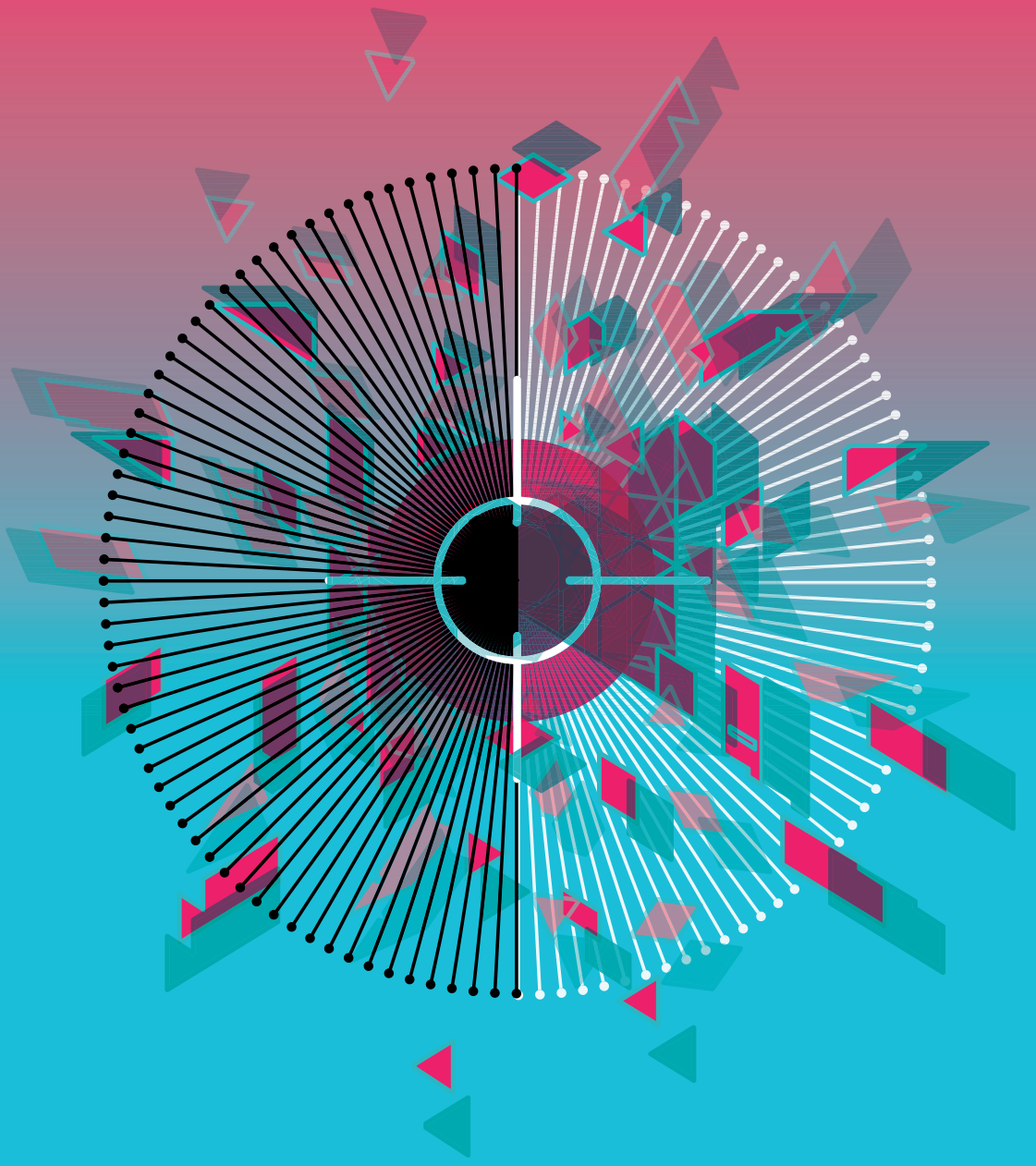
CENTRE FOR
CYBER SECURITY
BELGIUM

CYBER SECURITY
COALITION.be

CYBERSÉCURITÉ
GUIDE DE GESTION DES INCIDENTS

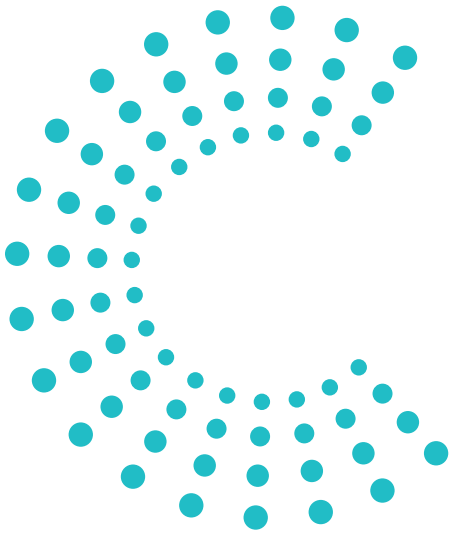


À PROPOS

La Cyber Security Coalition est un partenariat unique associant les acteurs du monde universitaire, les autorités publiques et le secteur privé qui mettent leurs forces en commun pour lutter contre la cybercriminalité. Actuellement, plus de 100 acteurs incontournables issus de ces 3 secteurs sont des membres actifs contribuant à la mission et aux objectifs de la Coalition.

La Coalition entend apporter une réponse au besoin urgent de développer la collaboration intersectorielle afin de mutualiser les connaissances et les expériences, d'initier, d'organiser et de coordonner des initiatives transversales concrètes, de **sensibiliser les citoyens et les entreprises**, de mettre en avant l'acquisition d'une expertise et de formuler des recommandations visant à renforcer l'efficacité des politiques et des réglementations.

Ce guide entend attirer l'attention des entreprises de toutes tailles sur l'importance de planifier au préalable la manière de gérer un incident de cybersécurité.



RÉSUMÉ

L' objectif de ce guide est d'attirer l'attention sur l'importance de planifier au préalable la gestion des incidents de cybersécurité.

Il ne s'agit pas d'un processus linéaire, mais d'un cycle comportant une **préparation**, une **détection et un confinement de l'incident, d'atténuation et de reprise**. La phase ultime consiste à tirer les enseignements de l'incident en vue d'améliorer le processus et de **se préparer pour les incidents futurs**. Pendant ce cycle, la **communication** avec les parties prenantes internes et externes revêt une importance capitale.

Nombreuses sont les organisations qui ne possèdent pas l'expertise et les compétences nécessaires en interne pour réagir de façon appropriée en cas d'incident de cybersécurité. Lorsqu'elles sont confrontées à un incident, ces organisations peuvent avoir besoin de **faire appel à des experts** en vue de confiner l'incident et/ou de mener une investigation forensic, ce qui ne signifie pas qu'elles ne peuvent rien faire à leur niveau. Au contraire, beaucoup de choses peuvent et doivent être faites en amont, avant qu'un incident ne survienne.

L'élaboration d'un **plan de réponse de l'organisation en cas d'incident de cybersécurité** constitue une première étape importante dans la gestion de ces incidents. En outre, il est primordial que ce plan soit **validé par la haute direction**, laquelle doit être impliquée à toutes les étapes du cycle de management de l'incident de cybersécurité.
Le plan de réponse en cas d'incident de cybersécurité comprendra 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;
- **l'équipement** et la **technologie**;
- 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.

Les fournisseurs de services essentiels et les fournisseurs de services numériques tels que décrits dans la Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information du 7 avril 2019, sont soumis à des obligations spécifiques en matière de sécurité de leurs systèmes d'information et la protection contre les incidents ainsi que leur notification. L'information contenue dans ce guide peut aider à prendre les bonnes mesures pour satisfaire à ces conditions.

Enfin, les organisations doivent envisager de contracter une police d'assurance couvrant les cyber-risques. Il n'est pas rare que le coût des incidents de cybersécurité se chiffre en centaines de milliers, voire en millions d'euros. Une assurance sérieuse contre les cyber-risques couvrira au moins en partie ce coût.

TABLE DES MATIÈRES

AVANT-PROPOS

Il n'y a que deux sortes d'entreprises : celles qui ont été attaquées et celles qui le seront.

Robert Mueller

Internet révolutionne notre manière de conduire notre activité : la quantité de données transférées sur Internet et notre dépendance envers leur disponibilité ne cessent d'augmenter. De toute évidence, si le monde connecté offre de belles opportunités, il génère également de nouveaux risques. La cybercriminalité est une entreprise de grande envergure et même la plus petite attaque malveillante peut porter gravement atteinte à la réputation d'une organisation, à sa productivité, à son système informatique, etc.

Aucune organisation ne saurait se considérer à l'abri de la cybercriminalité. La cible des cybercriminels ne se limite pas aux grandes organisations. Au contraire, une petite organisation peut s'avérer être une victime de choix, en raison des informations en sa possession ou des partenaires avec qui elle travaille.

Ce guide veut souligner l'importance de savoir qu'un jour ou l'autre votre organisation peut être la cible d'une cyberattaque. Et lorsque cela se produit, il vaut mieux être prêt ! Un plan de réponse en cas d'incident de cybersécurité digne de ce nom doit faire la distinction entre un incident de cybersécurité et une crise de cybersécurité. La rapidité à laquelle l'organisation est capable de repérer et d'analyser un incident, et d'y réagir, aura une influence sur le préjudice subi et sur le coût de la reprise.

Le plan de réponse en cas d'incident de cybersécurité ne saurait se limiter à la technologie ! Les processus, les personnes et d'autres aspects organisationnels sont tout aussi importants.

La lecture de ce guide ne fera pas instantanément de vous un expert en gestion des incidents de cybersécurité. Pourquoi ? La raison est simple : pour acquérir l'expertise nécessaire afin de gérer efficacement de tels incidents, il faut du temps. Alors ne perdez pas de vue que l'apprentissage passe bien souvent par un processus d'essais et d'erreurs.

Jan De Blauwe
Président de la Cyber Security Coalition

Miguel De Bruycker
Directeur du Centre pour la Cybersécurité Belgique (CCB)

PRINCIPES DE BASE & DÉFINITIONS ESSENTIELLES

Pendant la lecture de ce Guide de gestion des incidents de cybersécurité, vous devez à tout moment garder à l'esprit les principes de base et les définitions essentielles suivantes :

DÉFINITIONS ESSENTIELLES

Vous trouverez un glossaire complet à la fin de ce guide, et nous proposons ci-après un certain nombre de définitions essentielles pour comprendre la portée et le contenu de ce guide.

ÉVÉNEMENT DE CYBERSÉCURITÉ
Un changement de cybersécurité susceptible d'avoir un impact sur les opérations d'une organisation (y compris sa mission, ses capacités ou sa réputation).

INCIDENT DE CYBERSÉCURITÉ
Un événement ou une série d'événements de cybersécurité indésirables ou inattendus risquant de compromettre les opérations de l'organisation.

GESTION DES INCIDENTS DE CYBERSÉCURITÉ
Les processus visant à se préparer, à détecter, à rendre compte, à évaluer, à réagir, à prendre en charge et à tirer les enseignements des incidents de cybersécurité.

1.

Il n'existe aucune solution simple et universelle

Chaque organisation est différente, gardez bien cela à l'esprit. S'agissant de cybersécurité, **la solution universelle n'existe pas**. Ce qui fonctionnera pour votre organisation dépendra de sa mission et de ses objectifs, de la nature de l'infrastructure et des informations que vous protégez, des ressources disponibles, etc. Enfin, sachez que certaines techniques ne pourront être assimilées qu'avec **le temps et l'expérience**. Cela ne doit toutefois pas vous empêcher de vous lancer !

2.

Engagement de la haute direction

Les incidents de cybersécurité représentent un risque qui doit être intégré à la politique globale de gestion des risques de votre organisation. En outre, gérer les incidents de cybersécurité ne se limite pas à apporter une réponse technologique. Cela suppose également l'élaboration d'un plan qui doit être intégré aux processus et structures organisationnelles existants, de sorte à stimuler les fonctions critiques de l'entreprise, et non à les freiner. Par conséquent, la haute direction doit **s'impliquer activement** afin de définir le plan de prévention et de réponse de l'organisation en cas d'incident de cybersécurité, car le soutien explicite de la haute direction grâce à une communication interne appropriée et **l'affectation de personnel et de ressources financières** sont la clé du succès de ce plan. Un haut dirigeant bien informé sera conscient des risques de cybercriminalité et du **rôle exemplaire qu'il doit jouer** pour inciter tous les membres de l'organisation à assumer leurs responsabilités.

3.

Impliquer tous les membres de votre organisation

On considère souvent que le facteur humain est le maillon faible en matière de cybersécurité. Ceci étant dit, il faut également souligner que les membres de votre organisation offrent un réel potentiel pour vous aider à détecter et à identifier les incidents de cybersécurité. Veillez à ce que chaque membre de votre organisation ait **connaissance de votre plan de réponse en cas d'incident de cybersécurité et du rôle qui lui est attribué**, même si cela se limite à devoir informer la bonne personne des anomalies informatiques constatées.

4.

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.

5.

Ne reliez pas vos sauvegardes au reste de votre système

En matière de sauvegardes, il n'est pas seulement essentiel de les avoir à disposition ; il convient également de disposer d'une **sauvegarde qui ne soit reliée 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.

6.

Importance du log et de la conservation des journaux pendant une certaine durée (jusqu'à 6 mois)

Les journaux peuvent vous aider à retracer l'origine de l'incident de cybersécurité. Ils sont importants, non seulement pour pouvoir identifier le cybercriminel, mais également pour que votre organisation puisse reprendre le cours de ses activités le plus tôt possible.

7.

Tenez à jour votre plan de réponse en cas d'incident de cybersécurité ainsi que toutes les informations et tous les documents associés

8.

Lors de la gestion d'un incident de cybersécurité, veillez à prendre en compte tous les aspects juridiques

Les preuves ne seront recevables devant un tribunal que si elles ont été collectées dans le strict respect des lois et réglementations en vigueur. En outre, vous avez dans certains cas une obligation de notification aux autorités, à la personne concernée et/ou de l'Autorité de protection des données pour la notification des incidents de sécurité de l'information ou de réseau.

9.

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, les propriétaires du système et autres acteurs, etc. Cette documentation est votre « machine à remonter le temps ». Lorsque quelque chose tourne mal, elle vous permettra peut-être de revenir en arrière et de déterminer à quel moment le problème a émergé et pour quelle raison. En outre, en documentant la réponse à l'incident de cybersécurité, vous éviterez que toute l'information et la masse de connaissances concernant l'événement ne soient connues que de quelques personnes.

01 SE PRÉPARER EN VUE D'UN INCIDENT DE CYBERSÉCURITÉ

I. ÉLABORER UN PLAN DE RÉPONSE EN CAS D'INCIDENT DE CYBERSÉCURITÉ ET L'ACTUALISER RÉGULIÈREMENT

Confrontée à un incident de cybersécurité, l'organisation doit être capable de réagir rapidement et de manière appropriée. C'est pourquoi il est primordial de décider au préalable comment gérer certaines situations plutôt que d'attendre d'y être confronté pour la première fois lors d'un incident. Vous devez élaborer un plan (sur papier, pas seulement dans votre tête) visant à limiter les dommages, à réduire les coûts et le délai de la reprise et à communiquer avec les parties prenantes internes et externes.

