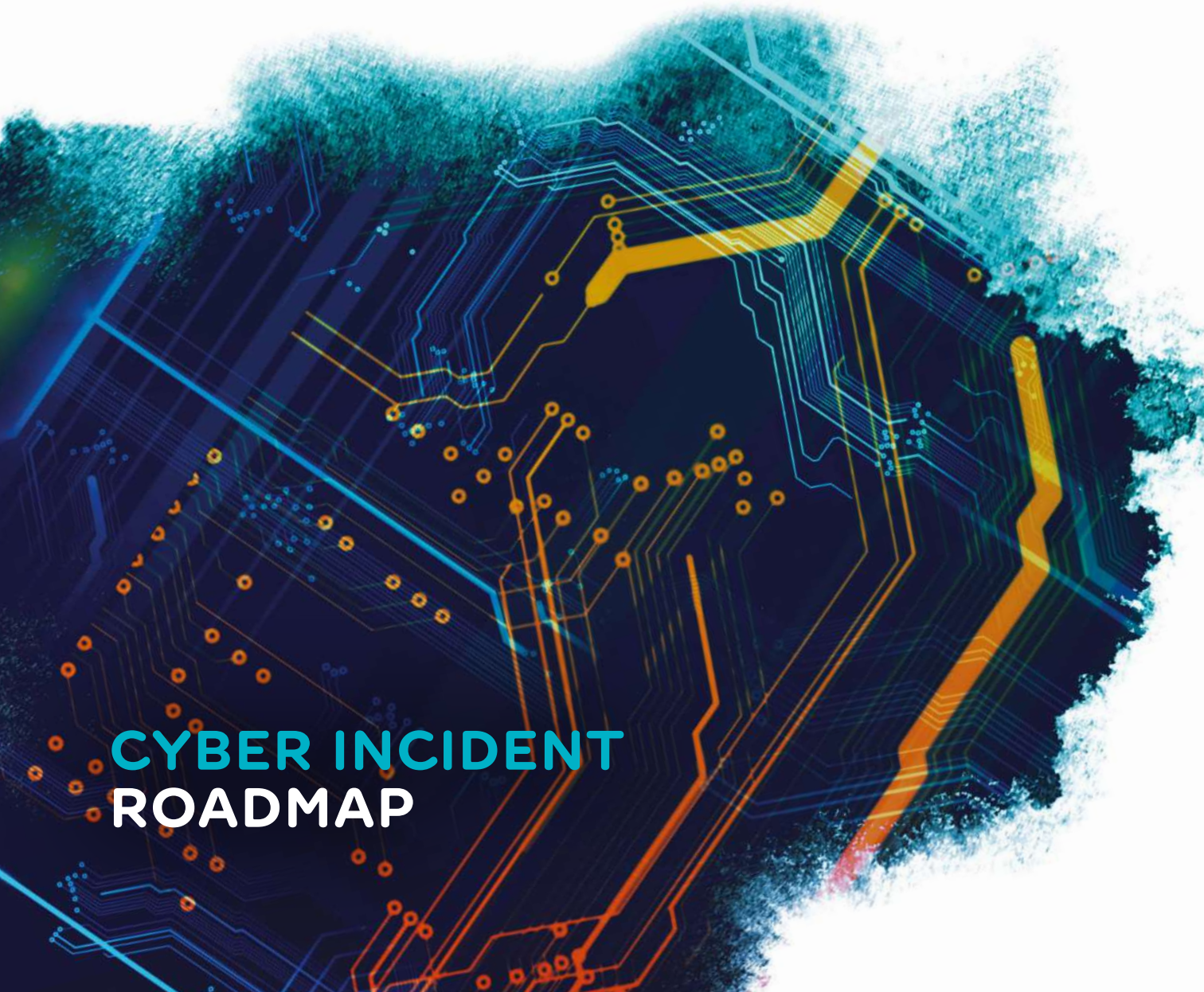
VBO FEB
Verbond van Belgische Ondernemingen
Fédération des Entreprises de Belgique



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

04

05

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.

De verwerkingsverantwoordelijke moet die melding doen bij de GBA binnen ten laatste 72 uur na er kennis van te hebben genomen.

De melding van een gegevenslek is niet verplicht wanneer dat gegevenslek waarschijnlijk geen risico inhoudt voor de rechten en vrijheden van de betrokkenen. Dat is bijvoorbeeld het geval wanneer het gaat om gegevens die al openbaar beschikbaar zijn of gegevens die voldoende versleuteld zijn en waarvan de verwerkingsverantwoordelijke over een back-up beschikt.

