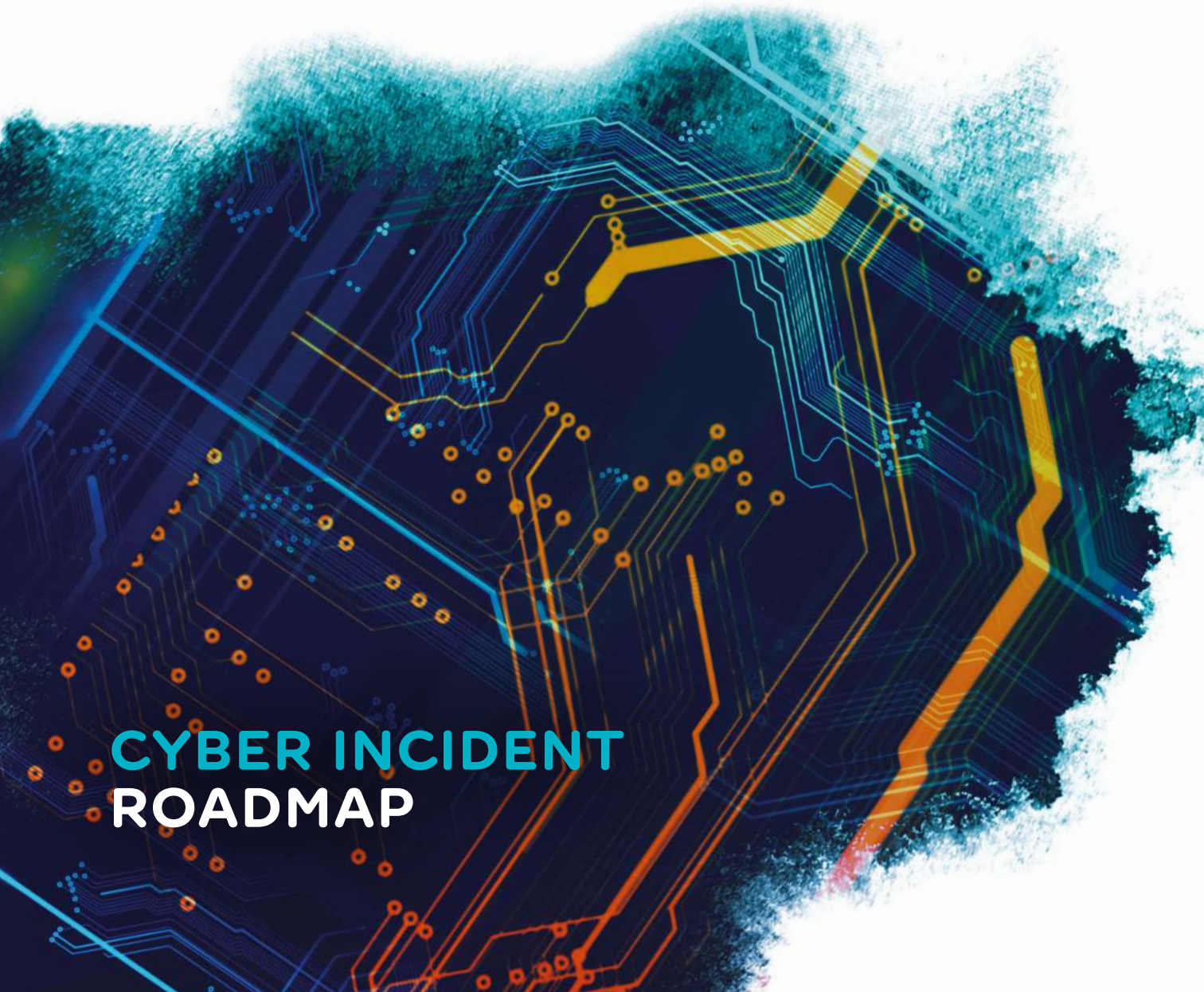
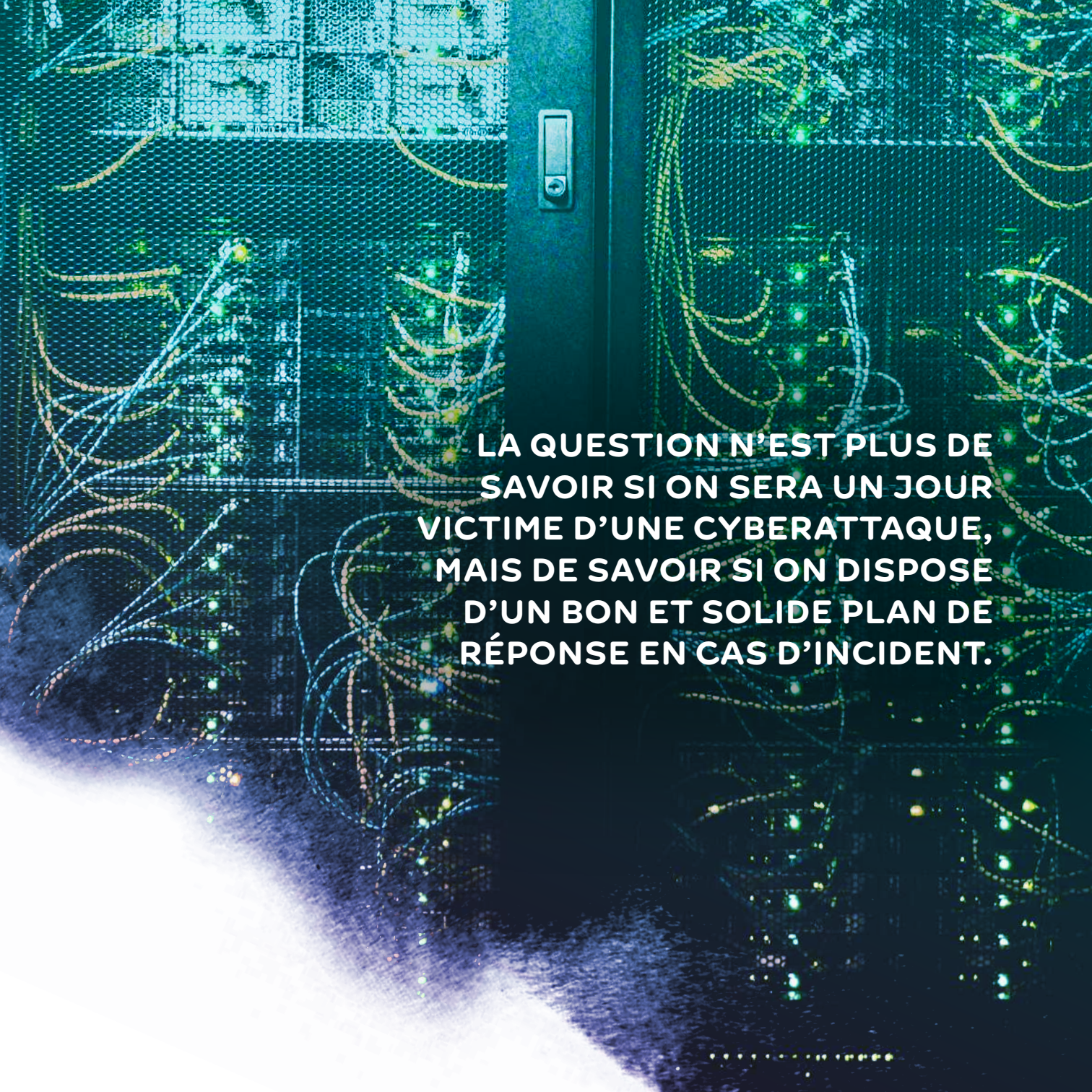
VBO FEB
Verbond van Belgische Ondernemingen
Fédération des Entreprises de Belgique



CYBER INCIDENT ROADMAP



LA QUESTION N'EST PLUS DE SAVOIR SI ON SERA UN JOUR VICTIME D'UNE CYBERATTAQUE, MAIS DE SAVOIR SI ON DISPOSE D'UN BON ET SOLIDE PLAN DE RÉPONSE EN CAS D'INCIDENT.