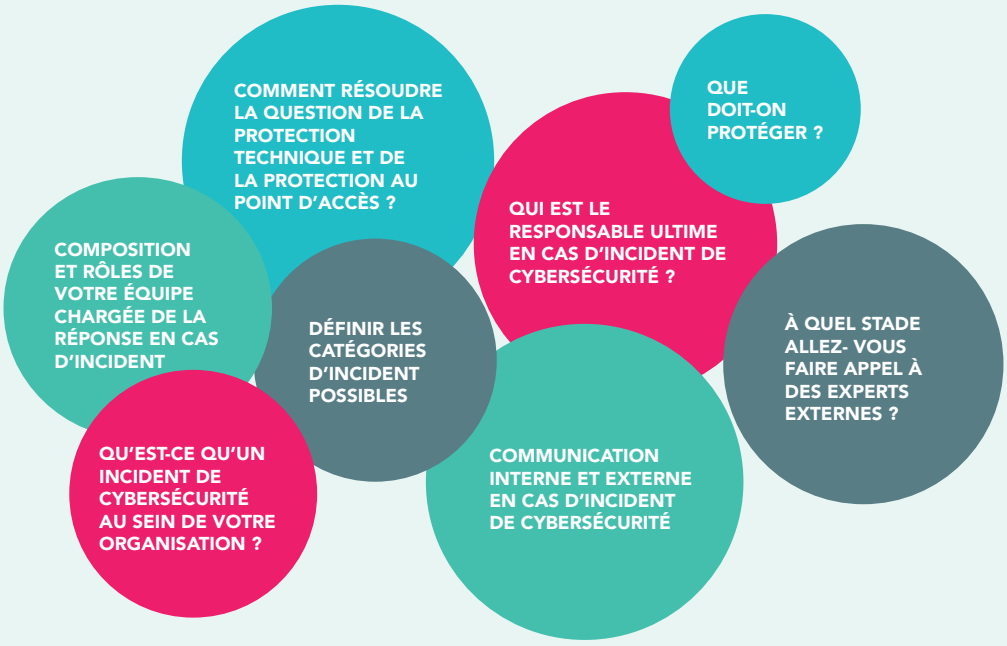
RÉEXAMINEZ RÉGULIÈREMENT VOTRE PLAN DE RÉPONSE EN CAS D'INCIDENT DE CYBERSÉCURITÉ

Un plan de réponse en cas d'incident de cybersécurité n'est pas un document figé. Il est primordial de l'intégrer à vos processus d'entreprise et de le réexaminer et l'actualiser régulièrement, tous les ans et dans le cadre du bilan post-incident.

PROCÉDURES DE RÉPONSE EN CAS D'INCIDENT DE CYBERSÉCURITÉ

Sur la base de votre plan de réponse en cas d'incident de cybersécurité, vous pourrez définir un certain nombre de procédures opérationnelles standard pour les incidents fréquents dont la probabilité au sein de votre organisation est avérée. Ces procédures doivent expliquer pas à pas comment un problème spécifique peut être abordé. Ces guides de réponse rapide pour des scénarios probables doivent être accessibles facilement.

PRINCIPAUX ÉLÉMENTS DU PLAN DE RÉPONSE EN CAS D'INCIDENT DE CYBERSÉCURITÉ



II. CONTENU DU PLAN DE RÉPONSE EN CAS D'INCIDENT DE CYBERSÉCURITÉ

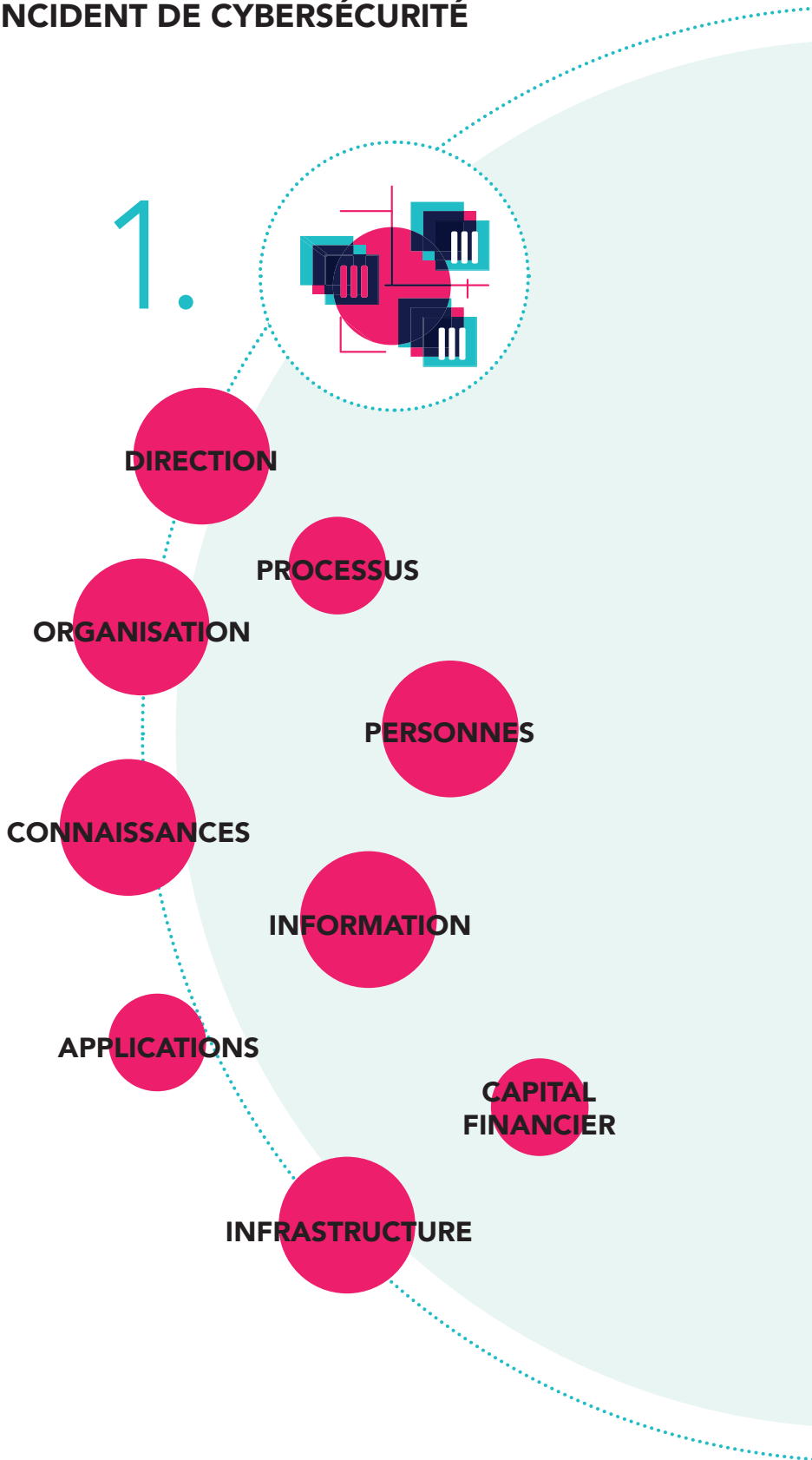
SAVOIR QUOI PROTÉGER

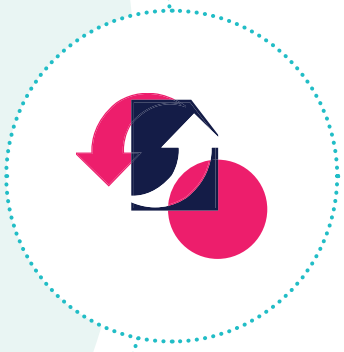
Recensez vos actifs et les menaces potentielles

Lorsqu'un incident survient, les premières questions qui se posent sont : quels sont les actifs en danger ? Et parmi ces actifs, lesquels sont vitaux pour l'activité de votre entreprise ? Vous devrez déterminer quels sont les actifs qui nécessitent votre attention en priorité afin de maintenir l'activité et de limiter au maximum le préjudice pour votre entreprise.

C'est pourquoi il est crucial de **recenser, de documenter et de catégoriser les « organes vitaux » de votre organisation** : les actifs dont votre organisation dépend pour mener ses activités de base. Cela vous permettra de déterminer quelles sont les mesures de protection à prendre et où les appliquer, et de prendre des décisions rapides et justifiées pendant la gestion de l'incident.

Voici une liste qui vous permettra de vous faire une idée quant à la nature de ces « organes vitaux » : la direction, l'organisation, les processus, les connaissances (par ex. en cas de vol de propriété intellectuelle), les personnes, l'information (par ex. vol ou détérioration d'ensembles de données), les applications (par ex. site Internet en panne ou dégradé), l'infrastructure (par ex. panne de système et/ou des connexions au réseau), le capital financier (par ex. les comptes bancaires). Il est également recommandé d'identifier les points faibles et les menaces potentielles.





2. Comment recenser, documenter et catégoriser les éléments essentiels de votre organisation, ses points faibles et les menaces potentielles ?

A. Identifiez l'activité et les ressources à protéger

- Déterminez quelles sont les activités de base qui permettent à votre organisation d'exister, d'atteindre ses objectifs d'entreprise et de générer des revenus : la production de biens, la vente de biens, le livraison de biens, etc.
- Pour chacune de ces activités, déterminez quels sont les systèmes informatiques (bases de données, applications, systèmes de commande) et les connexions réseau qui assurent leur bon fonctionnement.
- Déterminez également où sont hébergés ces systèmes informatiques : sur vos propres serveurs ou dans le cloud.
- Lors du recensement de ces actifs, n'oubliez pas les flux d'information à destination des tiers (fournisseurs, clients, etc.) ni les flux des systèmes de commande industriels.

B. Déterminez quelles sont vos ressources les plus précieuses

Il vous faut maintenant déterminer quels sont les actifs, les données, les processus ou les connexions réseau si importants pour votre organisation que leur perte (ou la perte de leur contrôle) vous plongerait dans de graves problèmes, voire vous conduirait à cesser toute activité.

C. Décidez des priorités de votre activité pour la reprise

La liste de ces priorités vous permettra de déterminer dans quel ordre les systèmes devront être rétablis. Le plus souvent, le réseau sous-jacent sera la priorité absolue, car il constitue tout à la fois le moyen d'atteindre vos actifs pour vos administrateurs système et le moyen utilisé par les cybercriminels pour attaquer vos systèmes. Tant que les cybercriminels peuvent utiliser vos connexions réseau, toute activité de reprise pourra être défaite par eux. Lorsque vos actifs bénéficient tous du même niveau de priorité, il peut être envisagé de conduire les activités de reprise en parallèle.

D. Documentez le mode de fonctionnement de vos systèmes et actualisez cette documentation

Veillez à ce que le mode de fonctionnement de vos systèmes soit documenté et que cette information soit actualisée régulièrement et accessible dans les systèmes de documentation de l'équipe chargée de la réponse en cas d'incident. En particulier, les documents suivants sont indispensables :

Schéma du réseau présentant l'architecture du réseau et sa segmentation interne ainsi que les différentes passerelles vers les réseaux externes, DMZ, VPN, et les ranges d'adresses IP utilisées. Ce schéma doit également inclure les différents dispositifs de sécurité en place susceptibles d'abriter les données de log de l'activité du réseau [pare-feu, serveurs proxy (reverse), systèmes de détection d'intrusion, systèmes de gestion des incidents]. Pour les grandes entreprises dotées de réseaux complexes, il est également nécessaire de disposer d'une version de haut niveau de l'architecture du réseau, afin que quiconque puisse avoir un aperçu du réseau en cas d'urgence.

Inventaire de l'équipement et des services. Cet inventaire inclura, pour les actifs vitaux au sein de votre environnement, les différents serveurs et composants du réseau utilisés pour mettre en œuvre les différents services de l'entreprise. Étant donné que certains de ces serveurs (physiques) peuvent être affectés à des fonctions multiples, il est primordial de savoir quels sont les services exécutés sur chaque serveur.

Listes de comptes et d'accès. À tout moment, il est important de savoir qui a le droit d'accéder au réseau et aux différents systèmes hébergés, de les utiliser ou de les gérer. Cela vous aidera à détecter tout compte étrange ou détourné pendant un incident.

Vos systèmes ne doivent pas être à vos yeux un simple amas de câbles et d'ordinateurs ! Il est primordial que l'administrateur de votre système connaisse son fonctionnement et soit capable de l'expliquer aux experts, à la police, etc.

III. ATTRIBUER LES RESPONSABILITÉS ET CRÉER UNE ÉQUIPE CHARGÉE DE CONDUIRE LA RÉPONSE EN CAS D'INCIDENT DE CYBERSÉCURITÉ

ATTRIBUER DES RESPONSABILITÉS ET DES RÔLES AUX PERSONNES POSSÉDANT LES COMPÉTENCES ADÉQUATES

Il est important que les rôles et les responsabilités en cas d'incident de cybersécurité soient documentés dans votre plan de réponse en cas d'incident de cybersécurité. Pour rédiger le descriptif de ces rôles et responsabilités, vous devez vous poser les questions suivantes :

1. Qui est le référent interne pour les incidents de cybersécurité ? Comment peut-il être contacté ?
2. Quelles sont les différentes tâches à exécuter pour mettre en œuvre la réponse en cas d'incident ? Et qui fait quoi ?
3. Qui doit gérer l'incident sur le plan métier/technique ? Il doit s'agir d'un membre de votre entreprise détenant un pouvoir de décision et qui suivra l'incident du début à la fin.
4. Qui se chargera de la liaison avec la direction générale ?
5. Qui est habilité à engager un partenaire externe spécialiste de la réponse en cas d'incident ?
6. Qui peut déposer une plainte auprès des autorités/informer les instances de réglementation ?
7. Qui est habilité à communiquer avec la presse et les parties prenantes externes ?

Vous réaliserez que, pour bien gérer un incident de cybersécurité, différentes compétences sont nécessaires pour assumer les différentes responsabilités et les différents rôles qui permettront une réponse efficace à l'incident.

COMPÉTENCES	RESPONSABILITÉS	RÔLES
Gestion de l'incident	Gestion de l'incident de cybersécurité depuis le moment où il est détecté jusqu'à sa clôture.	Responsable de la réponse en cas d'incident de cybercriminalité
Capacité décisionnelle dans l'entreprise	Évaluer l'impact pour l'activité et prendre des mesures appropriées. Faire intervenir les bonnes ressources. Prendre des décisions quant à la façon de procéder, par ex. en décidant si la connexion Internet du système attaqué peut être coupée et quel est le moment le plus approprié pour le faire. Décider à quel moment commencer les activités de nettoyage. Décider du dépôt d'une plainte ou non.	Gestion
Capacités de gestion du réseau	Savoir-faire technique concernant le réseau de l'organisation (pare-feu, proxys, systèmes de prévention d'intrusion, routeurs, switchs, etc.). Analyser, bloquer ou restreindre les flux de données entrant et sortant sur votre réseau. Opérations informatiques, sécurité de l'information et continuité de l'activité	Personnel d'assistance technique informatique
Capacités d'administrateur postes de travail et serveur (droits d'administrateur)	Analyser et gérer les postes de travail et les serveurs touchés.	Personnel d'assistance technique informatique
Conseil juridique	Évaluer l'impact contractuel et juridique d'un incident. Garantir que les activités de réponse à l'incident respectent les exigences légales et réglementaires ainsi que les stratégies de l'organisation. Dépôt de plainte.	Service juridique/avocat de l'entreprise
Aptitudes à la communication	Communiquer avec tous les groupes de parties prenantes de manière appropriée. Répondre immédiatement aux questions des clients, des actionnaires et de la presse.	Service communication ou relations publiques
Compétences en science forensic	Collecter et analyser des preuves de manière appropriée, c'est-à-dire de sorte à obtenir des preuves recevables par un tribunal.	Personnel d'assistance technique informatique
Sécurité physique	Gérer tous les aspects de l'incident associés à • l'accès physique aux locaux ; • la protection physique de l'infrastructure informatique.	Responsable de la sécurité
Gestion de crise	Gestion de crise	Gestion de crise

ÉQUIPE CHARGÉE DE CONDUIRE LA RÉPONSE EN CAS D'INCIDENT DE CYBERSÉCURITÉ

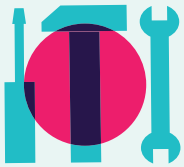
Idéalement, chaque organisation devrait être dotée d'une équipe chargée de la réponse en cas d'incident qui serait convoquée dès qu'un incident survient. Bien sûr, la taille et la structure de l'équipe chargée de la réponse en cas d'incident dépend de la taille de l'entreprise. Les petites entreprises ne disposant pas des ressources leur permettant de mettre sur pied une telle équipe peuvent cependant désigner un premier intervenant – idéalement quelqu'un doté d'un pouvoir décisionnel – parmi leur personnel. En cas d'incident de cybersécurité, cette personne doit solliciter une aide externe, mais reste la personne responsable de la réponse à l'incident au sein de l'organisation.