In alle andere gevallen gebeurt de melding van een gegevenslek aan de GBA via een elektronisch formulier dat, nadat het is ingevuld, via een webportaal wordt doorgestuurd. Per e-mail verstuurde formulieren worden niet behandeld.

Het formulier dient in een van de drie landstalen te worden ingevuld. Technische bijlagen bij het aanvraagformulier mogen naast de drie landstalen ook in het Engels worden opgesteld.

https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/datalek-van-persoonsgegevens

https://www.gegevensbeschermingsautoriteit.be/publications/handleiding-over-het-gebruik-van-invulformulieren.pdf

Wanneer de inbreuk op de persoonsgegevens vermoedelijk een hoog risico voor de rechten en vrijheden van een natuurlijk persoon inhoudt, is de verwerkingsverantwoordelijke, behoudens uitzondering, verplicht die persoon zo spoedig mogelijk te informeren.

Als het onmogelijk is om de slachtoffers van het gegevenslek te identificeren, kan de verwerkingsverantwoordelijke die personen inlichten via de media. De kennisgeving aan de betrokken personen moet duidelijk en makkelijk te begrijpen zijn.

De Gegevensbeschermingsautoriteit beveelt aan om tenminste de hiernavolgende informatie te verstrekken:

- Naam van de verantwoordelijke voor de gegevensverwerking;
- Contactgegevens om bijkomende informatie te kunnen verkrijgen;
- Korte samenvatting van het incident dat tot het gegevenslek heeft geleid;
- (Vermoedelijke) datum van het incident;
- Aard en strekking van de betrokken persoonsgegevens;
- Denkbare gevolgen van het gegevenslek voor de betrokken personen;
- Omstandigheden waaronder het gegevenslek plaatsvond;
- De maatregelen die de verantwoordelijke heeft genomen om het gegevenslek te verhelpen;
- De maatregelen die de verantwoordelijke aan de betrokken personen aanbeveelt om de mogelijke schade te beperken.

4.2.2 CERT.be

A **Vrijwillige melding door een bedrijf dat slachtoffer is van een cyberincident**

Een vrijwillige melding van een incident aan CERT.be (het Cyber Emergency Response Team, de operationele dienst van het Centrum voor Cybersecurity België) door een bedrijf dat niet onderworpen is aan de wettelijke verplichtingen ter zake is geen verzoek tot interventie. De reactie per e-mail van een CERT-operator is niet gegarandeerd en hangt af van de ernst van het incident en de hoedanigheid van het bedrijf dat de melding maakt. Het CCB geeft technisch en organisatorisch advies via zijn websites (https://www.cert.be/nl/richtlijnen) om een cyberincident te beheren, maar het helpt bedrijven niet om de noodzakelijke handelingen uit te voeren.

(1) NIS: wetgeving inzake de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.
(2) AED: Aanbieder van essentiële diensten, een publieke of private entiteit die actief is in België in een van de volgende sectoren: energie, vervoer, financiën, gezondheidszorg, drinkwater en digitale infrastructuren.

Het melden van uw incidenten helpt het CCB bij het verzamelen en analyseren van, waarschuwen voor en reageren op bevestigde dreigingen. De inhoud van de meldingen wordt automatisch uitgelezen en geanalyseerd om kennis te verzamelen die vervolgens kan worden gebruikt om waarschuwingen uit te sturen, bekende kwetsbaarheden te documenteren en de analyse van bedreigingen te vergemakkelijken

B **Verplichte melding van NIS-incidenten[1] (Network and Information Systems) door aanbieders van essentiële diensten[2] (AED)**

Aanbieders van essentiële diensten zijn wettelijk verplicht om cyberincidenten te melden aan het CCB. Afhankelijk van de sector waarin de getroffen onderneming actief is, kunnen ook andere meldingen vereist zijn. De tabel op pagina 19 geeft een overzicht van die verplichtingen, de meldingstermijnen en de te volgen procedure.

