plan d'intervention en cas d'incident cybernétique

Modèle

# Utilisation de ce document

* Ce document contient des lignes directrices et des exemples que les organisations peuvent suivre pour soutenir l'élaboration de leur propre plan d'intervention en cas d'incident cybernétique (CIRP). Le modèle n'est pas exhaustif. Le CIRP de chaque organisation doit être adapté à son environnement opérationnel, à ses priorités, à ses ressources et à ses engagements. Certains champs contiennent un **exemple de texte en vert**. Ce texte n'est donné qu'à titre d'exemple et ne doit pas être utilisé comme base de votre CIRP.
* Une boîte à outils CIRP supplémentaire est également disponible. Elle contient des listes de contrôle et des modèles qui peuvent être utilisés lors de l'élaboration de votre CIRP.

Contenu

[Utilisation de ce document 2](#_Toc170201951)

[Autorité et révision 3](#_Toc170201952)

[Contrôle et révision des documents 3](#_Toc170201953)

[Gestion des versions 3](#_Toc170201954)

[Buts et objectifs 4](#_Toc170201955)

[Normes et cadres 4](#_Toc170201956)

[Définitions et acronymes 4](#_Toc170201957)

[Processus de réponse aux incidents 5](#_Toc170201958)

[Incidents de sécurité courants et réponses 6](#_Toc170201959)

[Terminologie et définitions 6](#_Toc170201960)

[Vecteurs de menace courants 7](#_Toc170201961)

[Incidents cybernétiques courants 8](#_Toc170201962)

[Rôles et responsabilités 8](#_Toc170201963)

[Points de contact pour le signalement des cyberincidents 9](#_Toc170201964)

[Équipe de réponse aux incidents cybernétiques (CIRT) 9](#_Toc170201965)

[Équipe de gestion (MT) 9](#_Toc170201966)

[Rôles et relations 10](#_Toc170201967)

[Communications 11](#_Toc170201968)

[Communication interne 11](#_Toc170201969)

[Communication externe 11](#_Toc170201970)

[notification pour le NIS2 12](#_Toc170201971)

[Procédures d'appui et feuilles de route 13](#_Toc170201972)

[Soutenir les procédures opérationnelles standard (POS) 13](#_Toc170201973)

[Supports pour les livres de jeu 13](#_Toc170201974)

[Notification des parties prenantes et signalement des incidents 13](#_Toc170201975)

[Processus de réponse aux incidents 14](#_Toc170201976)

[Détection, recherche, analyse et activation 14](#_Toc170201977)

[Classification des incidents 14](#_Toc170201978)

[questions sur les enquêtes sur les incidents 15](#_Toc170201979)

[Escalade et désescalade 15](#_Toc170201980)

[Confinement, collecte de preuves et remédiation 16](#_Toc170201981)

[Confinement 16](#_Toc170201982)

[Documentation 16](#_Toc170201983)

[Collecte et conservation des preuves 17](#_Toc170201984)

[Plan d'action de remédiation 17](#_Toc170201985)

[Récupération 18](#_Toc170201986)

[Enseignements tirés. 18](#_Toc170201987)

# Autorité et révision

## Contrôle et révision des documents

|  |  |
| --- | --- |
| **Vérification des documents** |  |
| Auteur |  |
| Propriétaire |  |
| Date de création |  |
| Dernière révision par |  |
| Date de la dernière révision |  |

.

## Gestion des versions

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date d'approbation** | **Approuvé par** | **Description du changement** |
|  |  |  |  |

# Buts et objectifs

Décrivez ici l'objectif de votre plan d'intervention en cas d'incident cybernétique (CIRP).

*Par exemple :*

L'*objectif de ce CIRP est de favoriser une réponse rapide et efficace aux cyberincidents, en accord avec les objectifs de l'organisation en matière de sécurité et d'activité.*

*Objectifs du CIRP*

* *Fournir des conseils sur les mesures à prendre pour répondre aux cyberincidents.*
* *Décrire les rôles, les responsabilités, les obligations de rendre compte et l'autorité du personnel et des équipes nécessaires pour gérer les réponses aux cyberincidents.*
* *Décrire les exigences en matière de conformité aux cyberincidents.*
* *Décrire les processus de communication interne et externe en cas de cyberincidents.*
* *Fournir des conseils sur les activités post-incidents afin de soutenir l'amélioration continue.*

# Normes et cadres

Les documents de référence suivants ont servi d'inspiration pour l'élaboration de ce modèle. Les références ne sont pas datées. C'est toujours la dernière édition du document de référence (y compris les modifications éventuelles) qui s'applique.

* [Cadre des principes fondamentaux du cyberespace](https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework) (www.cyfun.be)
* [NIST SP 800-61](https://csrc.nist.gov/pubs/sp/800/61/r2/final)Manuel pour le traitement des incidents de sécurité informatique
* ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27035-3 Gestion des incidents de sécurité de l'information.
* ISO/IEC 27001, Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de gestion de la sécurité de l'information - Exigences
* ISO/IEC 27002, Sécurité de l'information, cybersécurité et protection de la vie privée

Systèmes de gestion de la sécurité de l'information - Mesures de gestion de la sécurité de l'information.

