Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Chiffrement ou effacement en cours

Qualification

2026

InterCERT FRANCE

A qui s'adresse-t-elle ?

- Responsables de la sécurité des systèmes d'information (RSSI)
- Administrateurs du système d'information

Quand l'utiliser ?

Utiliser cette fiche lorsqu'un logiciel malveillant de chiffrement ou d'effacement, par exemple de type rançongiciel, est détecté ou suspecté sur le système d'information.

A quoi sert-elle ?

L'objectif de cette fiche est de proposer une *aide à la qualification* d'une attaque de type rançongiciel. Les différentes actions proposées aideront à :

- *Confirmer* qu'un incident de sécurité est bien en cours, et qu'il est de type *rançongiciel*.
- Évaluer la *gravité* de l'incident en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie Conclusions attendues de la qualification correspond aux questions auxquelles la qualification devra répondre.
- La partie Méthode d'évaluation pas à pas correspond à la méthodologie pour aider à y répondre.

Cette fiche doit être exécutée en *temps court*. Pour cela, fixer un *temps contraint* selon l'urgence pressentie (ex : 30 minutes, 1 heure au maximum) et ne pas rechercher l'exhaustivité des réponses : des *réponses approximatives* et des réponses *"je ne sais pas répondre"* sont acceptables dans un premier temps. Par la suite, une qualification plus approfondie se fera sûrement, avec plus de recul ou l'appui d'une équipe spécialisée en réponse à incident.

SOMMAIRE

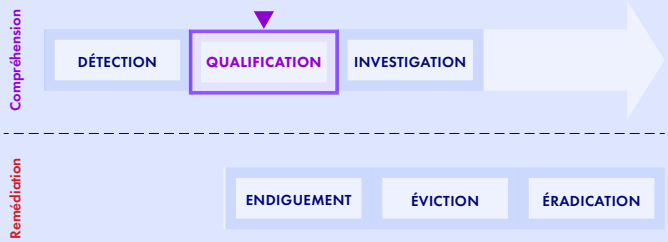
Prérequis 3

Conclusions attendues de la qualification 5

Méthode d'évaluation pas à pas 6

Suite des actions 11

Annexes 12



PRÉREQUIS

Demander de l'aide

Ne jamais rester seul face à un incident. Solliciter l'aide d'un collègue afin de ne pas assumer seul la responsabilité de son traitement et de pouvoir répartir efficacement les tâches. Par exemple, une personne peut se concentrer sur l'approfondissement de la qualification de l'incident, tandis que d'autres peuvent contacter un responsable hiérarchique et le CSIRT/CERT, initier les premières mesures d'endiguement, voire paralléliser les actions prioritaires.

Demander de l'aide

Ne jamais rester seul face à un incident ! Solliciter l'aide d'un collègue afin de ne pas porter seul la responsabilité et de pouvoir répartir efficacement les tâches. Par exemple, une personne peut se concentrer sur la qualification de l'incident tandis que l'autre contacte un responsable hiérarchique et le CSIRT/CERT, ou initie les premières mesures d'endiguement.

Disposer des personnes nécessaires

S'assurer que les personnes qui effectueront la qualification de l'incident aient les accès nécessaires au système d'information :

- Les *accès à l'administration et au monitoring* du système d'information.
- Les *accès aux équipements de sécurité* du système d'information.
- La connaissance des *priorités métier* de l'organisation.
- L'annuaire de contacts d'urgence.

Ces personnes peuvent être internes ou externes à l'organisation. Si le système d'information est infogéré, s'assurer de la capacité à mobiliser l'infogérant dans l'urgence.

Ouvrir une main courante

Dès le début de l'incident, ouvrir une *main courante* pour tracer tous les actions et événements survenus sur le système d'information dans un *ordre chronologique*.
Chaque ligne de ce document doit représenter une action avec au minimum trois informations :

1. La **date et l'heure** de l'action ou de l'évènement (si estimé nécessaire, ajouter le fuseau horaire UTC).
2. Le **nom de la personne** en charge de cette action ou ayant informé sur l'évènement (ou le nom du service de sécurité ayant détecté l'évènement).
3. La **description** de l'action ou de l'évènement, incluant les détails de son avancement ainsi que les comptes et machines concernés.