Vrijwillige melding

Wat?	Aan wie?	Binnen welke termijn?	Hoe?
Alle incidenten die aanzienlijke gevolgen hebben voor de continuïteit van een essentiële dienst. Deze vrijwillige melding mag er niet toe leiden dat de meldende entiteit verplichtingen worden opgelegd waaraan zij niet onderworpen zou zijn als zij die melding niet had gedaan.	Aan het CCB.	Zo vlug mogelijk.	Volgens de modaliteiten vermeld op de website van het Centrum voor Cybersecurity België (dienst CERT.be): https://cert.be/nl/een-incident-melden-form

Bron: CCB Belgium, www.ccb.belgium.be

Verplichte melding van een incident door een AED (samenvatting)

Wat?	Aan wie?	Binnen welke termijn?	Hoe?
a) Voor AED's, die niet onder het toezicht van de Nationale Bank van België "NBB" staan	a) Voor AED's, die niet onder het toezicht van de Nationale Bank van België "NBB" staan	Het incident moet **onverwijld** worden gemeld, dat wil zeggen zo vlug mogelijk.	a) Voor AED's, die niet onder het toezicht van de Nationale Bank van België "NBB" staan
Alle incidenten die gevolgen hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn.	Gelijktijdige melding van het incident aan drie autoriteiten: **1.** Het Centrum voor Cybersecurity België (CCB); **2.** Het Nationaal Crisiscentrum (NCCN); **3.** De sectorale overheid en/of haar sectorale CSIRT.	De AED moet niet wachten tot hij over alle relevante informatie over een incident beschikt om het te melden. Wanneer hij uit de informatie waarover hij beschikt kan afleiden dat het incident verplicht gemeld moet worden, moet hij dit onverwijld doen.	Het formulier op het NIS-meldingsplatform invullen: https://nis-incident.be De informatie wordt dan via het platform automatisch naar de verschillende betrokken autoriteiten gestuurd. Het platform is toegankelijk via internet door middel van een beveiligde verbinding en een voor elke aanbieder van essentiële diensten unieke identificatiesleutel. Indien het NIS-meldingsplatform niet beschikbaar is, moet de AED het incident melden volgens de modaliteiten vermeld op de website van het CCB (https://cert.be/nl/een-incident-melden-form).
b) Voor AED's die onder het toezicht van de NBB staan	b) Voor AED's die onder het toezicht van de Nationale Bank van België staan		b) Voor AED's die onder het toezicht van de Nationale Bank van België staan
Alle incidenten die **aanzienlijke gevolgen** hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn. De NBB is ermee belast deze aanzienlijke gevolgen te bepalen.	Rechtstreekse melding aan de Nationale Bank van België (NBB), volgens de door die laatste vastgestelde modaliteiten.		Rechtstreekse melding aan de Nationale Bank van België (NBB), volgens de modaliteiten vastgesteld door de NBB. Indien de NBB de AED verplicht om het meldingsplatform te gebruiken, wordt het incident ook tegelijk aan het CCB en het NCCN gemeld. Indien de NBB het gebruik van het meldingsplatform niet oplegt, bezorgt zij de melding zelf onverwijld aan het CCB en het NCCN.

Bron: CCB Belgium, www.ccb.belgium.be

C Verplichte melding van een NIS-incident voor digitaledienstverleners[1]

Digitaledienstverleners moeten ook zo snel mogelijk elk incident met een negatieve impact op de veiligheid van netwerk- en informatiesystemen melden aan het CCB, het Nationaal Crisiscentrum en de FOD Economie. In onderstaande tabel worden de verplichtingen in verband met die meldingen samengevat.

(1) Een digitaledienstverlener (DDV) is een rechtspersoon die een digitale dienst aanbiedt als bedoeld in bijlage II bij de NIS-wet, die zijn hoofdkantoor in België heeft en die geen micro- of kleine onderneming is.

Verplichte melding van een incident door een DDV (samenvatting)

