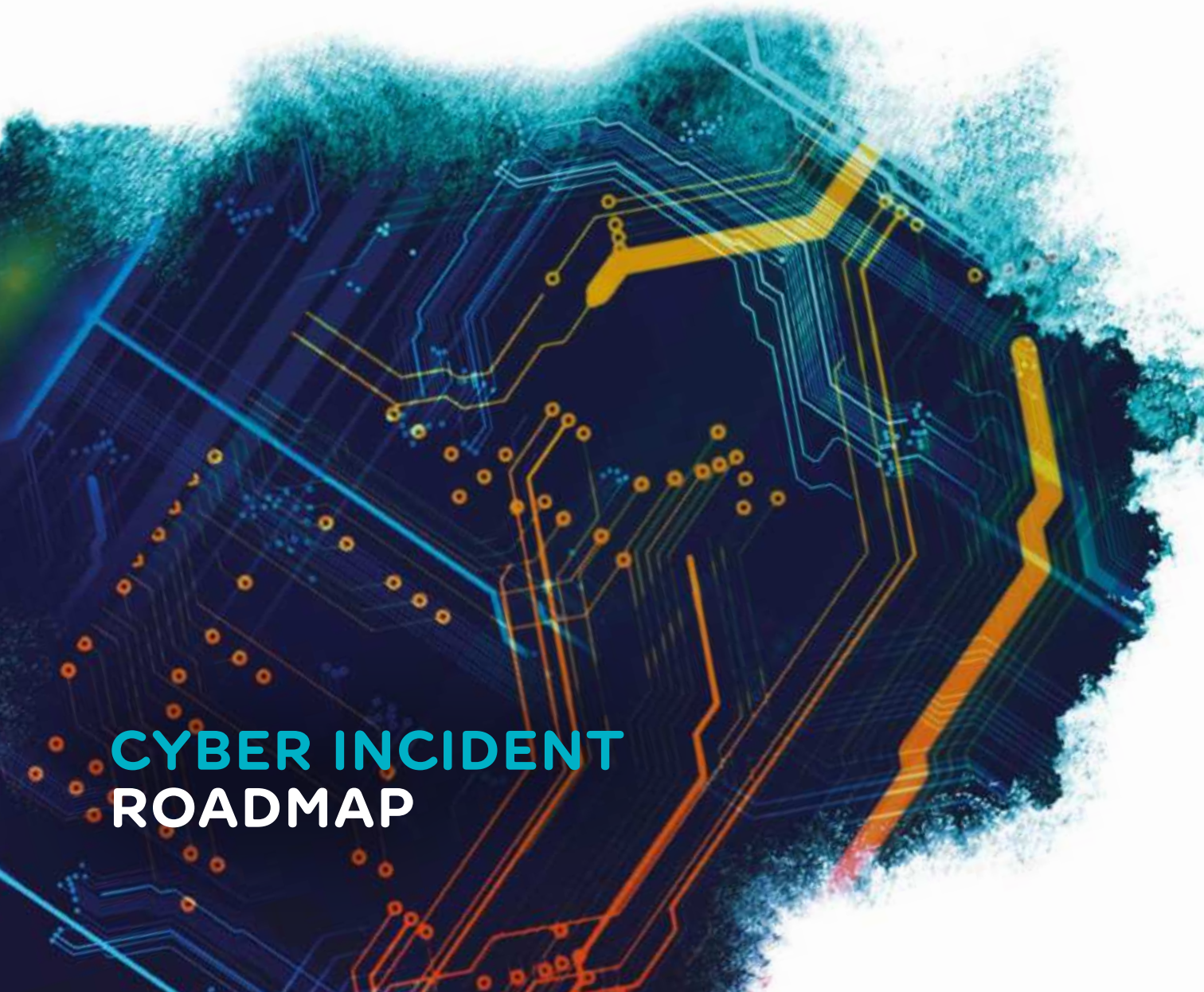
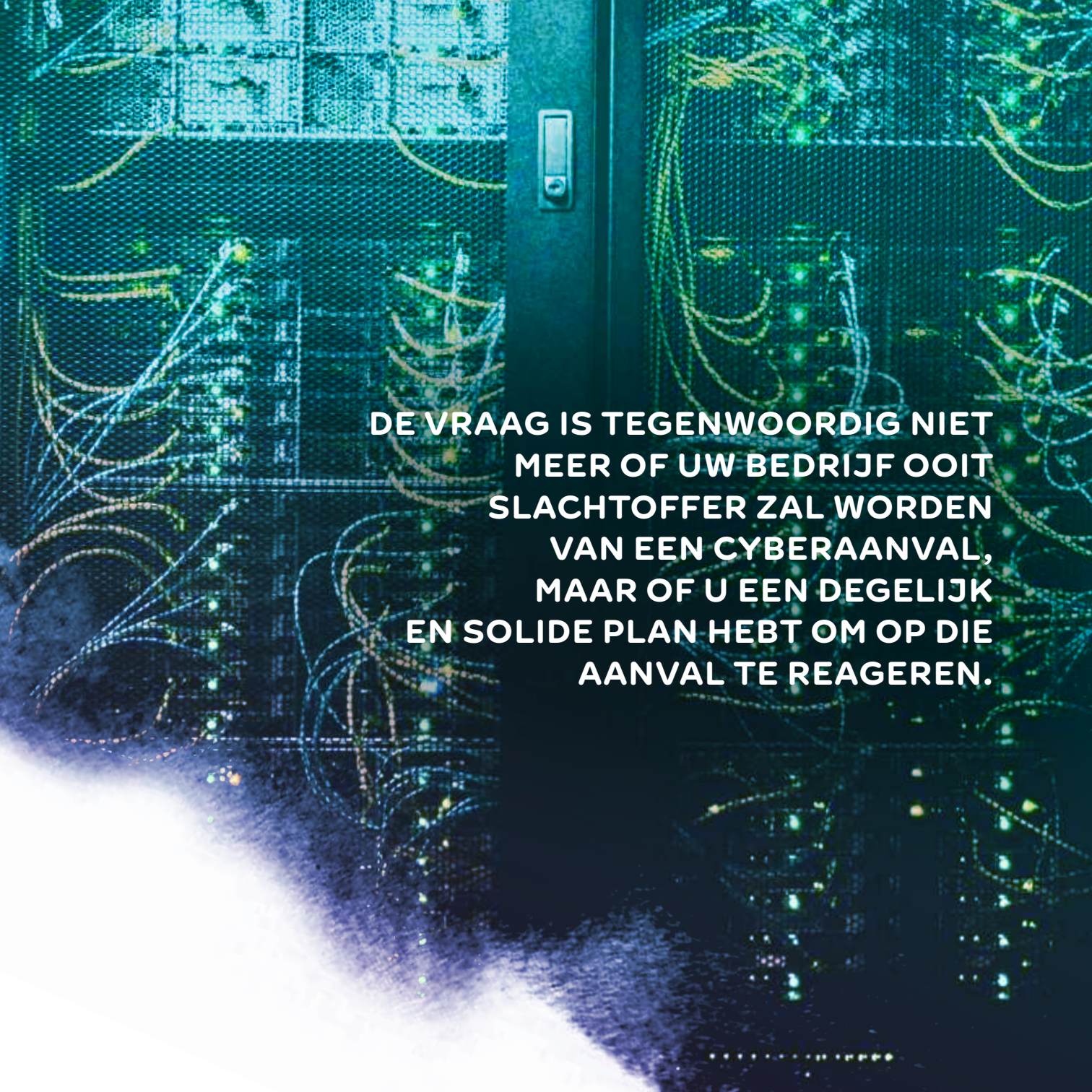
VBO FEB
Verbond van Belgische Ondernemingen
Fédération des Entreprises de Belgique