La composition de cette équipe chargée de la réponse à l'incident sera déterminée en fonction des différentes compétences nécessaires pour gérer un incident (voir également le tableau de la page 11). Pour les petites entreprises, le premier intervenant pourra rechercher ces compétences en externe et prendre contact avec des experts qui les détiennent.

UNE ÉQUIPE MINIMALE CHARGÉE DE LA RÉPONSE EN CAS D'INCIDENT DOIT RASSEMBLER LES RÔLES SUIVANTS :

RESPONSABLE DE LA RÉPONSE EN CAS D'INCIDENT

Il s'agit de la personne qui gérera l'incident dès qu'elle en aura connaissance et jusqu'à ce que l'incident soit confiné et réglé. Elle travaillera en liaison avec la direction, et au besoin avec d'autres membres du personnel en interne et des ressources externes pour gérer l'incident. Cette personne doit bien connaître les activités de votre organisation, car elle sera la première à prendre des décisions touchant l'entreprise.



PERSONNEL D'ASSISTANCE TECHNIQUE INFORMATIQUE

Cette personne doit également bien connaître votre infrastructure informatique, car elle sera chargée de rechercher des indicateurs, de confirmer l'incident et de mettre au point des solutions techniques pour le gérer.

C'EST LA TAILLE ET LA NATURE DE VOTRE ORGANISATION QUI DICTERONT LA NÉCESSITÉ D'ATTRIBUER DES RÔLES SUPPLÉMENTAIRES

Les organisations de petite taille ont souvent la souplesse nécessaire pour remonter rapidement l'information vers la direction afin de gérer l'incident. Ce n'est pas le cas des organisations importantes qui peuvent être confrontées à plusieurs incidents à gérer simultanément avec plus d'autonomie, les dirigeants n'étant sollicités pour les actions de réponse qu'en cas d'incident très grave.

Grandes organisations. Plus votre organisation est grande, plus la composition de votre équipe chargée de la réponse devra être variée. Pour les grandes organisations, en plus de l'équipe chargée de la réponse, une équipe de gestion de crise composée de représentants de la direction de l'entreprise peut être constituée pour prendre la responsabilité des décisions stratégiques et liées à l'activité ainsi que des communications lorsqu'elles sont confrontées à des incidents graves. Cela permettra au responsable de la réponse en cas d'incident de centrer ses efforts en priorité sur les aspects techniques de l'incident.

CERTAINES ORGANISATIONS DOIVENT DÉSIGNER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES OU UN POINT DE CONTACT

En vertu du règlement général sur la protection des données (RGPD), certaines organisations sont tenues de désigner un délégué à la protection des données (également appelé « DPD »). Plus précisément, cela s'applique aux organisations qui sont chargées du traitement de données à caractère personnel et qui nécessitent une observation régulière et systématique des personnes concernées à grande échelle. Il en va de même si le responsable du traitement des données est chargé du traitement à grande échelle de catégories particulières de données, par exemple des données relatives à la santé (ou des condamnations pénales et des infractions).

La loi sur la sécurité des réseaux et des systèmes d'information (NIS), impose aux fournisseurs de services essentiels (FSE) et aux fournisseurs de services numériques (FSN) de désigner un point de contact pour la sécurité des réseaux et des systèmes d'information afin de permettre une communication fluide avec les autorités compétentes en cas d'incidents.

IV. FAIRE APPEL À DES EXPERTS EXTERNES

EXPERTS EN MATIÈRE DE RÉPONSE EN CAS D'INCIDENT DE CYBERSÉCURITÉ

Que votre organisation soit une PME ou une grande entreprise, acquérir et actualiser l'expertise et les compétences nécessaires pour conduire en interne la réponse en cas d'incident peut s'avérer très coûteux. Ceci est vrai en particulier pour les compétences spécifiques en matière légale et d'investigation forensic dans le domaine de la cybersécurité. Il peut donc être plus rentable et plus efficace 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.

- Ces spécialistes de la réponse en cas d'incident, grâce à leur connaissance des menaces potentielles et des scénarios possibles, peuvent vous permettre de réduire le **délai** nécessaire pour établir un diagnostic de l'incident.
- Ils ont une approche scientifique forensic rigoureuse qui permet de recueillir et de documenter des preuves en reconstituant une chaîne de responsabilités **juridiquement recevable**. Ces preuves pourront ensuite être présentées devant un tribunal, le cas échéant.
- Leur expérience leur permet de procéder dans le bon ordre et ils maîtrisent les **outils** permettant de rechercher des traces dans la mémoire RAM, les machines virtuelles, les disques durs et les réseaux.
- Ces experts 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.

À QUEL MOMENT CONTACTER UN EXPERT ?

A. PENDANT LA PHASE DE PRÉPARATION

OU

B. LORSQU'UN INCIDENT DE CYBERSÉCURITÉ SURVIENT

Vous pouvez conclure un contrat avec un partenaire spécialiste de la réponse en cas d'incident de cybersécurité dès la phase de préparation, ou bien attendre qu'un incident de cybersécurité survienne. N'oubliez pas que l'établissement d'un tel contrat suppose du temps et du travail. Aussi, si vous savez à l'avance qu'une aide externe sera indispensable, il est sans doute préférable de ne pas attendre. Vous gagnerez ainsi un temps précieux au début de l'incident de cybersécurité. De nombreux cabinets de consultants spécialisés en services de réponse en cas d'incident et autres cabinets juridiques proposent des formules d'abonnement permettant de maintenir leurs capacités en alerte pour leurs abonnés. En outre, ils proposent pour la plupart des sessions de formation avec votre équipe chargée de la réponse en cas d'incident, afin de faciliter la coopération entre eux lorsqu'un incident survient.

LES AUTORITÉS PEUVENT VOUS AIDER DANS VOTRE ENQUÊTE

D'autres intervenants, tels que les organismes régulateurs du secteur, 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 également page 31, Signalement aux autorités).

Ces instances peuvent souvent fournir des informations sur la menace et des directives pratiques fondées sur des incidents antérieurs qu'elles ont eu à gérer. N'oubliez pas que l'objectif des autorités est d'identifier et d'interpeller l'auteur de l'attaque. La reprise et le retour à l'activité normale de votre entreprise ne sont pas de leur ressort. Il est possible que le moyen le plus efficace d'interpeller l'auteur ne soit pas le plus rapide pour reprendre une activité normale.

Par ailleurs, la plupart de ces enquêtes sont protégées par le secret professionnel, ce qui rend difficile l'obtention d'informations sur leurs résultats. Ces autorités peuvent cependant divulguer certaines informations qui vous aideront à identifier l'auteur de l'attaque et son mode opératoire, ce qui peut accélérer l'analyse de votre incident de cybersécurité.

La police peut demander à votre entreprise de ne pas couper le système immédiatement. Si vous le faites, l'auteur de l'attaque le remarquera et se retirera, ce qui rend souvent infructueuse toute tentative ultérieure de retrouver sa trace. Pour votre organisation, le moyen le plus rapide de reprendre son activité peut être de couper immédiatement le système et redémarrer après avoir fait table rase.

V. ÉQUIPER VOTRE ENTREPRISE EN VUE DE GÉRER UN INCIDENT DE CYBERSÉCURITÉ

VOTRE RÉSEAU D'EXPERTS – ÉTABLIR UNE LISTE DE CONTACTS

Demander de l'aide aux bons professionnels et au bon moment est crucial pendant un incident, car cela peut contribuer à limiter les dommages physiques et l'atteinte à la réputation de votre entreprise. Une liste de contacts reprenant toutes les personnes ou organisations vous aidera dans cette démarche. Cette liste doit contenir les noms, les rôles, les coordonnées et backups des différents personnes de l'équipe chargée de la réponse en cas d'incident, des intervenants externes en alerte, des autorités, etc.
Les coordonnées reprises doivent comprendre les numéros de téléphone fixe et mobile, les adresses électroniques professionnelles (y compris les clés de chiffrement public pour la confidentialité et l'intégrité des communications) et les adresses physiques pour l'envoi conventionnel de courrier et de colis. Veillez également à obtenir des coordonnées de contact alternatives (seconde adresse électronique, numéros de fax), car il est possible que l'équipe chargée de la réponse en cas d'incident ne puisse pas utiliser le réseau interne pendant l'incident.

Ces coordonnées doivent être conservées et accessibles en un lieu central, hors ligne, tel qu'un classeur physique ou un ordinateur non connecté au réseau. En plus de ces données de contact « brutes », ces informations d'urgence doivent également inclure les procédures de remontée des informations. Ces informations doivent être à la fois disponibles à tout moment et physiquement extrêmement sécurisées. Pour sécuriser et mettre ces informations à disposition à tout moment, il est possible de les chiffrer sur un ordinateur portable sécurisé spécialement dédié à cette fin, placé dans un coffre sécurisé, et de limiter l'accès au coffre aux personnes autorisées, telles que le responsable de l'équipe chargée de la réponse et le directeur des systèmes d'information (CIO) ou le directeur de la technologie (CTO).

Pour consulter un formulaire exhaustif à remplir, voir **Sans Institute**

NOM	ORGANISATION	RÔLE	COORDONNÉES DE CONTACT
Mme Incident Responsable équipe de réponse	En interne/externe	Gestion de la réponse en cas d'incident	Adresse Téléphone Adresse électronique Information de contacts **weekends et remplaçant**
M. Juriste	En interne/externe	Expert juridique	
Mme Forensic	Externe	Expert en forensic	
M. Police	Autorité de répression	Autorité de répression	

MATÉRIEL ET LOGICIELS POUR LA GESTION DES INCIDENTS DE CYBERSÉCURITÉ

Pour améliorer la maturité et l'efficacité de l'équipe chargée de la réponse, des outils appropriés doivent être mis à sa disposition. L'équipe chargée de la réponse doit absolument disposer de systèmes et d'outils autonomes permettant de prendre en charge un incident même si le réseau de l'entreprise est endommagé. Cela signifie que lorsque les systèmes ou réseaux de votre entreprise ne sont plus disponibles, le système de l'équipe chargée de la réponse l'est encore. Les procédures d'incident et les listes de contacts doivent être stockées dans ces systèmes.

VI. PRÉPARER VOTRE STRATÉGIE DE COMMUNICATION

La communication est un **élément vital** à chaque étape de la réponse aux incidents de sécurité. Le contrôle des flux de communication est nécessaire pour vous assurer que **la bonne information** soit transmise **au bon moment** par **les bons émetteurs** vers **les bons destinataires**. Cela est valable tant pour les communications internes que pour les communications adressées au monde extérieur. Nous recommandons de coordonner toutes les communications externes avec les représentants des services juridiques et relations publiques.

QUE DEVEZ-VOUS COMMUNIQUER, ET À QUI ?

Le type d'incident et son impact (possible) dicteront le type de communication requis. Par exemple, un cas de fraude interne ou de tentative de piratage interne interdira certainement toute communication aux médias pour divulguer l'incident. Au contraire, lorsque les données à caractère personnel des clients d'une entreprise sont piratées, il est opportun de contacter au moins les clients concernés et l'Autorité de protection des données et de préparer un communiqué de presse. En outre, toutes les communications doivent viser un équilibre approprié entre ouverture et protection. Dans la plupart des cas, la communication interne sera plus ouverte, par rapport à la communication externe. Toutefois, même pour la communication interne, un principe de restriction au « need to know » doit être observé.

IDENTIFIER LES PARTIES PRENANTES INTERNES ET EXTERNES

Pendant les activités de réponse à l'incident, les nombreuses parties prenantes auront constamment besoin d'informations. Chacune d'elle aura besoin d'un type d'information différent. Dressez votre propre liste de parties prenantes potentielles et veillez à obtenir des coordonnées actualisées ! (voir également le tableau de la page 15). Il faut souligner que l'organisation est censée disposer de ces informations, mais qu'elle ne doit pas systématiquement les communiquer à toutes les parties prenantes.

QUI ? PARTIES PRENANTES INTERNES	QUOI ? TYPE D'INFORMATION DONT CETTE PARTIE PRENANTE A BESOIN
Direction générale	Quels sont les éléments touchés par l'incident ? Quelle est la réponse appropriée ? Quel résultat est attendu et quand pourra-t-on reprendre le cours normal de l'activité ?
Cadres concernés par l'incident	Quand les activités normales doivent-elles reprendre ?
Employés	Que doit faire un employé ? Combien de temps cette situation doit-elle perdurer ?

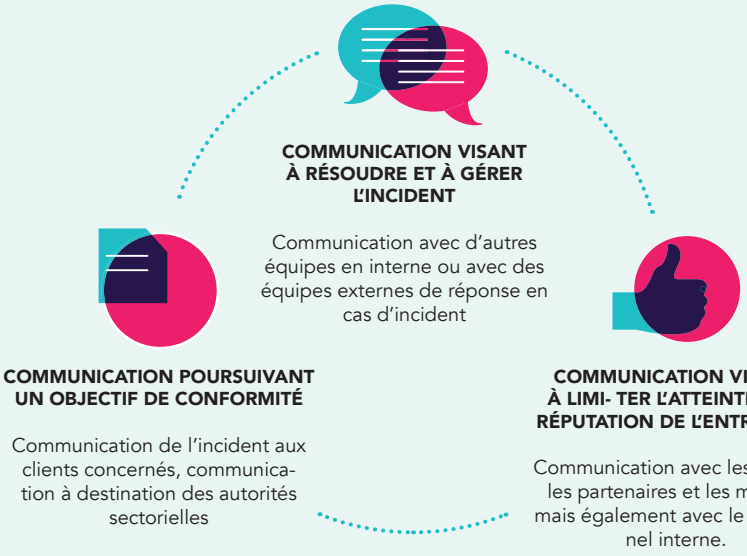
QUI ? PARTIES PRENANTES INTERNES	QUOI ? TYPE D'INFORMATION DONT CETTE PARTIE PRENANTE A BESOIN
Médias	Un compte-rendu de l'incident et de son impact. Pour les entreprises et/ou les incidents ayant une visibilité importante, les médias peuvent être associés. L'attention des médias sur un incident de sécurité est rarement souhaitable, mais peut parfois être inévitable. L'exposition médiatique peut permettre à l'entreprise d'adopter une posture volontariste en communiquant sur l'incident, démontrant ainsi son engagement et sa capacité à gérer l'incident. Le plan de communication doit désigner de façon claire les personnes habilitées à s'exprimer devant les représentants de la presse (il s'agit habituellement des personnes des services relations publiques ou juridique).
Clients	Ont-ils pu subir des conséquences de l'incident de cybersécurité ? Leurs données (personnelles) ont-elles été perdues ou volées ? Sont- ils la cible première de l'attaque ? Dans certains cas, l'entreprise est soumise à une obligation légale de prévenir l'autorité de réglementation du secteur (voir également page 31, Signalement aux autorités).
Fournisseurs	Ont-ils pu subir des conséquences de l'incident de cybersécurité ? Sont-ils la cible première de l'attaque ?
Autres (partenaires) Équipe chargée de la réponse en cas d'incident de cybersécurité	La communication avec d'autres équipes chargées de la réponse en cas d'incident peut offrir une assistance technique, permettant ainsi une résolution plus rapide de l'incident (par ex., le même type d'incident a peut-être déjà été rencontré/résolu auparavant). Ce type de communication comportera généralement les détails techniques des preuves recensées.
Fournisseur d'accès Internet	La communication avec votre fournisseur d'accès Internet peut offrir une assistance technique, permettant ainsi une résolution plus rapide de l'incident (par ex., le même type d'incident a peut-être déjà été rencontré/résolu auparavant). Ce type de communication comportera généralement les détails techniques des preuves recensées.