Wat?	Aan wie?	Binnen welke termijn?	Hoe?
De DDV moet **alle incidenten** melden **die aanzienlijke gevolgen hebben voor de verlening van de door hem in de Europese Unie aangeboden digitale dienst(en)** (onlinemarkt- plaats, onlinezoekmachine of cloudcomputer- dienst). **Een incident** is elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen. **De beveiliging van netwerk- en informatie- systemen** is het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen.	a) **Gelijktijdige** melding van het incident aan drie autoriteiten: - **Het Centrum voor Cybersecurity België** (CCB); - **Het Nationaal Crisiscentrum** (NCCN); - **De FOD Economie (sectorale overheid)**. b) De DDV die een digitale dienst verleent aan een AED moet de betrokken AED (zijn klant) ook onverwijld alle incidenten melden die verband houden met de aan die AED verleende digitale dienst(en) en die aanzienlijke gevolgen hebben voor de continuïteit van de essentiële diensten van de betrokken AED (bij een incident moet de DDV dus al zijn klanten ondervragen die getroffen zijn door het incident en AED's zijn). Vervolgens moet de AED het incident melden volgens de meldingsprocedures voor AED's.	Het incident moet **onverwijld** worden gemeld, dat wil zeggen zo vlug mogelijk vanaf het ogenblik dat de DDV toegang heeft tot de informatie die nodig is om de gevolgen van een incident volledig of gedeeltelijk te beoordelen. De DDV moet niet wachten tot hij over alle relevante informatie over een incident beschikt om het te melden.	Het formulier op het NIS-meldingsplatform invullen: https://nis-incident.be. De DDV moet zelf bij de FOD Economie (nis- dsp@economie.fgov.be) **een login** (gebruikersnaam/ paswoord) aanvragen om toegang te krijgen tot het NIS- meldingsplatform. De informatie wordt dan via het platform **automatisch** naar de verschillende betrokken autoriteiten **gestuurd**. Het platform is **toegankelijk via internet door middel van een beveiligde verbinding en een** voor elke DDV **unieke identificatiesleutel**. Indien het NIS-meldingsplatform niet beschikbaar is, moet de DDV het incident melden volgens de modaliteiten vermeld op de website van het CCB (https://cert.be/nl/een-incident-melden- form).

Bron: CCB Belgium, www.ccb.belgium.be

Tijdens een incident houden we ons vaak bezig met de meest dringende zaken en verliezen we uit het oog dat ook in het dagelijks beheer ten aanzien van overheidsdiensten of -organen snel moet worden opgetreden. Daarom hebben we geprobeerd u via dit stappenplan enkele aanknopingspunten voor hulp en directe contactpersonen te geven om u te helpen het incident zo goed mogelijk door te komen en uw activiteit voort te zetten. Tijdens de voorbereidende vergaderingen hebben we met de verschillende betrokken autoriteiten gezocht naar praktische oplossingen, contactpunten en versoepelingen van de bestaande procedures. De hier voorgestelde oplossingen kunnen nog evolueren en verbeterd worden. Maar de eerste stappen zijn alvast gezet.

4.2.3 FOD Financiën

Wegens de talrijke en uiteenlopende fiscale verplichtingen bij de FOD Financiën en om de procedure voor ondernemingen die het slachtoffer zijn van een cyberincident te vergemakkelijken, stelt de Algemene Administratie van de Fiscaliteit, **AAFisc**, ook voor om een contactpunt voor aangiftes van melding op te richten.

- **Hoe een cyberincident melden aan de fiscale administratie?**
  In eerste instantie zal de AAFisc optreden als contactpunt en de meldingen doorgeven aan de andere betrokken belastingdiensten.
  - Voor kmo's: secr.pmekmo@minfin.fed.be
  - Voor grote ondernemingen: goge.beheer.gestion@minfin.fed.be

Op basis van de gegevens die de getroffen onderneming meedeelt, kan de AAFisc uitmaken welke fiscale verplichtingen werkelijk betrokken zijn. Daarom moeten de ondernemingen, zodra ze het cyberincident vaststellen, dat zo snel mogelijk melden aan het contactpunt van de FOD Financiën.

Volgende gegevens moeten worden meegedeeld door de wettelijke vertegenwoordiger van de onderneming of zijn gemachtigde:

- **Gegevens van de betrokken personen:**
  Bedrijfsnaam, ondernemingsnummer, contactpersoon.

- **Gegevens over de impact van het cyberincident:**
  - (Geraamde) termijn om de gegevens terug te krijgen.
  - Maakt de onderneming deel uit van een groep – een btw-eenheid?
  - Heeft de onderneming internationale uitwisselingsverplichtingen? BEPS 13 – CRS/FATCA – DAC.

- **Gegevens over de impact bij de FODFIN:**
  - Is de MyMinfin-account geblokkeerd?
  - Probleem voor het mandaat / toepassing van het mandaat?
  - Controle/bezwaar lopend bij de FODFIN?

- **Bewijs van het cyberincident:**
  Gelieve een kopie van de aangifte van het incident bij de federale politie bij te voegen.

- **Welke fiscale verplichtingen zijn betrokken?**
  Een overzicht van deze verplichtingen is te vinden via de link https://finances.belgium.be/nl/ondernemingen, dit teneinde de te contacteren fiscale administraties te kunnen bepalen.

