’s die totaal outside the box zijn. Sommige organisaties oefenen bijvoorbeeld met een zombiegame. Dat klinkt misschien gek, maar het doel is om collega’s echt te laten nadenken, zonder dat ze kunnen terugvallen op routine.

‘Mijn werk is eigenlijk continu afwegen wat we willen beschermen en waar de grootste risico’s liggen, vooral op fysieke infrastructuur. Ik doe dat in nauwe samenwerking met mijn collega’s van cybersecurtiy. We hebben te maken met dertigduizend zeeschepen en negentigduizend binnenvaartschepen per jaar. Voedsel, onderdelen en medicijnen komen door de haven.

‘We zien dreigingen veranderen en dichterbij komen. De meeste crisismanagers hebben hun noodpakket wel gereed; bedrijven hebben noodpakketten cadeau gedaan met kerst. Bang ben ik niet. We zijn nationaal in geval van een crisis goed voorbereid. We kunnen dan niet alleen naar de overheid kijken, maar hebben ook een eigen verantwoordelijkheid. Voorheen werd daar heel voorzichtig over gesproken. Nu hoor je generaals buiten dienst en experts regelmatig aandacht vragen voor de effecten van mogelijke dreigingen. Ik ben blij met die extra aandacht; het maakt ons als mens en als samenleving weerbaar.’

# BIANCA LITWINCZUK

**Manager businessteam Toezicht en Handhaving, MB-ALL ntro**

‘Al twintig jaar leiden we boa’s op, buitengewoon opsporingsambtenaren. We hebben nu zo’n 250 boa’s in dienst en zij worden gedetacheerd bij 150 gemeenten. Onze mensen kom je overal tegen. Op straat, dan geven ze je een bonnetje voor fout parkeren. Maar ze zijn ook de boswachters in het buitengebied, de controleurs in het openbaar vervoer.

‘Weerbaarheid is een belangrijk onderdeel in de opleiding. Boa’s komen allerlei onverwachte situaties tegen. Agressie op straat, in het openbaar vervoer. Tijdens oud en nieuw gebeurt natuurlijk ook van alles. Er is blijkbaar niets leukers dan vuurwerk op de boa’s afschieten. Mensen hebben tegenwoordig een kort lontje. Tegen een uniform is dat nog vele malen korter.