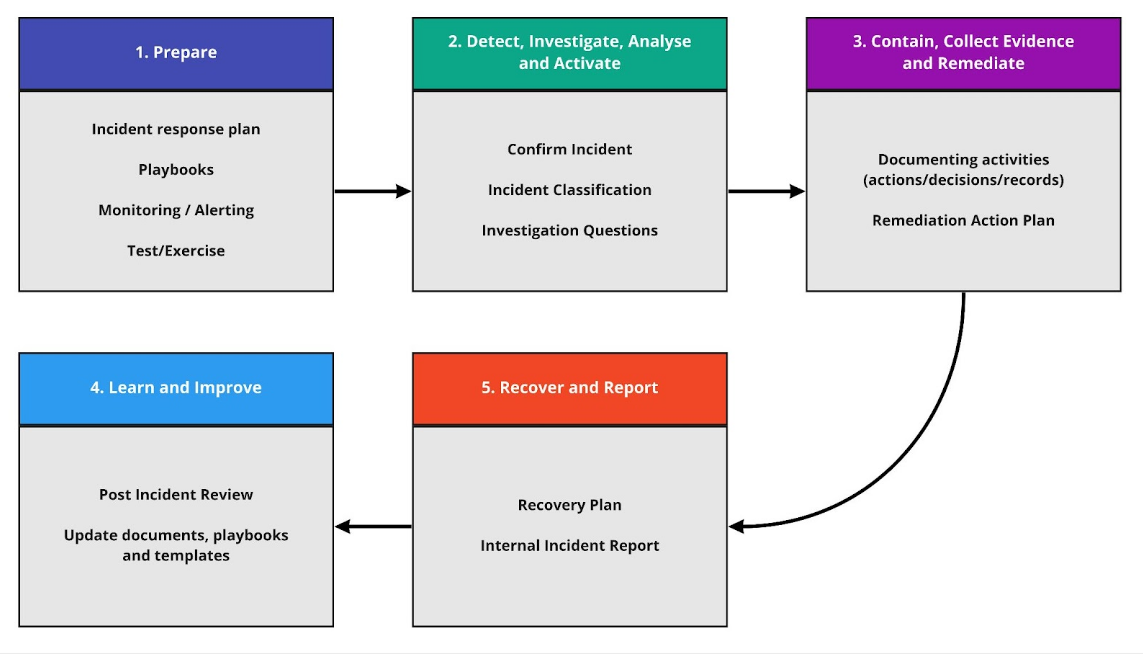
* Centre australien de cybersécurité, plan de réponse aux incidents cybernétiques.

# Définitions et acronymes

Dans le présent document, les termes et définitions des normes ISO/CEI 17000 et ISO/CEI 27000 ainsi que les abréviations suivantes s'appliquent.

|  |  |
| --- | --- |
| **PDG** | Directeur général |
| **DIRECTEUR FINANCIER** | Directeur financier |
| **DPI** | directeur de l'information |
| **CIRP** | Plan de réponse aux incidents cybernétiques |
| **CIRT** | Équipe de réponse aux incidents cybernétiques |
| **RSSI** | responsable de la sécurité de l'information |
| **COO** | chef des opérations |
| **DDoS** | Déni de service distribué |
| **DoS** | Déni de service |
| **DPD** | Délégué à la protection des données |
| **GBA** | Autorité de protection des données |
| **ICS** | Système de contrôle industriel |
| **MT** | L'équipe de direction |
| **RPO** | Point de récupération Objectif |
| **RTO** | Objectif de délai de récupération |
| **SN** | Numéro de série |
| **SPOC** | Point de contact unique |

# Processus de réponse aux incidents



# Incidents de sécurité courants et réponses

## Terminologie et définitions

L'utilisation d'une terminologie cohérente et prédéfinie pour décrire les incidents et leurs conséquences peut s'avérer utile lors d'une intervention. Incluez dans votre plan d'intervention en cas d'incident cybernétique (CIRP) les termes courants utilisés dans votre organisation. Les menaces, événements, alertes et incidents cybernétiques sont définis comme suit :