Ce document sera utile pour :

- Réaliser un historique du traitement de l'incident et partager la connaissance.
- Piloter la coordination des actions et suivre leur état d'avancement.
- Évaluer l'efficacité des actions et leurs potentiels impacts non prévus.

Cette main courante doit être éditable et consultable par tous les intervenants. Il est déconseillé de la stocker sur le système d'information compromis, où elle serait accessible par l'attaquant. En revanche, cette main courante peut être accessible sur un partage de fichiers en ligne (cloud) ou intégrée dans le logiciel de gestion d'incident ou le SIEM si l'organisation en possède un, voire être au format papier.

Avoir pris connaissance des actions déjà entreprises

Avoir pris note des personnes ayant déjà agi en réponse à l'incident en cours et des actions qu'elles ont déjà entreprises sur le système d'information. Commencer à reporter ces notes d'intervention dans la main courante.

CONCLUSIONS ATTENDUES DE LA QUALIFICATION

Cette section présente les conclusions attendues des évaluations, qui permettront de qualifier l'incident.
La section suivante détaillera les questions et actions à mener pour guider ces évaluations étape par étape.

Évaluer l'incident

Mesure 1 - Confirmer l'incident de type rançongiciel

- ☐ *L'incident est-il confirmé ou nécessite-t-il des investigations complémentaires ? Est-il de type rançongiciel ?*
- ☐ *Le chiffrement a-t-il déjà été constaté ? Sinon, la menace demeure-t-elle suffisamment crédible ?*

Mesure 2 - Évaluer le périmètre de l'incident

- ☐ *L'incident est-il circonscrit à une partie du système d'information identifiable ?*
- ☐ *Les ressources d'administration ont-elles été compromises (comptes, postes, serveurs) ? Un compte à haut niveau de privilège semble-t-il avoir été compromis ?*
- ☐ *D'autres systèmes d'information interconnectés avec celui de l'organisation sont-ils en risque ?*

Mesure 3 - Évaluer l'impact métier de l'incident

- ☐ *Quelles activités vitales sont perturbées ?*
- ☐ *Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?*
- ☐ *La DSI a-t-elle les compétences en interne pour reconstruire les systèmes d'information impactés ?*
- ☐ *La DSI a-t-elle les compétences en interne pour maintenir les activités vitales ?*

Mesure 4 - Évaluer l'urgence à résoudre l'incident

- ☐ *Quelles sont les activités vitales à l'arrêt, pour lesquelles un rétablissement d'urgence doit être opéré ?*
- ☐ *Quelles sont les activités vitales maintenues en mode dégradé, pour lesquelles il faut préparer dès maintenant un rétablissement ?*

Qualifier l'incident

Conclure quant à la gravité de l'incident

- ☐ L'incident de type rançongiciel est-il *confirmé* ?
- ☐ L'incident est-il *circonscrit* sur mon système d'information, ou est-il étendu ?
- ☐ L'incident présente-t-il un *impact fort* pour mon *activité métier* et le fonctionnement de mon *système d'information* ?
- ☐ L'incident est-il *urgent* à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?

- ☐ Au final, quelle *gravité* représente cet incident de sécurité ?

1. Anomalie courante
2. Incident mineur
3. Incident majeur
4. Crise cyber

MÉTHODE D'ÉVALUATION PAS À PAS

Cette partie détaillera des actions qui aideront à conduire les évaluations et à aboutir à la qualification de l'incident.

Évaluer l'incident

Mesure 1 - Confirmer l'incident de type rançongiciel

Action 1.a : Évaluer les signaux forts sur son système d'information

- ☐ Détection d'un code malveillant de type rançongiciel :
  - ☐ Détection des outils de sécurité (antivirus et EDR).
  - ☐ Détection du SOC.
  - ☐ Détection proactive via un scan de marqueurs positif.
  - ☐ Détection par un outil de surveillance des données de type *Data Detection and Response* (DDR).
- ☐ Signalement d'utilisateurs :
  - ☐ Signalement d'apparition d'une fenêtre, une pop-up ou un fichier demandant de payer une rançon (souvent nommé *README.txt*).
  - ☐ Signalement d'apparition de fichiers illisibles et avec des extensions anormales (*.encrypt, .abc, .aaa, .p5tkjw*, etc.).
  - ☐ Signalement de création d'archives en masse.
- ☐ A quand remonte la première constatation d'un de ces signaux forts ?