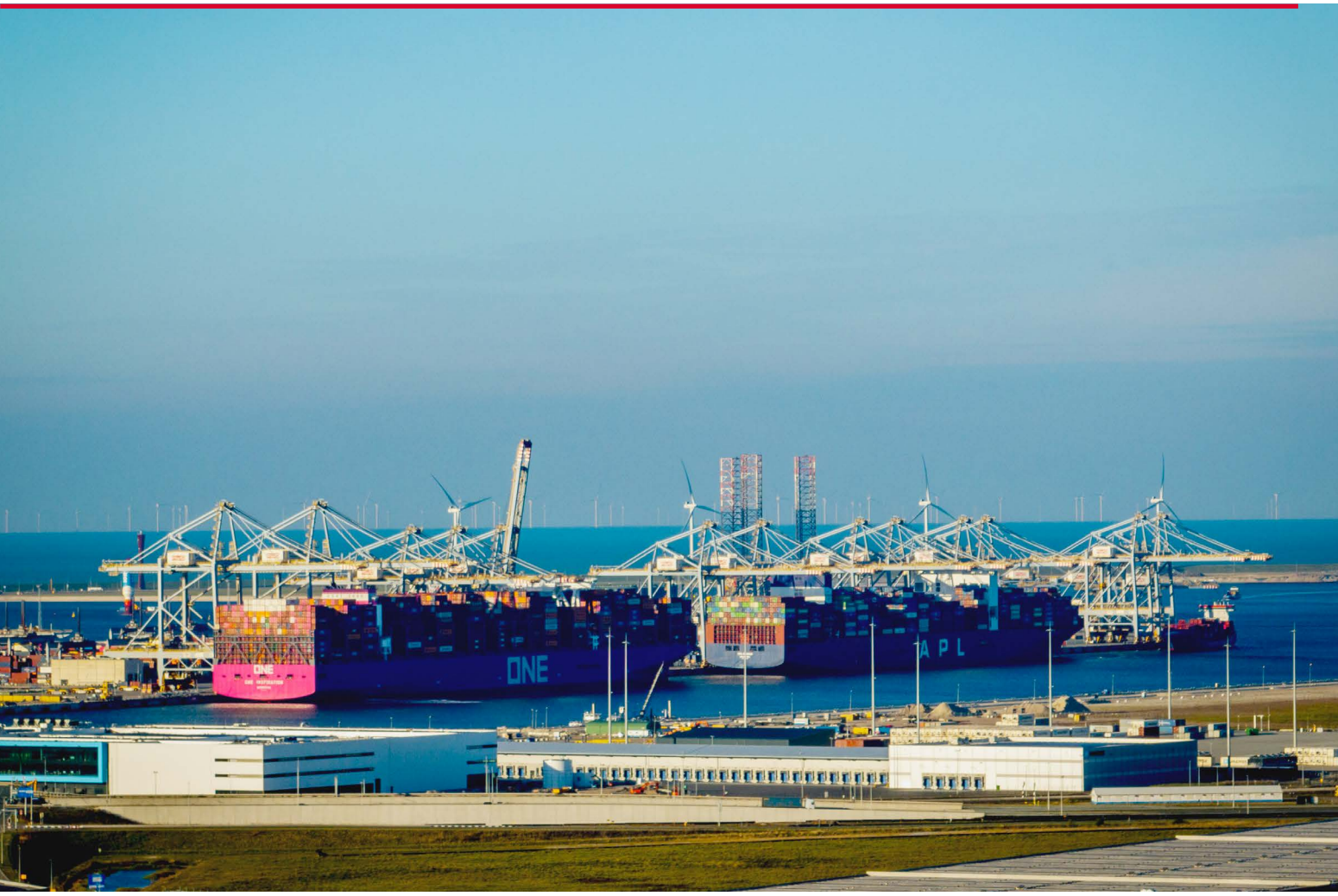
‘We hebben hier een opleidingsstraat waar we situaties zo goed mogelijk nabootsen. Hoe kun je mensen onder controle krijgen? Het gaat vooral om de-escaleren. Hoe zorg je dat je eigen houding en gedrag niet meteen agressie uitlokken? Maar een training blijft anders dan buiten op straat. Een situatie kan ineens ontploffen. In de trein gebeurt dat vaak. Maar ook op straat. Dan kan iemand die heel rustig lijkt, ineens uit z’n plaat gaan vanwege een parkeerbon.

‘Ik weet heel goed hoe plotseling een situatie kan omslaan, want ik heb ruim twintig jaar bij de politie gewerkt. Ik zeg altijd tegen mijn boa’s: ‘Als je je niet veilig voelt, draai om en loop weg.’ Eigen veiligheid eerst. Maar dat is heel lastig. Ze willen de situatie graag oplossen en doorpakken. Toch kan dat niet altijd. Boa’s hebben geen geweldsbevoegdheid, ze hebben alleen handboeien. That’s it.

Vergeet niet: dit zijn toch vaak mensen die handelen. Ze doen een stap vooruit waar de rest een stap achteruit doet. Dat zit ze in het bloed. Ze zijn ook getraind om mensen kalm te houden, ook in een paniekssituatie. Je hoort nu van die oproepen dat Nederland weerbaarder moet worden.

‘We zijn hier niet gewend om met crisissituaties om te gaan. Wat als hier een oorlog uitbreekt? Dan komen we erachter wie bevriest, vlucht of vecht.’ ◘