|  |  |
| --- | --- |
| **incident important** | tout incident qui affecte de manière significative la fourniture de l'un des services dans les secteurs ou sous-secteurs énumérés aux annexes I et II de l'Acte et qui :   * a causé ou peut causer une grave perturbation opérationnelle de l'un des services dans les secteurs ou sous-secteurs énumérés aux annexes I et II ou des pertes financières pour l'entité concernée ; ou * A affecté ou peut affecter d'autres personnes physiques ou morales en causant des dommages matériels ou immatériels significatifs. |
| **incidents évités de justesse** | un événement qui aurait pu compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des services offerts ou accessibles par les réseaux et les systèmes d'information, mais qui a été empêché avec succès ou ne s'est pas produit ; |
| **Cybermenace** | Une cybermenace est une circonstance ou un événement susceptible d'endommager des systèmes ou des informations. Les organisations peuvent dresser une liste des cybermenaces qui les préoccupent. La liste suivante présente l'environnement des menaces et les principales tendances en matière de cybersécurité :   * Courriels d'hameçonnage et escroqueries * Ransomware * Utilisation abusive des faiblesses en matière de sécurité * Compromis sur la chaîne d'approvisionnement en logiciels * Compromettre le courrier électronique professionnel * Cybercriminalité |
| **Événement sur la cybersécurité** | Un événement de cybersécurité est un événement dans un système, un service ou un réseau qui indique une éventuelle violation de la politique de sécurité, une défaillance de la sécurité ou une situation précédemment inconnue qui peut être pertinente pour la sécurité. Un incident de cybersécurité peut devenir un cyberincident, mais n'en est pas encore un.  Parmi les exemples d'événements liés à la cybersécurité, on peut citer (sans s'y limiter) :   * Un utilisateur a désactivé l'antivirus sur son ordinateur * Un utilisateur a supprimé ou modifié des fichiers système * Un utilisateur a redémarré un serveur * Accès non autorisé à un serveur ou à un système. |
| **Alerte à la cybersécurité** | Une alerte de cybersécurité est une notification générée en réponse à un écart par rapport à un comportement normal. Les alertes de cybersécurité sont utilisées pour mettre en évidence des événements de cybersécurité. |
| **Cyberincident** | Un cyberincident est un événement indésirable ou inattendu lié à la cybersécurité, ou une série d'événements de ce type, qui a une forte probabilité de compromettre les activités de l'entreprise. Un cyberincident nécessite une action corrective.  Parmi les exemples d'incidents de cybersécurité, on peut citer (sans s'y limiter) :   * Attaques par déni de service (DoS) * Accès ou tentative d'accès non autorisé à un système * Compromission d'informations sensibles * Apparition de virus ou de logiciels malveillants (y compris les logiciels rançonneurs). |

### Vecteurs de menace courants

Le tableau suivant contient des vecteurs de menace courants tirés du guide de traitement des incidents de sécurité informatique du NIST.

|  |  |
| --- | --- |
| **Type** | **Description** |
| **Supports externes/amovibles** | Une attaque menée à partir d'un support amovible ou d'un périphérique (par exemple, un code malveillant se propageant sur un système à partir d'une clé USB infectée). |
| **Échec** | Une attaque dans laquelle des méthodes de force brute sont utilisées pour compromettre ou détruire des systèmes, des réseaux ou des services (par exemple, un DDoS visant à empêcher ou à refuser l'accès à un service ou à une application ou une attaque par force brute contre un mécanisme d'authentification, tel que les mots de passe). |
| **Web** | Attaque menée à partir d'un site web ou d'une application web (par exemple, une attaque par script intersite utilisée pour voler des informations d'identification ou une redirection vers un site qui exploite une vulnérabilité dans le navigateur et installe des logiciels malveillants). |
| **Courriel** | Une attaque menée par le biais d'un message électronique ou d'une pièce jointe (par exemple, un code d'exploitation déguisé en pièce jointe ou un lien vers un site web malveillant dans le corps d'un message électronique). |
| **Interdiction dans la chaîne d'approvisionnement** | Attaque antagoniste contre du matériel ou des logiciels à l'aide d'implants physiques, de chevaux de Troie ou de portes dérobées, en interceptant et en modifiant des marchandises en transit depuis le vendeur ou le fournisseur. |
| **Imitation** | Une attaque où quelque chose de bénin est remplacé par quelque chose de malveillant (par exemple, l'usurpation d'identité, les attaques de l'homme du milieu, les points d'accès sans fil malveillants et les attaques par injection SQL sont tous liés à l'usurpation d'identité). |
| **Utilisation inappropriée** | Tout incident résultant d'une violation de la politique d'utilisation acceptable d'une organisation par un utilisateur autorisé, à l'exclusion des catégories ci-dessus (par exemple, un utilisateur installe un logiciel de partage de fichiers, ce qui entraîne la perte de données sensibles). |
| **Perte ou vol de matériel** | Perte ou vol d'un appareil ou d'un support informatique utilisé par une organisation (par exemple, un ordinateur portable, un smartphone ou un jeton de vérification). |

### Incidents cybernétiques courants

Le tableau suivant énumère les types courants de cyberincidents et les activités de réponse initiale correspondantes.  
 Décrivez brièvement la réponse initiale à l'incident. Par exemple : avertir les personnes concernées, isoler les dispositifs affectés, suivre les procédures et livres de jeu   
pertinents.