QUI ? PARTIES PRENANTES INTERNES	QUOI ? TYPE D'INFORMATION DONT CETTE PARTIE PRENANTE A BESOIN
Autorité de protection des données	Y a-t-il eu brèche des données ? Quelles sont les personnes concernées ? Dans certains cas, l'entreprise est soumise à une obligation légale de prévenir l'Autorité de protection des données (législation des télécommunications et future législation européenne et RGPD). (Voir également page 31, Signalement aux autorités).
CCB (division CERT.be)	Détails techniques des preuves recensées
Police	Souhaitez-vous déposer une plainte ? Lorsque l'événement a eu un impact important et qu'il existe un soupçon d'intention criminelle, il convient éventuellement de signaler l'incident aux autorités de répression. Elles auront besoin d'informations techniques et juridiques.
Autorité sectorielle	Quelle est la nature de l'incident ? Quel est le statut de l'incident ? Dans certains cas, l'entreprise est soumise à une obligation légale de prévenir certaines autorités ou l'autorité de réglementation du secteur (voir également page 27, Signalement aux autorités).

Les organisations victimes d'un incident doivent avoir conscience qu'une fois une partie prenante informée, cette dernière demandera à être tenue informée régulièrement de l'incident concerné. Cela ne se limite généralement pas à une simple information ponctuelle, et le programme de communication doit tenir compte de ces actualisations régulières.

LES CONSÉQUENCES DE L'INCIDENT DÉTERMINERONT LES OBJECTIFS DE LA COMMUNICATION

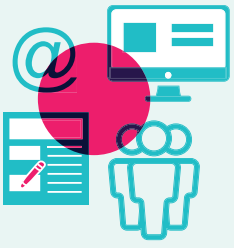
Pour savoir quels sont les éléments à communiquer, et à qui, l'organisation doit évaluer l'impact (potentiel) de l'incident de cybersécurité : les parties prenantes concernées sont-elles uniquement des parties prenantes internes ou également externes ? Y a-t-il eu fuite de données ? En fonction des conséquences répertoriées, votre plan de communication sur l'incident de sécurité visera différents objectifs, par exemple :



VEILLER À CE QUE PLUSIEURS CANAUX DE COMMUNICATION SOIENT DISPONIBLES

L'incident peut avoir un impact sur les canaux de communication existants (en compromettant le système de courrier électronique, par exemple). Pour l'organisation, des canaux de communication de substitution sécurisés doivent être accessibles. Plusieurs méthodes de communication sont disponibles et il appartient à l'organisation de sélectionner la méthode la plus adaptée pour un incident particulier.

Une **bonne pratique** fréquente utilisée par de nombreuses organisations consiste à utiliser un numéro de téléphone passerelle pour la conférence téléphonique qui peut être activé instantanément. Les numéros d'accès doivent être communiqués à l'équipe chargée de la réponse à l'incident et à toutes les parties prenantes, mais pas le numéro de contrôle nécessaire pour établir une conférence. Cette tâche appartient habituellement au manager de crise, qui est chargé de gérer, de contrôler et d'organiser les appels de crise.



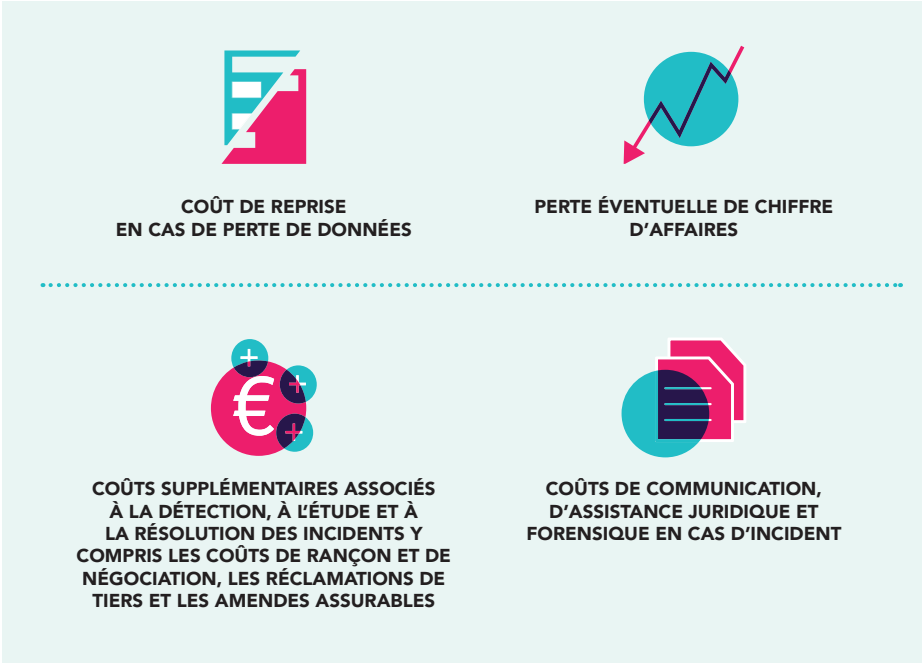
MÉTHODES DE COMMUNICATION POSSIBLES

- Courrier électronique (de préférence en utilisant le chiffrement PGP pour assurer la confidentialité et l'intégrité des communications)
- Site Web (intranet pour les employés, site Web public...)
- Appels téléphoniques
- En personne (par ex., réunions d'information quotidiennes)
- Support papier (par ex., l'affichage d'avis sur les tableaux d'affichage et les portes, la distribution d'avis d'information à toutes les entrées)

VII. ASSURANCE CONTRE LES CYBER-RISQUES

Certains assureurs proposent des contrats d'assurance personnalisés, systématiquement précédés d'une analyse des risques propres à l'organisation concernée. Cette analyse permet à l'organisation de déterminer si une assurance contre les cyber-risques est nécessaire et, si oui, dans quelle mesure. L'assureur utilisera également l'analyse de risques pour déterminer la couverture nécessaire. Les facteurs pris en compte sont les suivants :

- exposition de l'entreprise : haute technologie avec processus de production exclusif et activité importante en recherche et développement ;
- type de réseau de distribution : commerce électronique ;
- volume et type de données (critiques ou non), existence d'un cadre juridique.



L'indemnisation est versée au-delà d'un seuil de dépassement qui doit être négocié avec l'assuré. Les montants assurés par sinistre et/ou par année d'assurance sont toujours déterminés en fonction des besoins de l'entreprise et des capacités de la compagnie d'assurance.

02 DÉTECTER ET IDENTIFIER DES INCIDENTS DE CYBERSÉCURITÉ POTENTIELS

I. CATÉGORIES D'INCIDENTS

DÉFINITION DE L'INCIDENT DE CYBERSÉCURITÉ ET TERMINOLOGIE ASSOCIÉE

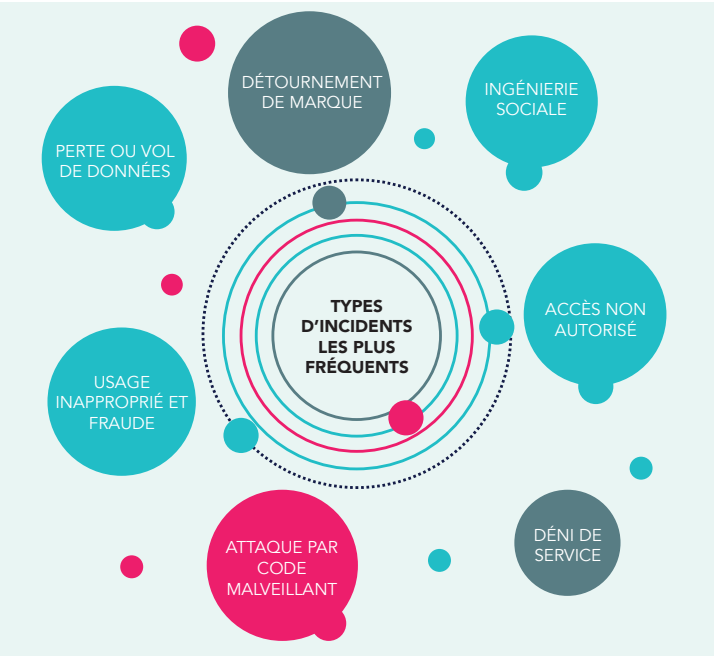
Pour commencer, il semble opportun de définir ce qu'est un « incident de cybersécurité » et d'étudier la terminologie qui s'y rapporte au sein de votre organisation. Cela permettra de fluidifier la communication au sujet de l'incident. Vous trouverez des éléments dont vous pourrez vous inspirer pour ces définitions dans le chapitre préliminaire de ce guide, sous l'intitulé « Principes de base et définitions essentielles ». Il vous appartient, par exemple, de décider à quel moment un événement de cybersécurité devient un incident de cybersécurité pour votre organisation. En d'autres termes, quels types d'événements de cybersécurité peuvent avoir des conséquences néfastes sur de votre organisation

DÉFINIR LES CATÉGORIES D'INCIDENTS DE CYBERSÉCURITÉ POSSIBLES

Pour être en mesure de détecter et d'identifier les incidents de cybersécurité, vous devez au moins avoir une idée de ce que vous cherchez. C'est pourquoi disposer d'une liste des catégories d'incidents de cybersécurité les plus susceptibles d'atteindre votre organisation n'est pas un luxe. En outre, lorsque vous détectez un événement de cybersécurité, il est souvent difficile de savoir immédiatement quelle sera l'ampleur des conséquences. Cela ne change toutefois pas la donne pour vous : vous devez agir. Les catégories d'incidents vous permettent de prioriser les événements de cybersécurité et de prendre des décisions en conséquence. Cette section dresse une typologie d'un certain nombre d'incidents de cybersécurité. L'intention n'est pas ici de présenter une vue d'ensemble « définitive » de tous les types d'incidents, mais plutôt de vous donner une idée des types d'incidents les plus fréquents (au moment de la rédaction de ce guide). Un incident peut appartenir à plus d'une catégorie. Vous trouverez en annexe une explication plus détaillée de ces types d'incidents.

CLÉ USB OU ESPION USB ?
En 2013, la Russie a accueilli une réunion des dirigeants du G20. À la fin de cet événement, tous les participants, et parmi eux Herman Van Rompuy, ont reçu un sac cadeau contenant un stylo clé USB et un chargeur de téléphone mobile. Bien que le Kremlin l'ait toujours démenti, il se dit que ces deux dispositifs étaient capables de télécharger secrètement des informations, telles que les courriers électroniques, les messages textes et les appels téléphoniques, depuis des ordinateurs portables et des téléphones.

UN CRYPTOLOCKER PEUT ÉGALEMENT CHIFFRER VOS SAUVEGARDES
Une société reçoit un courrier électronique contenant une facture en pièce jointe, en tous points semblable à celles d'un de ses fournisseurs. Le comptable de la société clique sur la pièce jointe, et quelques secondes plus tard un message apparaît à l'écran : « Toutes vos informations ont été chiffrées ! Si vous souhaitez obtenir la clé permettant de déverrouiller le chiffrement, vous devez me payer 1 000 Bitcoins ». La société se refuse à payer le cybercriminel. Après tout, elle ne dispose d'aucune garantie quant au fait qu'il restituera bien les données perdues une fois la rançon versée. Pour récupérer ses données, la société décide de les restaurer à partir d'une sauvegarde. C'est alors que l'employé remarque que, puisque la sauvegarde était reliée au système, elle a également été chiffrée...



II.

MÉTHODES DE DÉTECTION DES INCIDENTS

LE PERSONNEL DE VOTRE ORGANISATION PEUT DÉTECTER DES INCIDENTS

On considère souvent que le facteur humain est le maillon faible en matière de cybersécurité. Toutefois, le personnel offre également le meilleur potentiel pour aider l'organisation à détecter et identifier les incidents de cybersécurité. Assurez-vous que chaque membre de votre organisation soit informé des risques de cybersécurité et du rôle qu'il peut jouer pour les détecter. Faites-en votre pare-feu humain ! Chaque membre de votre organisation doit savoir comment effectuer un signalement lorsqu'il constate quelque chose d'anormal sur son ordinateur ou son téléphone portable. Veillez à ce que les coordonnées de contact prévues à cette fin soient facilement accessibles et que le contact soit associé à un niveau d'accès bas.

Comment organiser concrètement le signalement d'incident par le personnel (et d'autres partenaires) ?
- Un numéro de téléphone doit être dédié au signalement des urgences
- Une adresse électronique pour le signalement informel d'incident
- Un formulaire en ligne pour un signalement formel d'incident

Pour éviter les codes malveillants, effectuez les mises à jour de vos logiciels, antivirus, etc. ! Mettez à jour régulièrement vos logiciels ou installez les patchs dès qu'ils sont disponibles.

N'utilisez pas de versions non prises en charge de systèmes d'exploitation tels que Windows XP et Windows 2003. « Non pris en charge » (ou « Non supporté ») signifie que le logiciel n'est plus mis à jour et que votre ordinateur n'est donc plus protégé contre les logiciels malveillants connus ou nouveaux.

PROTECTION DE LA TECHNOLOGIE ET DES ÉQUIPEMENTS

Technologie

La technologie est l'un des principaux atouts lorsqu'il s'agit d'accélérer la détection des incidents, les enquêtes, l'éradication et la reprise. Lorsqu'un incident survient, le déploiement d'une technologie appropriée est encore possible, mais vos recherches seront souvent limitées aux événements en cours. Déployer la bonne technologie pendant la phase de préparation vous permettra d'appréhender de manière exhaustive les événements actuels et passés. Cela augmentera vos chances de pister l'incident et de remonter à sa source.

Protection des équipements

Il s'agit des dispositifs connectés au réseau de votre organisation, tels que les ordinateurs portables, les smartphones, etc. Chacun de ces dispositifs est un point d'entrée potentiel pour les cybercriminels. Par conséquent, une protection adaptée de ces dispositifs est primordiale.

OUTILS DE DÉTECTION

Chaque outil de détection (par ex. l'IDS) a une finalité spécifique et peut effectuer son travail de surveillance suivant différentes perspectives : en réseau ou hébergé. Étant donné l'éventail des menaces existantes, ces outils doivent utiliser les bonnes données source et être réglés en conséquence.

En réseau

Il pourrait être utile de commencer par mettre en place un système de prévention des intrusions, tel que le Snort network IDS sensor, sur la liaison uplink Internet. En outre, de nombreuses organisations ont déjà mis à disposition beaucoup d'informations qui peuvent être utilisées pour détecter un incident insoupçonné. Ces informations peuvent revêtir la forme de :
- logs d'accès aux serveurs et dispositifs ;
- logs d'exploitation issus de systèmes (par ex., la création de processus) ;
- logs de politique de pare-feu.

Ces données peuvent être utilisées pour créer des règles et des tendances, ce qui favorise la détection de trafic inattendu ou non valide (par ex., le trafic vers des sites inhabituels, des tentatives de connexion d'utilisateurs inexistants, etc.).

Hébergé

Les solutions antivirus ne sont pas suffisantes pour lutter contre les attaques sophistiquées contre les équipements. Aujourd'hui, de nombreux logiciels malveillants sont polymorphes (ils changent en fonction du comportement du système hôte), ce qui les rend difficiles à détecter sur des signatures statiques par les antivirus classiques. Les outils avancés de protection d'équipement recherchent des comportements suspects et peuvent ainsi être plus efficaces dans bien des cas.
Cela ne signifie toutefois pas qu'il ne faille pas déployer de solution antivirus. Au contraire, les antivirus sont nécessaires pour couvrir la plupart des menaces les plus connues.