> ⚠ ATTENTION
>
> Si un chiffrement est déjà en cours ou que la menace paraît imminente, il convient d'envisager les premières mesures d'endiguement dès maintenant. Parallèlement, la qualification doit se poursuivre par d'autres intervenants, car elle permettra une meilleure compréhension de la compromission et contribuera à rendre l'endiguement plus efficace. Aussi, envisager de demander de l'aide à une équipe spécialisée CERT/CSIRT (voir la partie Suite des actions).

Si aucun des signaux forts mentionnés ci-dessus n'est apparu, mais que vous avez des soupçons concernant un éventuel chiffrement en cours, analysez les dysfonctionnements typiques d'une attaque par rançongiciel :

Action 1.b : Évaluer les signaux faibles sur son système d'information

- ☐ Impossibilité d'accéder à des serveurs.
- ☐ Indisponibilité de plusieurs services.
- ☐ Impossibilité de lire des fichiers.
- ☐ Désactivation de l'antivirus ou de l'EDR sur une portion significative du parc.
- ☐ Extinctions de machines virtuelles en masse.
- ☐ Détection d'une grosse exfiltration de données sur les sondes réseau.
- ☐ A quand remonte la première constatation d'un de ces signaux faibles ?

Action 1.c : Évaluer la visibilité

Quels sont les moyens d'observations sur l'incident ?

- ☐ *Moyens de supervision* :
  - ☐ puits de logs ou SIEM
  - ☐ console antivirus ou EDR

- ☐ console d'alertes des sondes réseau ou des proxy web

- ☐ *Moyens de monitoring* : console de monitoring des serveurs et du trafic réseau.
- ☐ *Vérification manuelle* : accès aux serveurs de fichiers et aux serveurs de sauvegardes.
- ☐ *Signalements du SOC ou d'utilisateurs* en heures ouvrées.
- ☐ Pensez-vous disposer d'une bonne visibilité sur l'incident, ou au contraire être dans le flou quant à la situation réelle et à ce qui pourrait encore se produire ?

Action 1.d : (Conclure) Confirmer l'incident de type rançongiciel

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

- ☐ *L'incident est-il confirmé ou nécessite-t-il des investigations complémentaires ? Est-il de type rançongiciel ?*
- ☐ *Le chiffrement a-t-il déjà été constaté ? Sinon, la menace demeure-t-elle suffisamment crédible ?*

Mesure 2 - Évaluer le périmètre de l'incident

Action 2.a : Identifier le type de machines chiffrées

- ☐ Postes de travail ?
  - ☐ bureautique (emails et navigation web)
  - ☐ métier ou opérationnel (et autres environnements non bureautique)
- ☐ Serveurs ?
  - ☐ Windows
  - ☐ Linux
- ☐ Serveurs de stockage ?
  - ☐ Serveurs de fichiers (interne ou cloud)
  - ☐ Serveurs de sauvegardes
- ☐ Hyperviseurs ?
- ☐ Machines virtuelles ?
  - ☐ Fichiers chiffrés sur le système invité
  - ☐ Enveloppe de la machine virtuelle chiffrée sur l'hyperviseur
- ☐ Equipements industriels ou équipements embarqués (si vous êtes en capacité de l'observer)

Action 2.b : Identifier le niveau de compromission

- ☐ Des postes, des serveurs d'administration ou d'infrastructure ont-ils été chiffrés ?
- ☐ Des comptes à privilèges se sont-ils authentifiés pendant les heures inhabituelles ou peu avant le chiffrement :
  - ☐ sur le système d'information via un moyen d'accès depuis Internet ?
  - ☐ sur les systèmes chiffrés (ex : l'hyperviseur) ?
- ☐ Pour l'annuaire Active Directory :
  - ☐ Des comptes illégitimes ont-ils été ajoutés aux groupes *Administrateurs de domaine*, *Administrateurs d'entreprise*, *Administrateurs intégrés* ou *Administrateurs de schéma* ?
  - ☐ Un groupe `ESXi Admins` a-t-il été créé récemment dans l'annuaire et semble illégitime ?
- ☐ De manière plus générale, existe-t-il un compte à privilèges élevés qui ait, d'une manière ou d'une autre, suscité un soupçon en raison d'un comportement inhabituel ? Si oui, lequel et quelles actions a-t-il effectuées ?