|  |  |
| --- | --- |
| **Type/Description** | **Réponse** |
| **Déni de service (DoS) et déni de service distribué (DDoS) :** inondation d'un service avec du trafic, affectant parfois la disponibilité. | *Comme décrit dans le manuel de jeu X et les procédures....., prenez d'abord des mesures locales pour résoudre le problème.*  *Si cela n'est pas efficace, selon XYZ, demander la permission de passer à la deuxième ligne, etc.* |
| **Phishing :** messages trompeurs visant à obtenir des informations sensibles de la part des utilisateurs (telles que les identifiants bancaires ou professionnels) ou à exécuter un code malveillant pour permettre un accès à distance. | *Si le personnel l'identifie par un contenu nocif réussi*  *Formation, avertissement et remise d'une copie à l'agent de sécurité. Aperçu suivant*  *et d'autres actions de notification externes et internes, etc*. |
| **Ransomware :** utilitaire utilisé pour verrouiller ou crypter les fichiers des victimes jusqu'au paiement d'une rançon. |  |
| **Malware :** cheval de Troie, virus, ver ou autre logiciel malveillant susceptible d'endommager un système informatique ou un réseau. |  |
| **Violation de données :** accès non autorisé à des informations et divulgation de celles-ci. |  |
| **Compromission d'un système de contrôle industriel :** accès non autorisé à un système de contrôle industriel. |  |

# Rôles et responsabilités

Cette section détaille les rôles et les responsabilités des personnes et des équipes clés chargées de la réponse aux incidents et de la prise de décision, notamment l'équipe de réponse aux incidents cybernétiques (CIRT) au niveau opérationnel et l'équipe de gestion (MT) au niveau stratégique.

Tous les membres du personnel énumérés ici doivent connaître leurs responsabilités dans le cadre de ce plan et s'entraîner à réagir.

### Points de contact pour le signalement des cyberincidents

Points de contact internes primaires et secondaires (de secours) pour signaler les cyberincidents pendant une période de 24/7.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nom** | **Heures d'ouverture** | **Coordonnées de la personne à contacter** | **Titre** | **Responsabilités** |
| *Jean Dupont* | *09:00-18:00* | *Numéro de téléphone mobile,* | *Contact principal en cas d'incident* | *SPOC* |

### Équipe de réponse aux incidents cybernétiques (CIRT)

Indiquez les coordonnées de la CIRT chargée de gérer les réponses aux cyberincidents. La composition de votre CIRT variera en fonction de la taille de votre organisation et des compétences et ressources disponibles. Indiquez les coordonnées des fournisseurs externes qui fournissent ou gèrent vos systèmes/applications TIC. Le cas échéant, donnez des détails sur vos fournisseurs externes de réponse aux incidents et sur les services qu'ils fournissent.

Membres de la CIRT chargés de gérer les réponses aux cyberincidents :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nom** | **Rôle de l'organisation** | **Coordonnées de la personne à contacter** | **Rôle du CIRT Titre** | Responsabilités CIRT |
|  |  |  | *Responsable des incidents cybernétiques* | *Programmation des réponses*  *Opérations CIRT* |
|  |  |  | *les ingénieurs de réseau,* |  |
|  |  |  | *les administrateurs de système,* |  |
|  |  |  |  |  |
|  |  |  |  |  |

Pour les incidents de cybersécurité plus importants, la CIRT peut être élargie :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nom** | **Rôle de l'organisation** | **Coordonnées de la personne à contacter** | **Rôle du CIRT Titre** | **Responsabilités CIRT** |
|  |  |  | *Responsable de la communication* | *Informations et avertissements*  *Communication interne* |
|  |  |  | *Conseiller juridique* | *Conseil juridique*  *(y compris la conformité réglementaire)* |
|  |  |  |  |  |

### Équipe de gestion (MT)

Les incidents cybernétiques importants peuvent nécessiter la formation d'une équipe de gestion chargée d'assurer la supervision, l'orientation et le soutien stratégiques de la CIRT, en mettant l'accent sur les points suivants :

* Identifier et gérer les questions stratégiques
* Engagement et communication avec les parties prenantes (y compris les contacts avec l'administration et les ministères, le cas échéant)
* Demande de ressources et de capacités (y compris les besoins logistiques ou financiers urgents et les considérations relatives au personnel pendant l'effort de réponse).

Membres de l'équipe MT chargés de gérer les réponses aux cyberincidents :

|  |  |  |  |
| --- | --- | --- | --- |
| **Nom** | **Coordonnées de la personne à contacter** | **Titre** | **Rôle du MT** |
|  |  | *PDG* | *Président* |
|  |  | *DPI* | *Vice-président* |
|  |  | *RSSI* | *Alerte de sécurité et surveillance de la CIA.* |
|  |  | *COO* | *Fonctions opérationnelles de l'entreprise* |
|  |  | *DIRECTEUR FINANCIER* | *Achats d'urgence et suivi des dépenses* |
|  |  | *Conseil juridique* | *Conformité réglementaire, cyber-assurance* |
|  |  | *Responsable de la communication* | *Relations publiques et engagement des parties prenantes* |
|  |  |  |  |

### Rôles et relations

Le diagramme suivant montre la relation entre le personnel clé et les équipes impliquées dans la réponse.