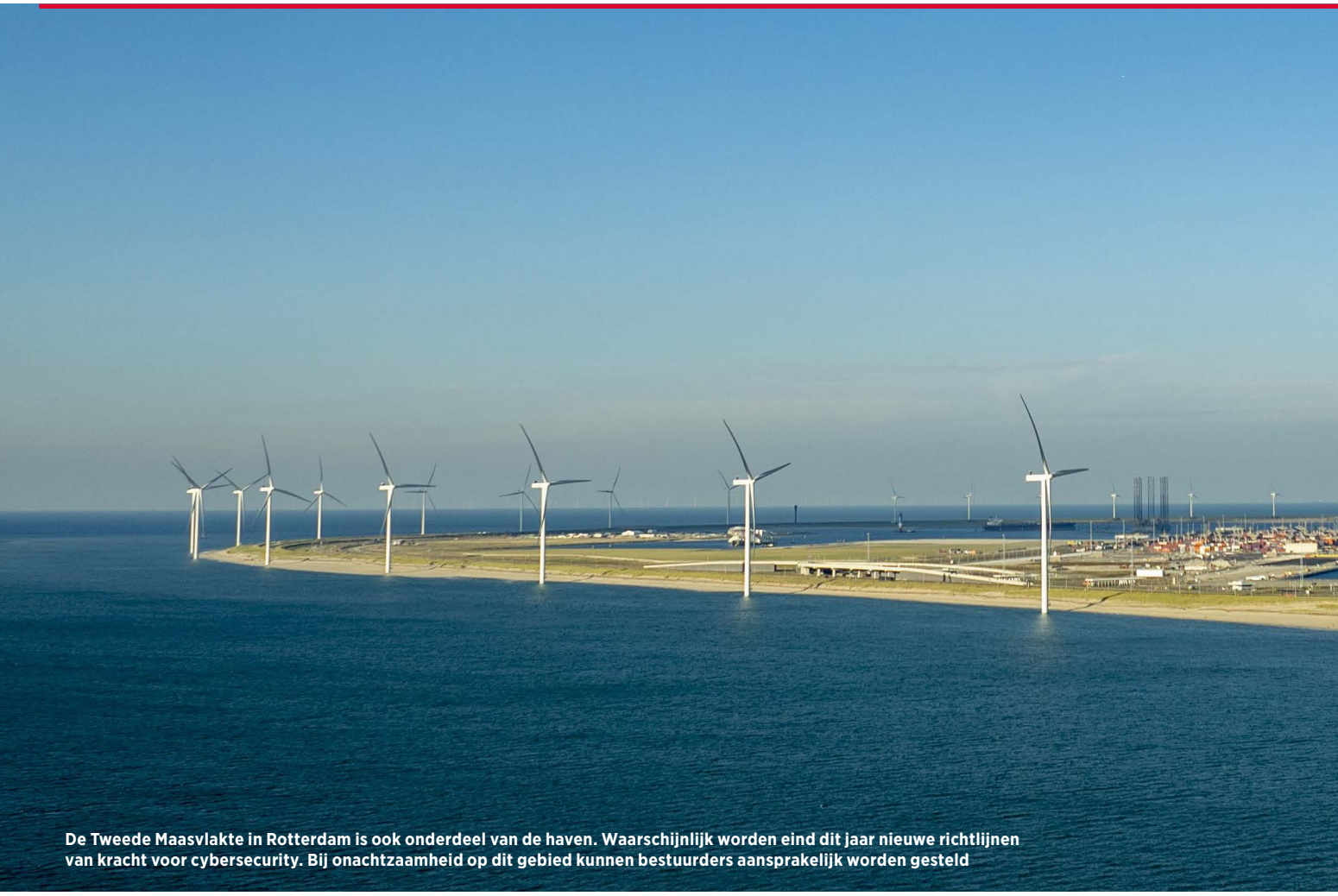

**‘ONZE MENSEN ZIJN GETRAIND OM TE DE-ESCALEREN’**




HAVEN ROTTERDAM

# ELK JAAR EEN ‘RAMP’

Elk uur krijgt de Rotterdamse haven, belangrijke schakel in de Nederlandse logistiek, wel een cyberaanval te verduren. Maar de systemen zijn weerbaar, mede dankzij een jaarlijkse grote oefening. Private en publieke partijen trainen dan hun samenwerking. ‘In andere wereldhavens kennen ze dit niet.’



De Tweede Maasvlakte in Rotterdam is ook onderdeel van de haven. Waarschijnlijk worden eind dit jaar nieuwe richtlijnen van kracht voor cybersecurity. Bij onachtzaamheid op dit gebied kunnen bestuurders aansprakelijk worden gesteld

De Rotterdams Waalhaven, dicht bij het centrum van Rotterdam, oogt rustig deze middag. Achter de rug van Bas Janssen ligt een vrachtschip voor anker. Het wordt omringd door kleinere schepen die af en aan varen. Aan de hardblauwe lucht prijken enkele witte wolken.