Le risque de cyberattaques ne cesse d'augmenter. De nombreux témoignages d'entreprises victimes de telles attaques révèlent les difficultés rencontrées lorsqu'elles surviennent mais aussi après. Les entreprises victimes sont totalement démunies ; elles doivent faire face à une situation inédite qui les prive, la plupart du temps, de tout ou partie de leur outil de travail numérique, voire de tout ou partie de leurs données essentielles pour poursuivre leurs activités et remplir leurs obligations.

L'objectif de cette roadmap est d'aider les entreprises victimes d'un cyberincident dans leur organisation en interne, mais surtout de les aider dans leur interaction avec leurs contacts externes, notamment les autorités publiques, et ce, dans le cadre de leurs obligations légales. Comment signaler un cyberincident à l'ONSS ? À l'Administration générale de la fiscalité ? Quelles démarches dois-je entreprendre à l'égard de l'ONEM pour notifier les périodes prévues de chômage temporaire dues au manque de travail pour des raisons économiques ou pour cause de « désordre technique » ?

Le premier conseil à donner est bien sûr d'éviter la cyberattaque, et donc de prendre toutes les mesures de prévention. C'est, évidemment, ce que nous espérons tous.

Plusieurs documents peuvent aider les entreprises à améliorer leur cyberrésilience, à prévenir les cyberincidents et à faire face à ceux-ci. En 2014, la FEB a collaboré, avec ICC Belgium, EY (Ernst & Young), B-CCENTRE, ISACA et Microsoft, au lancement du Belgian Cyber Security Guide[1]. Par le biais de ce guide, ces organisations entendent convaincre toutes les entreprises de l'importance de se prémunir contre les cybermenaces, en fonction de leurs besoins spécifiques. La Cyber Security Coalition[2], dont la FEB est un membre fondateur, a également publié un excellent Guide de gestion des incidents[3].

Mais la question n'est plus aujourd'hui de savoir si son entreprise sera un jour victime d'une cyberattaque, mais de savoir si l'on dispose d'un bon et solide plan de réponse en cas d'incident.

Cette roadmap vise à vous fournir un aperçu de différentes étapes de prise en charge de l'incident, depuis le repérage jusqu'à la clôture, et surtout à vous orienter, pour chacune d'entre elles, vers les différents organismes, parties prenantes et experts externes en mesure de vous aider à traverser cette épreuve, à sauvegarder vos activités et à continuer à remplir vos obligations à l'égard notamment des autorités publiques. Elle n'est pas un aboutissement, mais le reflet d'un exercice permanent et fera à ce titre l'objet de mises à jour régulières à dater de **décembre 2022**, première date de parution.

Nathalie Ragheno
Premier conseiller
au centre de compétence
Droit & Entreprise VBO FEB

Pieter Timmermans
CEO VBO FEB

(1) https://www.feb.be/publications/guide-belge-de-la-cyber-securite_2014-05-26/
(2) La Cyber Security Coalition est un partenariat unique entre des acteurs du monde universitaire, des services publics et des entreprises privées qui unissent leurs forces dans leur combat contre la cybercriminalité. À ce jour, plus de 100 acteurs clés issus de ces 3 secteurs en sont des membres actifs. Ils contribuent aux missions et objectifs de la Coalition.
(3) https://www.cybersecuritycoalition.be/fr/resource/guide-gestion-incidents/

TABLE DES MATIÈRES

01

MESURES DE PRÉVENTION

PLANIFIER AU PRÉALABLE LA GESTION DES INCIDENTS POUR PLUS DE RÉSILIENCE

Faut-il encore rappeler l'importance de mesures de prévention adéquates ainsi que d'une bonne préparation à un cyberincident ? Tous les membres du personnel doivent être informés et sensibilisés à ce risque, dont les conséquences peuvent être très lourdes en termes de réputation, d'organisation et de charges financières.

La mise en place de procédures est donc indispensable pour se préparer à un cyberincident.

Les entreprises doivent être en mesure d'y répondre pour rétablir et restaurer leurs activités, les systèmes et les données critiques affectés, bref afin de rétablir un fonctionnement normal. La planification et la préparation doivent être mises en place avant un incident et jouent un rôle important dans l'efficacité de la cyberrésilience.

02

« CYBERRÉSILIENCE », UN ÉTAT D'ESPRIT À ADOPTER

Agoria, la fédération de l'industrie technologique, dispose d'une grande expertise en matière de cybersécurité et de résilience face aux menaces. Quand on lui demande de présenter sa vision de la cyberrésilience, elle la résume par le slogan 'ABC for Executive'.

A Pour Asset management

La grande faiblesse de nombreux dirigeants ou administrateurs d'entreprise aujourd'hui est qu'ils n'ont pas toujours une vue claire des assets ou actifs informatiques à protéger. Qu'est-ce que je dois protéger en priorité ? Serveurs, données, applications… ? Pour des raisons budgétaires, vous ne pouvez sans doute pas tout protéger de la même façon. Mais savez-vous quels sont vos assets les plus cruciaux ? Cette réflexion manque souvent dans les entreprises.

B Pour Business modelling

Les dirigeants ou administrateurs d'entreprise manquent aussi parfois d'une vision schématique claire de leur business. La modélisation du business est souvent sous-estimée, elle est pourtant essentielle. Comment est structuré votre business ? Quand vous offrez une proposition de valeur à un client, sur quel service est-elle basée ? Via quelle application ? Hébergée sur quel serveur ? Quel réseau… ? Avoir cette vision schématique vous aidera beaucoup en cas de cyberattaque.

C Pour Continuité

Êtes-vous prêt ? Quel est votre plan, en cas d'attaque, pour continuer à fonctionner ? Et comment testez-vous ce plan ? Disposez-vous d'un back-up offline de vos assets prioritaires ? Avez-vous un plan de communication de crise vers l'extérieur ? C'est aussi quelque chose qui fait défaut dans de nombreuses entreprises.

Cyber Poverty Line

Le principal conseil est de ne surtout pas attendre une cyberattaque pour mettre en place un plan d'action. Il existe une « cyber poverty line », c'est-à-dire un niveau minimum d'hygiène informatique à adopter pour toute entreprise.

La cyberrésilience est un état d'esprit à adopter et une manière de travailler. Toutes les entreprises devraient régulièrement se mettre en « mode attaque », tout comme chaque entreprise doit avoir un plan d'évacuation en cas d'incendie et le tester régulièrement. C'est d'autant plus important qu'une entreprise qui ne se prépare pas à une éventuelle cyberattaque peut être vue comme une entreprise qui ne fait pas de risk management. Ce qui est évidemment désastreux pour le business mais aussi pour l'image de l'entreprise et de ses dirigeants.