CYBER INCIDENT ROADMAP



DE VRAAG IS TEGENWOORDIG NIET MEER OF UW BEDRIJF OOIT SLACHTOFFER ZAL WORDEN VAN EEN CYBERAANVAL, MAAR OF U EEN DEGELIJK EN SOLIDE PLAN HEBT OM OP DIE AANVAL TE REAGEREN.

Het risico op cyberaanvallen neemt elke dag toe. Tal van getuigenissen van bedrijven die het slachtoffer zijn geworden van dergelijke aanvallen geven blijk van de moeilijkheden die zich op het moment zelf, maar ook daarna voordoen. De gedupeerde ondernemingen staan totaal machteloos. Ze komen in een ongekende situatie terecht die hen meestal berooft van alle of van een deel van hun digitale werkinstrumenten of essentiële gegevens die ze nodig hebben om hun activiteiten voort te zetten en hun verplichtingen na te komen.

Het doel van deze roadmap is om ondernemingen die het slachtoffer zijn van een cyberincident te ondersteunen bij hun interne organisatie, vooral bij hun interactie met hun externe contacten, met name de publieke overheden, en dat in het kader van hun wettelijke verplichtingen. Hoe meld ik een cyberincident aan de RSZ? Of aan de Algemene Administratie van de Fiscaliteit? Welke stappen moet ik met betrekking tot de RVA ondernemen om geplande periodes van tijdelijke werkloosheid wegens gebrek aan werk om economische redenen of wegens een 'technische stoornis' te melden?

Het eerste advies is natuurlijk de cyberaanval te voorkomen, en dus alle mogelijke voorzorgsmaatregelen te nemen. Dat is uiteraard het ideale scenario.

Er zijn verschillende documenten die bedrijven kunnen helpen hun cyberweerbaarheid te versterken en cyberincidenten te voorkomen en aan te pakken. In 2014 publiceerde het VBO in samenwerking met ICC Belgium, EY (Ernst & Young), B-CCENTRE, ISACA en Microsoft de Belgische Cyber Security Gids[1]. Met die gids willen de organisaties alle bedrijven ervan overtuigen om zich, naargelang hun specifieke behoeften, te wapenen tegen cyberdreigingen. De Cyber Security Coalition[2],waarvan het VBO een stichtend lid is, publiceerde ook een uitstekende gids voor incidentbeheer[3].

De vraag is tegenwoordig niet meer of uw bedrijf ooit slachtoffer zal worden van een cyberaanval, maar of u een degelijk en solide plan hebt om op die aanval te reageren.