Maar de directeur van Deltalinqs, de ondernemersvereniging van de Rotterdamse haven- en industriebedrijven, ziet ze niet. Hij heeft het over andere wolken, donkere, die boven het havencomplex samentrekken, namelijk de verstorende gevolgen van cybercriminaliteit. Het is een zorgelijk vraagstuk, herhaalt hij een paar keer gedurende het interview.

'Het zijn niet alleen criminele bendes die willen infiltreren voor losgeld of voor *storage spoofing* (de online verkoop van niet-bestaande opslag van goederen, red.). Het zijn ook statelijke actoren die rotzooi willen trappen door de boel plat te leggen. Of ze willen om economische redenen spioneren. Mijn nachtmerrie is een grote verstoring die als een olievlek door de haven gaat en uiteindelijk de maatschappij ontwricht.'

**'JE KOMT NIET MEER WEG MET EEN FIRE-WALL EN EEN MANNE-TJE VOOR DE ICT'**

## IT-SYSTEMEN ONTWRICHT

Dat gevaar is niet denkbeeldig. In 2017 werden de it-systemen van containeroverslagbedrijf APM gehackt, met een eenvoudig boekhoudprogramma uit Oekraïne met een link naar Rusland. Laden en lossen ging niet meer. De schade liep uiteindelijk in de honderden miljoenen euro's, om nog maar te zwijgen van de reputatieschade.

Janssen: 'Cyberdreiging komt dus uit een heleboel hoeken. Er staat ook geen hek om het havencomplex en er is er niet één baas van de haven, om het zo te zeggen. Het maakt de aanpak van computercriminaliteit uitdagend. Het is dan ook goed dat we vanuit Deltalinqs nauw samenwerken met publieke partijen als politie, douane,

ROBIN UTRECHT/ANP/HH

gemeente en het Havenbedrijf Rotterdam. We zijn in Rotterdam vrij goed in publiek-private samenwerking, het poldermodel. In andere wereldhavens kennen ze dat niet. Samen met FERM, het Port Cyber Resilience-programma van de Rotterdamse haven, maken we ondernemers bewust dat hun ict-systemen de ruggengraat zijn van hun bedrijf. Zo maken we de totale haven weerbaarder.' Over FERM zo meer. Wat Janssen signaleert, bracht de Nationaal Coördinator Terrorismebestrijding en Veiligheid, Pieter-Jaap Aalbersberg, vorig jaar oktober in het Cybersecuritybeeld Nederland 2024 al naar buiten. 'Eén van de belangrijkste bevindingen in dit beeld is dat statelijke actoren hun cyberactiviteiten intensiveren en hun cybercapaciteiten verbreden', zei Aalbersberg bij de presentatie. 'Het tempo en de complexiteit van statelijke cybercampagnes wordt opgevoerd. Ook zetten ze andere actoren in, zoals bedrijven of hacktivisten, om digitale aanvallen uit te kunnen voeren.'

## DDOS-AANVALLEN

In het Cybersecuritybeeld valt te lezen dat in Australië grote havens al te kampen hadden met een cyberaanval: 'DP World, de op een na grootste havenbeheerder van dat land, had uit voorzorg het internetverkeer stilgelegd nadat er een cyberaanval was ontdekt. In Nederland werden websites van havens in juni 2023 tijdelijk onbereikbaar door DDoS-aanvallen. De website van de Groningse Zeehavens was twee dagen niet te bereiken. De aanvallen zijn opgeëist door een pro-Russische hacktivistische groepering.' Marijn van Schoote kijkt net als Janssen uit over zijn werkgebied. Vanuit het World Port Center op de Wilhelminapier, met aan de voet de voorbijstromende Maas, bestuurt hij de stichting FERM. Dat is geen afkorting, maar de Rotterdamse vertaling van het begrip *resilience*. 'Wij helpen bedrijven en daarmee de Rotterdamse haven weerbaar te maken tegen digitale verstoringen', legt Van Schoote uit.

'In FERM gaat het om bewustwording. Met cruciale bedrijven maken we daarom afspraken over het beveiligingsniveau en de noodzaak van het delen van kennis. Daarom hebben we ook een verbinding met het Hit And Run Cargo-team. Dat is een samenwerkingsverband van douane, FIOD, zeehavenpolitie en het Openbaar Ministerie. Zij houden zich bezig met ondermijningsonderzoeken in en rondom de Rotterdamse haven. Ze weten veel over het opsporen en aanpakken van een *insider threat*, een kwetsbare medewerker.'