# Communications

Lors d'une intervention en cas d'incident, de nombreuses parties prenantes différentes ont constamment besoin d'informations. Chacune d'entre elles aura besoin d'un type d'information différent. Dressez votre propre liste de parties prenantes potentielles et assurez-vous que les bonnes informations de contact sont disponibles ! Notez que l'organisation doit disposer de ces informations de contact, mais qu'elle n'a pas toujours besoin de communiquer avec toutes les parties.

Les organisations doivent garder à l'esprit qu'une fois qu'une partie est notifiée, elle demandera des mises à jour périodiques concernant l'incident en question. Il n'y a généralement pas de communication unique et le calendrier de communication doit tenir compte de ces mises à jour périodiques.

La première étape de votre plan de communication spécifique à l'incident consiste à déterminer avec qui vous allez communiquer. Pour ce faire, vous devez déterminer quelles sont les parties prenantes potentielles susceptibles d'être affectées (négativement) par l'incident de cybersécurité auquel vous êtes confronté et si vous êtes légalement tenu de notifier certaines entités.

* Parties prenantes internes : direction générale, cadres concernés, employés
* Parties prenantes externes : médias, clients, fournisseurs, autres partenaires, etc.
* Parties prenantes officielles : GBA, superviseur de secteur, police, ....

Lorsqu'il s'agit de décider ce qu'il faut communiquer et avec qui, une bonne règle de base consiste à ne communiquer que si l'on a besoin de savoir. Il y aura des parties prenantes avec lesquelles vous voudrez communiquer pour contenir l'incident de cybersécurité, et d'autres avec lesquelles vous devrez communiquer parce qu'elles vous demandent des informations (par exemple, les médias) ou parce que vous êtes légalement obligé de les informer.

### Communication interne

*Conseils :*

Outre les rapports de situation réguliers, il peut être nécessaire d'informer les employés de votre organisation d'un cyberincident. C'est important si les réseaux informatiques, les systèmes d'exploitation ou les applications de l'organisation ne fonctionnent plus comme prévu, ou si la situation est susceptible de susciter l'intérêt des médias ou du public.

Les messages clés à l'intention des employés sont les suivants

* Que s'est-il passé et pourquoi ?
* Que se passera-t-il dans un avenir proche ?
* Qu'attend-on des employés ?
* À qui les employés peuvent-ils s'adresser s'ils ont des questions ?

### Communication externe

*Conseils :*

En fonction de l'impact et de la gravité d'un cyberincident, il peut être nécessaire de communiquer avec les parties prenantes externes (y compris les ministres, les médias et le public). Cela est particulièrement important si l'incident touche des réseaux informatiques, des systèmes de contrôle ou des applications dont dépendent des tiers, comme des sites web ou des services destinés au public.

Les messages importants à prendre en compte lors de la communication avec les parties prenantes externes sont les suivants :

* Que s'est-il passé et pourquoi ?
* Quels sont les systèmes/services concernés ?
* Quelles sont les mesures prises pour résoudre la situation ?
* Est-il possible de dire quand la situation sera résolue ?
* Qu'attend-on des parties prenantes externes ?
* Qui les parties prenantes externes peuvent-elles contacter si elles ont des questions/préoccupations ?

**Toutes les communications doivent être examinées et approuvées par le *responsable des communications et le responsable des incidents* avant d'être diffusées.**

### notification pour le NIS2

Entités essentielles et importantes, telles que définies au chapitre 4 (art. 11 et art. 12) du règlement belge sur le [NIS2](https://www.ejustice.just.fgov.be/cgi/article.pl?language=nl&sum_date=2024-05-17&lg_txt=n&pd_search=2024-05-17&s_editie=1&numac_search=2024202344&caller=sum&2024202344=4&view_numac=2024202344f) sont **tenues** de se conformer à un certain nombre d'exigences concernant le signalement d'alertes précoces ou d'**incidents importants\*** au CSIRT national ([CERT.be](https://ccb.belgium.be/nl/cert)).

Ces alertes ou incidents significatifs doivent être signalés à la CERT dans les **vingt-quatre heures** suivant leur découverte. Cette notification comprendra, entre autres, les informations suivantes :

* L'incident résulte-t-il d'un acte illicite ou malveillant ?
* L'incident à chaud a-t-il des implications transfrontalières ?

**Dans les soixante-douze heures** suivant la déclaration de l'incident, l'organisme doit - le cas échéant - fournir un :

* Mise à jour des informations ci-dessus
* Une première évaluation de l'incident significatif, y compris de sa gravité et de ses conséquences.
* Indicateurs de dégradation.

Au **plus tard un mois** après le signalement de l'incident significatif, un rapport final est préparé et transmis à la CERT :

* Description détaillée de l'incident, y compris sa gravité et ses conséquences.
* Le type de menace ou la cause profonde qui a probablement conduit à l'incident.
* Mesures d'atténuation des risques appliquées et en cours (tant sur le plan technique qu'organisationnel).
* Le cas échéant, l'impact transfrontalier de l'incident.

Si l'incident n'est toujours pas résolu après ces 30 jours, un rapport d'avancement sera préparé et transmis à la CERT. Un rapport final sera préparé et envoyé dans un délai d'un mois après la résolution de l'incident.