03 PRENDRE EN CHARGE UN INCIDENT RÉEL : CONFINER, ÉRADIQUER ET RÉTABLIR

Dans ce chapitre, vous allez découvrir ce que vous devez faire pour reprendre le contrôle après avoir détecté un incident de cybersécurité. Des décisions importantes devront être prises quant à la manière de contenir l'incident, de l'éradiquer et de rétablir le système. Il est primordial que ces décisions soient validées par la haute direction de votre organisation. Un incident peut appartenir à plus d'une catégorie.

I. RÉUNISSEZ VOTRE ÉQUIPE CHARGÉE DE LA RÉPONSE EN CAS D'INCIDENT

En cas d'incident avéré, il est primordial d'évaluer rapidement les risques afin de prendre les mesures appropriées. Le responsable de la réponse en cas d'incident de cybersécurité doit être informé immédiatement et convoquer une réunion de l'équipe chargée de la réponse lorsqu'elle existe au sein de votre organisation (voir également page 11, Équipe chargée de la réponse en cas d'incident de cybersécurité). Le responsable de la réponse en cas d'incident de cybersécurité et son équipe rendront compte au CEO, qui devra valider leurs décisions.

II. CONNAISSANCE DE LA SITUATION

Après la détection d'un incident, il est primordial de recueillir toute information disponible concernant les activités réalisées au cours de la période précédant et suivant immédiatement l'incident. La collecte et l'archivage centralisés des informations de sécurité (journaux système, journaux de politique de pare-feu) permettent à l'analyste d'accéder facilement à ces informations. L'intégrité de l'information et l'indexation sont des facteurs importants à prendre en considération.

Une investigation forensic peut être diligentée pour collecter tous les artefacts et pour examiner l'ampleur et la gravité de l'attaque. Les outils servant à créer et à analyser des images complètes de disque, à effectuer un vidage à distance de la mémoire d'une machine suspecte et autres bloqueurs d'écriture sont utiles pour réaliser cette analyse. Pour évaluer l'ampleur de l'incident, les artefacts ou les indicateurs collectés dans le cadre de l'investigation forensic initiale peuvent être ensuite utilisés pour rechercher d'autres intrusions à grande échelle sur tous les dispositifs administrés. Un point de management centralisé du parc informatique permet d'interroger tous les dispositifs plus rapidement. Vous devez également vérifier si des données ont été perdues ou volées.

ÉVALUATION DES RISQUES DE FUITES DE DONNÉES À CARACTERE PERSONNEL

Un élément clé pour faire face à une fuite de données à caractère personnel est de déterminer le niveau de risque de la fuite en question. Quelle est la gravité de la fuite et quelles sont les conséquences possibles pour la personne dont les données ont été divulguées ? La réponse à cette question est un facteur important pour déterminer les mesures à prendre. Chaque niveau de risque (aucun risque, risque, risque élevé), nécessite une approche différente, notamment dans le contexte de la notification obligatoire. Par conséquent, une évaluation précise et cohérente des risques est la clé pour traiter efficacement une violation des données personnelles. Cela permettra de s'assurer que les bonnes actions sont prises pour se conformer aux dispositions législatives.

L'évaluation d'une fuite de données à caractère personnel dans son intégralité permet de formuler un niveau de risque adéquat et réaliste, et de prendre les mesures de suivi appropriées. Pour évaluer les risques pour les droits et libertés des personnes, un certain nombre d'éléments doivent être pris en compte. Les éléments les plus importants sont décrits ci-dessous :

Nature et sensibilité des données personnelles	*Données sensibles* Plus les données personnelles sont sensibles, plus le risque de préjudice pour les personnes concernées est élevé. *Publicité des données* Outre le caractère sensible des données ayant fait l'objet de la fuite, le niveau de publicité déjà donné à ces données est également important. Il convient d'examiner si les données personnelles de l'individu étaient déjà (publiquement) accessibles. *Données à caractère personnel liées* Les violations de données portant sur des données de santé, des documents d'identité ou des données financières, telles que les informations relatives aux cartes de crédit, peuvent chacune causer des dommages en soi, mais, combinées à des informations accessibles au public, elles peuvent également donner lieu à des infractions graves, telles que l'usurpation d'identité. Pour cette raison, les données personnelles liées présentent un risque plus élevé qu'une catégorie isolée de données personnelles.
Quantité de données personnelles et nombre de personnes concernées	Cet élément porte sur la quantité d'informations concernées par la fuite et le nombre total de personnes dont les données sont affectées. Plus le nombre de données et d'individus touchés est important, plus les risques sont élevés.
Facilité d'identification des personnes	Cet élément porte sur la facilité avec laquelle une partie ayant accès aux données à caractère personnel ayant fait l'objet d'une violation pourra identifier une personne (éventuellement après comparaison avec d'autres informations disponibles). Le risque dépend de la question de savoir si les personnes peuvent être directement identifiées sans certaines autres données personnelles, ou si des informations supplémentaires provenant d'autres catégories de données sont nécessaires pour identifier les personnes.
Gravité des conséquences	Il faut établir les dommages potentiels causés aux personnes et la gravité de ces dommages. Les violations de données peuvent être extrêmement dommageables, dans des cas tels que l'usurpation d'identité, les dommages physiques, le stress psychologique, l'humiliation ou l'atteinte à la réputation. Si la fuite concerne des données à caractère personnel de personnes vulnérables (par exemple, des patients, des enfants), un risque plus élevé de préjudice peut être attribué.
Mesures d'atténuation existantes	Les mesures d'atténuation déjà en place au moment de la violation des données doivent être prises en compte dans l'évaluation globale des risques, en examinant si, et comment, ces mesures protègent les personnes concernées.

Registre des fuites de données

En raison du principe de responsabilité, toutes les considérations et conclusions de l'évaluation des risques doivent être documentées dans un registre des violations de données. Ce registre doit contenir au moins les informations suivantes :

Date et heure de la fuite de données	La date et l'heure exactes auxquelles l'organisation a eu connaissance de la fuite de données personnelles. Ces informations sont importantes pour respecter le délai de 72 heures pour la notification à l'Autorité de protection des données et à toute personne concernée.
Chronologie et description de la fuite de données	Description des événements relatifs à la fuite de données personnelles : date à laquelle la fuite a été signalée, date à laquelle elle a (vraisemblablement) eu lieu, aperçu des systèmes concernés et autres descriptions.
Personne de contact	Il est important d'avoir une personne de contact centrale, qui est informée des circonstances de la fuite de données personnelles et qui peut être contactée en cas de questions de suivi. En général, la personne qui a signalé la fuite est le délégué à la protection des données ou le responsable du service concerné.
Parties externes concernées	Contient des informations sur la nature et le rôle de l'organisation (responsable du traitement, sous-traitant, responsable conjoint du traitement) et les tiers qui peuvent être affectés et doivent donc être informés.
Évaluation des risques - motivation et conclusion	Analyse détaillée des risques et évaluation globale des risques, sur la base des éléments permettant de déterminer le niveau de risque (voir section ci-dessus).
Contrôles et mesures correctives existants	Une liste des mesures techniques et organisationnelles existantes, et de celles qui seront prises pour réduire les risques existants pour les personnes concernées.
Notifications	Un aperçu des notifications qui ont eu lieu et à qui (Autorité de protection de données, personne concernée, tiers).

III.

CONFINER UN INCIDENT DE CYBERSÉCURITÉ

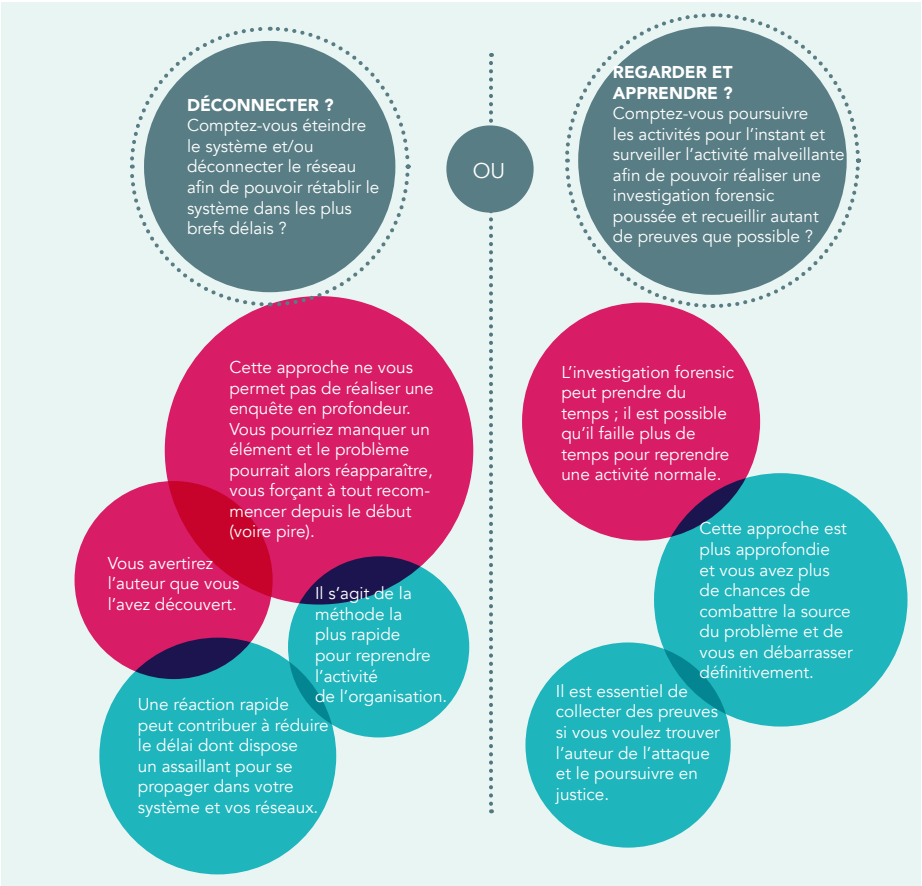
PRIVILÉGIER UNE REPRISE RAPIDE OU COLLECTER DES PREUVES ?

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 organisation devra prendre une décision stratégique importante : faut-il déconnecter le système immédiatement pour une reprise la plus rapide possible ? Ou bien faut-il prendre le temps de réunir des preuves contre le cybercriminel qui s'est attaqué au système ?

Vous devrez probablement trouver un compromis entre ces deux options. De la décision que prendra votre organisation à cet égard dépendront la portée, l'ampleur et l'impact de l'incident. Les critères suivants peuvent vous aider dans votre évaluation :

1. Que se passera-t-il si l'incident n'est pas confiné ?
2. L'attaque ou la brèche provoque-t-elle des dommages graves immédiats ?
3. L'incident entraîne-t-il des dommages ou un vol (potentiels) pour les actifs de l'organisation ?
4. Est-il nécessaire de préserver les preuves ? Si oui, quelles sources de preuves l'organisation doit-elle acquérir ? Où seront stockées les preuves ? Combien de temps les preuves devront-elles être conservées ?
5. Doit-on éviter d'alerter le pirate informatique ?
6. Devez-vous maintenir la disponibilité du service, ou bien est-il acceptable de mettre le système hors ligne (par exemple, les services fournis à des tiers) ?



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

Pendant un incident, la pression sera importante pour qu'une action rapide soit entreprise. Toutefois, pour éviter toute erreur inutile, il est important de prendre un peu de recul et de réfléchir avant d'agir.

ENQUÊTER : RASSEMBLER DES PREUVES

Si vous voulez vous attaquer à la racine du problème et identifier l'auteur de l'attaque pour le poursuivre, la préservation des preuves est primordiale. Pour rassembler des preuves, **l'enquête forensic** doit être effectuée avant l'éradication de l'incident. Si vous ne disposez pas en interne de l'expertise nécessaire pour effectuer vous-même cette investigation, faites appel à des experts externes possédant les outils appropriés pour rassembler des preuves dans le respect des exigences légales (voir également page 13, Experts en réponse en cas d'incident).
N'oubliez pas que, même si votre organisation peut compter sur une équipe informatique très compétente, un incident de cybersécurité complexe peut toujours nécessiter une aide extérieure. Cela ne signifie pas pour autant que vos professionnels informatiques ont échoué. Au contraire, cela signifie qu'ils ont décelé rapidement que la complexité de l'incident nécessitait une expertise complémentaire.

POUR CONTRER UNE ATTAQUE DDoS, IL FAUT DE L'EXPÉRIENCE

Une attaque DDoS est une attaque ciblée visant à mettre hors service votre système. Ce genre d'attaque peut donc avoir des conséquences très graves pour la disponibilité de votre système. Ces attaques sont extrêmement sophistiquées et difficiles à contrer. La plupart des organisations sont incapables de contrer une attaque DDoS seules et elles devront faire appel à des experts externes en présence d'une telle attaque.

N'oubliez surtout pas que, pour qu'elles soient recevables devant un tribunal, les preuves doivent être collectées selon des procédures satisfaisant à toutes les lois et réglementations en vigueur. Vous ne devez rien faire qui puisse compromettre vos preuves. Par exemple, **les actions suivantes ne sont pas recommandées** :

ÉTEINDRE IMMÉDIATEMENT VOTRE SERVEUR

- Il se peut que vous ne soyez pas en mesure d'identifier la cause de l'incident ou son auteur. Si vous éteignez votre serveur, vous videz la mémoire du serveur. Cela signifie que vous ne pourrez effectuer aucune investigation forensic sur la mémoire du serveur, car il n'y aura plus rien à analyser.
- Vous pourriez détruire des preuves cruciales, car la mémoire RAM contient souvent de nombreuses traces de programmes malveillants. Avant d'éteindre votre serveur, les données doivent être transférées sur un disque USB.

DÉCONNECTER IMMÉDIATEMENT LE SERVEUR D'INTERNET

- Vous risquez de détruire des preuves cruciales. Une coupure immédiate empêche de déterminer l'ampleur des dégâts sur votre infrastructure, car un serveur qui a été éteint et déconnecté d'Internet ne communique plus avec son serveur de commande et de contrôle sur Internet ni avec les autres postes de travail/serveurs infectés sur votre réseau.
- Vous pourriez aussi indiquer au cybercriminel que vous êtes sur ses traces, ce qui n'est pas non plus une bonne idée à ce stade.

RESTAURER VOTRE SYSTÈME À PARTIR D'UNE SAUVEGARDE SI VOUS N'ÊTES PAS CERTAIN QUE LA SAUVEGARDE N'EST PAS ELLE-MÊME INFECTÉE

Votre sauvegarde peut également être infectée : les APT (de l'acronyme « Advanced Persistant Threat », ou menaces persistantes avancées) peuvent infecter votre réseau pendant une longue période avant que vous ne le remarquiez. Cela augmente le risque d'infection des sauvegardes. Installer une sauvegarde infectée peut recréer l'infection.

RÉINSTALLER SUR LE MÊME SERVEUR SANS FAIRE UNE COPIE AUX FINS DE L'INVESTIGATION FORENSIC

TYPES D'INCIDENTS LES PLUS FRÉQUENTS

À ce stade, il est utile de disposer d'une liste des catégories d'incidents les plus susceptibles de frapper votre organisation (voir également page 20, Définir les catégories d'incidents de cybersécurité possibles). Cette liste peut contenir les types d'incidents les plus probables pour votre organisation et les instructions de base quant à la manière de les résoudre. Un exemple est proposé en annexe.

IV.

ÉRADIQUER ET NETTOYER

Une fois l'investigation numérique effectuée, vous pouvez lancer l'éradication. Pendant cette phase, vous devez supprimer tous les éléments associés à l'incident, tous les artefacts laissés par le pirate informatique (codes malveillants, données, etc.) et combler toute lacune ou toute faiblesse utilisée par le pirate pour s'introduire dans votre système la première fois.

Ne lancez jamais le nettoyage tant que vous n'avez pas analysé entièrement l'incident ! Vous devez donc commencer par déterminer la source du problème. Ce n'est pas une tâche facile. Par ailleurs, vous devez vous assurer d'avoir au moins analysé toutes les machines présentant la même vulnérabilité, car elles peuvent également être infectées. Dès lors que la décision de commencer l'éradication a été prise, il faut agir vite, de manière synchronisée et méticuleuse afin de laisser à votre adversaire le moins de chances possible de réagir (idéalement aucune).