## ELK JAAR EEN GROTE OEFENING

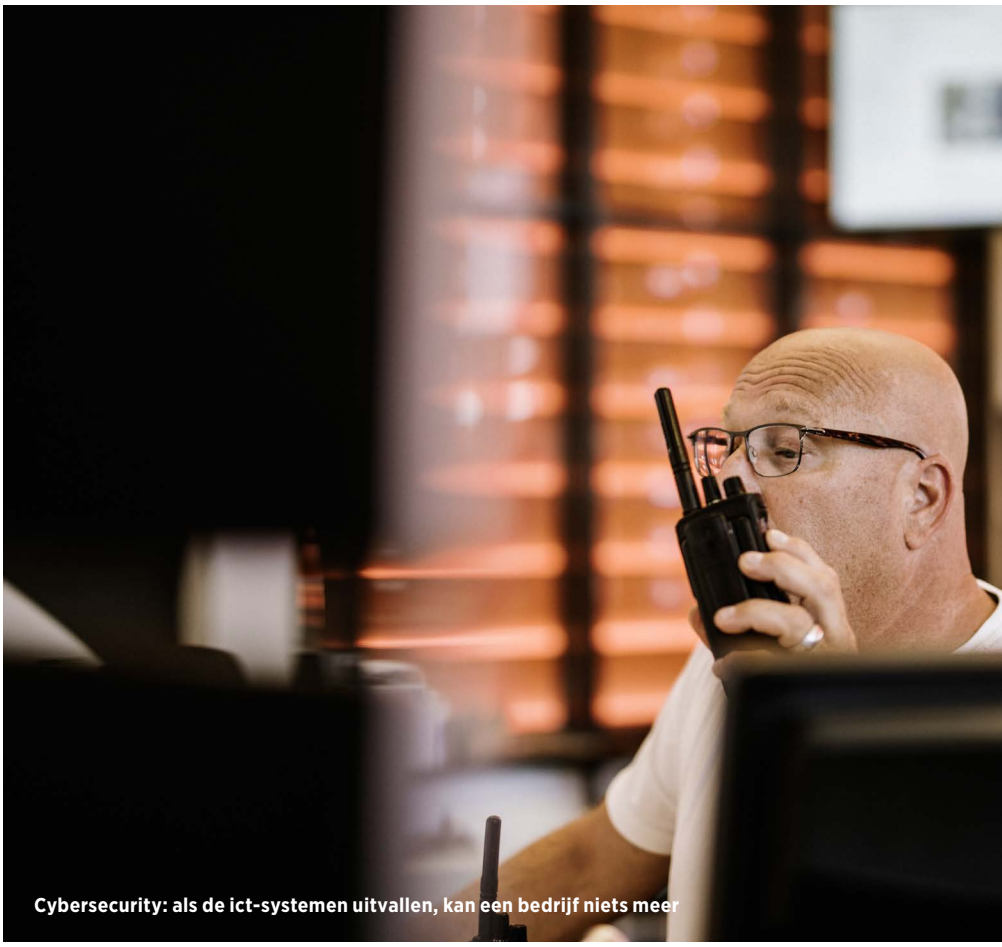
Elk jaar, in september, organiseert FERM voor het havenbedrijfsleven een grote cyberaanval

– om te oefenen. FERM-voorman Van Schoote: 'We hebben een toolkit ontwikkeld waarmee bedrijven hun eigen crisisstructuur kunnen testen. De jaarlijkse oefening betreft altijd een keten: de processen en partners die betrokken zijn bij het afwikkelen van scheepvaartverkeer of de olie- of gasindustrie. Zo leggen we de urgentie van beveiliging vóór een aanval, zoals die bij APM plaatsvond.'

Bij de laatste oefening viel hem op: 'Op bestuurlijk niveau doen we het goed. Iedereen op dat niveau is wel rolvast. Het knelt echter bij de technisch specialisten om de boel weer op orde te brengen. Veel mensen denken: we herstellen het en twee uur later werkt het weer. Maar in de praktijk kunnen daar best twee tot drie dagen overheen gaan. Dat komt door een tekort aan it-specialisten, de verdere digitalisering als gevolg van het personeelstekort én de complexiteit van de computersystemen.'