En plus de l'obligation de déclaration susmentionnée, des déclarations **volontaires** peuvent être faites au CERT :

* *Pour les entités essentielles et importantes* : incidents, cybermenaces, quasi-incidents.
* *Autres organisations, qu'elles relèvent ou non du champ d'application du NIS2* : incidents significatifs, cybermenaces et quasi-incidents.

# Procédures d'appui et feuilles de route

### Soutenir les procédures opérationnelles standard (POS)

Les procédures opérationnelles standard (POS) disponibles pour soutenir la réponse aux incidents :

* *Détection, triage et analyse des événements*
* *Plan de continuité des activités*
* *Plan de reprise après sinistre.*

### Supports pour les livres de jeu

Les livres de jeu disponibles fournissent des lignes directrices étape par étape pour les réponses à des incidents courants :

* *Plan de réponse aux incidents de cybersécurité -* ***Phishing***
* *Plan d'intervention en cas d'incident de cybersécurité* ***- intrusion/vol de données***
* *Plan de réponse aux incidents de cybersécurité* ***- Malware***
* *Plan de réponse aux incidents de cybersécurité* ***- Ransomware***
* *Cyber Security Incident Response Playbook* ***- Denial of Service (Déni de service).***

# Notification des parties prenantes et signalement des incidents

Les procédures de notification interne et externe et de signalement des incidents sont les suivantes :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type d'incident/**  **seuil** | **Organisation  souhaitant  recevoir une  notification  ou un rapport** | **Coordonnées  de l'organisation notifiante.** | **Principales exigences en matière de notification et de rapport et lien avec les informations organisationnelles** | **Personnel responsable** |
| Ransomware | Centre de cybersécurité de Belgique. CERT.BE | info@ccb.belgium.be | https://www.cert.be/en/report-incident-0 | Responsable des incidents cybernétiques |
| Violation de données à caractère personnel | Autorité de protection des données | +32 (0)2 274 48 00  +32 (0)2 274 48 35  contact@apd-gba.be | https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/datalek-van-persoonsgegevens | Conseiller juridique ou DPD |

* **dresser la liste des exigences légales et réglementaires pour votre entreprise.**
* **S'il existe une police d'assurance cybernétique, vérifiez les exigences qu'elle contient pour vous assurer que vous vous y conformez.**

# Processus de réponse aux incidents

# Détection, recherche, analyse et activation

Référez-vous à vos propres procédures opérationnelles standard pour détecter, enquêter et analyser les incidents. Celles-ci peuvent inclure la manière dont vous prenez connaissance d'un événement ou d'un incident et ce que vous faites immédiatement en réponse.

Les incidents peuvent être détectés de différentes manières, y compris mais sans s'y limiter :

* Incidents autodétectés (par exemple, systèmes de détection et de prévention des intrusions)
* Réception de notifications de la part de prestataires de services ou de vendeurs
* Rapports reçus de tiers de confiance tels que le Centre for Cyber Security Belgium, MITRE ATT&CK, ENISA....

### Classification des incidents

Cela peut aider à hiérarchiser les ressources. Les facteurs de classification peuvent être

* Conséquences de l'incident (confidentialité, intégrité et disponibilité des informations et des systèmes)
* Parties prenantes impliquées (internes et externes)
* Type d'incident
* Impact sur les entreprises et la communauté.

|  |  |
| --- | --- |
| **Classification des incidents** | **Descriptions** |
| **Critique** | *Un incident critique ayant un impact très important. Il s'agit souvent d'une défaillance complète d'un système, d'une perte de données clients, d'une atteinte majeure à la sécurité ou d'une défaillance d'une infrastructure critique.* |
| **Haut** | *Un incident majeur ayant un impact important. Il peut inclure des défaillances partielles du système ou affecter des fonctionnalités critiques.* |
| **Moyen** | *Incident à impact modéré pouvant affecter des fonctionnalités non critiques ou causer des désagréments aux utilisateurs.* |
| **Faible** | *Un petit incident à faible impact qui peut consister en des défaillances de fonctions non critiques ou des plaintes d'utilisateurs de faible priorité.* |

### questions sur les enquêtes sur les incidents

Une liste de questions d'enquête peut vous aider à répondre à un incident et à en comprendre la portée et l'impact. Les données disponibles ne permettent pas de répondre à toutes les questions et celles-ci peuvent évoluer au fur et à mesure que l'enquête progresse.

* *Qui a découvert ou signalé l'incident ?*
* *Quand l'incident a-t-il été découvert ou signalé ?*
* *Où l'incident a-t-il été découvert ou localisé ?*
* *Quel est l'impact de l'incident sur les opérations ?*
* *Quelle est l'étendue de l'incident concernant le réseau et les applications ?*

### Escalade et désescalade

Les cyberincidents peuvent faire l'objet d'une escalade ou d'une désescalade. Les rôles qui peuvent escalader ou désescalader doivent être présentés dans un tableau.