Voir aussi « Nos recommandations pour assurer votre cybersécurité ».

Cliquez ici

03

LES DIFFÉRENTES ÉTAPES DE LA PRISE EN CHARGE DE L'INCIDENT

L'élaboration d'un plan de réponse constitue, pour toute entreprise ou organisation victime, une première étape importante dans la préparation et la gestion d'un incident de cybersécurité. Ce plan doit être validé par la plus haute direction, laquelle doit être impliquée dans toutes les étapes du cycle de management de l'incident. Il doit aussi être tenu à jour.

Ce plan de réponse comprend entre autres les éléments suivants :

- L'inventaire des actifs à protéger (quelles informations, quels systèmes, réseaux, produits ?) ;
- Le recensement et l'attribution des responsabilités ;
- Les capacités en interne ou les contrats conclus avec des consultants experts externes pour élaborer la réponse à l'incident et/ou l'investigation « forensic » (recherches et investigations numériques) ;
- Une stratégie de base en matière de confinement : est-il souhaitable de déconnecter immédiatement les systèmes pour une reprise la plus rapide possible ? Ou bien faut-il prendre le temps de réunir des preuves ? ;
- Une stratégie de communication à l'intention des parties prenantes internes et externes et des autorités, telles que l'Autorité de protection des données et les instances compétentes pour la notification des incidents de sécurité des réseaux et de l'information.

3.1 QUI DOIT-ON AVERTIR ?

Disposer d'une procédure et des listes de parties prenantes internes et externes à informer en fonction des scénarios et des critères identifiés, tels que la gravité de l'incident, ainsi que les notifications réglementaires et légales requises fait partie des bonnes pratiques et d'une politique de cyberrésilience de toute entreprise.

Quelles sont les parties prenantes susceptibles d'être affectées par l'incident de cybersécurité et vous incombe-t-il d'informer certaines entités telles que l'Autorité de protection des données ou d'autres autorités ?

- Parties prenantes internes : top management, cadres concernés par l'incident, employés.
- Parties prenantes externes : médias, clients, fournisseurs, autres partenaires, etc.
- Parties prenantes institutionnelles : Autorité de protection des données, autorité sectorielle, Centre pour la cybersécurité Belgique (CCB, division CERT.be), Centre national de crise, police…

3.2 QUI DOIT-ON INFORMER EN INTERNE ?

Lorsqu'une entreprise est victime d'un cyberincident, il est essentiel que les bonnes personnes en soient rapidement informées au sein de l'entreprise.

Comme tout autre risque affectant l'entreprise, la cybersécurité nécessite une stratégie claire de la part de l'organe d'administration. Celui-ci n'a pas à comprendre tous les aspects techniques, mais il n'en demeure pas moins responsable de la gouvernance des risques de cybersécurité[1]. Cela implique la prévention des risques, la sensibilisation du personnel, la conclusion éventuelle d'une assurance contre les cyberrisques… Rappelons que tant le Règlement général sur la protection des données (RGPD) que les normes relatives à la sécurité des TIC (telles que la norme ISO 27001), pour ne citer qu'elles, confient à l'organe d'administration la responsabilité générale de la sécurité informatique.

Au sein d'une entreprise, le conseil d'administration est chargé de piloter la stratégie de gestion des risques et de fixer des objectifs clairs et réalisables afin de renforcer la cyberrésilience de l'organisation. La cybersécurité est également un élément essentiel d'une bonne politique ESG.

La direction générale prend, pour sa part, les décisions nécessaires pour déployer les procédures à mettre en place pour prévenir les cyberincidents mais aussi pour gérer une situation de crise. Elle met en place un environnement organisationnel où le personnel, notamment, est encouragé à signaler ou à faire remonter jusqu'à elle les cyberincidents.

En pratique, chaque entreprise, chaque organisation devrait être dotée d'une équipe chargée de la réponse en cas d'incident, susceptible d'être convoquée dès qu'un incident survient. Bien sûr, la taille et la structure de l'équipe chargée de cette réponse dépendent de la taille de l'entreprise. Il peut aussi être plus rentable et plus efficace dans certains cas de faire appel à des partenaires externes dans le domaine de la réponse en cas d'incident de cybersécurité pour pallier le manque de compétences au sein de votre organisation.

Les petites entreprises ne disposant pas des ressources leur permettant de mettre sur pied une telle équipe peuvent cependant désigner un premier intervenant – en principe quelqu'un doté d'un pouvoir décisionnel – parmi leur personnel. En cas d'incident de cybersécurité, cette personne peut solliciter une aide externe, mais reste la personne responsable de la réponse à l'incident au sein de l'organisation.

La composition de l'équipe chargée de la réponse à l'incident sera déterminée en fonction des différentes compétences nécessaires pour gérer l'incident. Pour les petites entreprises, le premier intervenant pourra rechercher ces compétences en externe et prendre contact avec des experts qui les détiennent.

Lorsqu'un cyberincident intervient, le conseil d'administration doit donc être informé sans délai. Ensuite, il y a lieu de convoquer tous les responsables de services qui peuvent intervenir dans la gestion de la crise : IT en premier lieu, ressources humaines, département juridique, communication, département financier, et ce, en fonction de l'incident et de la procédure prévue par l'entreprise.

(1) Cette responsabilité sera encore renforcée dans le cadre de la directive NIS II.

3.3 QUI DOIT-ON INFORMER EN EXTERNE ?

3.3.1 Les experts externes

Les experts externes vous aideront à déterminer les causes de l'incident et vous fourniront des conseils sur la manière de confiner et d'éradiquer l'incident et d'empêcher qu'il se reproduise. D'autres intervenants, tels que les organismes régulateurs du secteur – par exemple la FSMA ou encore l'IBPT ou la CREG –, l'Autorité de protection des données, le Centre pour la cybersécurité Belgique (CCB), division CERT.be, et les autorités chargées de l'application de la loi (police et magistrats) peuvent apporter une aide précieuse lorsque vous êtes confrontés à un incident de cybersécurité de nature criminelle ou en cas de fuite de données à caractère personnel. Certaines législations vous obligent même à informer ces instances dès que vous détectez un incident de nature particulière (voir infra).

3.3.2 Les personnes concernées par les données : clients, fournisseurs…

Le type d'incident et son impact (possible) dicteront le type de communication requis.

Si certaines obligations auprès des clients et/ou fournisseurs ne peuvent pas être respectées, celles-ci doivent être identifiées et les personnes concernées doivent en être informées. Il est important dans ce cadre de communiquer sur la situation pour rassurer les partenaires de confiance.

En cas d'indisponibilité du système informatique, une communication peut être réalisée auprès des clients sur les règles d'utilisation des services et des outils temporaires mis en place.

Lorsque les données à caractère personnel des clients ou de fournisseurs d'une entreprise sont piratées, il est opportun de contacter au moins les clients et/ou fournisseurs concernés et de préparer, le cas échéant, un communiqué de presse. En effet, dans le cadre d'un cyberincident, si la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les personnes physiques concernées par les données volées ou perdues, le responsable de traitement tel que désigné dans le cadre de la règlementation en matière de protection des données (RGPD et loi vie privée) a l'obligation d'en informer les personnes concernées dans les meilleurs délais. Il peut le faire directement en s'adressant aux personnes impactées ou, si cela s'avère trop complexe, par l'intermédiaire des médias publics. (voir infra)

3.3.3 Les assurances

Assuralia, la fédération belge du secteur des assurances, est très active dans le développement et la promotion des assurances couvrant les cyberrisques. Les entreprises ont tout intérêt à contracter une police d'assurance couvrant les cyberrisques. Car le coût des incidents de cybersécurité peuvent se chiffrer en centaines de milliers, voire en millions d'euros. Une assurance contre les cyberrisques couvrira au moins en partie ce coût.