Verwachtingen in de samenleving managen is dus nodig, zegt Van Schoote. 'En we moeten zorgen dat er in het systeem voldoende buffers zijn ingebouwd. Vanuit Defensie hebben we geleerd rekening te houden met het *most dangerous* scenario: een glasvezel die niet op één maar op 25 plekken is verstoord en waarvan het meer dan een week duurt om deze te herstellen. Hoe zien dan je redundantie (voorzieningen waar je op kunt terugvallen, red.) en back-upplan eruit?'

ANP/LAIF AGENTUR FUER PHOTOS & REPORTAGEN



Cybersecurity: als de ict-systemen uitvallen, kan een bedrijf niets meer

## EEN FIREWALL IS KINDERSPEL

Bas Janssen is nog niet helemaal tevreden als het gaat om die bewustwording op bestuursniveau. 'De Chief Information Officer (cio) is zich er terdege bewust van, maar de ceo kan nog best wat bewuster worden gemaakt. Op korte termijn laten we dan ook samen met FERM ceo's serious gamen. Zij moeten echt gaan inzien hoe belangrijk hun digitale backbone is. Je komt niet meer weg met een firewall en een mannetje dat de ict doet.'

De invoering van Europese wetgeving gaat cybermaatregelen deels stroomlijnen. Waarschijnlijk wordt eind dit jaar in Nederland NIS2-richtlijn geïmplementeerd in de Cyberbeveiligingswet. De richtlijn moet de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten verbeteren.

In het Rotterdamse havencomplex moeten circa 150 bedrijven aan NIS2 voldoen. Van Schoote: 'Het is goed dat NIS2 inwerking gaat treden. Het betekent dat je als bestuurder op de hoogte moet zijn van de risico's. Je kunt niet meer je hoofd in het zand steken. Als bestuurder kun je bij onachtzaamheid aansprakelijk worden gesteld. Het kan leiden tot strafmaatregelen. Cybersecurity is echt geen vrijblijvend onderwerp meer.'

## SAMENWERKING OPGESCHAALD

Het succes van FERM is inmiddels buiten Rotterdam ook gesignaleerd. De organisatie wordt nu opgeschaald naar een landelijke samenwerking van alle zeehavens. Van Schoote is als kwartiermaker belast met de opbouw van deze landelijke cybersamenwerking.

Hij zegt: 'Amsterdam, Groningen, Moerdijk en North Sea Port (een fusie tussen de zeehavens Gent, Terneuzen en Vlissingen, red.) komen erbij. Want cyberdreiging is complex en zal

**'BENDES ÉN STATELIJKE ACTOREN PROBEREN HIER ROTZOOI TE TRAPPEN'**

nooit meer verdwijnen. Door die samenwerking is de financiering van FERM op een goede manier gewaarborgd en kunnen we een robuust systeem opzetten voor al onze zeehavens. Zo kunnen we ook oefeningen doen 'over de rand van de Rotterdamse haven heen'. Want als de functie Rotterdam wegvalt, zijn we dan ook in staat om schepen over te zetten naar een andere haven?' ◘

## Supersamenwerking krijgt vorm

**In de Rotterdamse haven werken publieke en private partijen al samen aan weerbaarheid. Elders in Nederland kan dat beter. Een groep van 22 organisaties, uit overheid en bedrijfsleven, zet zich daarvoor in.**

Zij hebben zich verenigd om bij te dragen aan het versterken van de veiligheid en weerbaarheid van Nederland. Het gaat om publiek-private organisaties en hulporganisaties. Hun initiatief is mede geïnspireerd door een moreel appèl van NAVO-admiraal Rob Bauer. Veiligheid is niet langer vanzelfsprekend en vereist een integrale aanpak, stellen de organisaties. Overheden, bedrijven en burgers moeten hun verantwoordelijkheid nemen en onderling meer samenwerken. Volgens hen is Nederland, met zijn open samenleving en economie, extra gevoelig voor dreigingen als geopolitieke conflicten, hybride oorlogsvoering en natuurrampen.
Onder de aangesloten organisaties zijn vertegenwoordigers uit de financiële sector (ABN Amro), de levensmiddelenbranche (Albert Heijn), telecom (KPN), de energie- en watervoorziening (Waternet) de ministeries van Justitie en Defensie, de gemeente Rotterdam en het Havenbedrijf in die stad. Ook VNO-NCW is aangesloten.