L'éradication peut revêtir de nombreuses formes. Elle implique souvent des actions telles que :

- exécuter une analyse antivirus ou une recherche de logiciels espions pour supprimer les fichiers et les services hostiles ;
- actualiser les signatures ;
- supprimer les logiciels malveillants ;
- désactiver les comptes utilisateur piratés ;
- modifier les mots de passe des comptes utilisateur piratés ;
- repérer les vulnérabilités exploitées et les corriger ;
- détecter les brèches de sécurité et les corriger ;
- informer les employés à propos de la menace et leur communiquer des instructions sur les choses à éviter à l'avenir ;
- informer les parties prenantes externes telles que les médias et vos clients (voir également page 26, La communication pendant un incident de cybersécurité).

Important : la haute direction doit également être informée des résultats de l'éradication et du nettoyage ainsi que de la situation du réseau.

Les fichiers individuels seront détectés, mis en quarantaine ou supprimés des systèmes par la solution antivirus. Celle solution doit être ouverte pour vous permettre de lui fournir des définitions de virus spécifiques.

Les courriers électroniques de hameçonnage peuvent être bloqués sur le système de messagerie par un filtrage sur l'expéditeur, le relais de messagerie ou certaines parties du contenu.

Les adresses IP ou les indicateurs fondés sur le nom de domaine peuvent être bloqués sur la base du trafic réseau en les ajoutant aux listes d'accès, aux politiques de pare-feu ou aux politiques de proxy. Par conséquent, il est primordial de disposer des capacités nécessaires pour effectuer ces modifications de manière ponctuelle.

V.

REPRISE

Par reprise, nous entendons la restauration des systèmes en vue d'un retour à l'activité normale et (le cas échéant) la correction des vulnérabilités pour prévenir tout autre incident similaire. Il existe de nombreuses manières de restaurer un système après un incident de cybersécurité. Elles ont toutes des répercussions différentes en termes de durée de reprise, de limitation des coûts ou de perte de données.

	DURÉE DE LA REPRISE	COÛT	PERTE DE DONNÉES	REMARQUES
Nettoyer les artefacts malveillants et remplacer les fichiers endommagés par des versions non infectées	Courte	Rentable		Vous risquez de ne pas détecter certains artefacts.
Restaurer à partir d'une sauvegarde	Moyenne	Rentable		Ce n'est possible qu'à la condition de disposer d'une sauvegarde que vous savez saine. Dans certains cas, il est difficile de déterminer l'horodatage exact de l'incident initial ou de savoir si l'incident s'est produit pendant une certaine durée si l'on ne dispose pas d'une sauvegarde antérieure
Reconstruire le (les) système(s) ou l'environnement à partir de zéro	Longue, perte de temps	à l'incident.	Risques de perte de données	Cela reste toutefois le seul moyen totalement fiable de vous débarrasser du pirate.

Les statistiques démontrent que, très souvent, les incident ne sont révélés qu'après plusieurs mois. À quand remontent les sauvegardes de votre organisation ?

Le type de reprise dépendra non seulement du temps et des moyens financiers dont vous disposez, mais également des dommages causés à votre infrastructure. Par exemple, il est possible que vous ne disposiez d'aucune sauvegarde non infectée parce que même votre sauvegarde la plus ancienne a été effectuée après l'intrusion du pirate dans votre système. Il est donc primordial de vérifier la présence éventuelle de virus, de maliciels furtifs (« rootkits ») et de portes dérobées (« backdoors ») dans votre sauvegarde avant de l'utiliser pour restaurer votre système. Si aucune sauvegarde fiable ne peut être trouvée, alors il n'y a d'autre choix que de réinstaller le système en repartant de zéro (y compris le système d'exploitation !). Après la restauration du système, vous devrez corriger les vulnérabilités qui ont permis au pirate de s'introduire dans votre système.

Il s'agit notamment de l'installation de patchs (correctifs), au niveau tant du système d'exploitation que des applications, la modification des mots de passe, la modification des comptes, le resserrement du périmètre de sécurité du réseau, par exemple en changeant de pare-feu, en utilisant des listes de contrôle d'accès au boundary routeur, etc. et le verrouillage de services.

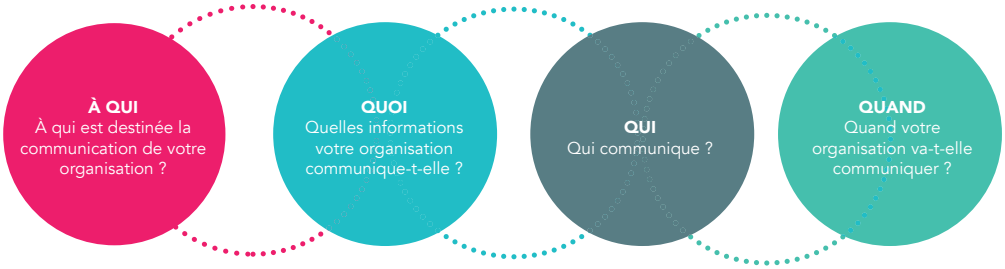
Vous devez également prendre en compte qu'une fois une ressource piratée, il existe un risque qu'elle le soit à nouveau ou que d'autres ressources de votre organisation fassent l'objet d'une attaque similaire. Vous devez donc renforcer vos défenses, par exemple en passant à un niveau supérieur de log du système ou de surveillance du réseau.

Enfin, avant de connecter à nouveau le système au réseau, il doit être validé tant pour les aspects de sécurité que pour les fonctions associées à l'activité. Du point de vue de la sécurité, la validation du système peut se faire par un scanning du système à l'aide d'un outil qui vérifiera si des vulnérabilités persistent. Pour valider les fonctions associées à l'activité, une personne compétente doit vérifier que toutes les fonctions nécessaires à l'activité fonctionnent correctement.

Et n'oubliez pas, si vous ne disposez pas de l'expertise nécessaire en interne, faites appel à des experts externes, et n'oubliez pas de vérifier que votre assurance contre les cyber-risques couvre bien le coût de cette intervention.

04 LA COMMUNICATION PENDANT UN INCIDENT DE CYBERSÉCURITÉ

Lorsqu'un incident de cybersécurité survient, l'équipe chargée de la réponse en cas d'incident de cybersécurité doit élaborer immédiatement un plan de communication concret pour cet incident particulier. Le plan de communication doit se fonder sur les préparatifs généraux que vous avez effectués pendant la phase de préparation (voir également page 16, Préparer votre stratégie de communication). Vous devrez essentiellement répondre aux questions suivantes : (n'oubliez pas que nous recommandons de coordonner toutes les communications externes avec les représentants des services juridique et relations publiques) Réfléchissez avant de communiquer !



I. OUTILS

Si vous êtes bien préparé, votre équipe chargée de la réponse en cas d'incident de cybersécurité aura déjà un certain nombre d'outils à sa disposition. Pendant la phase de préparation, votre organisation a dressé (voir également page 16, Préparer votre stratégie de communication) une liste des parties prenantes devant éventuellement être contactées (parties prenantes internes, externes et institutionnelles) et une liste des coordonnées de contact de ces différentes parties prenantes (la personne désignée et son suppléant).

II. PLAN DE COMMUNICATION SPÉCIFIQUE EN CAS D'INCIDENT

AVEC QUI COMMUNIQUER ET QUE COMMUNIQUER À CHAQUE CATÉ- GORIE DE PARTIES PRENANTES

La première étape de votre plan de communication spécifique en cas d'incident consiste à déterminer à quelles parties prenantes vous destinez vos communications. Pour ce faire, vous devez déterminer quelles sont les parties prenantes susceptibles d'être affectées (négativement) par l'incident de cybersécurité et s'il vous incombe d'informer certaines entités telles que l'Autorité de protection des données, qui est l'autorité belge compétente en matière de protection des données, ou l'autorité sectorielle.

- Parties prenantes internes : haute direction, 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, CCB (division CERT.be). Centre national de crise, police

Pour déterminer ce que vous devez communiquer et à qui, une règle d'or de base consiste à ne communiquer que sur la base du principe de restriction au « need to know ». Vous souhaiterez communiquer avec certaines parties prenantes afin de confiner l'incident de cybersécurité, tandis que vous devrez communiquer avec d'autres parties prenantes soit parce qu'elles vous pressent de leur communiquer des informations (par exemple les médias), soit parce que vous êtes soumis à une obligation légale d'information à leur égard (par ex. l'Autorité de protection des données, les autorités sectorielles, les personnes dont les données ont été piratées).

Données à caractère personnel

En cas de perte ou de vol de données à caractère personnel (brèche de données), il est recommandé d'avertir l'Autorité de protection des données. Dans certains cas vous serez soumis à une obligation légale de le faire. Par exemple :

- les fournisseurs de services de communication électronique accessibles au public (fournisseurs de télécommunications) sont tenus légalement de signaler les cas de brèche de données à caractère personnel à l'Autorité de protection des données et aux personnes dont les données ont été piratées ;
- dans le RGPD, la loi impose de signaler toute brèche de données à caractère personnel susceptible de présenter un risque élevé pour les personnes dont les données ont été piratées, à la fois à l'Autorité de protection des données (dans un délai de 72 heures) et aux personnes dont les données ont été piratées.[1]

Infrastructure critique nationale et sectorielle

Les opérateurs d'infrastructures nationales et commerciales critiques sont contraints par la loi de signaler aux autorités sectorielles et même au public les incidents de cybersécurité ayant des conséquences graves.[2]

OBLIGATION DE RAPPORT : LÉGISLATION NIS

FSE et FSN ont l'obligation de signaler tout incident ayant des conséquences majeures à la CCB (département CERT.be), au Centre National de Crise et à leurs autorités sectorielles par une plateforme de signalement sécurisée. Le CCB fait office de CSIRT national. La profondeur des conséquences d'un incident doit être évaluée en fonction de la disponibilité, de la confidentialité, de l'intégrité ou de l'authenticité des systèmes d'information dont le DEA / DDV.

- La disponibilité fait référence à la capacité des utilisateurs à accéder aux services de l'AED / DDV. Par exemple, une attaque DDoS peut paralyser le réseau d'un DEA et compromettre la disponibilité du service.
- Un exemple d'incident de confidentialité est une « man in the middle attack » où les données entre les utilisateurs et le DAE / DDV sont interceptées. Un tel incident peut également donner lieu à une obligation de déclaration à l'Autorité de protection des données (voir p. 29).
- Un incident d'intégrité se produit lorsque les données d'un DEA / DDV sont détruites lors d'une panne du système.
- Un incident d'authenticité se produit, par exemple, lorsqu'un fournisseur de noms de domaine ne peut plus garantir l'authenticité des noms de domaine.

Il est possible que les niveaux d'impact et/ou les valeurs seuils soient déterminés par (sous-)secteur par arrêté royal, mais ce n'est pas encore le cas.

Sachez que de graves sanctions administratives et pénales peuvent être imposées en cas de violation de l'obligation de déclaration

1 Le réglement européen général en matière de protection des données.
2 La directive européenne relative à la sécurité des réseaux et de l'information (NIS).

QUAND COMMUNIQUER ?

Une fois établie la liste des parties prenantes destinataires de vos communications 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 (voir également l'illustration de la page 18).

Il est important pour les raisons suivantes :

- certaines parties prenantes auront besoin d'informations le plus tôt possible, car elles peuvent contribuer à confiner l'incident de cybersécurité (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) ; et, enfin
- d'autres 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 l'auteur du piratage 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. Si l'auteur est averti, il se retirera probablement et effacera les traces de son passage, ou pire, il causera des dégâts irréparables tels que le vol de vos données précieuses les plus récentes ou l'installation de portes dérobées (backdoors). Pour éviter toute fuite pendant cette phase de silence, vous pouvez dresser une liste des personnes informées de l'incident de cybersécurité. Cela vous permettra de découvrir plus facilement qui est responsable d'une éventuelle fuite d'informations. Une action en justice peut être intentée à l'encontre de toute personne qui divulgue des informations.

En ce qui concerne le signalement des incidents NIS, il convient de signaler tout incident sans délai. Il n'est pas nécessaire d'attendre que toutes les informations pertinentes soient disponibles. Lorsqu'il est clair que l'incident doit être signalé, et donc lorsqu'au moins un des critères est rempli, il faut le faire le plus rapidement possible.

SIGNALEMENT AUX AUTORITÉS

Le signalement aux autorités est un pan spécifique de votre communication qui est important à différents égards :

- dans certains cas, le signalement de fuites de données ou d'autres incident de sécurité est une **obligation légale** ;
- certaines autorités peuvent vous **aider**. L'incident de cybersécurité auquel vous êtes confrontés peut ne pas être un cas isolé et les autorités compétentes peuvent disposer d'informations vous permettant de confiner plus rapidement l'incident ;
- si vous souhaitez déposer une plainte contre l'auteur présumé de l'incident de cybersécurité, vous devez contacter les autorités de répression. Il s'agit en principe de **la police** ;
- en outre, le signalement aux autorités est une étape nécessaire qui permet **d'inventorier et de quantifier la cybercriminalité** dans le pays. Il est utile d'améliorer la connaissance et la compréhension du phénomène et de sa prévalence afin d'améliorer globalement la sécurité, par exemple grâce à l'élaboration de mesures préventives et de contre-offensives.

L'assistance proposée par le CCB (Division CERT.be) est gratuite et strictement confidentielle. Le CERT apporte une aide initiale à la lutte contre les incidents de cybersécurité et des conseils sur la manière de résoudre ces problèmes. Vous pouvez signaler un incident de cybersécurité par courrier électronique en écrivant à l'adresse cert@cert.be ou par téléphone en appelant au +32 (0)2 790 33 85 (tous les jours ouvrables de 8 heures à 18 heures).

Après votre signalement, vous recevrez un accusé de réception et un numéro d'incident. Vous pouvez toujours faire référence à votre signalement grâce à ce numéro d'incident. Le CCB (division CERT.be) prendra contact avec vous le plus tôt possible pour répondre à vos questions.

NL EN FR

Signalement volontaire au CCB (Division CERT.be)

Les organisations sont invitées à envisager sérieusement le signalement des incidents de cybersécurité à la Cyber Emergency Response Team, ou « équipe fédérale d'intervention d'urgence en sécurité informatique », CCB (Division CERT.be). Pour prévenir les attaques contre d'autres systèmes informatiques, les équipes du CCB (Division CERT.be) ont besoin en particulier de ce qu'elles appellent des « indicateurs de compromission » (IOC). Il s'agit d'artefacts observés sur un réseau ou un système d'exploitation et qui indiquent une forte probabilité d'intrusion. Le signalement du CCB (Division CERT.be) est primordial pour déterminer si l'incident est un cas isolé ou non et permet d'effectuer un suivi des tendances au niveau des menaces en Belgique. Le CCB (Division CERT.be)sera également en mesure de fournir certaines informations et certains conseils concernant l'incident qui peuvent aider la victime à prendre des contremesures efficaces. En outre, l'information fournie par votre organisation peut participer à la prévention des attaques contre d'autres systèmes informatiques.

LES INFORMATIONS SUIVANTES DOIVENT ÊTRE COMMUNIQUÉES

1. Vos coordonnées
2. Le type d'incident
3. La date de l'incident
4. L'incident est-il toujours en cours ?
5. Comment avez-vous constaté l'incident ?
6. Quel est l'impact de l'incident ?
7. Avez-vous déjà entrepris des actions ou pris des mesures ? Si oui, lesquelles ?
8. Disposez-vous de journaux ou d'autres données utiles ?
9. Qui avez-vous déjà informé ?
10. Qu'attendez-vous de ce signalement ?