Action 2.c : Évaluer l'étendue de la compromission

- ☐ Quelles zones du système d'information contiennent des machines ayant des fichiers chiffrés ?
  - ☐ DMZ
  - ☐ systèmes bureautiques
  - ☐ systèmes métiers ou opérationnels

- ☐ systèmes d'administration
- ☐ systèmes de sauvegarde
- ☐ systèmes dans le cloud
- ☐ autres ?

☐ Les machines Windows chiffrées appartiennent-elles à plusieurs domaines Active Directory ou un seul ?
☐ Des mesures d'endiguement ont-elles déjà été entreprises ?

- ☐ Si oui, ont-elles permis d'arrêter la propagation ou l'incident semble-t-il se propager encore ?

Action 2.d : Identifier les interconnexions

☐ Le système d'information est-il interconnecté avec d'autres systèmes d'information ?
☐ Quelles sont tous les moyens d'accès vers mon système d'information depuis l'extérieur ?

- ☐ Passerelle VPN
- ☐ Infrastructure de bureau distance (VDI)
- ☐ Passerelle RDS
- ☐ Bastion
- ☐ Autre ?

Action 2.e : (Conclure) Évaluer le périmètre de l'incident

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

☐ *L'incident est-il circonscrit à une partie du système d'information identifiable ?*
☐ *Les ressources d'administration ont-elles été compromises (comptes, postes, serveurs) ? Un compte à haut niveau de privilège semble-t-il avoir été compromis ?*
☐ *D'autres systèmes d'information interconnectés avec celui de l'organisation sont-ils en risque ?*

Mesure 3 - Évaluer l'impact métier de l'incident

Action 3.a : Évaluer les impacts sur l'activité métier

☐ Quelles *activités métier* sont perturbées, à usage interne ou externe ?

- ☐ Quelles activités perturbées sont *vitales* pour l'organisation ?
  - ☐ Si votre organisation possède un BIA (Business Impact Analysis) ou un PCA/PRA (Plan de Continuité/Reprise d'Activité), les activités perturbées en font-elles partie ?
- ☐ Parmi les activités perturbées, certaines provoquent-elles une importante *perte financière* ?

Action 3.b : Évaluer les impacts réglementaires

☐ Le système d'information affecté est-il soumis à une réglementation particulière (Opérateurs de Services Essentiels (OSE), Opérateurs d'Importance Vitale (OIV), etc.) ?
☐ Le système d'information affecté stocke-t-il des données sensibles ?

- ☐ données classifiées
- ☐ données personnelles
- ☐ données à statut protégé : de santé, financières
- ☐ données soumises à engagement contractuel ou réglementaire autre.

REMARQUE

Pour évaluer les impacts réglementaires, il est recommandé de solliciter les personnes compétentes, comme le service juridique ou le délégué à la protection des données (DPO) chargé du RGPD.

Action 3.c : Évaluer les impacts pour la continuité et reprise d'activité

- ☐ Quelles ressources informatiques support aux *activités vitales* identifiées ci-dessus ont été chiffrées ?
  - ☐ Les données ?
  - ☐ Les serveurs ?
- ☐ Les *serveurs de fichiers* ont-ils été chiffrés ?
  - ☐ Si oui, étaient-ils sauvegardés ?
- ☐ Concernant les *sauvegardes* :
  - ☐ Les sauvegardes ont-elles été chiffrées ?
  - ☐ Existe-t-il des sauvegardes hors ligne ?
  - ☐ Les sauvegardes saines sont-elles sur un site distant ou seraient-elles très longues à restaurer ?
  - ☐ L'infrastructure de restauration est-elle disponible et opérationnelle ?
- ☐ Quels *serveurs d'infrastructure critiques* pour le fonctionnement du système d'information ont été chiffrés ?
  - ☐ Contrôleur de domaine
  - ☐ DNS
  - ☐ Hyperviseur
  - ☐ Autres ?
- ☐ Y a-t-il encore des *postes d'administration* fonctionnels ?

Action 3.d : Évaluer les impacts des actions d'endiguement entreprises

- ☐ Des actions d'isolation ont-elles déjà été entreprises ? Si oui :
  - ☐ Des flux ont-ils été coupés ? Si oui :
    - ☐ Sur quels équipements ?
  - ☐ Quelles sont les activités métiers qui en ont été impactées ?