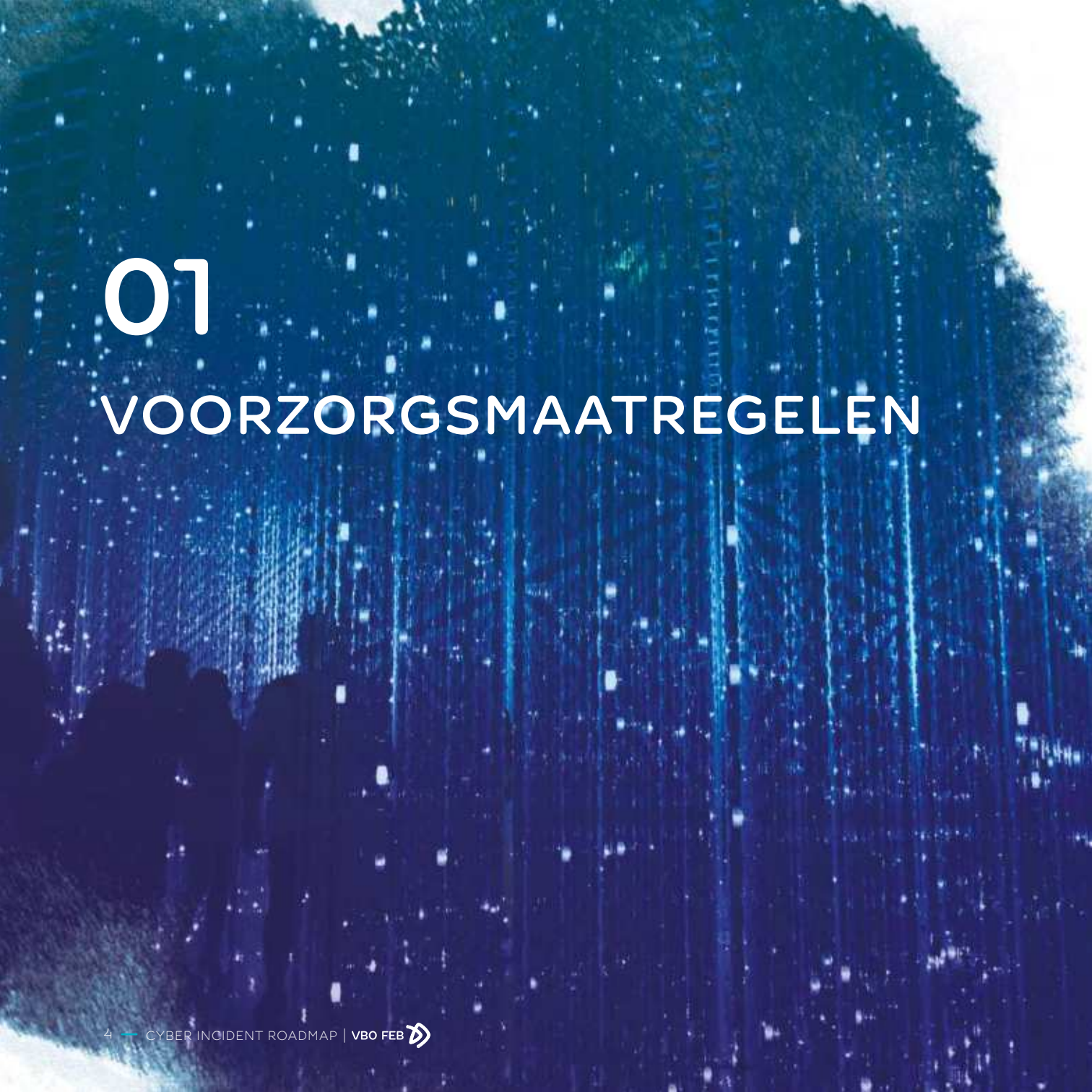
Met deze nieuwe roadmap geven we u een overzicht van de verschillende fasen van het incidentbeheer, van de detectie tot de afsluiting. In elke fase verwijzen we u door naar de verschillende organisaties, belanghebbenden en externe experts die u door die beproeving kunnen helpen en uw activiteiten veilig kunnen stellen zodat u uw verplichtingen ten aanzien van bv. de overheid kunt blijven nakomen. Ze vormt geen eindpunt, maar weerspiegelt een voortdurende oefening. De roadmap zal dus regelmatig updates krijgen na de eerste publicatiedatum in december 2022.

Nathalie Ragheno
Eerste adviseur van
het competentiecentrum
Recht & Onderneming VBO FEB

Pieter Timmermans
CEO VBO FEB

(1) https://www.vbo.be/publicaties/belgische-gids-voor-cyberveiligheid_2014-05-26/
(2) De Cyber Security Coalition is een uniek samenwerkingsverband tussen spelers uit de academische wereld, de publieke sector en particuliere bedrijven met als doel de krachten te bundelen tegen cybercriminaliteit. Meer dan 100 kernspelers uit die drie sectoren zijn op dit moment actief lid. Zij dragen bij tot de missies en doelstellingen van de Coalition.
(3) https://www.cybersecuritycoalition.be/nl/resource/incident-management-guide/