Signalement obligatoire des incidents NIS

Les signalements doivent être effectués par la plateforme de rapports NIS (https://nis-incident.be/). La plateforme est accessible par internet via une connexion sécurisée et une clé d'identification unique pour chaque FSE et FSN (login/nom d'utilisateur et mot de passe). Si la plateforme n'est pas disponible, l'incident doit être signalé via le site web du CCB (https://cert.be/nl/een-incident-melden). La plate-forme veille à ce que le rapport parvienne au CCB, au Centre national de crise et à l'autorité sectorielle.

Ci-dessous, pour chaque secteur, l'autorité du secteur respectif est indiquée.

Secteur	Autorité du secteur
Énergie	Ministre fédéral chargé de l'énergie (SPF Économie DG Énergie)
Transports	Ministre fédéral compétent en matière de transports ou de mobilité maritimes (SPF Mobilité et Transports)
Soins de santé	Ministre fédéral compétent en matière de santé publique (SPF Santé publique)
Eau potable	Comité national pour la sécurité de l'approvisionnement et de la distribution de l'eau potable
Infrastructures numériques	Ministre fédéral de l'Économie (IBPT)
Finance	BNB (institutions financières) ; FSMA (plateformes de négociation financière)

Le signalement comprend toutes les informations disponibles qui permettent de déterminer la nature, les causes, les effets et les conséquences de l'incident :
- le nom et les coordonnées du prestataire et le service qu'il fournit ;
- la date et l'heure de l'incident ;
- la durée de l'incident ;
- l'étendue de la zone géographique touchée par l'incident et son éventuel caractère transfrontalier ;
- le nombre d'utilisateurs concernés ;
- des informations sur la nature de l'incident ;
- l'ampleur de l'impact de l'incident, en particulier sur les activités sociales et économiques ;
- l'importance des systèmes ou des informations concernés ;
- l'impact de l'incident sur les organisations internationales basées en Belgique ;
- les actions entreprises ;
- la description de la situation actuelle.

Le signalement initial, qui doit être effectué dès que possible, est une étape de la procédure de notification. Au total, la procédure peut comporter trois phases :

- le signalement initial doit être fait sans délai, même si le FSE ou le FSN ne dispose pas encore de toutes les informations pertinentes. L'objectif de cette notification initiale est de sensibiliser le CCB, le gouvernement sectoriel ou son CSIRT sectoriel, et le NCCN à l'incident et à ses éventuelles conséquences.

- Des signalements supplémentaires doivent être envoyés régulièrement ou dès que le FSE ou le FSN dispose de nouvelles informations. L'objectif de ces notifications supplémentaires est de tenir le CCB, le gouvernement sectoriel ou son CSIRT sectoriel, et le NCCN informés de l'état de l'incident. Le FSE ou le FSN effectue alors un nouveau rapport sur la plateforme, en indiquant uniquement les nouvelles données et le numéro de référence du rapport initial.

- Un rapport final (à la demande d'une des autorités susmentionnées) avec toutes les informations envoyées au CCB, à l'autorité sectorielle ou à son CSIRT sectoriel, et au NCCN. L'objectif de ce rapport final est de donner un aperçu de l'incident et d'en tirer des conclusions.

Le FSE ou le FSN doit tenir le CCB et l'autorité sectorielle, ou le cas échéant le CSIRT sectoriel, informés de l'évolution de l'incident et des mesures correctives prises.

Déposer une plainte auprès des autorités compétentes

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 des actions à mettre en œuvre (identification Internet, etc.). Pour que les poursuites aient une chance d'aboutir, la chaîne de conservation doit être préservée dans le respect des procédures légales, ce qui suppose de préserver les preuves immédiatement après la détection de l'incident.

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. Il est absolument primordial que vos services apportent toute l'assistance nécessaire et fournissent toutes les informations demandées par les agents compétents pour faire avancer l'enquête.

Par défaut, vous devez vous rendre à votre poste de police local ou celui de votre choix. Les informations concernant les zones de police sont disponibles à cette adresse :

NL FR

I. Police

Si votre organisation est victime d'un incident et, par conséquent, d'une infraction, vous avez la possibilité de déposer une plainte. Par défaut, vous devez vous rendre à votre poste de police local ou celui de votre choix. Pour les cas plus complexes, la police locale sera assistée par les unités régionales de cybercriminalité, les CCU régionaux (ou RCCU), qui sont des unités spécialisées dans la criminalité informatique (piratage, sabotage, espionnage), et/ou par l'unité fédérale de cybercriminalité (ou FCCU). Si l'affaire concerne une infrastructure critique ou un secteur soumis à des règles spécifiques, une procédure spéciale pourra s'appliquer.

II. Juge d'instruction

Il est également possible de saisir directement un magistrat (juge d'instruction). Il s'agit là uniquement d'une mesure exceptionnelle. Par ailleurs, votre organisation aura probablement à faire l'avance des frais d'enquête, car le magistrat conduit alors l'enquête à votre demande.

SIGNALER UNE BRÈCHE DE DONNÉES À CARACTÈRE PERSONNEL À L'AUTORITÉ DE PROTECTION DES DONNÉES

Certaines fuites de données à caractère personnel, c'est-à-dire toute donnée relative à une personne physique qui est ou peut être directement ou indirectement identifiée, doivent être signalées à l'autorité chargée de la protection des données. Pour rappel : les données personnelles désignent toutes les données relatives à une personne physique qui est ou peut être identifiée directement ou indirectement. Un numéro, tel qu'une adresse IP, sera donc dans de nombreux cas considéré comme une donnée personnelle.

Le signalement à la Commission de la protection de la vie privée peut être réalisé en ligne grâce à une application de formulaire électronique sécurisée.
Toutes ces informations sont expliquées en détail dans le manuel d'utilisation du formulaire de signalement.

NL FR

L'obligation de signaler concerne les fuites qui comportent un risque pour les droits et libertés des personnes concernées. Un exemple en est la perte de confidentialité d'une communication, à la suite de laquelle les données de facturation, les adresses, etc. deviennent temporairement visibles pour des tiers. En principe, le délai de notification est de 72 heures après la découverte de la fuite de données

Lorsque votre organisation informe l'Autorité de protection des données, cette dernière peut estimer l'impact de la brèche des données en coopération avec la personne chargée du traitement des données piratées et formuler des recommandations concernant les règles relatives au traitement des données et la nécessité de sécuriser ce traitement. En outre, la ou les personnes responsables du traitement des données devront reconsidérer leur organisation du traitement des données et leur sécurisation, maintenant et à l'avenir. Les organisations issues de secteurs spécifiques, tels que les fournisseurs de services financiers ou les réseaux de communications électroniques, ne doivent pas oublier qu'elles sont déjà soumises à une obligation de signaler à l'Autorité de protection des données tout incident impliquant une brèche de données à caractère personnel.

NOTIFICATION AUX PERSONNES DONT LES DONNÉES À CARACTÈRE PERSONNEL ONT ÉTÉ PIRATÉES

Si la brèche des données va de pair avec un risque élevé pour les intéressés, les personnes dont les données sont concernées par un cas de brèche de données doivent être informées. Le responsable du traitement des données doit signaler la brèche des données aux personnes concernées en utilisant un moyen de communication garantissant que l'information soit reçue le plus tôt possible. Lorsque l'identification des victimes de la brèche est impossible, le responsable du traitement peut les informer par l'intermédiaire des médias publics tout en poursuivant ses efforts en vue d'identifier les personnes concernées afin de les informer en personne.
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 brèche des données ;
- la date (présumée) de l'incident ;
- le type et la nature des données à caractère personnel en cause ;
- les conséquences possibles de la brèche des données pour les personnes concernées ;
- les circonstances dans lesquelles la brèche des données s'est produite ;
- les mesures prises par le responsable du traitement pour prévenir la brèche des données ;
- les mesures recommandées par le responsable du traitement aux personnes concernées pour limiter le préjudice.

BRÈCHE DE DONNÉES

Rex mundi a obtenu les données de votre entreprise. Elles contiennent des informations sensibles à propos de vos clients ; ainsi, leur vie privée est en jeu. Il menace de publier toutes les informations sur Internet via son Twitter.

05 SUIVI ET CLÔTURE DE L'INCIDENT : TIRER LES ENSEIGNEMENTS DE CHAQUE INCIDENT !

À l'instar de tout autre type d'incident, la clôture des incidents de cybersécurité doit être faite dans les règles. En outre, il est primordial de tirer les enseigne- ments de chaque incident afin de définir les améliorations à apporter à l'avenir.

ÉVALUATION DES ENSEIGNEMENTS TIRÉS ET ACTIONS FUTURES : ORGANISER UN BILAN POST-INCIDENT

Le bilan post-incident est un document très utile car il s'appuie sur des données et des préjudices réels. Il permet à l'organisation d'évaluer son plan de réponse en cas d'incident de cybersécurité et le budget qu'elle y consacre.

OBJECTIF
Après leur résolution, tous les incidents de cybersécurité doivent faire l'objet d'un examen formel pour vérifier si des mécanismes de sécurité ou des contrôles d'atténuation doivent être mis en place ou adaptés pour prévenir tout incident similaire à l'avenir.

POURQUOI ?
Les incidents de cybersécurité peuvent révéler des défaillances importantes de votre stratégie ou de vos pratiques en matière de sécurité. Chaque incident important doit être analysé pour déterminer si des enseignements peuvent en être tirés en vue d'apporter des améliorations à l'avenir.

COMMENT DOIT SE PRÉSENTER CE BILAN POST-INCIDENT ?
Le bilan post-incident et ses éventuels enseignements doivent faire partie intégrante de la gestion de tous les incidents de cybersécurité.
Voici une liste de questions utiles pour l'évaluation :

- Le plan et les procédures de gestion en cas d'incident de cybersécurité ont-ils été observés ? Se sont-ils révélés appropriés ? Le plan doit-il être aménagé sur certains points ?
- L'information était-elle disponible à temps ? Dans la négative, aurait-il été possible de l'obtenir plut tôt, et si oui comment ?
- Parmi les mesures et les actions que vous avez mises en œuvre, certaines se sont-elles révélées être un frein à la reprise ?
- Pouvez-vous apporter des améliorations en matière de partage d'informations avec d'autres organisations ?
- Quelles actions correctives sont susceptibles de prévenir tout incident similaire à l'avenir ?
- Existe-t-il certains précurseurs ou indicateurs qui pourraient être surveillés afin de détecter plus facilement des incidents similaires à l'avenir ?
- Quels outils ou ressources supplémentaires sont nécessaires pour détecter, analyser et atténuer les incidents de cybersécurité à l'avenir ?
- L'équipe chargée de la réponse en cas d'incident de cybersécurité a-t-elle disposé d'une autorité organisationnelle appropriée pour conduire la réponse à l'incident ? Devez-vous recruter d'autres personnes ou signer un contrat avec un cabinet de consultants, d'avocats, etc. pour vous assurer leurs services en cas d'incident de cybersécurité à l'avenir ?

II. SUIVI DE L'INCIDENT ET COMPTE-RENDU

Chaque incident et toutes les actions entreprises doivent absolument être documentés et tous ces documents doivent être conservés ensemble. Des incidents similaires pourraient se produire et nécessiter d'utiliser les mêmes procédures, ou un incident de moindre importance pourrait faire partie d'un incident de grande ampleur découvert ultérieurement. En outre, il faut également signaler l'incident aux parties prenantes concernées, tant en interne qu'en externe. Utilisez les résultats de votre bilan post-incident pour déterminer quelles parties prenantes doivent être informées. En interne, la haute direction de l'organisation doit toujours être considérée comme une partie prenante et, par conséquent, recevoir un rapport documenté sur les événements, les actions entreprises, les points qui ont posé problème ou les points qui ont été un succès, etc.

OBJECTIF

SUIVI
Tous les incidents de cybersécurité et les corrections appliquées doivent être documentés.

COMPTE-RENDU
Tous les incidents de cybersécurité et les corrections appliquées doivent faire l'objet d'un rapport adressé à la haute direction et, lorsque cette fonction existe au sein de votre organisation, au responsable de la sécurité de l'information.

POURQUOI ?

SUIVI
Des incidents similaires pourraient se produire et nécessiter d'utiliser les mêmes procédures, ou un incident de moindre importance pourrait faire partie d'un incident de grande ampleur découvert ultérieurement.

COMPTE-RENDU
La haute direction et/ou les personnes de votre organisation chargées d'analyser les risques dans votre organisation (par exemple, un comité du risque opérationnel ou équivalent) doivent être informées de tout incident de cybersécurité.

COMMENT DOIT SE PRÉSENTER CE DOCUMENT DE SUIVI ET DE COMPTE- RENDU ?

Un rapport dûment documenté doit être rédigé pour tous les incidents de cybersécurité et conservé avec les autres rapports d'incident de cybersécurité. Ce rapport peut s'appuyer sur les conclusions du bilan post-incident.
Tous les incidents de sécurité graves doivent être signalés immédiatement à la haute direction.
Au moins une fois par an, tous les incidents de cybersécurité doivent faire l'objet d'un rapport et d'explications à la haute direction et aux personnes de votre organisation chargées de l'analyse des risques dans votre organisation.

GLOSSAIRE

Actif Toute ressource ou capacité. Les actifs d'un fournisseur de services incluent tout ce qui contribue à la prestation d'un service. Les actifs peuvent entrer dans l'une des catégories suivantes : gestion, organisation, processus, connaissances, personnes, informations, applications, infrastructures et capital financier.

APT APT est l'acronyme d'« Advanced Persistant Threat », qui signifie « menace persistance avancée ». Il désigne un ensemble de processus de piratage informatique furtifs et continus. Dans le cas d'un APT, l'auteur du piratage procède par phases multiples pour pénétrer dans un réseau afin d'éviter d'être détecté, et récolte des informations précieuses sur le long terme.

Artefact Un artefact est un objet présentant un intérêt d'archéologie numérique.

Backdoor Littéralement « porte dérobée » en français. Dans un logiciel ou un système informatique, il s'agit d'une méthode pour contourner les dispositifs de sécurité. Peut être utilisé par les administrateurs système ou les programmeurs à des fins légitimes, mais dans ce guide, nous utilisons ce terme pour faire référence à sa version illégitime, c'est-à-dire une porte secrète utilisée par les pirates informatiques et les agences de renseignement pour accéder de manière illicite aux systèmes informatiques sans être détectés.

Botnet Un parc d'ordinateurs (souvent des dizaines de milliers) exploités par une ou plusieurs personnes (appelés « botmasters ») à l'aide de programmes malveillants, ou maliciels. Les botnets [terme construit de l'anglais par la contraction de « robot » et de « net » (pour réseau), littéralement « robots en réseau »] sont utilisés pour envoyer des spams (messages indésirables), pour lancer une attaque DDoS, pour propager un programme malveillant, etc.

DDoS DDoS est l'acronyme de « Distributed Denial of Service » (attaque par déni de service). Dans le cas d'une attaque DDoS, un botmaster ordonne aux ordinateurs de son botnet d'accéder à un site déterminé. Le serveur du site Web visé subira une surcharge et cessera de fonctionner normalement.

DMZ DMZ est un acronyme signifiant « zone démilitarisée » et fait référence au sous-réseau physique ou logique (zone) qui sépare un réseau local (LAN) interne des autres réseaux non fiables, par exemple Internet. L'objet d'une DMZ est d'ajouter une couche de sécurité supplémentaire. Son nom est tiré de l'expression « zone démilitarisée », qui désigne une zone séparant des États souverains dans laquelle les opérations militaires sont interdites.

Hôte Un ordinateur qui héberge un site Web ou d'autres données accessibles sur Internet ou qui fournit d'autres services à un réseau.

IDS IDS est l'acronyme d'« Intrusion Detection System » (système de détection d'intrusion). Il s'agit d'un système automatisé détectant le piratage et l'accès non autorisé à un système informatique ou un réseau.

IP IP est l'acronyme désignant le protocole d'adresse Internet. Il s'agit d'une étiquette numérique attribuée à chaque dispositif participant à un réseau informatique. Les adresses IP sont utilisées pour identifier et localiser les dispositifs.