Mogelijk neemt de AAFisc contact op met de getroffen onderneming om na te gaan of de belangrijkst geachte fiscale verplichtingen effectief in aanmerking werden genomen.

Daarna zullen de bevoegde diensten contact opnemen met de getroffen onderneming om uit te maken welke 'passende maatregelen' mogelijk zijn.

Contactadres:

secr.pmekmo@minfin.fed.be

goge.beheer.gestion@minfin.fed.be

4.2.4 RSZ

Ondernemingen zijn verplicht om een aantal aangiftes te doen bij de Rijksdienst voor Sociale Zekerheid (RSZ). Wanneer ze slachtoffer zijn van een cyberincident, kan het gebeuren dat ze die aangiftes niet kunnen doen door bijvoorbeeld verlies of onbeschikbaarheid van hun gegevens of een blokkering van hun computersysteem.

De belangrijkste verplichte aangiftes zijn:

1. **Dimona** - Onmiddellijke aangifte waarmee de werkgever de indiensttreding en uitdiensttreding van een werknemer aangeeft.

   Uiterste datum: vóór de indiensttreding.

2. **Limosa** - Kennisgeving voor gedetacheerde werknemers die tijdelijk of deeltijds in België komen werken.

   Uiterste datum: vóór de indiensttreding.

3. **DmfA** - Kwartaalaangifte waarmee de werkgever aan de RSZ arbeidsprestaties en loongegevens van zijn werknemers doorgeeft.

   Termijn: binnen een maand na het kwartaal waarop de aangifte betrekking heeft.

4. **Aangifte van werken**
   (Geldt slechts voor bepaalde sectoren).

   Uiterste datum: vóór de start van de werken.

5. **Checkinatwork** – Dagelijkse aanwezigheidsregistratie bij (bepaalde) werken in onroerende staat en activiteiten binnen de vleessector.

   Termijn: dagelijks en vóór de persoon die de werken uitvoert aan het werk gaat.

6. **Betaling van socialezekerheidsbijdragen**

   Termijn: de werkgever stort de bijdragen elk kwartaal. De RSZ moet de bijdragen uiterlijk ontvangen op de laatste dag van de maand die volgt op het kwartaal.

De RSZ beseft welke problemen ondernemingen kunnen ondervinden na een cyberincident en stelt ze daarom een procedure voor om hun situatie te melden. De melding moet gebeuren binnen 24 uur na de vaststelling van het incident. Na de melding zullen de betrokken diensten van de RSZ indien nodig contact opnemen met de ondernemingen in kwestie en aangepaste oplossingen voorstellen.

4.2.4.1 Hoe een cyberincident melden bij de RSZ?

- Via het contactformulier van de RSZ: https://www.rsz.be/contacteer-ons;
- De melding moet gebeuren door een wettelijk vertegenwoordiger van de onderneming;
- Selecteer als onderwerp: 'Cyber incident';
- Selecteer als profiel: 'Onderneming';
- Vul de velden 'Voornaam', 'Naam', 'E-mail', 'Ondernemingsnummer', 'Naam van de onderneming' in;
- Geef ook het telefoonnummer op van de persoon of de dienst binnen uw onderneming die we kunnen contacteren in verband met de melding. Bijkomende gegevens kunnen worden ingegeven in het veld 'Boodschap';
- Gelieve in het veld 'Boodschap':
  - Het incident te beschrijven;
  - Op te geven welke RSZ-verplichtingen (zie hierboven) niet langer mogelijk zijn;
  - Te melden of het beheer van de toegang tot de RSZ voor uw onderneming tijdelijk moet worden geblokkeerd (de toegang voor uw afgevaardigde(n) blijft behouden);
  - Indien mogelijk, in te schatten hoelang het incident zal duren.
- Belangrijk: voeg een kopie toe van de aangifte van het incident bij de federale politie.

4.2.4.2 Wat gebeurt er na de melding?

- U ontvangt een ontvangstbewijs;
- Uw verslag wordt intern doorgegeven aan de verschillende betrokken diensten van de RSZ. Indien nodig en afhankelijk van de concrete problemen zal de RSZ u contacteren;
- Na die melding is een bijkomende melding 'noodprocedure Dimona' niet nodig. U moet het einde van het cyberincident zodra mogelijk melden via hetzelfde contactformulier (https://www.rsz.be/contacteer-ons).