INHOUDSTAFEL



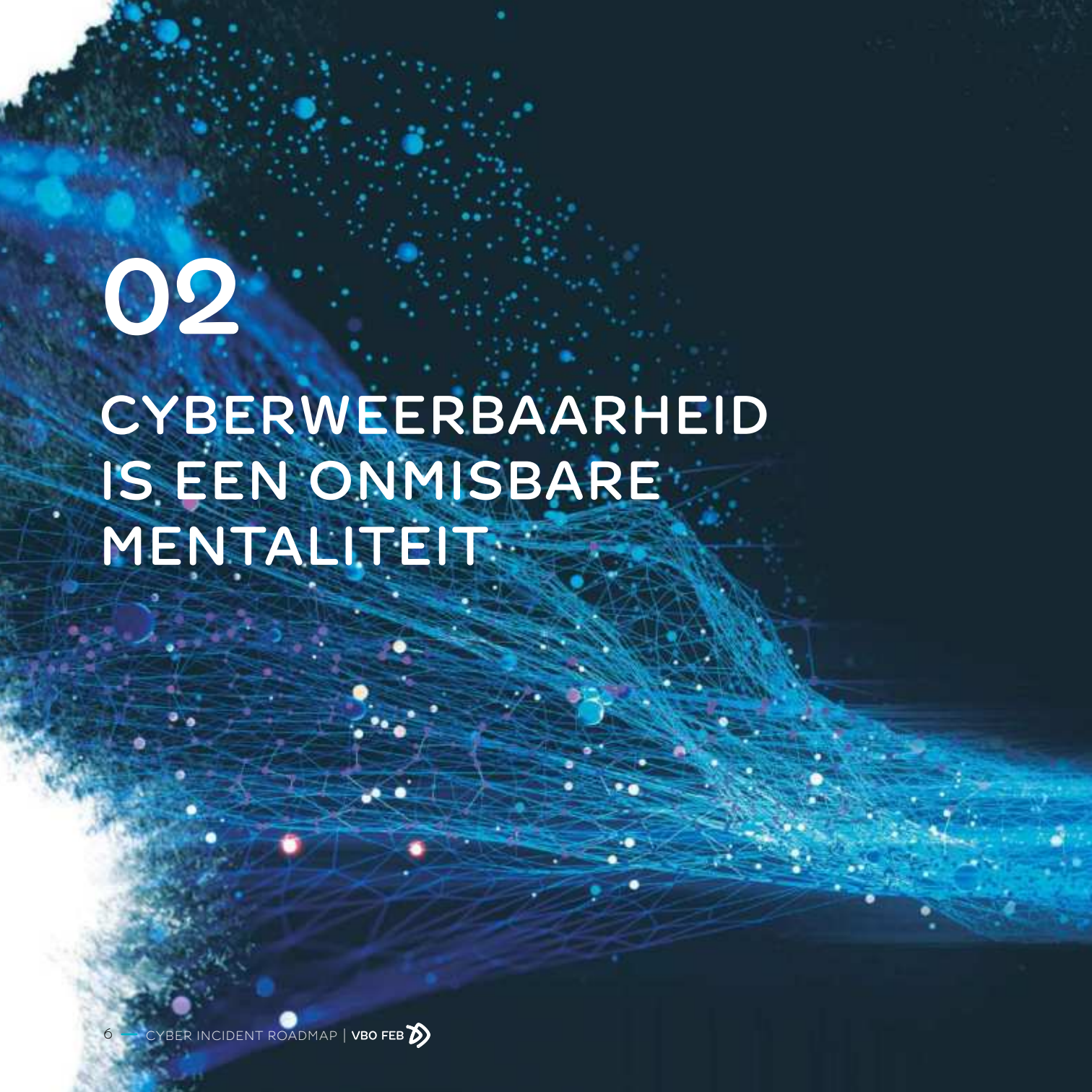
01 VOORZORGSMAATREGELEN

HET INCIDENTBEHEER OP VOORHAND PLANNEN VOOR MEER VEERKRACHT

We kunnen het niet genoeg herhalen: de juiste voorzorgsmaatregelen en een goede voorbereiding op cyberincidenten zijn essentieel. Alle personeelsleden moeten over het risico worden geïnformeerd en gesensibiliseerd, want de gevolgen op het vlak van reputatie, organisatie en financiële lasten kunnen zeer ernstig zijn.

Er moeten dus procedures worden ingesteld om op een cyberincident voorbereid te zijn.

Bedrijven moeten kunnen reageren om hun getroffen kritieke activiteiten, systemen en gegevens te herstellen. Kortom: om weer normaal te kunnen functioneren. De planning en voorbereiding moeten vóór een incident worden geïmplementeerd en zijn bepalend voor het niveau van cyberweerbaarheid.



02

CYBERWEERBAARHEID IS EEN ONMISBARE MENTALITEIT

Agoria, de federatie van de technologische industrie, beschikt over uitgebreide expertise op het gebied van cyberveiligheid en weerbaarheid tegen bedreigingen. Gevraagd naar haar visie op cyberweerbaarheid vat ze die samen met de slogan 'ABC for Executive'.

A Voor 'asset management'

De grote zwakte van veel bestuurders en bedrijfsleiders van vandaag is dat ze niet altijd een duidelijk beeld hebben van de te beschermen IT-activa. Wat moet ik eerst beschermen? Servers, data, applicaties ...? Om budgettaire redenen kunt u waarschijnlijk niet alles even grondig beschermen. Weet u wat uw belangrijkste 'assets' zijn? Die bedenking maken bedrijven zich vaak niet.

B Voor 'business modelling'

Bestuurders of bedrijfsleiders hebben soms ook geen duidelijk schematisch overzicht van hun bedrijf. 'Business modelling' wordt vaak onderschat, maar is essentieel. Hoe is uw bedrijf gestructureerd? Wanneer u een klant een waardevoorstel doet, op welke dienst is dat dan gebaseerd? Via welke applicatie? Gehost op welke server? Op welk netwerk? ... Dat schematische overzicht is een grote hulp bij een cyberaanval.

C Voor continuïteit

Bent u voorbereid? Wat is uw plan om, in geval van een aanval, verder te kunnen werken? En hoe test u dat plan? Beschikt u over een offline back-up van uw prioritaire 'assets'? Hebt u een extern crisiscommunicatieplan? Ook dat is in veel bedrijven een ontbrekend element.