Patch Un patch, ou correctif en français, est un petit logiciel, souvent développé par les producteurs d'un logiciel spécifique en vue d'actualiser, de réparer (des bogues ou des vulnérabilités) ou d'améliorer ce même logiciel. Il permet de modifier un logiciel sans devoir le réinstaller complètement.

PGP PGP est l'acronyme de « Pretty Good Privacy », qui est un programme informatique de chiffrement et de déchiffrement cryptographique de données se proposant de garantir la confidentialité et l'authentification pour la communication des données. PGP peut être utilisé pour la signature, le chiffrement et le déchiffrement de textes, de courriers électroniques, de fichiers, de répertoires et de partitions de disque entières, ainsi que pour augmenter la sécurité des communications par courrier électronique.

Poste de travail Un ordinateur (matériel).

RAM RAM est l'acronyme de « Random Access Memory » (mémoire vive en français). La RAM constitue le type de stockage de données le plus fréquent sur les ordinateurs et d'autres dispositifs, tels que les imprimantes. Dans un dispositif RAM, toutes les données sont accessibles dans (pratiquement) le même délai, quel que soit leur emplacement physique à l'intérieur de la mémoire.

Réseau Un réseau de télécommunication permettant à des ordinateurs ou autres dispositifs d'échanger des données. Internet est le réseau informatique le plus célèbre.

Rootkit Un ensemble de logiciels informatiques, souvent malveillants, conçus dans un double objectif : 1) permettre l'accès à un ordinateur ou à des zones où ce logiciel serait normalement interdit, tout en 2) masquant son existence ou l'existence d'autres logiciels. La détection des rootkits est difficile, car un rootkit peut être capable de tromper le logiciel censé le découvrir. Leur éradication peut s'avérer compliquée, voire pratiquement impossible.

Sauvegarde Les procédures de sauvegarde sont utilisées pour copier des fichiers sur un second support, tel qu'un disque dur ou une bande magnétique, ou encore dans le cloud. Les fichiers de sauvegarde doivent être conservés dans un lieu hors site. Les sauvegardes sont habituellement automatisées en utilisant des commandes du système d'exploitation ou des programmes utilitaires de sauvegarde. La plupart des programmes de sauvegarde compressent les données afin de limiter l'espace de stockage utilisé.

Serveur de commande et de contrôle Un serveur centralisé capable d'envoyer des commandes et de recevoir des informations provenant d'ordinateurs intégrés à un botnet. Le serveur de commande et de contrôle permet au botmaster de contrôler à distance le groupe d'ordinateurs intégrés à son botnet.

SNORT Snort est un système de prévention et de détection des intrusions libre et ouvert. www.snort.org

Spoofing Terme anglais signifiant « usurpation ». Une attaque de spoofing est une situation dans laquelle une personne ou un programme parvient à se faire passer pour un(e) autre en falsifiant des données et se procurant ainsi un avantage illégitime. Par exemple, le spoofing par courrier électronique consiste à créer des messages électroniques avec une adresse d'expéditeur falsifiée.

VPN VPN est l'acronyme de « Virtual Private Network » (réseau privé virtuel en français). Il désigne un groupe d'ordinateurs mis en réseau par l'intermédiaire d'un réseau public tel qu'Internet. Les entreprises utilisent les VPN pour connecter des centres de données distants ou pour permettre à leurs employés d'accéder de manière sécurisée à l'intranet de l'entreprise lorsqu'ils sont hors de leurs locaux.

Vulnérabilité Une faiblesse dans un système, une application ou un réseau qui permet une exploitation ou une utilisation malveillante.

BIBLIOGRAPHIE

CERT-EU (2012), *Guidelines of the CERT-EU for data acquisition for investigation purposes (Directives de CERT-EU pour l'acquisition de données aux fins d'enquête).*
Source : http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_04_Guideline_DataAcquisition_v1_4_4.pdf.

CREST (2013), *Cyber Security Incident Response Guide (Guide de la réponse en cas d'incident de cybersécurité).*
Source : http://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide.pdf.

ENISA (2010), *Good Practice Guide for Incident Management (Bonnes pratiques pour la gestion d'incident).*
Source : https://www.enisa.europa.eu/activities/cert/support/incident-management.

FEB, ICC, B-CCentre, *Isaca, EY, Microsoft (2013), Belgian Cyber Security Guide (Guide belge de la cybersécurité).*
Source FEB : https://www.feb.be/publications/guide-belge-de-la-cyber-securite_2014-05-26/

ISO/IEC 20000-1 (2011), *Technologies de l'information - Gestion des services - Partie 1 : Exigences du système de gestion des services.*
Source : http://www.iso.org/iso/fr/catalogue_detail?csnumber=51986

ISO/IEC 27001 (2013), *Technologies de l'information - Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Exigences.*
Source : http://www.iso.org/iso/fr/catalogue_detail?csnumber=54534

Mars (2015), *European 2015 Cyber Risk Survey Report (Rapport d'étude européen sur les cyber-risques 2015).* Source : http://belgium.marsh.com/Portals/95/Documents/15%2010-023%20European%20Cyber%20 survey%20report.pdf.

Microsoft TechNet, *Réponse aux incidents de sécurité informatique.*
Source : https://technet.microsoft.com/fr-be/library/cc700825.aspx?f=255&mspperror=-2147217396.

NIST (2012), *Framework for Improving Critical Infrastructure Cyber Security – Version 1.0 (Cadre de travail pour améliorer la cybersécurité des infrastructures critiques – Version 1.0).*
Source : http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

NIST (2012), *Computer Security Incident Handling Guide – Recommendations of the National Institute of Standards and Technology (Guide de gestion des incidents de sécurité informatique – Recommandations du National Institute of Standards and Technology).*
Source : http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

SANS Institute, *SCORE Security Checklist on APT Incident Handling (Institut SANS, liste de contrôle de sécurité SCORE pour la gestion des incidents APT).*
Source : https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist.pdf.

SANS Institute (2003), *Sample Incident Handling Forms [Institut SANS (2003), Modèles de formulaires pour la gestion d'incident].*
Source : https://www.sans.org/score/incident-forms/.

SANS Institute (2007), *An Incident Handling Process for Small and Medium Businesses [Institut SANS (2007), Processus de gestion des incidents pour les petites et moyennes entreprises].*
Source : https://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791.

SANS Instiute (2008), I*ncident Handling for SMEs (Small to Medium Enterprises) [Institut SANS (2008), Gestion des incidents pour les PME (petites et moyennes entreprises)].*
Source : https://www.sans.org/reading-room/whitepapers/incident/incident-handling-smes-small-medium-enterprises-32764.

SANS Institute (2008), *Security Incident Handling in Small Organizations [Institut SANS (2008), Gestion des incidents de sécurité dans les petites organisations].*
Source : https://www.sans.org/reading-room/whitepapers/incident/security-incident-handling-small-organizations-32979.

REMERCIEMENTS

GROUPE DE RÉDACTION

Cathy Suykens (Cyber Security Coalition)
Anneleen Dammekens (VBO)
Daniel Letecheur (BOSA - formerly FEDICT)
Georges Ataya (Solvay Brussels School)
Luc Beirens (Deloitte)
Ferdinand Casier (Agoria)
Phédra Clouner (CCB)
Walter Coenraets (FCCU)
Miguel De Bruycker (CCB)
Dirk De Nijs (ICT CONTROL)
Pedro Deryckere (CCB - Afdeling CERT.be)
Nathalie Dewancker (Proximus)
Steven Goossens (Proximus)
Ann Mennens (European Commission, formerly B-CCENTRE)
Philippe Mermuys (Allianz)
Benoit Montens (Assuralia)
Ronny Tronquo (KBC Groep)
Erik Van Buggenhout (Nviso)
Geoffrey Schreiber (KPMG Advisory)
Kara Segers (KPMG Advisory)
Mathieu Tulpinck (Legal consultant)

EDITEUR RESPONSABLE

Jan De Blauwe
8 rue des Sols
1000 Bruxelles
info@cybersecuritycoalition.be
www.cybersecuritycoalition.be

DATE DE LA PREMIERE PARUTION

Janvier 2016

DATE DE LA DEUXIEME PARUTION

Septembre 2021

ANNEXE

Types d'incidents les plus fréquents et moyens de les neutraliser

TYPE D'INCIDENT	DÉFINITION	CIBLE POSSIBLE	VULNÉRABILITÉS SUSCEPTIBLES D'ÊTRE EXPLOITÉES	RÉPONSES POSSIBLES
Ingénierie sociale : hameçonnage (phishing), harponnage (spear phishing), vishing (hameçonnage par téléphone)	Manipuler et piéger quelqu'un en vue de lui soutirer des informations (par ex., un mot de passe ou des informations financières) utilisables pour attaquer des systèmes ou des réseaux.	CEO Comptabilité		
Hameçonnage (phishing), harponnage (spear phishing), vishing (hameçonnage par téléphone)	Tentative d'obtenir des informations sensibles (par ex., des identifiants et des mots de passe de clients) auprès de clients en se faisant passer pour une personne ou organisation légitime et de confiance.			
Accès non autorisé	Lorsqu'une personne parvient à accéder physiquement ou logiquement à un réseau, un système, une application, des données ou d'autres ressources informatiques, sans autorisation.	Informations de clients Informations de cartes de crédit Applications créant ou traitant des paiements Sites et services Web	Mot de passe craqué ou reniflé Vulnérabilités des systèmes non corrigées Ingénierie sociale Utilisateurs imprudents ou procédures non fiables	Corriger les vulnérabilités ou suspendre l'exploitation Vérification de la présence de programmes malveillants (maliciels furtifs, portes dérobées, chevaux de Troie, etc.) Modification de mots de passe ou désactivation de comptes Collecte de preuves forensics Bloquer l'accès (réseau) aux ressources ciblées
Déni de service	Toute attaque empêchant ou perturbant l'utilisation autorisée de réseaux, de systèmes ou applications en épuisant les ressources.	Système de courrier électronique Dispositifs de réseau Serveurs d'application Sites et services Web	Faiblesses des filtres antispam Vulnérabilités des systèmes non corrigées Mauvaise configuration des systèmes ou dispositifs	Bloquer le trafic Contacter le FAI (Fournis- seur d'Accès Internet) Déconnecter le(s) système(s) infecté(s)
Attaque par code malveillant Logiciel à demande de rançon (ransomware en anglais) : type de programme malveillant qui restreint l'accès au système informatique qu'il infecte et qui réclame une rançon à verser au(x) créateur(s) du programme malveillant en contrepartie de la levée de la restriction d'accès. Certaines formes de rançongiciels chiffrent les fichiers sur le disque dur du système alors que d'autres verrouillent simplement le système et affichent un message pour persuader l'utilisateur de payer la rançon demandée.	Une attaque de code malveillant désigne une infection ou une menace d'infection (à grande échelle) par un virus, un ver informatique, un cheval de Troie ou toute autre entité malveillante à base de code informatique.	N'importe quel serveur ou même dispositif du réseau peut être la cible d'une attaque de code malveillant, mais certains systèmes présentent un profil de risque accru (par ex., les systèmes qui sont connectés directement ou indirectement au monde extérieur). Les utilisateurs de postes de travail peuvent être la cible d'une telle attaque par l'intermédiaire du courrier électronique, de dispositifs de stockage USB, de la consultation de sites Web ou d'applications Web, etc.	Vulnérabilités des systèmes non corrigées (par ex., Flash ou JavaScript) Antivirus non installé, inactif ou fichier de signature non mis à jour Comportement inapproprié ou imprudent de l'utilisateur (par ex., l'utilisation de dispositifs de mémoire USB infectés)	Bloquer le trafic Web malveillant Appliquer des correctifs Mettre à jour les fichiers de signature antivirus Exécuter un outil de nettoyage des virus si disponible Exécuter un outil d'évaluation des vulnérabilités pour obtenir une liste des ressources vulnérables Réinstaller complètement le système infecté Éteindre les dispositifs vulnérables Éteindre ou déconnecter le(s) système(s) infecté(s)

TYPE D'INCIDENT	DÉFINITION	CIBLE POSSIBLE	VULNÉRABILITÉS SUSCEPTIBLES D'ÊTRE EXPLOITÉES	RÉPONSES POSSIBLES
Usage inapproprié	Un incident lié à un usage inapproprié est un incident impliquant un employé interne ou un sous-traitant violant un code de conduite ou une politique informatique. Un comportement inapproprié n'est pas toujours malveillant ou ciblé. Parfois, un utilisateur agira simplement de manière imprudente, voire ignorera purement et simplement qu'il a enfreint une politique ou un code de conduite. Le comportement inapproprié constituera parfois un incident de sécurité grave en soi, mais il peut également être la cause ou le déclencheur d'un autre incident grave (par ex., l'infection par un programme malveillant, la perte de données critiques).	Opérations de paiement Informations de cartes de crédit Informations commerciales et personnelles sur les clients Information confidentielle en général	Mauvaise gestion ou mauvais contrôle des données confidentielles Mauvaise gestion des mots de passe utilisateur Absence de séparation des responsabilités, accumulation de droits d'accès Absence de sécurité ou de surveillance des applications Absence de procédures ou de contrôles visant à faire appliquer les politiques et codes de conduite	Informer le service conformité et/ou juridique et leur demander conseil Désactiver des utilisateurs ou retirer des droits d'accès Faire des copies des logs et autres informations cruciales recevables devant les tribunaux en vue de garantir une traçabilité et d'apporter des preuves des événements Vérifier les journaux et autres informations pour trouver des traces de l'infraction
Fraude	La fraude est un type de comportement inapproprié malveillant par nature et visant un enrichissement personnel en détournant les systèmes, applications on informations d'une entreprise.			
Perte ou vol de données	Il s'agit d'un incident impliquant la perte ou le vol d'informations confidentielles. Une information peut être confidentielle en raison de sa valeur pour l'entreprise, ou parce qu'elle est protégée par des lois et règlements internes ou externes. Les incidents liés à une perte de données peuvent avoir des conséquences financières importantes en raison de la responsabilité financière ou des atteintes possibles à l'image de la société, pour peu que l'information elle-même ou le fait qu'elle ait été perdue soit rendu public ou porté à la connaissance des mauvaises personnes.	Informations personnelles à propos des employés ou des clients (protégées par des lois ou des considérations associées à la vie privée) Informations de cartes de crédit Informations commerciales sur les clients Informations confidentielles sur les bilans Informations confidentielles à propos de la stratégie de l'entreprise, de ses projets en cours et de ses décisions, etc.	Mauvaise utilisation des dispositifs de stockage portables (clés USB, CD, sauvegarde sur bande, etc.) Mauvaise utilisation de l'équipement mobile (ordinateurs portables, smartphones, etc.) Mauvaise utilisation des informations confidentielles imprimées Manquement à la politique en matière de rangement de bureau	Évaluer le niveau de protection des données, le cas échéant (chiffrement, protection par mot de passe, dispositif spécifique nécessaire pour lire les données) Informer le service conformité et/ou juridique ou votre conseiller juridique externe et leur demander conseil Informer le service communication et la direction, définir une stratégie de communication Informer le propriétaire des données perdues ou volées
Détournement de marque	Il s'agit d'un incident impliquant une personne qui détourne votre marque et vos marques déposées.	Enregistrement de noms DNS contenant la marque Usurpation (spoofing) de conceptions de sites Web Usurpation d'adresses et de modèles de courrier électronique	Non applicable	Informer la police (en cas de vol) Réclamer une mise hors service du site Web Informer les clients


VBO
Verbond van
Belgische
Ondernemingen


b·ccentre
BELGIAN CYBERCRIME CENTRE OF EXCELLENCE
FOR TRAINING, RESEARCH & EDUCATION


ICT CONTROL
Your Trusted Advisor


BNP PARIBAS
FORTIS


Solvay Brussels School
Economics & Management


KBC


proximus


Deloitte.


KPMG