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification des incidents** | **Action** | **Raison de l'escalade/désescalade** | **Décideur** |
|  |
| **Critique** | Désescalade à un niveau élevé |  |  |  |
| **Haut** | L'escalade de la critique |  |  |  |
| Désescalade vers la moyenne |  |  |  |
| **Moyen** | De plus en plus élevé |  |  |  |
| Désescalade vers le bas |  |  |  |
| **Faible** | De l'escalade à la moyenne |  |  |  |

# Confinement, collecte de preuves et remédiation

### Confinement

Le confinement est important avant qu'un incident ne submerge les ressources ou n'aggrave les dommages. La plupart des incidents doivent être maîtrisés, c'est pourquoi il est important d'en tenir compte dès le début de la gestion d'un incident. L'endiguement donne le temps d'élaborer une stratégie de rétablissement adaptée. Un élément essentiel du confinement est la prise de décision (par exemple, arrêter un système, se déconnecter d'un réseau, désactiver certaines fonctions). Ces décisions sont beaucoup plus faciles à prendre s'il existe des stratégies et des procédures prédéterminées pour contenir l'incident. Les organisations doivent définir les risques acceptables en cas d'incident et élaborer des stratégies en conséquence.

Les stratégies de confinement varient en fonction du type d'incident. Par exemple, la stratégie de confinement d'une infection par un logiciel malveillant via le courrier électronique est très différente de celle d'une attaque DDoS sur un réseau. Les organisations devraient préparer des stratégies de confinement distinctes pour chaque type d'incident majeur, avec des critères clairement documentés pour faciliter la prise de décision. Les critères permettant de déterminer la bonne stratégie sont notamment les suivants

* Risque de détérioration et de vol des ressources
* Conservation des preuves
* Disponibilité des services (par exemple, connectivité du réseau, services fournis à des parties externes)
* Le temps et les ressources nécessaires à la mise en œuvre de la stratégie
* Efficacité de la stratégie (par exemple, endiguement partiel, endiguement total)
* Durée de la solution (par exemple, solution d'urgence à retirer dans les quatre heures, solution temporaire à retirer dans les deux semaines, solution permanente).

Dans certains cas, certaines organisations redirigent l'attaquant vers un bac à sable (une forme de confinement) afin de pouvoir surveiller les activités de l'attaquant, généralement pour recueillir des preuves supplémentaires. L'équipe de réponse aux incidents doit discuter de cette stratégie avec le service juridique afin de déterminer si elle est réalisable. Si une organisation sait qu'un système a été compromis et qu'elle laisse la compromission se poursuivre, elle peut être tenue pour responsable si le pirate utilise le système compromis pour attaquer d'autres systèmes. La stratégie de confinement retardé est dangereuse car un attaquant peut étendre l'accès non autorisé ou compromettre d'autres systèmes.

Un autre problème potentiel lié à l'endiguement est que certaines attaques peuvent causer des dommages supplémentaires lorsqu'elles sont endiguées. Par exemple, un hôte compromis peut exécuter un processus malveillant qui envoie périodiquement des pings à un autre hôte. Lorsque le gestionnaire de l'incident tente de contenir l'incident en déconnectant l'hôte compromis du réseau, les pings suivants échouent. À la suite de cet échec, le processus malveillant peut écraser ou chiffrer toutes les données du disque dur de l'hôte. Les gestionnaires ne doivent pas supposer que le simple fait qu'un hôte ait été déconnecté du réseau a permis d'éviter d'autres dommages à l'hôte.

### Documentation

Il est essentiel de documenter toutes les informations relatives à l'incident. La liste suivante est une indication des informations pertinentes qui doivent être documentées. Si des rapports sont rédigés à l'intention de la direction ou d'autres parties prenantes, ces informations doivent figurer dans le rapport.

* Date et heure de l'incident
* Situation actuelle de l'incident
* Coordonnées des personnes concernées (responsable de l'incident, RSSI, PDG, ....)
* Portée et impact
* Ernst
* Type d'incident et classification
* Besoin d'une aide extérieure ? OUI / NON. Veuillez indiquer les coordonnées de la personne à contacter.
* Mesures prises pour contenir et résoudre l'incident.
* Informations sur la prochaine mise à jour de l'incident (date, heure, qui sera informé)

### Collecte et conservation des preuves

Lorsque vous recueillez des preuves, tenez un registre détaillé qui documente clairement la manière dont toutes les preuves ont été recueillies. Ce registre doit indiquer qui a recueilli ou manipulé les preuves, quand les preuves ont été recueillies et manipulées, et les détails de chaque élément recueilli (y compris l'emplacement physique, le numéro de série, le numéro de modèle, le nom d'hôte, les fichiers journaux, l'adresse IP, le système d'exploitation, ....).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date et heure de la collecte** | **Recueilli par** | **Détails des preuves** | **Localisation des preuves** | **Accès** |
| *01/01/2024* | *Monsieur Janssens* | *Disque dur pour ordinateur portable avec SN, modèle no.* | *Disque avec SN....*  *Conservé dans un coffre-fort dans la salle des serveurs* | *Responsable TIC, équipe CIRT* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Plan d'action de remédiation

Établir un plan d'action pour résoudre l'incident, après avoir réussi à le circonscrire et à recueillir des preuves.