3.3.3.1 Services offerts par le secteur des assurances

Les services proposés par les entreprises d'assurances actives sur ce marché se répartissent en trois volets principaux :

- **Assistance des entreprises victimes de cyberincidents :** helpdesk téléphonique, assistance informatique (sécurisation des systèmes touchés, recherche des causes, remise en état, restauration des données…), services de relations publiques ou de gestion de crise…
- **Indemnisations des dommages propres à l'entreprise assurée :** prise en charge des frais permettant de conserver ou de revenir à une activité normale, des frais de reconstitution de données – réparation de données et software, indemnisations des pertes d'exploitation, voire prise en charge totale ou partielle de la rançon et des frais de cyberextorsion…
- **Indemnisations des dommages aux tiers (RC) :** indemnisation des dommages éventuels occasionnés aux clients et fournisseurs, assurance responsabilité civile contractuelle (RC professionnelle) couvrant les indemnités contractuelles, responsabilité civile extracontractuelle permettant d'indemniser par exemple des dommages liés à une fuite de données à caractère personnel, à une atteinte à la sécurité des réseaux, à la transmission de programmes malveillants…

Il convient par ailleurs de rappeler que la souscription d'un contrat d'assurance doit être préalable à la survenance du sinistre.

Remarques importantes : tous les assureurs n'offrent pas l'ensemble de ces garanties. De plus, l'octroi de celles-ci dépend du profil du client et de son secteur d'activité. Chaque contrat est établi sur la base d'une approche individuelle (« sur-mesure »).

3.3.3.2 Conditions d'accès à l'assurance (points d'attention)

La souscription d'une assurance cyberrisques est soumise à des conditions dans le chef de l'entreprise candidate à l'assurance : analyse et gestion des risques, mesures de prévention visant à diminuer les risques (publication de politiques, d'un crisis management plan, audit, tests d'intrusion…), mesures de sensibilisation et de formation du personnel.

La mise en œuvre des bonnes pratiques de sécurité est essentielle dans ce cadre : protection antivirus, firewall, mises à jour automatiques et régulières, back-up réguliers et conservés off site, méthode d'authentification à facteurs multiples, sensibilisation et trainings réguliers du personnel, etc.

D'autres conditions peuvent également être imposées par l'assureur, par exemple des (sous-)limites pour le ransomware, des coassurances avec l'assuré, etc.

3.3.3.3 Que doit faire l'entreprise assurée en cas de cyberattaque ?

L'entreprise victime d'une cyberattaque doit, si elle est assurée contre les cyberrisques, appeler en priorité le numéro du partenaire privilégié indiqué dans le volet « assistance » du contrat d'assurance, qui coordonnera toutes les opérations avec les équipes de crise et les équipes IT de l'entreprise.

Si l'entreprise n'est pas assurée spécifiquement contre les cyberrisques, il est néanmoins possible que des garanties plus générales d'assurance puissent jouer : par exemple l'assurance Protection juridique, l'assurance RC exploitation (pour les dommages aux tiers)… L'entreprise victime doit alors déclarer le sinistre dès que possible auprès de son intermédiaire d'assurance (courtier) ou de l'assureur ou des assureurs concernés.

3.4 DÉPÔT D'UNE PLAINTE AUPRÈS DE LA POLICE

La première démarche essentielle est de déposer une plainte auprès de la police contre l'auteur présumé de l'incident de cybersécurité. Ce dépôt de plainte doit être effectué auprès de la zone de police locale du siège de votre entreprise.

Depuis début 2022, à l'initiative du directeur de la Direction générale judiciaire de la police fédérale, celle-ci dispose d'un outil pour aider à l'enregistrement de ces plaintes : **CyberAid**. Il s'agit d'une plateforme accessible à tous les policiers de Belgique. 21 cyberinfractions y ont déjà été répertoriées. Sur la base de quelques questions, le policier qui acte votre plainte peut tout d'abord déterminer de quelle infraction il s'agit. Il est ensuite guidé afin d'enregistrer efficacement la plainte et dispose en outre de toute une série de conseils pratiques qu'il peut dispenser à la victime.

Cette plateforme est par ailleurs également accessible à l'ensemble des magistrats sur simple demande.

04

OBLIGATIONS LÉGALES LIÉES À L'INCIDENT

Lorsqu'une entreprise est victime d'un cyberincident, elle est confrontée à plusieurs intervenants externes auprès desquels elle devra expliquer sa situation.

Il est important dans ce cadre d'avoir pris des mesures suivantes permettant de mieux répondre à la situation :

- Conservez une copie hors ligne des documents dont vous aurez besoin en cas d'incident. Souvenez-vous que, lorsqu'un incident de cybersécurité survient, il se peut que vous n'ayez pas accès aux fichiers de votre ordinateur. Il est donc toujours opportun de conserver une copie papier/hors ligne de tout document dont vous pourriez avoir besoin pendant un incident ou une crise de cybersécurité.
- Ne reliez pas vos sauvegardes au reste de votre système. Il n'est pas seulement essentiel de les avoir à disposition ; il convient également de disposer de sauvegardes qui ne soient reliées d'aucune manière au reste de votre système. Dans le cas contraire, il existe un risque que l'infection de votre système contamine également vos sauvegardes, et les rende inutilisables.
- Documentez chaque étape de l'incident de cybersécurité. En période de crise, ne vous fiez pas uniquement à votre mémoire ! Veillez à consigner par écrit toute action entreprise, par exemple le signalement de l'incident, la collecte des preuves, les conversations avec les utilisateurs, etc.

4.1 OBLIGATIONS GÉNÉRALES

Une fois établie la liste des destinataires de votre communication sur l'incident de cybersécurité et la teneur des informations que vous leur révélerez, il vous reste à décider du moment opportun pour les contacter. Ce moment est déterminé en fonction des objectifs de communication :

- Certaines parties prenantes auront besoin d'informations le plus tôt possible, car elles peuvent contribuer à confiner l'incident (par exemple, la haute direction et les employés de l'entreprise) ;
- D'autres parties prenantes devront être contactées dans un délai imposé par la loi (par exemple, l'Autorité de protection des données) ;
- D'autres parties prenantes pourront entrer en contact avec vous, auquel cas vos réponses doivent être prêtes (par exemple, les médias). Gardez à l'esprit que, pour ne pas alerter le cybercriminel que vous êtes sur ses traces, il peut s'avérer nécessaire de prévoir une phase de silence (sans aucune communication) entre le moment où l'incident est détecté et le moment où vous aurez une vue d'ensemble complète de l'incident et disposerez d'un plan d'action ;
- En outre, le signalement aux autorités judiciaires est indispensable afin de disposer d'une preuve qu'un incident est effectivement survenu (voir supra). C'est le document de dépôt de plainte qui sera exigé par les administrations pour prendre en considération vos déclarations.

L'incident de cybersécurité auquel vous êtes confrontés peut ne pas être un cas isolé et les autorités compétentes disposent peut-être d'informations vous permettant de confiner plus rapidement l'incident.