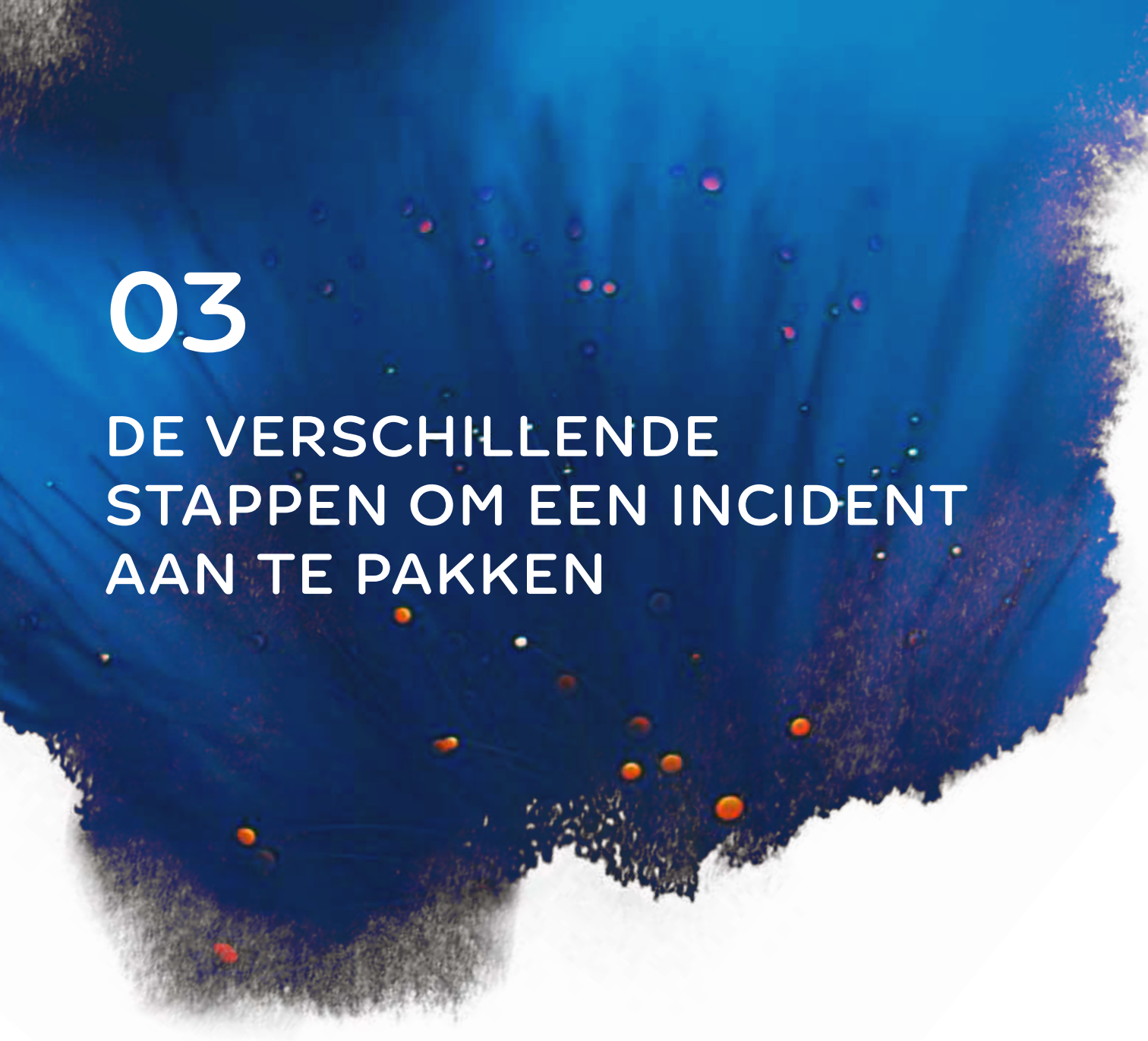
Cyber Poverty Line

Het belangrijkste advies is: wacht niet op een cyberaanval om een actieplan uit te rollen. Er bestaat zoiets als een 'cyberarmoedegrens', d.w.z. een minimumniveau van informaticahygiëne dat elk bedrijf zou moeten hanteren.

Cyberweerbaarheid is een mentaliteit die we ons eigen moeten maken en een manier van werken. Alle bedrijven zouden regelmatig in 'aanvalsmodus' moeten gaan, net zoals elk bedrijf een evacuatieplan moet hebben en dat regelmatig moet testen. Dat is des te belangrijker omdat een bedrijf dat zich niet voorbereidt op een mogelijke cyberaanval kan worden gezien als een bedrijf dat niet aan risicobeheer doet. Dat is uiteraard rampzalig voor het bedrijf zelf, maar ook voor het imago van het bedrijf en zijn bestuurders.

Zie ook 'Onze aanbevelingen om uw cyberveiligheid te waarborgen'.

Klik hier



03

DE VERSCHILLENDE STAPPEN OM EEN INCIDENT AAN TE PAKKEN

Een responsplan uitwerken is een belangrijke eerste stap voor elke onderneming of organisatie bij de voorbereiding op en het beheer van een cyberveiligheidsincident. Het topmanagement moet dat plan goedkeuren en betrokken zijn bij elke stap van de incidentbeheercyclus. Het plan moet ook up-to-date worden gehouden.

Het responsplan omvat onder meer de volgende elementen:

- Een inventaris van de te beschermen activa (welke informatie, systemen, netwerken, producten?);
- Een identificatie en toewijzing van verantwoordelijkheden;
- Interne bekwaamheden of gesloten contracten met externe experts voor de aanpak van incidenten en/of forensisch onderzoek (digitaal opzoekwerk en onderzoek);
- Een basisinperkingsstrategie: de systemen onmiddellijk loskoppelen om zo snel mogelijk te herstellen? Of de tijd nemen om bewijzen te verzamelen?;
- Een communicatiestrategie voor zowel interne als externe belanghebbenden en voor autoriteiten zoals de Gegevensbeschermingsautoriteit en de bevoegde instanties voor het melden van netwerk- en informatiebeveiligingsincidenten.

3.1 WIE MOET WORDEN INGELICHT?

Een procedure en lijsten van interne en externe belanghebbenden die moeten worden ingelicht volgens vastgestelde scenario's en criteria (zoals de ernst van het incident, de vereiste regelgevende en wettelijke kennisgevingen) maken deel uit van de goede praktijken en moeten dus worden opgenomen in elk cyberweerbaarheidsbeleid.

Welke belanghebbenden kunnen worden getroffen door het cyberveiligheidsincident? En is het uw verantwoordelijkheid om bepaalde instanties zoals de Gegevensbeschermingsautoriteit of andere autoriteiten in te lichten?

- Interne belanghebbenden: topmanagement, getroffen kaderleden, werknemers;
- Externe belanghebbenden: media, klanten, leveranciers, andere partners …
- Officiële belanghebbenden: Gegevensbeschermingsautoriteit, sectorale toezichthouder, Centrum voor Cybersecurity België (CCB, afdeling CERT.be), Nationaal Crisiscentrum, politie ...

3.2 WIE INTERN INLICHTEN?

Wanneer een bedrijf getroffen wordt door een cyberincident, is het essentieel dat de juiste mensen binnen het bedrijf snel worden geïnformeerd.

Net als elk ander risico voor de onderneming, vereist cyberveiligheid een duidelijke strategie van het bestuursorgaan. Dat bestuursorgaan hoeft niet alle technische aspecten te begrijpen, maar is toch verantwoordelijk voor het **beheer van cyberveiligheidsrisico's**[1]. Dat houdt in: **risicopreventie, bewustmaking van het personeel, eventueel het afsluiten van een verzekering tegen cyberrisico's** ... Zowel de Algemene Verordening Gegevensbescherming (GDPR) als ICT-beveiligingsnormen (zoals de ISO-norm 27001), om er maar een paar te noemen, leggen de algemene verantwoordelijkheid voor IT-beveiliging bij het bestuursorgaan.