Lors de l'élaboration du plan d'action de reconstitution, il convient de se poser les questions suivantes. Ces questions sont limitées et n'ont qu'une valeur indicative.

* Quelles sont les actions nécessaires pour résoudre l'incident ?
* Quelles sont les ressources (internes et externes) nécessaires pour résoudre l'incident ?
* À qui appartient l'incident en cours de résolution ?
* Existe-t-il une priorité pour les systèmes ou les services nécessaires à la résolution de l'incident ?
* Qui et quoi est concerné par la résolution ?
* Quel est le calendrier de clôture de l'incident ?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date, heure de l'incident** | **Catégorie**  **(Contrôle, récupération,...)** | **Action** | **Propriétaire de l'action** | **Statut**  **(non attribué, en cours d'élaboration, clôturé)** |
| *01/01/2024* | *Contient* | *Déconnecter l'hôte infecté du réseau.* | *Administrateur du système (y compris le nom)* | *En cours* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Récupération

Élaborer des plans de reprise pour différents scénarios. Le plan de reprise doit détailler l'approche adoptée pour restaurer les réseaux, les systèmes et les applications informatiques et/ou électroniques une fois que les mesures de confinement et d'assainissement sont terminées.

Lors de l'élaboration d'un plan de reprise, il convient de garder à l'esprit les éléments suivants :

* L'objectif de temps de récupération (RTO) et l'objectif de point de récupération (RPO).
* Créer un processus de surveillance des systèmes pour s'assurer qu'ils ne sont plus compromis et qu'ils fonctionnent comme prévu.
* Que peut-on mettre en œuvre pour éviter des incidents similaires ?

# Enseignements tirés.

L'une des parties les plus importantes de la réponse aux incidents est aussi la plus souvent négligée : l'apprentissage et l'amélioration. Chaque équipe de réponse aux incidents doit évoluer pour tenir compte des nouvelles menaces, de l'amélioration des technologies et des leçons tirées de l'expérience. La tenue d'une réunion sur les "enseignements tirés" avec toutes les parties concernées après un incident majeur, et éventuellement périodiquement après des incidents moins importants si les ressources le permettent, peut être très utile pour améliorer les mesures de sécurité et le processus de réponse à l'incident lui-même. Plusieurs incidents peuvent être examinés au cours d'une même réunion sur les "enseignements tirés". Cette réunion permet de conclure un incident en discutant de ce qui s'est passé, de ce qui a été fait pour intervenir et de l'efficacité de l'intervention. La réunion doit avoir lieu dans les jours qui suivent la fin de l'incident.

Les questions auxquelles il sera répondu au cours de la réunion sont notamment les suivantes

* Que s'est-il passé exactement et à quelles heures ?
* Le personnel et la direction ont-ils bien géré l'incident ? Les procédures documentées ont-elles été suivies ? Ont-elles été adéquates ?
* Quelles informations étaient nécessaires auparavant ?
* Des mesures ou des actions ont-elles été prises qui auraient pu entraver la guérison ?
* Que feraient différemment le personnel et la direction si un incident similaire se produisait la prochaine fois ?
* Comment l'échange d'informations avec d'autres organisations aurait-il pu être amélioré ?
* Quelles sont les mesures correctives susceptibles de prévenir des incidents similaires à l'avenir ?
* Quels sont les précurseurs ou les indicateurs à surveiller à l'avenir pour détecter des incidents similaires ?

Les réunions sur les enseignements tirés présentent d'autres avantages. Les comptes rendus de ces réunions constituent un bon matériel pour la formation des nouveaux membres de l'équipe en leur montrant comment les membres plus expérimentés de l'équipe réagissent aux incidents. La mise à jour des politiques et procédures de réponse aux incidents est un autre élément important du processus d'apprentissage. Une analyse rétrospective de la manière dont un incident a été traité révèle souvent une étape manquante ou une inexactitude dans une procédure, ce qui incite à la modifier. En raison de la nature changeante des technologies de l'information et des changements de personnel, l'équipe de réponse aux incidents devrait revoir périodiquement l'ensemble de la documentation et des procédures relatives au traitement des incidents.

**Il est important de tester régulièrement le plan de réponse aux incidents cybernétiques pour s'assurer que ces documents restent à jour et connus du personnel concerné. Les méthodes de test peuvent inclure des discussions ou des exercices fonctionnels.**

**Les exercices de formation au plan de réponse aux incidents cybernétiques, qui comportent différents scénarios, sont très utiles pour obtenir de plus en plus d'informations à partir des leçons tirées de l'expérience. Au cours de ces scénarios de test, de nombreuses informations peuvent manquer ou les processus ne sont pas exécutés comme prévu. Il s'agit là d'excellents résultats qui vous permettront d'adapter les procédures et les processus au moment où vous aurez réellement besoin du plan d'intervention en cas de cyberincident !**