La communication aux autorités de répression compétentes doit être faite le plus tôt possible après la découverte de l'incident de cybersécurité, étant donné la volatilité des traces et les actions à mettre en œuvre (identification Internet, etc.).

Les autorités judiciaires ont besoin de toutes les informations disponibles concernant l'incident pour procéder à la qualification de l'infraction et à l'identification du suspect. Les informations à communiquer à la police en cas de fraude sur Internet (une infraction « conventionnelle » commise par des moyens électroniques) pourront différer en partie de celles dont la police aura besoin en cas de crime informatique (piratage, sabotage, espionnage). Au cours de l'enquête, les enquêteurs réclameront, collecteront et rechercheront des informations complémentaires.

4.2 OBLIGATIONS À L'ÉGARD DES PARTIES PRENANTES INSTITUTIONNELLES

4.2.1 APD

Une fuite de données, c'est-à-dire une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, le vol, la divulgation,… non autorisée de données à caractère personnel doit être notifiée à l'Autorité de protection des données (APD) en vertu des dispositions du RGPD. Il s'agit d'une obligation légale dont le non-respect peut être lourdement sanctionné.

Le responsable du traitement doit faire cette notification à l'APD dans un délai de 72 heures au plus tard après en avoir pris connaissance.

La notification d'une fuite de données n'est pas obligatoire lorsque la fuite de données ne présente probablement pas un risque pour les droits et libertés des personnes.

Tel sera par exemple le cas lorsqu'il s'agit de données qui appartiennent déjà au domaine public ou de données qui sont suffisamment cryptées et que le responsable du traitement dispose d'un backup de ces données.

Dans tous les autres cas, la notification d'une fuite de données à l'APD se fait au moyen d'un formulaire électronique qui, après avoir été complété, est transmis via un portail Internet. Les formulaires simplement transmis par e-mail ne seront pas traités.

Le formulaire doit être complété dans une des trois langues nationales. Les annexes techniques au formulaire de demande peuvent également être rédigées en anglais, en plus des trois langues nationales

https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles

https://www.autoriteprotectiondonnees.be/publications/mode-d-emploi-relatif-a-l-utilisation-de-formulaires-electroniques.pdf

Sauf exception, lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable de traitement a l'obligation d'en informer la personne dans les meilleurs délais.

Lorsque l'identification de victimes de la fuite de données est impossible, le responsable du traitement peut les informer par l'intermédiaire des médias publics. La notification aux personnes concernées doit être claire et facile à comprendre.

L'Autorité de protection des données recommande de fournir au minimum les informations suivantes :

- Le nom du responsable du traitement des données ;
- Les coordonnées de contact pour informations complémentaires ;
- Une description succincte de l'incident ayant donné lieu à la fuite de données ;
- La date (présumée) de l'incident ;
- Le type et la nature des données à caractère personnel en cause ;
- Les conséquences possibles de la fuite des données pour les personnes concernées ;
- Les circonstances dans lesquelles la fuite des données s'est produite ;
- Les mesures prises par le responsable du traitement pour prévenir la fuite des données ;
- Les mesures recommandées par le responsable du traitement aux personnes concernées pour limiter le préjudice.

4.2.2 CERT.be

A Notification volontaire par une entreprise victime d'un cyberincident

Une notification volontaire d'un incident auprès de CERT.be (ou Cyber Emergency Response Team, le service opérationnel du Centre pour la cybersécurité Belgique) par une entreprise non soumise aux obligations légales en la matière ne signifie pas une demande d'intervention. La réponse par e-mail d'un opérateur de CERT.be n'est pas garantie et dépend de la gravité de l'incident et du statut de l'entreprise qui notifie. Le CCB fournit des conseils techniques et organisationnels accessibles via ses sites web (https://www.cert.be/fr/conseils) pour maîtriser un cyberincident, mais il n'assiste pas les entreprises dans la mise en œuvre des opérations nécessaires.

(1) NIS : législation relative à la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.
(2) OSE : Opérateur de services essentiels, une entité publique ou privée active en Belgique dans les secteurs suivants : énergie, transports, finances, santé, eau potable et infrastructures numériques.

Signaler vos incidents aide le CCB à collecter, analyser, alerter et agir sur des menaces confirmées. Le contenu des signalements est extrait et analysé automatiquement pour consolider de la connaissance qui, par la suite, permet de fournir des avertissements et alertes, documenter les vulnérabilités connues et faciliter l'analyse de la menace.

B Notification obligatoire d'un incident NIS[1] (Network and Information Systems) pour les Opérateurs de services essentiels[2] (OSE)

Les Opérateurs de services essentiels sont soumis à une obligation légale de notification des cyberincidents auprès du CCB. D'autres notifications peuvent également être obligatoires en fonction du secteur d'activité de l'entreprise victime. Le tableau page 19 reprend en synthèse ces obligations, les délais de notification ainsi que la procédure à suivre.

Notification volontaire

Quoi ?	À qui ?	Dans quel délai ?	Comment ?
Tous les incidents ayant un impact significatif sur la continuité d'un service essentiel. Cette notification volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine de la notification des obligations auxquelles elle n'aurait pas été soumise si elle n'avait pas procédé à ladite notification.	Au CCB.	Dans les meilleurs délais.	Via les modalités prévues sur le site du Centre pour la cybersécurité Belgique (service CERT.be) : https://cert.be/fr/signaler-un-incident

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

Notification obligatoire d'un incident NIS par un OSE (résumé)

Quoi ?	À qui ?	Dans quel délai ?	Comment ?
a) Pour les OSE, sauf ceux supervisés par la BNB	a) Pour les OSE, sauf ceux supervisés par la BNB	Notification de l'incident **sans retard**, c'est-à-dire le plus rapidement possible. L'OSE ne doit pas attendre de disposer de toutes les informations pertinentes sur un incident pour procéder à la notification. Lorsque les informations en sa possession lui permettent de savoir qu'il s'agit d'un incident soumis à notification, il doit le faire sans attendre.	a) Pour tous les OSE, sauf ceux supervisés par la BNB
Tous les incidents ayant un impact sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les service(s) essentiel(s) qu'il fournit.	Notification simultanée de l'incident à trois autorités : **1.** le Centre Cybersécurité (CCB) ; pour la Belgique **2.** le Centre de Crise national (NCCN) ; **3.** l'autorité sectorielle et/ou le CSIRT sectoriel.		Compléter le formulaire disponible sur la plate- forme de notification NIS : https://nis-incident.be La plate-forme assure alors l'envoi automatique des informations aux différentes autorités concernées. La plate-forme est accessible par le biais d'internet au moyen d'une connexion sécurisée et l'utilisation d'une clé d'identification unique à chaque opérateur de services essentiels. En cas d'indisponibilité de la plate-forme de notification NIS, l'OSE doit notifier l'incident via les modalités reprises sur le site du CCB (https://cert.be/fr/signaler-un-incident).
b) Pour les OSE supervisés par la BNB	b) Pour les OSE supervisés par la BNB		b) Pour les OSE supervisés par la BNB
Tous les incidents ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit. La BNB est chargée de déterminer cet impact significatif.	Notification directe à la BNB, selon les modalités fixées par celle-ci.		Notification directe à la BNB, selon les modalités fixées par celle-ci. Si la BNB impose à l'OSE d'utiliser la plate-forme de notification, la notification est simultanément aussi faite au CCB et au NCCN. Si la BNB n'impose pas l'utilisation de la plate- forme de notification, la BNB transmettra elle- même la notification, sans retard, au CCB et au NCCN.