Ter herinnering en om elke soort fraude of oplichterij te vermijden, moeten werkgevers die geen provinciale of lokale overheid zijn, de verschuldigde bedragen storten op het volgende rekeningnummer van de RSZ:

IBAN-code: BE63 6790 2618 1108
BIC-code: PCHQ BEBB

Contactadres:

www.rsz.be/contacteer-ons

Die link is eveneens te gebruiken voor meldingen in verband met de RIZIV-verplichtingen.

4.2.5 RIZIV

Ondernemingen hebben ook verplichtingen tegenover verzekeringsinstellingen (ziekenfondsen) en het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering (RIZIV), opdat de betrokken werknemers kunnen worden vergoed door de verzekeringsinstellingen.

De werkgevers worden verzocht om de vereiste gegevens in te vullen in een elektronisch of papieren formulier dat, afhankelijk van het geval, zijzelf of de betrokken werknemers aan het ziekenfonds moeten bezorgen. Het gaat om de volgende formulieren:

1. Inlichtingenblad uitkeringen.
2. Verklaring betreffende de voorwaarden van verzekering.
3. Verklaring in geval van een aangepaste activiteit als loontrekkende.
4. Verklaring van toegelaten werk in een onderneming voor aangepast werk die onder paritair comité 327 valt.
5. Verklaring van uitoefening van een onbezoldigde activiteit tijdens een periode van arbeidsongeschiktheid.
6. Getuigschrift voor de toekenning van een moederschapsuitkering aan werkneemsters die van het werk werden verwijderd.
7. Maandelijkse inkomensaangifte na een maatregel van moederschapsbescherming.
8. Getuigschrift voor een uitkering voor borstvoedingspauzes .
9. Vakantieattest.
10. Getuigschrift van arbeidshervatting.
11. Getuigschrift van arbeidshervatting door de werkneemster die arbeidsdagen en verlofdagen van postnatale rust afwisselt.
12. Getuigschrift in te vullen wanneer de werkneemster alle verlofdagen van postnatale rust heeft opgenomen.

Hoe een cyberincident melden aan het RIZIV?

De meeste aangiftes verlopen elektronisch en binnen een opgelegde termijn. Maar bij sommige aangiftes worden nog papieren formulieren gebruikt.

In geval van een cyberincident waardoor de werkgever verwacht dat hij onmogelijk nog tijdig het vereiste (elektronische en/of papieren) formulier kan invullen, meldt hij het incident aan de RSZ (https://www.rsz.be/contacteer-ons) die op zijn beurt zo spoedig mogelijk het Nationaal Intermutualistisch College, de zes verzekeringsinstellingen en de Dienst voor administratieve controle van het RIZIV informeert.

De getroffen onderneming moet de volgende gegevens meedelen:

- Via het contactformulier van de RSZ: https://www.rsz.be/contacteer-ons;
- De melding moet gebeuren door een wettelijk vertegenwoordiger van de onderneming;
- Selecteer als onderwerp: 'Cyber incident'.
- Selecteer als profiel: 'Onderneming';
- Vul de velden 'Voornaam', 'Naam', 'E-mail', 'Ondernemingsnummer', 'Naam van de onderneming' in;
- Geef ook het telefoonnummer op van de persoon of de dienst binnen uw onderneming die we kunnen contacteren in verband met de melding. Bijkomende gegevens kunnen worden ingegeven in het veld 'Boodschap';
- Gelieve in het veld 'Boodschap':
  - De situatie rond het cyberincident en de gevolgen ervan te beschrijven;
  - De getroffen RIZIV-verplichtingen (zie hierboven) en de betrokken personen op te geven;
  - Indien mogelijk, in te schatten hoelang het incident zal duren;
  - De situatie rond het cyberincident en de gevolgen ervan te beschrijven.

Belangrijk: voeg een kopie toe van de aangifte van het incident bij de federale politie.

Er moet ook worden aangestipt dat, ook al moet de aangifte in principe elektronisch gebeuren, de werkgever bij een dergelijk geval van overmacht het papieren formulier kan invullen (wanneer de elektronische verzending niet langer mogelijk is).

Zodra het incident beëindigd is, meldt de werkgever dat via hetzelfde adres aan de RSZ die op zijn beurt de sector uitkeringen verwittigt.

Contactadres:

www.rsz.be/contacteer-ons

Het incident wordt gesignaleerd aan de RSZ die het op zijn beurt meldt aan het Nationaal Intermutualistisch College, de zes verzekeringsinstellingen en de Dienst voor administratieve controle van het RIZIV.