Binnen een organisatie is de raad van bestuur verantwoordelijk voor het aansturen van risicobeheerstrategieën en het vaststellen van duidelijke en haalbare doelstellingen om de cyberweerbaarheid van de organisatie te versterken. Cyberveiligheid is een essentieel onderdeel van een goed ESG-beleid.

Van haar kant neemt de algemene directie de nodige beslissingen om procedures in te voeren om cyberincidenten te voorkomen, maar ook om een crisissituatie te beheren. Ze moet het bedrijf zo organiseren dat met name het personeel wordt aangemoedigd om cyberincidenten te melden of onder de aandacht te brengen van de directie.

In de praktijk zou elk bedrijf en elke organisatie een incidentresponsteam moeten hebben dat kan worden samengeroepen zodra zich een incident voordoet. Uiteraard bepaalt de grootte van het bedrijf de grootte en structuur van het incidentresponsteam. In bepaalde gevallen kan het ook goedkoper en doeltreffender zijn om een beroep te doen op externe partners voor het aanpakken van cyberveiligheidsincidenten en zo de leemten in de vaardigheden van uw organisatie te dichten.

Kleinere bedrijven die niet over de middelen voor een echt team beschikken, kunnen een eerste aanspreekpunt – idealiter iemand met beslissingsbevoegdheid – aanstellen onder het personeel. In geval van een cyberveiligheidsincident moet hij of zij extern hulp zoeken, maar blijft hij of zij de uiteindelijke verantwoordelijke voor de incidentrespons binnen de organisatie.

De samenstelling van dit incidentresponsteam wordt ook bepaald door de verschillende vaardigheden die nodig zijn om een incident aan te pakken. Bij kleinere bedrijven kan het nodig zijn om die vaardigheden buiten de organisatie te zoeken en neemt het eerste aanspreekpunt contact op met de nodige experts.

Wanneer zich een cyberincident voordoet, moet de raad van bestuur dus onmiddellijk worden ingelicht. Vervolgens moeten alle diensthoofden die bij het beheer van de crisis betrokken kunnen zijn, worden samengeroepen in functie van het incident en de procedure van het bedrijf: IT in de eerste plaats, maar ook human resources, de juridische afdeling, communicatie, de financiële afdeling …

(1) Die verantwoordelijkheid wordt nog verder uitgebreid in het kader van de NIS II-richtlijn.

3.3 WIE EXTERN INLICHTEN?

3.3.1 Externe experts

De externe experts helpen u de oorzaken van het incident te bepalen en bieden advies om het incident in te perken, weg te werken en te vermijden dat het nog eens voorvalt. Andere partijen, zoals sectorale toezichthouders – zoals de FSMA, het BIPT of de CREG –, de Gegevensbeschermingsautoriteit, het Centrum voor Cybersecurity België (CCB), afdeling CERT.be en de wetshandhavingsinstanties (politie en magistraten), kunnen waardevolle bijstand verlenen wanneer u wordt geconfronteerd met een cyberveiligheidsincident van criminele aard of in geval van een lek van persoonsgegevens. Sommige wetgeving verplicht u zelfs om die partijen in te lichten wanneer u een incident van specifieke aard hebt gedetecteerd (zie hieronder).

3.3.2 Betrokken personen: klanten, leveranciers

Het type incident en de (mogelijke) impact ervan bepalen welk type communicatie nodig is.

Indien bepaalde verplichtingen tegenover klanten en/of leveranciers niet kunnen worden nagekomen, moeten die worden geïdentificeerd en moeten de betrokken personen worden ingelicht. Het in zo'n geval belangrijk om over de situatie te communiceren om de vertrouwde partners gerust te stellen.

Als het IT-systeem niet beschikbaar is, kunt u de klanten inlichten over de regels voor het gebruik van de tijdelijk ter beschikking gestelde diensten en hulpmiddelen.

Wanneer de persoonsgegevens van de klanten of leveranciers van een organisatie gehackt zijn, is het een goed idee om ten minste met die klanten en/of leveranciers contact op te nemen en om een persbericht voor te bereiden. In het geval van een cyberincident, en indien het persoonsgegevenslek vermoedelijk een hoog risico inhoudt voor de betrokken natuurlijke personen door de gestolen of verloren gegevens, is de in de regels over de bescherming van persoonsgegevens (GDPR en privacywet) aangewezen verwerkingsverantwoordelijke immers verplicht de betrokkenen zo spoedig mogelijk te informeren. Dat kan rechtstreeks door zich tot de betrokken personen te richten of, als dat te ingewikkeld is, via de media (zie hieronder).

3.3.3 De verzekeringen

Assuralia, de Belgische federatie van de verzekeringssector, is zeer actief in het ontwikkelen en promoten van cyberverzekeringen. Ondernemingen doen er goed aan om een cyberverzekering af te sluiten. De kosten van cyberveiligheidsincidenten kunnen immers oplopen tot honderdduizenden of zelfs miljoenen euro's. Een betrouwbare cyberverzekering dekt in elk geval een deel van die kosten.

3.3.3.1 Door de verzekeringssector aangeboden diensten

De diensten die de op deze markt actieve verzekeringsmaatschappijen aanbieden, kunnen worden onderverdeeld in drie grote categorieën:

- **Bijstand aan ondernemingen die het slachtoffer zijn van cyberincidenten:** telefonische helpdesk, IT-bijstand (beveiliging van getroffen systemen, onderzoeknaaroorzaken,herstelvangegevens...), publicrelationsdiensten, crisisbeheer ...
- **Vergoeding van schade eigen aan de verzekerde onderneming:** betaling van kosten om de normale activiteit te handhaven of te hervatten, kosten voor het reconstrueren van gegevens, voor het herstel van gegevens en software, vergoeding van exploitatieverliezen, zelfs volledige of gedeeltelijke betaling van het losgeld en de kosten van cyberafpersing ...
- **Vergoeding van schade aan derden (BA):** vergoeding van eventuele schade aan klanten en leveranciers, een contractuele verzekering BA (beroepsaansprakelijkheid) die contractuele schadevergoedingen dekt, extracontractuele burgerlijke aansprakelijkheid voor het vergoeden van schade in verband met een persoonsgegevenslek, een inbreuk op de netwerkbeveiliging, de overdracht van malware ...