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

C Notification obligatoire d'un incident NIS pour les Fournisseurs de service numérique[1]

Les Fournisseurs de service numérique doivent également notifier, le plus rapidement possible, tout incident ayant un impact négatif sur la sécurité des réseaux et des systèmes d'information auprès du CCB, du Centre de Crise national et au SPF Économie. Le tableau ci-dessous résume les obligations liées.

(1) Un fournisseur de service numérique (FSN) est une personne morale qui fournit un service numérique visé à l'annexe II de la loi NIS, qui a son siège principal en Belgique et qui n'est pas une micro ou petite entreprise.

Notification obligatoire d'un incident NIS par un FSN (résumé)

Quoi ?	À qui ?	Dans quel délai ?	Comment ?
Le FSN doit notifier **tout incident ayant un impact significatif sur la fourniture du ou des service(s) numérique(s)** (place de marché en ligne ou moteur de recherche en ligne ou service d'informatique en nuage) **qu'il offre dans l'Union européenne**. Un incident est tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information. **La sécurité des réseaux et des systèmes d'information** correspond à la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.	a) Notification **simultanée** de l'incident à trois autorités : - **Le Centre pour la cybersécurité Belgique** (CCB) ; - **Le Centre de Crise national** (NCCN) ; - **Le SPF Économie (l'autorité sectorielle)**. b) **Le FSN qui fournit un service numérique à un OSE doit également notifier**, sans retard, à l'OSE concerné (son client) tous les incidents liés au(x) service(s) numérique(s) fourni(s) à cet OSE et qui ont un impact significatif sur la continuité des services essentiels de l'OSE concerné (en cas d'incident, le FSN se doit donc d'interroger tous ses clients impactés par l'incident et qui seraient OSE). **L'OSE doit notifier ensuite** l'incident, selon les procédures de notification prévues pour les OSE.	Notification de l'incident **sans retard**, c'est-à-dire le plus rapidement possible à partir du moment où le FSN a accès aux informations nécessaires pour évaluer, complètement ou partiellement, l'impact d'un incident. Le FSN ne doit pas attendre de disposer de toutes les informations pertinentes sur un incident pour procéder à la notification.	Compléter le formulaire disponible sur la plate-forme de notification NIS : https://nis-incident.be Le FSN doit demander d'initiative au SPF Economie (nis-dsp@economie.fgov.be) la **création d'un login** (nom d'utilisateur/mot de passe) pour accéder à la plate-forme de notification NIS. La plate-forme assure alors **l'envoi automatique** des informations aux différentes autorités concernées. La plate-forme est **accessible par le biais d'internet au moyen d'une connexion sécurisée et l'utilisation d'une clé d'identification unique** à chaque FSN. En cas d'indisponibilité de la plate-forme de notification NIS, le FSN doit notifier l'incident via les modalités reprises sur le site du CCB (https://cert.be/fr/signaler-un-incident).

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

Pendant un incident, on pare souvent au plus pressé, et on perd un peu de vue que des actions rapides doivent être entreprises, dans le cadre de la gestion quotidienne, à l'égard d'administrations ou d'organismes publics. C'est pourquoi nous avons tenté, au travers de cette roadmap, de vous donner des pistes d'aide et de contacts directs pour vous aider à traverser cet événement tout en poursuivant le mieux possible votre activité. Lors des réunions en vue de son élaboration, nous avons cherché avec les différentes autorités concernées des solutions pratiques, des points de contact et des assouplissements des procédures existantes. Les solutions proposées ici peuvent encore évoluer, être améliorées. Mais un premier pont est jeté.

4.2.3 SPF Finances

En raison des nombreuses et diverses obligations fiscales existant au sein du SPF Finances et afin de faciliter la procédure pour les entreprises victimes d'un cyberincident, l'Administration générale de la fiscalité, **AGFisc**, propose également de mettre en place un point de contact des déclarations de signalement.

- **Comment signaler un cyberincident à l'administration fiscale ?**
  AGFisc sera dans un premier temps ce point de contact et relayera les signalements auprès des autres administrations fiscales concernées.
  - Pour les PME : secr.pmekmo@minfin.fed.be
  - Pour les grandes entreprises : goge.beheer.gestion@minfin.fed.be

Sur base des informations communiquées par l'entreprise victime, l'AGFisc pourra déterminer les obligations fiscales réellement impactées. À cette fin, les entreprises victimes veilleront à signaler le plus rapidement possible le cyberincident au point de contact du SPF Finances après sa découverte.

Les informations reprises ci-après devront être communiquées par le représentant légal de l'entreprise ou son mandataire :

- **Coordonnées des personnes concernées :**
  Nom de l'entreprise, numéro d'entreprise, données de la personne de contact.

- **Informations sur l'impact du cyberincident :**
  - Délai (estimé) de récupération des données.
  - L'entreprise fait-elle partie d'un groupe – d'une unité TVA ?
  - L'entreprise a-t-elle des obligations d'échange international ? BEPS 13 – CRS/FATCA - DAC.

- **Informations sur l'impact des données au sein du SPFFIN :**
  - Le compte MyMinfin est-il bloqué ?
  - Problème pour le mandat/application du mandat ?
  - Contrôle/réclamation en cours au sein du SPFFIN ?

- **Preuve du cyberincident :**
  Joindre une copie de la déclaration de l'incident auprès de la police fédérale.

- **Quelles sont les obligations fiscales concernées ?**
  ous pouvez consulter l'aperçu de ces obligations via le lien https://finances.belgium.be/fr/entreprises afin de pouvoir préciser les administrations fiscales à contacter.

L'AGFisc prendra éventuellement contact avec l'entreprise victime afin de s'assurer que les obligations fiscales (jugées) prioritaires soient effectivement prises en compte.

L'entreprise victime sera ensuite contactée par les services compétents afin que soient envisagées des mesures « d'aménagement » possibles.

Adresses de contact :

secr.pmekmo@minfin.fed.be

goge.beheer.gestion@minfin.fed.be

4.2.4 ONSS

Les entreprises sont soumises à une série de déclarations à l'égard de l'Office national de sécurité sociale (ONSS). Lorsqu'elles sont victimes d'un cyberincident, elles peuvent être dans l'impossibilité de faire ces déclarations suite à la perte ou à l'indisponibilité de leurs données ou au blocage de leur système informatique, par exemple.

Les principales obligations de déclarations sont les suivantes :

1. **Dimona** - La déclaration immédiate d'embauche, par laquelle un employeur signale le début et la fin d'une relation de travail avec un employé.

   Date limite : avant l'embauche.

2. **Limosa** - Notification pour les travailleurs détachés qui viennent travailler en Belgique de manière temporaire ou partielle.

   Date limite : avant l'embauche.

3. **DmfA** - La déclaration trimestrielle par laquelle l'employeur communique à l'ONSS les données relatives aux salaires et aux performances des employés.

   Délai : dans le mois qui suit le trimestre auquel la déclaration se rapporte.

4. **Déclaration de travaux**
   (Ne concerne que certains secteurs).

   Date limite : avant le début des travaux.

5. **Checkinatwork** – Enregistrement de la présence quotidienne à (certains) travaux dans l'immobilier et les activités appartenant au secteur de la viande.

   Délai : tous les jours avant le début des travaux de la personne qui les effectue.