Action 3.e : (Conclure) Évaluer l'impact de l'incident

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

- ☐ *Quelles activités vitales sont perturbées ?*
- ☐ *Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?*
- ☐ *La DSI a-t-elle les compétences en interne pour reconstruire les systèmes d'information impactés ?*
- ☐ *La DSI a-t-elle les compétences en interne pour maintenir les activités vitales ?*

Mesure 4 - Évaluer l'urgence à résoudre l'incident

Action 4.a : Évaluer l'urgence à résoudre l'incident

Pour chacune des *activités vitales* impactées identifiées précédemment :

- ☐ Existe-t-il une procédure de continuité d'activité en **mode nominal** ?
- ☐ Existe-t-il une procédure de maintien d'activité en **mode dégradé** ?
- ☐ Si oui :
  - ☐ Ces procédures sont-elles déjà en cours de mise en œuvre ?
  - ☐ Combien de temps pourraient-elles tenir ?
- ☐ Des actions de restauration ont-elles déjà été entreprises ?

Action 4.b : (Conclure) Évaluer l'urgence à résoudre l'incident

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

- ☐ *Quelles sont les activités vitales à l'arrêt, pour lesquelles un rétablissement d'urgence doit être opéré ?*
- ☐ *Quelles sont les activités vitales maintenues en mode dégradé, pour lesquelles il faut préparer dès maintenant un rétablissement ?*

Qualifier l'incident

Conclure quant à la *gravité* que représente l'incident de sécurité pour mon organisation, en prenant en compte le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre :

- ☐ L'incident de type rançongiciel est-il *confirmé* ?
- ☐ L'incident est-il *circonscrit* sur mon système d'information, ou est-il étendu ?
- ☐ L'incident présente-t-il un *impact fort* pour mon *activité métier* et le fonctionnement de mon *système d'information* ?
- ☐ L'incident est-il *urgent* à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?

- ☐ Au final, quelle *gravité* représente cet incident de sécurité ?

    1. Anomalie courante
    2. Incident mineur
    3. Incident majeur
    4. Crise cyber

SUITE DES ACTIONS

Endiguer et traiter l'incident selon sa gravité

Si l'incident est confirmé et qu'il est de type rançongiciel alors, en cohérence avec le *périmètre de compromission* évalué :

- ► Mettre en œuvre des **mesures d'endiguement** pour contenir l'attaque.
  - Fiche suivante conseillée : Fiche réflexe - Chiffrement ou effacement en cours - Endiguement.

Parallèlement, piloter la suite du traitement de cet incident. Il peut être utile de solliciter de l'aide pour résoudre l'incident, en cohérence avec les *impacts* identifiés :

- ► Mettre en œuvre une **gestion d'incident cyber** pour piloter la résolution de l'incident.
  - Voir les annexes *Contacts* et *Déclarations*.

De plus, si l'incident a un *périmètre étendu* sur le système d'information, qu'il a un *impact fort* et qu'il nécessite une *résolution urgente* :

- ► Activer le dispositif de **gestion de crise cyber** de l'organisation pour piloter la résolution de l'incident et la continuité d'activité.
  - Guide conseillé : Crise cyber, les clés d'une gestion opérationnelle et stratégique

REMARQUE

Dans le cas d'une attaque par rançongiciel, des aides spécifiques au dépôt de plainte sont mises à disposition par le CERT Santé, en collaboration avec le CSIRT-PJ : https ://cyberveille.esante.gouv.fr/dossier-thematique/aide-au-depot-de-plainte-en-cas-dattaque-par-rancongiciel. Lors du dépôt de plainte, le *Rapport Initial d'Incident* (*R2IP*) est à annexer systématiquement à la plainte. Le CSIRT-PJ peut vous accompagner dans cette démarche.

Communiquer

Informer la direction de la situation et du niveau de gravité estimé de l'incident.
Communiquer en interne que l'organisation fait face à un incident et que certains services pourraient être temporairement indisponibles. Il est inutile de saturer le helpdesk d'appels : une prochaine communication fera un point sur l'état des services. Aussi, si l'organisation doit être isolée d'Internet, il ne faut pas tenter de contourner cette mesure en utilisant un point d'accès mobile ou un réseau Wi-Fi externe.