Er dient overigens aan herinnerd te worden dat een verzekeringscontract moet worden gesloten voordat de schade zich voordoet.

Belangrijke opmerkingen: niet alle verzekeraars bieden al die garanties. Bovendien hangt de toekenning ervan af van het profiel van de klant en zijn activiteitensector. Elk contract wordt op maat opgesteld op basis van een individuele aanpak.

3.3.3.2 Voorwaarden voor toegang tot een verzekering (aandachtspunten)

Het afsluiten van een verzekering tegen cyberrisico's is onderworpen aan voorwaarden voor de onderneming die de verzekering aanvraagt: risicoanalyse en -beheer, preventieve maatregelen om risico's te beperken (publicatie van beleid, van een crisisbeheerplan, audit, penetratietests ...), bewustmakingsacties en opleidingsmaatregelen voor het personeel.

De toepassing van goede beveiligingsmethoden is in dit verband essentieel: antivirusbescherming, firewall, automatische en regelmatige updates, regelmatige back-ups die off-site worden opgeslagen, multifactorauthenticatiemethode, regelmatige bewustmaking en opleiding van het personeel ...

De verzekeraar kan ook andere voorwaarden opleggen, bijvoorbeeld (sub)limieten voor ransomware, medeverzekering bij de verzekerde ...

3.3.3.3 Wat moet een verzekerde onderneming doen bij een cyberaanval?

Een onderneming die het slachtoffer is van een cyberaanval moet, als ze verzekerd is tegen cyberaanvallen, allereerst de voorkeurspartner opbellen die in het deel 'bijstand' van het verzekeringscontract vermeld staat. Die zal alle operaties coördineren met de crisis- en IT-teams van de onderneming.

Indien de onderneming niet specifiek tegen cyberrisico's is verzekerd, is het niettemin mogelijk dat meer algemene verzekeringsgaranties van toepassing zijn: bijvoorbeeld een rechtsbijstandsverzekering, een verzekering BA uitbating (voor schade aan derden) ... De benadeelde onderneming moet de schade dan zo snel mogelijk aangeven aan zijn verzekeringstussenpersoon (makelaar) of de betrokken verzekeraar(s).

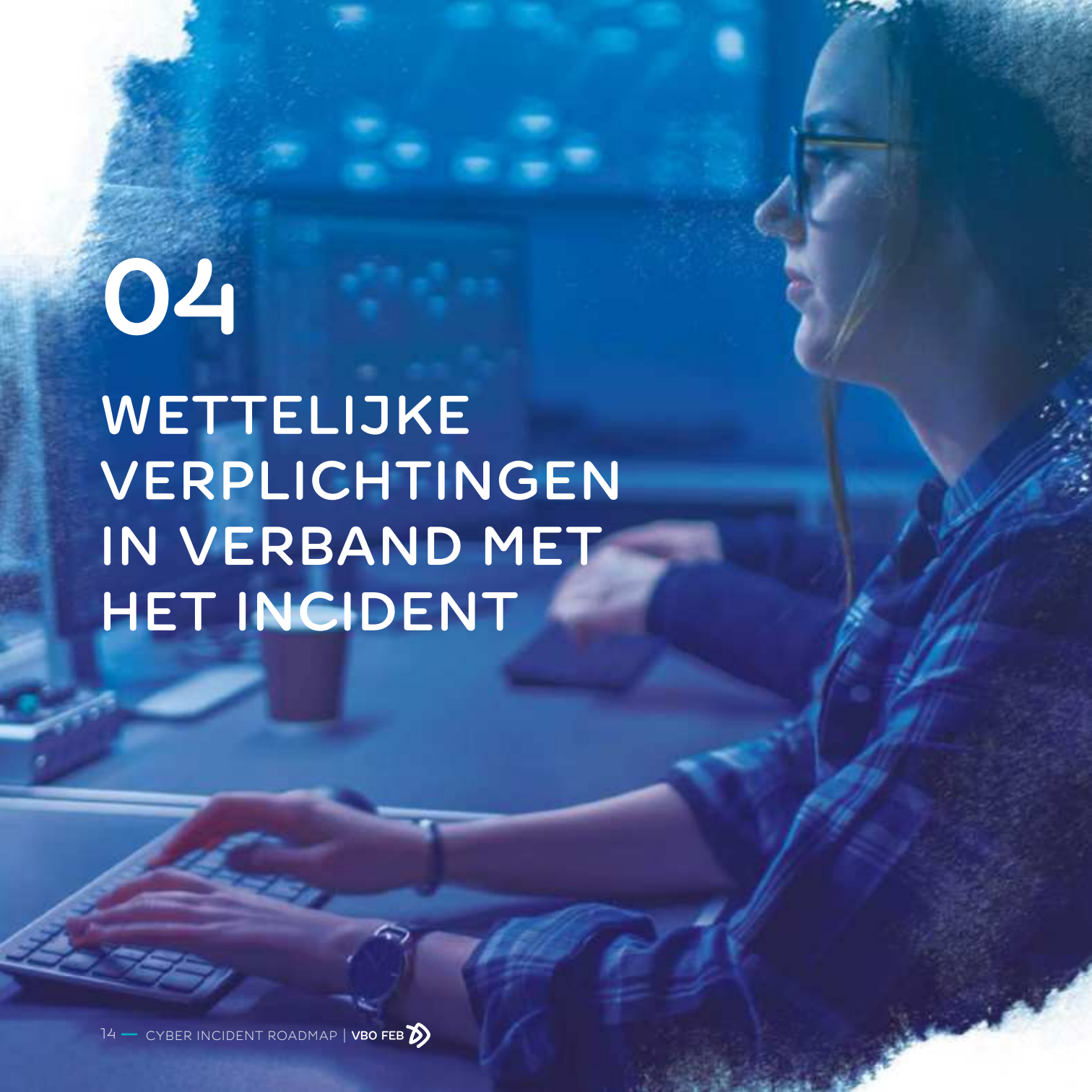
3.4 KLACHT INDIENEN BIJ DE POLITIE

De eerste essentiële stap is het indienen van een klacht bij de politie tegen de vermoedelijke dader van het cyberveiligheidsincident. Die klacht moet worden ingediend bij de lokale politiezone van het hoofdkantoor van uw onderneming.