6. **Paiement des cotisations de sécurité sociale**

   Délai : l'employeur verse les cotisations trimestriellement. Ces contributions doivent parvenir à l'ONSS au plus tard le dernier jour du mois suivant le trimestre.

L'ONSS, conscient des difficultés que peuvent rencontrer les entreprises victimes de cyberincidents, propose à celles-ci une procédure de signalement de leur situation. Ce signalement doit avoir lieu dans les 24 heures suivant la découverte de l'incident. À la suite de ce signalement, les services concernés de l'ONSS prendront contact, si nécessaire, avec les entreprises concernées et proposeront des solutions adaptées à la situation.

4.2.4.1 Comment signaler un cyberincident à l'ONSS ?

- Via le formulaire de contact de l'ONSS : https://www.onss.be/contactez-nous ;
- La notification doit être effectuée par un représentant légal de l'entreprise ;
- Sélectionnez comme sujet : « report cyberincident » ;
- Sélectionnez comme profil : « entreprise » ;
- Remplissez les champs « prénom », « nom », « e-mail », « numéro d'entreprise », « nom de l'entreprise » ;
- Indiquez également le numéro de téléphone de la personne ou du service de votre entreprise que nous pouvons contacter au sujet de cette notification. Des coordonnées supplémentaires peuvent être saisies dans le champ « Message » ;
- Dans le champ « Message », veuillez :
  - Donner une description de l'incident ;
  - Préciser quelles obligations envers l'ONSS (voir plus haut) ne sont plus possibles ;
  - Dire si la gestion de l'accès à l'ONSS pour votre entreprise doit être temporairement bloquée (les accès pour votre/vos mandataire(s) seront maintenus) ;
  - Si possible, donner la durée estimée de l'incident.
- Important : Joindre une copie de la déclaration de l'incident auprès de la police fédérale.

4.2.4.2 Que se passe-t-il après la notification ?

- Vous recevrez un accusé de réception ;
- Votre rapport sera transmis en interne aux différents services concernés de l'ONSS. Si nécessaire et en fonction des problèmes concrets, l'ONSS vous contactera ;
- Après cette notification, une notification supplémentaire « procédure d'urgence Dimona » n'est pas nécessaire. La fin du cyberincident doit être signalée dès que possible via le même formulaire de contact (https://www.onss.be/contactez-nous).

Pour rappel et pour éviter tout type de fraude ou d'arnaque, les employeurs qui ne sont pas des autorités provinciales ou locales doivent verser les montants dus sur le numéro de compte ONSS suivant :

Code IBAN : BE63 6790 2618 1108
Code BIC : PCHQ BEBB

Adresse de contact :

www.onss.be/contactez-nous

Ce lien est également à utiliser pour les notifications relatives aux obligations INAMI

4.2.5 INAMI

Les entreprises ont également des obligations à l'égard des organismes assureurs (mutualités d'affiliations) et de l'Institut national d'assurance maladie-invalidité (INAMI), et ce, afin que les travailleurs concernés puissent être indemnisés par les organismes assureurs.

Les employeurs sont invités à remplir les informations requises dans un formulaire électronique ou papier que, selon le cas, eux-mêmes ou les travailleurs concernés doivent remettre à l'organisme assureur. Il s'agit principalement des situations suivantes :

1. Feuille de renseignements indemnités.
2. Attestation relative aux conditions d'assurance.
3. Déclaration en cas d'activité adaptée comme travailleur salarié.
4. Déclaration d'un travail autorisé dans une entreprise de travail adapté relevant de la commission paritaire 327.
5. Déclaration d'une activité non rémunérée pendant une période d'incapacité de travail.
6. Attestation pour l'octroi d'une indemnité de maternité à la travailleuse écartée du travail.
7. Déclaration mensuelle des revenus à la suite d'une mesure de protection de la maternité.
8. Attestation pour l'indemnisation des pauses d'allaitement.
9. Attestation de vacances.
10. Attestation de reprise du travail.
11. Attestation de reprise du travail par la travailleuse qui alterne jours de travail et jours de congé de repos postnatal.
12. Attestation à compléter lorsque la travailleuse a pris tous les jours de congé de repos postnatal.

Comment signaler un cyberincident à l'INAMI ?

La plupart de ces déclarations se font par voie électronique et dans un délai imparti. Néanmoins, certaines déclarations sont encore réalisées au moyen de formulaires papier.

En cas de cyberincident qui rend impossible pour l'employeur d'espérer pouvoir remplir à temps le formulaire requis (électronique et/ou papier), l'employeur signale cet incident à l'ONSS (https://www.onss.be/contactez-nous) qui, à son tour, en informe le Collège Iintermutualiste National (National Intermutual Board), les six organismes assureurs et le Service de contrôle administratif de l'INAMI, et ce, dans les plus brefs délais.

L'entreprise victime doit communiquer les informations suivantes :

- Via le formulaire de contact de l'ONSS : https://www.onss.be/contactez-nous ;
- La notification doit être effectuée par un représentant légal de l'entreprise ;
- Sélectionnez comme sujet : « report cyberincident »
- Sélectionnez comme profil : « entreprise » ;
- Remplissez les champs « prénom », « nom », « e-mail », « numéro d'entreprise », « nom de l'entreprise » ;
- Indiquez également le numéro de téléphone de la personne ou du service de votre entreprise que nous pouvons contacter au sujet de cette notification. Des coordonnées supplémentaires peuvent être saisies dans le champ « Message ».
- Dans le champ « Message », veuillez :
  - Donner une description de la situation liée au cyberincident et de ses conséquences de l'incident ;
  - Préciser quelles obligations envers l'INAMI (voir plus haut) sont concernées et les personnes concernées ;
  - Si possible, donner la durée estimée de l'incident ;
  - Donner une description de la situation liée au cyberincident et de ses conséquences.

Important : Joindre une copie de la déclaration de l'incident auprès de la police fédérale.

Il convient également de préciser que si la déclaration doit être faite en principe par voie électronique, l'employeur peut remplir le formulaire papier en cas de force majeure (si la transmission électronique n'est plus possible).

Une fois l'incident terminé, l'employeur en informe l'ONSS via la même adresse, qui à son tour informe le secteur des indemnités.

Adresse de contact :

www.onss.be/contactez-nous

L'incident est signalé via l'ONSS qui, à son tour, en informe le National Intermutual Board, les six institutions d'assurance et le département de contrôle administratif de l'INAMI

4.2.6 ONEM

L'Office national de l'emploi (ONEM) a, lui aussi, mis en place des mesures permettant aux entreprises victimes de cyberattaques de remplir leurs obligations.

Les obligations légales des entreprises à l'égard de l'ONEM sont les suivantes :

1. **Notification** :
   - Des périodes de chômage temporaire prévues en raison du manque de travail pour des raisons économiques.
     Délai : au plus tard un certain nombre de jours avant la date effective de la période de chômage économique (en principe 7 jours mais variable selon le secteur).
   - Du premier jour effectif de chômage en cas de chômage temporaire dû à des intempéries ou à un manque de travail pour des raisons économiques.
     Délai : le premier jour effectif de suspension
   - De chômage temporaire pour cause de désordre technique.
     Délai : le premier jour effectif de suspension.
2. **Inscription des numéros de carte de contrôle** du chômage temporaire dans un livre de validation électronique.
   Délai : au plus tard au moment où la carte de contrôle doit être délivrée.
3. **Remise des déclarations électroniques de risque social**.
   Délai : pas de délai obligatoire, à l'exception du formulaire C4 qui doit être livré au plus tard le dernier jour ouvrable.