4.2.6 RVA

Ook de Rijksdienst voor Arbeidsvoorziening (RVA) voorziet in maatregelen om ondernemingen die het slachtoffer zijn van een cyberaanval te helpen hun verplichtingen na te komen.

De wettelijke verplichtingen van ondernemingen tegenover de RVA zijn:

1. **Mededeling van:**
   - De voorziene periodes van tijdelijke werkloosheid wegens gebrek aan werk omwille van economische oorzaken.
     Termijn: uiterlijk een bepaald aantal dagen voorafgaand aan de ingangsdatum van de periode van economische werkloosheid (in principe 7 dagen maar verschilt per sector).
   - De eerste effectieve werkloosheidsdag in geval van tijdelijke werkloosheid wegens slecht weer of wegens gebrek aan werk omwille van economische oorzaken.
     Termijn: de eerste effectieve schorsingsdag.
   - Tijdelijke werkloosheid wegens technische stoornis.
     Termijn: de eerste effectieve schorsingsdag.
2. **Inschrijven van nummers van controlekaarten** tijdelijke werkloosheid in een elektronisch validatieboek.
   Termijn: uiterlijk op het ogenblik waarop de controlekaart moet worden afgeleverd.
3. **Afleveren van de elektronische aangiften van sociaal risico**.
   Termijn: geen verplichte termijn, met uitzondering van het C4-formulier, dat uiterlijk de laatste arbeidsdag moet worden afgeleverd.

Hoe een cyberincident melden bij de RVA?

Een cyberincident moet u melden op het ogenblik dat u contact opneemt met de RVA om een van de verplichtingen te vervullen.

De RVA stelt voor zijn procedures te versoepelen om rekening te houden met de moeilijkheden bij de getroffen onderneming. Daarom:

1. Meldingen in het kader van tijdelijke werkloosheid moeten in principe elektronisch gebeuren, maar het reglement bepaalt dat in geval van 'technische problemen', dat kan gebeuren per aangetekende brief.
2. De inschrijving van controlekaarten is ook mogelijk in een papieren validatieschrift, of de werkgever kan de RVA contacteren om de nodige gegevens gedurende een korte periode rechtstreeks door te geven.
3. De aangiftes van sociaal risico moeten, met uitzondering van het C4-formulier, elektronisch gebeuren. Maar voor die aangiftes op zich is geen termijn opgelegd. Een aangifte op papier zou een oplossing in uitzonderlijke situaties moeten zijn.

Contactadres:

Het contactpunt voor de betrokken ondernemingen is het RVA-kantoor van de plaats waar de onderneming gevestigd is.

05

MAATREGELEN VOOR SYSTEEMHERSTEL

Een cyberaanval kan zeer uiteenlopende gevolgen hebben voor de activiteit van de getroffen onderneming (onbeschikbaarheid van diensten en digitale hulpmiddelen, gevolgen van de aanval die doorwerken bij partners enz.). De teams voor crisismanagement moeten dus het incident indammen en de werking van de organisatie op een gecontroleerde manier terug opstarten.

Het beheer van de gevolgen kan meerdere weken in beslag nemen. Het is dus belangrijk om van bij het begin een degelijke crisisorganisatie op te zetten.

5.1 MITIGEREN VAN HET INCIDENT EN CONTINUÏTEIT VAN DE ACTIVITEITEN

De getroffen ondernemingen treffen mitigerende maatregelen om te verhinderen dat de situatie verergert of om, op zijn minst, de impact ervan op de werking en diensten van de onderneming tijdig te af te zwakken.

Een cyberveiligheidsincident indijken houdt in dat u de schade beperkt en de aanvaller tegenhoudt. U moet een manier vinden om het risico voor uw organisatie te beperken en tegelijk uw activiteiten voort te zetten. U moet voorkomen dat het incident uitdijt naar andere systemen, toestellen en netwerken binnen en buiten uw organisatie.

Bij het begin van deze fase moet uw onderneming een belangrijke strategische beslissing nemen: het systeem onmiddellijk loskoppelen om dan zo snel mogelijk terug op te starten? Of de tijd nemen om bewijzen te verzamelen tegen de cybercrimineel die uw systeem heeft aangevallen?

Soms is het gewoonweg onmogelijk om (onmiddellijk) terug normaal te gaan werken. De doelstelling van de inperking moet zijn om alles in het werk te stellen voor een terugkeer naar de normale werking, dus om het systeem terug bruikbaar te maken door de toegang ervan te beperken tot de bevoegde gebruikers en de aanvaller te blokkeren.