### Studiereis Finland

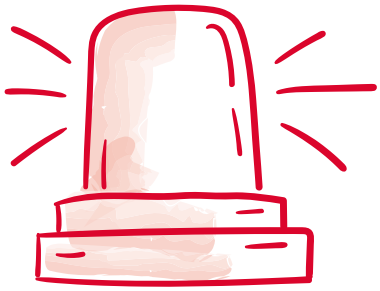
Begin november reisden deelnemers naar Finland om te kijken hoe de publiek-private samenwerking daar bijdraagt aan de weerbaarheid van dat land. Nu werken zij drie inzichten uit die ze daar opdeden. Allereerst: de noodzaak voor overkoepelende regie. Die kan vorm krijgen in een nationale raad met brede vertegenwoordiging (overheid, bedrijfsleven, hulporganisaties en kennisinstellingen), zoals het Finse Security Committee. Ten tweede: verbetering van de samenwerking tussen vitale sectoren als het gaat om voorbereiding en respons op dreigingen en gevaren. Finland heeft daar de National Emergency Supply Agency (NESA) voor. Die werkt samen met meer dan 1.500 publieke en private partijen. Tot slot: verbetering van de communicatie met de burgers, om het gevoel van urgentie onder de aandacht te brengen.

**TEKST:** PAUL SCHEER **ILLUSTRATIES:** ANOESKA KRUITHOF

CRISISPROOF

# 10 TIPS OM JE VOOR TE BEREIDEN

Minimaliseer de paniek, maak nu al werk van ellende die op je af kan komen. Wie weet gooi je je hele bedrijfsstrategie wel om, om risico te spreiden. Plus 9 andere tips. Aan de slag!



## #1 MAAK EEN NOODPLAN


Of een bedrijfscontinuïteitsplan, dat klinkt wat minder dreigend. Heb je nog niet zo'n plan, begin daar dan snel mee, want een crisis (bijvoorbeeld brand of stroomstoring) komt vaak onverwacht en voorbereiden kost tijd.
Breng dus de risico's binnen je bedrijf in kaart. Dat kan met behulp van de verplichte risico-inventarisatie en -evaluatie en door de kwetsbaarheden te bepalen, zoals de energievoorziening en de aanvoer van grondstoffen. Zorg voor zo veel mogelijk back-ups om snel de draad weer op te pakken.

**DIT GA IK DOEN**

## #2 FORMEER EEN CRISISTEAM

Zet een alvast een crisismanagementteam op. Dan hoef je dat niet te doen als de crisis net is uitgebroken. In zo'n team moeten de verschillende onderdelen van het bedrijf zijn vertegenwoordigd. De leden van het team moeten niet bang zijn om aan te pakken en besluiten te nemen, maar ook weer niet zo dat ze dat in hun eentje doen. Een crisis is geen one(wo)manshow.

**DIT GA IK DOEN**

## #3 OEFEN EEN CRISIS

Een noodplan is mooi, maar het moet bekend zijn bij de medewerkers. En het moet werken. Dat betekent: oefenen. Dat gaat verder dan de reguliere ontruimingsoefening. Want omgaan met stress, tijdsdruk en complexe situaties doen medewerkers niet elke dag. Situaties en scenario's kun je oefenen met behulp van serious gaming. Dan wordt een crisis gesimuleerd (bijvoorbeeld een hack die het computersysteem lamlegt) en gaat een groep medewerkers in teamverband de crisis te lijf. Ook virtual reality (dan ervaar je een digitale omgeving door een speciale bril) wordt gebruikt om een crisis te 'ondergaan'. Zo kan een crisisoefening nog leuk worden!