Comment signaler un cyberincident à l'ONEM ?

En cas de cyberincident, celui-ci doit être déclaré au moment de la prise de contact avec l'ONEM pour remplir une des obligations.

L'ONEM propose d'assouplir ses procédures pour tenir compte des difficultés de l'entreprise victime.
Pour ce faire :

1. Les notifications dans le cadre du chômage temporaire doivent en principe être effectuées obligatoirement par voie électronique mais la réglementation prévoit qu'en cas « de problèmes techniques », cela peut se faire par lettre recommandée.
2. L'enregistrement des cartes de contrôle peut également se faire dans un carnet de validation papier, ou l'employeur peut contacter l'ONEM pour lui transférer directement les données nécessaires pendant une courte période.
3. Les déclarations de risques sociaux, à l'exception du formulaire C4, doivent être effectuées par voie électronique. Toutefois, ces dernières ne sont pas soumises à un délai en soi. La déclaration sur papier devrait être une solution dans des situations exceptionnelles, et ce, pour éviter des retards. En effet, les institutions de paiement ne peuvent traiter les informations qu'électroniquement.

Adresse de contact :

Le point de contact pour les entreprises concernées est le bureau du chômage du lieu où se trouve l'entreprise.

05

MESURES DE RESTAURATION DU SYSTÈME

Une cyberattaque peut avoir des effets très variés sur l'activité de l'entreprise victime (indisponibilité des services et outils numériques, impacts de l'attaque étendus à des partenaires, etc.). Il convient donc, pour les équipes de gestion de crise, d'endiguer l'incident et de relancer de manière maîtrisée le fonctionnement de l'organisation.

La gestion des impacts peut s'étaler sur plusieurs semaines. Il est donc important de mettre en place dès le début une solide organisation de crise.

5.1 ATTÉNUATION DE L'INCIDENT ET CONTINUITÉ DES ACTIVITÉS

Les entreprises victimes mettent en place des mesures d'atténuation pour empêcher l'aggravation de la situation ou, à tout le moins, atténuer leur impact sur les opérations et les services de l'entreprise, et ce, en temps utile.

Confiner un incident de cybersécurité, c'est limiter les dommages et stopper l'assaillant. Vous devez trouver un moyen de limiter le risque pour votre organisation tout en continuant d'exercer vos activités. Il vous faut prévenir la propagation de l'incident à d'autres systèmes, dispositifs et réseaux au sein de votre organisation et au-delà.

Au début de cette phase, votre entreprise devra prendre une décision stratégique importante : faut-il déconnecter le système immédiatement pour une reprise la plus rapide possible ? Ou faut-il prendre le temps de réunir des preuves contre le cybercriminel qui s'est attaqué au système ?

Dans certains cas, le retour (immédiat) à une activité normale sera tout simplement impossible. L'objectif du confinement doit être de tout mettre en œuvre pour un retour au fonctionnement normal, c'est-à-dire pour retrouver un système utilisable en préservant l'accès pour les utilisateurs légitimes et en bloquant l'assaillant.

Une fois le périmètre de l'attaque identifié, il s'agit de protéger les systèmes informatiques contre de nouvelles attaques. Ces nouvelles mesures peuvent entraîner une modification importante des pratiques, notamment d'administration, ainsi que dans l'utilisation des services et des outils numériques.

En fonction de la gravité du cyberincident, les entreprises victimes ont recours à des **plans de continuité des activités** pour pouvoir, sur la base d'un processus de hiérarchisation prédéfini, maintenir les opérations essentielles. Ainsi, pour garantir cette continuité, elles peuvent décider de mesures d'urgence pour faciliter le traitement des transactions critiques pendant que les efforts de restauration du système se poursuivent, ou de faire appel à un fournisseur de services alternatif si le fournisseur principal n'est pas en mesure de se remettre de l'incident dans un délai raisonnable.

La stratégie de gestion d'un cyberincident, adossée aux dispositifs de continuité d'activité, doit aussi prévoir des solutions opérationnelles permettant de **maintenir sur une durée parfois très longue le fonctionnement de l'organisation sans outils numériques**.

La fin d'un incident de cybersécurité ne signifie pas que l'entreprise victime retrouve dès cet instant un fonctionnement opérationnel, puisque **la reconstruction et la reconsolidation de l'ensemble des systèmes peuvent prendre plusieurs mois**. La sortie de crise s'envisage au contraire lorsque les activités essentielles de l'organisation peuvent reprendre de manière habituelle.

Enfin, lorsque la crise est passée, il est important de **restaurer la confiance** tant en interne, auprès des collaborateurs, qu'en externe, chez les clients, les fournisseurs et l'ensemble des parties prenantes.

SITES WEB UTILES

CERT.be
The Federal Cyber Emergency Team

www.cert.be/fr/signaler-un-incident

CYBER SECURITY COALITION.be

www.cybersecuritycoalition.be/tools/

.AGORIA

www.agoria.be/agoriaconnect-trouvez-votre-specialiste-en-cybersecurite

febelfin

www.febelfin.be/fr/themes/fraude-et-securite

CENTRE FOR CYBER SECURITY BELGIUM

www.ccb.belgium.be/fr

Safeonweb.be

www.safeonweb.be/fr/home

Safeonweb.be a pour ambition d'informer rapidement et efficacement les citoyens belges en matière de sécurité informatique, des plus récentes et plus importantes menaces numériques et de sécurité sur Internet.

Vous avez reçu un message suspect ? Envoyez-le à l'adresse suspect@safeonweb.be et supprimez-le ensuite. Avez-vous une question sur la cybersécurité ? Avez-vous une suggestion ? Voulez-vous témoigner en tant que victime ? Envoyez votre question à info@safeonweb.be. Une équipe de cyber-experts répondra à votre question.

LA FEB

+50.000

petites, moyennes et grandes entreprises

75%

de l'emploi dans le secteur privé

2/3

de la valeur ajoutée

80%

des exportations

3 Régions

Boussole par excellence pour les entreprises en Belgique

BUSINESSEUROPE

La FEB est le membre belge de BusinessEurope

Coordination et rédaction finale
Nathalie Ragheno

Secrétariat de rédaction
Anne Michiels, Charlotte Jonné

Traduction
Service de traduction FEB

Responsable des publications
Stefan Maes

Mise en page
Landmarks

Illustrations
Shutterstock

Impression
Graphius

Éditeur responsable
Stefan Maes,
rue Ravenstein 4, 1000 Bruxelles

Date de publication :
Décembre 2022

Deze publicatie is ook beschikbaar in het Nederlands.
This publication is also available in English.

www.feb.be > Publications

Dépôt légal D/2022/0140/8
ISBN 9789075495744

VBO FEB
Verbond van Belgische Ondernemingen
Fédération des Entreprises de Belgique

Porte-parole des entreprises de Belgique, la FEB représente – au travers d'une quarantaine de fédérations sectorielles membres – plus de 50.000 petites, moyennes et grandes entreprises. Ensemble, elles assurent 75% de l'emploi dans le secteur privé, 80% des exportations et 2/3 de la valeur ajoutée créée en Belgique.
Seule coupole d'employeurs au niveau interprofessionnel, la FEB représente les entreprises des trois Régions du pays.

Retrouvez nos dernières publications
sur notre site web

WWW.FEB.BE