Wanneer de perimeter van de aanval eenmaal is vastgesteld, komt het erop aan de computersystemen te beschermen tegen nieuwe aanvallen. Die nieuwe maatregelen kunnen leiden tot een ingrijpende aanpassing van de werkwijzen, onder meer op het vlak van het beheer en gebruik van digitale diensten en hulpmiddelen.

Afhankelijk van de ernst van het cyberincident gebruiken getroffen ondernemingen plannen voor bedrijfscontinuïteit om op basis van een vooraf bepaald prioriteringsproces de essentiële verrichtingen verder te kunnen uitvoeren. Zo kunnen ze om die continuïteit te verzekeren noodmaatregelen treffen om de afhandeling van kritieke transacties mogelijk te maken terwijl aan het systeemherstel wordt gewerkt, of een beroep doen op een alternatieve dienstverlener als de hoofdleverancier niet in staat is om zich binnen een redelijke termijn van het incident te herstellen.

De strategie om een cyberincident te beheren moet, in combinatie met maatregelen voor de continuïteit van de activiteit, ook voorzien in operationele oplossingen om de organisatie gedurende soms langere tijd in staat te stellen te functioneren zonder digitale hulpmiddelen.

Het einde van een cyberveiligheidsincident betekent niet dat de getroffen onderneming meteen weer operationeel is, want het kan maanden duren voor alle systemen hersteld en opnieuw geconsolideerd zijn. De crisis is pas echt afgelopen als de organisatie haar essentiële activiteiten weer zoals vroeger kan uitvoeren.

En tot slot is het na de crisis belangrijk het vertrouwen te herstellen, zowel intern bij de medewerkers, als extern, bij de klanten, leveranciers en alle stakeholders.

NUTTIGE CONTACTEN

CERT.be
The Federal Cyber Emergency Team

www.cert.be/nl/een-incident-melden

CYBER SECURITY COALITION.be

www.cybersecuritycoalition.be/tools/

.AGORIA

https://www.agoria.be/agoriaconnect-vind-uw-cybersecurity-specialist

febelfin

www.febelfin.be/nl/themas/fraude-veiligheid

CENTRE FOR CYBER SECURITY BELGIUM

https://ccb.belgium.be/nl

Safeonweb.be

www.safeonweb.be/nl/home

Safeonweb wil Belgische burgers op een snelle en correcte manier informeren en adviseren over cybersecurity, grote actuele digitale dreigingen en online veiligheid.

Een verdacht bericht ontvangen? Stuur het door naar het adres suspect@safeonweb.be en wis het daarna meteen. Een vraag over cybersecurity? Een suggestie? Wil je getuigen als slachtoffer? Stuur je vraag naar info@safeonweb.be. Een team van cyberexperts staat voor je klaar.

HET VBO

+50.000
kleine, middelgrote en grote ondernemingen

75%
van de tewerkstelling in de privésector

2/3
van de toegevoegde waarde

80%
van de export

3 gewesten
Kompas bij uitstek voor de ondernemingen in België

BUSINESSEUROPE

Het VBO is het Belgische lid van BusinessEurope

Redactie
Nathalie Ragheno

Eindredactie
Anne Michiels, Charlotte Jonné

Vertaling
Vertaaldienst VBO

Publicatieverantwoordelijke
Stefan Maes

Vormgeving
Landmarks

Fotografie
Shutterstock

Druk
Graphius

VERANTWOORDELIJKE UITGEVER
Stefan Maes,
Ravensteinstraat 4, 1000 Brussel

Publicatiedatum:
December 2022

Cette publication est également disponible en français.
This publication is also available in English.

www.vbo.be > Publicaties

Wettelijk depot D/2022/0140/9
ISBN 9789075495751

VBO FEB
Verbond van Belgische Ondernemingen
Fédération des Entreprises de Belgique

Het VBO, dé stem van de ondernemingen in België, staat – via een 50-tal lid-bedrijfs-federaties – voor meer dan 50.000 kleine, middelgrote en grote ondernemingen die 75% van de tewerkstelling in de private sector voor hun rekening nemen. Onze leden zorgen voor 80% van de export en creëren 2/3 van de toegevoegde waarde in ons land. Als enige overkoepelende interprofessionele werkgeversorganisatie vertegenwoordigen we ondernemingen uit de drie gewesten van ons land.

Lees onze recentste publicaties
op onze website

WWW.VBO.BE