**DIT GA IK DOEN**

## #4 BEVEILIG JE ICT

Een oorlog verwachten ondernemers niet zo snel, blijkt uit de enquête die VNO-NCW hield (zie pagina 10). Maar een digitale aanval wel. Zorg dus dat je ict goed beveiligd is. Laat een specialist een nulmeting van je systeem doen en pak vervolgens de zwakke plekken aan.
Meet ook de bewustwording van de medewerkers, want daar gaat het vaak mis. Voor je het weet klikt iemand op een phishingmail. En denk vast na over de vraag: losgeld betalen of niet? Dan hoef je die discussie niet te voeren als het systeem platligt en is gegijzeld. Op www.digitaltrustcenter.nl van het ministerie van Economische Zaken is per bedrijfsgrootte (zzp'er, mkb, grootbedrijf) aangegeven wat ondernemers moeten doen om cybersecure te zijn. Zoals: inloggen in meerdere stappen.

**DIT GA IK DOEN**

## #5 WERK THUIS

Als je bedrijf tijdelijk niet toegankelijk is, is zo veel mogelijk thuiswerken weer het devies. Zorg dus dat je ict dat mogelijk kan maken. Je systeem moet ook veilig zijn, want hackers loeren overal. Borduur voort op de ervaringen uit de coronaperiode.

DIT GA IK DOEN

## #6 ZORG VOOR EEN BUFFER

Een crisis kost geld. Check of je goed verzekerd bent. En zorg dat je een financiële buffer hebt. Misschien zelfs contant geld (of toch maar niet). Zorg voor andere inkomsten door niet te afhankelijk te zijn van één markt of product. Wat voor de Nederlandse economie geldt, geldt ook voor jou. Neem geen gok, maar spreid je kansen.

DIT GA IK DOEN

## #7 COMMUNICEER

Een crisis kun je niet in stilte afhandelen. Communiceer dus. Met medewerkers, zodat die weten wat er aan de hand is en hoe zij moeten handelen. Met zakelijke partners, zodat die weten dat je tijdelijk niet 'normaal' kunt leveren. En met de buitenwereld, die wil weten wat er aan de hand is bij je bedrijf. Daar open over zijn is beter dan proberen de crisis binnenskamers te houden.

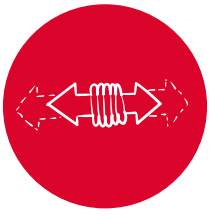
DIT GA IK DOEN

## #8 KEEP CALM AND CARRY ON


Bij een crisis moet je niet als een bang konijn in de koplampen blijven kijken tot de auto je vermorzelt. Actie dus. Maar niet als een kip zonder kop. Want dan krijg je paniekvoetbal. Kom dus in actie, maar blijf kalm. Het helpt natuurlijk om in zo'n situatie terug te vallen op alles wat je al hebt voorbereid, zie de voorgaande tips.

**DIT GA IK DOEN**

## #9 WEES FLEXIBEL



Een goede voorbereiding is het halve werk. Maar niet het hele, want een crisis houdt zich niet aan wat jij in je noodplan hebt bedacht. Pas je tactiek aan als het nodig is. Die flexibiliteit moet in je bedrijf zijn ingebouwd, én in je crisismanagementteam.

**DIT GA IK DOEN**

## #10 KIJK NAAR DE TOEKOMST

Aan elke crisis komt een eind, en dan moet je er ook weer staan als bedrijf. Snijden in de kosten kan helpen om de crisis door te komen. Maar na de crisis moet business as usual nog wel mogelijk zijn. Medewerkers die je ontsloeg tijdens de crisis, zijn mogelijk moeilijk te vervangen als de markt aantrekt. De krapte op de arbeidsmarkt is dan immers ook weer terug.

**DIT GA IK DOEN**


Malie Academy®

*Powered by VNO-NCW & MKB-Nederland*

# Cursussen voor verenigingen en branche-organisaties

## Word een goede branchebestuurder

Ontwikkel jouw leiderschap en vaardigheden om een brancheorganisatie effectief te besturen.

**11 april 2025**

Scan de QR-code om je aan te melden.

---

## Lobby 2.0:
## Verdieping in Verbinding en Resultaat

Deze driedaagse in company cursus is ontwikkeld voor professionals die hun lobbyskills naar een hoger niveau willen tillen.

Scan de QR-code om je aan te melden.

FORUM

Retouradres:
VNO-NCW, t.a.v. dhr. L. van Houdt
Postbus 93002, 2509 AA Den Haag

Port Betaald postnl