Sinds begin 2022 beschikt de federale politie, op initiatief van de directeur-generaal van de algemene directie van de gerechtelijke politie, over een instrument om die klachten te helpen registreren: **CyberAid**. CyberAid is een platform dat toegankelijk is voor alle politieagenten in België. Er werden er al 21 cyberinbreuken op geregistreerd. Op basis van enkele vragen kan de agent die uw klacht opneemt ten eerste bepalen om welke inbreuk het gaat.

Vervolgens wordt hij begeleid om de klacht op een efficiënte manier te registreren en om het slachtoffer een reeks praktische tips te geven.

Het CyberAid-platform is op aanvraag bovendien ook beschikbaar voor alle magistraten.



04

WETTELIJKE VERPLICHTINGEN IN VERBAND MET HET INCIDENT

Als uw onderneming het slachtoffer is van een cyberincident, wordt u geconfronteerd met verschillende externe partijen aan wie u uw situatie moet toelichten.

Het is daarom van belang dat u de volgende maatregelen treft om beter op de situatie te kunnen reageren:

- Houd de documenten die u nodig hebt tijdens een incident ook offline beschikbaar. Tijdens een cyberveiligheidsincident hebt u niet noodzakelijk altijd toegang tot de bestanden op uw computer. Het is altijd een goed idee om een gedrukt exemplaar/ offline kopie te bewaren van elk document dat u tijdens een cyberveiligheidsincident of -crisis waarschijnlijk nodig zult hebben.
- Back-ups horen niet verbonden te zijn met de rest van uw systeem. Als het om back-ups gaat, is het niet alleen van het grootste belang dat ze bestaan. Het is ook heel belangrijk om een back-up te hebben die op geen enkele manier met de rest van uw systeem is verbonden. Als uw back-up met uw systeem is verbonden, is de kans groot dat de besmetting van uw systeem uitbreidt naar uw back-up, zodat uw back-up nutteloos wordt.
- Documenteer elke stap van het cyberveiligheidsincident. Vertrouw in tijden van crisis niet uitsluitend op uw geheugen! Noteer elke ondernomen actie, zoals het rapporteren van het incident, het verzamelen van bewijzen, gesprekken met gebruikers ...

4.1 ALGEMENE VERPLICHTINGEN

Zodra u heeft beslist met wie u zult communiceren over het cyberveiligheidsincident en wat u hen zult vertellen, dient u alleen nog te beslissen wanneer u met hen contact opneemt. Dat moment wordt bepaald op basis van de communicatiedoelstellingen:

- Sommige betrokkenen hebben zo snel mogelijk inlichtingen nodig omdat zij kunnen helpen bij het onder controle krijgen van het cyberveiligheidsincident (bv. het topmanagement en de werknemers van uw organisatie);
- Andere belanghebbenden (bv. Gegevensbeschermingsautoriteit) moeten binnen een wettelijk opgelegde termijn worden gecontacteerd;
- En ten slotte kunnen andere belanghebbenden contact met u opnemen en in dat geval moet u uw antwoorden voorbereid hebben (bv. media). Om te voorkomen dat de cybercrimineel te weten komt dat u hem op het spoor bent, kan het noodzakelijk zijn om een periode zonder communicatie in te lassen vanaf het ogenblik van detectie van het incident tot het ogenblik waarop u een volledig overzicht van het incident en een actieplan hebt.
- Bovendien is het noodzakelijk om het incident bij de gerechtelijke instanties aan te geven om te kunnen bewijzen dat het daadwerkelijk heeft plaatsgevonden (zie hierboven). De overheden zullen u namelijk om het attest van klachtneerlegging vragen alvorens uw verklaring in aanmerking te nemen.

Het cyberveiligheidsincident waarmee u wordt geconfronteerd, is mogelijk geen alleenstaand geval. De overheidsdiensten beschikken misschien over informatie waarmee u uw incident sneller onder controle kunt krijgen.

De wetshandhavingsinstanties moeten zo snel mogelijk na de ontdekking van het cyberveiligheidsincident worden geïnformeerd, gezien de vluchtigheid van sporen en de acties die moeten worden ondernomen (internetidentificatie enz.).

De gerechtelijke instanties hebben alle beschikbare informatie over het incident nodig om over te kunnen gaan tot de kwalificatie van het misdrijf en de identificatie van de verdachte. De informatie die aan de politie moet worden gegeven in geval van internetfraude (een 'klassiek' misdrijf dat met behulp van elektronische middelen wordt gepleegd) is mogelijk niet helemaal dezelfde als de informatie die de politie nodig heeft in geval van een ICT-misdrijf (hacking, sabotage, spionage). In de loop van het onderzoek zal er bijkomende informatie gevraagd, verzameld en gezocht worden door de speurders.

4.2 VERPLICHTINGEN T.A.V. OFFICIËLE BELANGHEBBENDEN

4.2.1 GBA

Een gegevenslek, d.w.z. een inbreuk op de beveiliging die op onopzettelijke of onwettige wijze leidt tot de vernietiging, het verlies, de diefstal, de openbaarmaking ... van persoonsgegevens moet op grond van de GDPR-bepalingen worden gemeld aan de Gegevensbeschermingsautoriteit (GBA). Dat is een wettelijke verplichting en niet-naleving ervan kan leiden tot zware sancties.