ANNEXES

Liens utiles

Lors d'une lecture préparatoire de cette fiche ou pour aller plus loin dans la compréhension et la mise en œuvre des notions évoquées, certains documents annexes peuvent être utiles :

- Fiche réflexe - Chiffrement ou effacement en cours - Endiguement
- Comment réagir en cas d'incident rançongiciel
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- Cyberattaques et remédiation

Contacts

La gestion d'un incident cyber implique de faire appel à des équipes spécialisées au sein de CERT/CSIRT, qui appuieront les équipes internes dans la réalisation de leurs actions de défense.

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation	Se référer aux procédures internes.	Pour les organisation disposant d'une équipe de réponse à incident interne.
CERT/CSIRT externe en prestation de réponse à incident	`https://www.cybermalveillance.gouv.fr/diagnostic/accueil` `https://cyber.gouv.fr/prestataires-de-reponse-aux-incide`	Pour les petites organisations : consulter le registre des prestataires spécialisés sur Cybermalveillance Pour les organisations opérant un système d'information complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS)
CSIRT régional	`https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux`	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations

CERT sectoriel	`https://www.cert-aviation.fr`
	`https://www.m-cert.fr`
	`https://esante.gouv.fr/produits-services/cert-sante`
		Pour les organisations du secteur de l'aviation, maritime ou santé

CERT-FR	`https://www.cert.ssi.gouv.fr/contact`	Pour les administrations et les opérateurs d'importance vitale et de services essentiels

De plus, pour les incidents complexes, une aide externe est également recommandée pour :

- Gérer la crise
- Gérer la communication interne et externe
- Augmenter les ressources humaines et capacitaires de reconstruction de votre direction informatique

Pour faciliter la mobilisation de tous ces acteurs, il est conseillé de s'appuyer sur des annuaires tenus à jour en amont et accessibles même en cas d'indisponibilité du système d'information.

Déclarations

Conjointement à la résolution de l'incident, des déclarations doivent être effectuées :

Qui ?	Comment ?	Pourquoi ?
Assureurs		Notifier son assurance cyber permet de démarrer la prise en compte de la couverture et d'identifier des prestataires que l'assureur pourra recommander ou mandater.

Qui ?	Comment ?	Pourquoi ?
ANSSI	`https://www.cert.ssi.gouv.fr/contact/` `https://cyber.gouv.fr/notifications-reglementaires`	L'administration, les opérateurs d'importance vitale et de services essentiels, et toute organisation impliquant des informations classifiées, doivent déclarer leurs incidents à l'ANSSI.
Dépôt de plainte	`https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/comment-porter-plainte-en-cas-de`	Déposer plainte permet de déclencher une enquête et de dégager votre responsabilité en cas de propagation de l'attaque à d'autres victimes.
CNIL	`https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles`	Les incidents affectant des données personnelles doivent faire l'objet de déclaration à la CNIL dans un délai de 72 heures. En cas de doute, il faut faire une pré-déclaration précisant avoir subi une potentielle compromission même si aucune exfiltration de données n'a été confirmée.
Autres autorités		Une organisation d'un domaine réglementé (finance, santé, etc.) est astreinte à des obligations de déclaration spécifiques. Dans le doute, consulter le service juridique.

Préparation

En *prévention* d'un incident, une fiche réflexe sera d'autant plus efficace si elle a pu être préparée en amont, contextualisée et traduite en une *procédure interne et actionnable immédiatement* à son système d'information. Dans une situation d'urgence, elle augmentera la rapidité de la réponse, minimisera les erreurs de manipulation et permettra à une personne d'astreinte moins expérimentée de mener ces actions.
Il est également conseillé d'imprimer les fiches réflexes afin qu'elles restent disponibles en cas d'indisponibilité du système d'information. Il en va de même pour les autres documents utiles, comme la notice d'aide au dépôt de plainte ou votre annuaire de contacts.

Définitions

Axes d'évaluation

- *Périmètre* : Le périmètre d'un incident désigne son étendue sur le système d'information et dans son administration.
- *Impact* : L'impact d'un incident désigne le niveau de perturbation et de dommage potentiel qu'il engendre pour l'organisation.
- *Urgence* : L'urgence d'un incident désigne la rapidité avec laquelle il faut réagir pour rétablir les activités essentielles impactées.

Compromission d'un compte de messagerie

Une *compromission d'un compte de messagerie* désigne un accès non autorisé à un compte de messagerie, par un attaquant. Ce dernier peut alors lire et envoyer des courriels à l'insu de l'utilisateur légitime du compte, et accéder à ses données.

Compromission système

Une *compromission système* est l'activité d'un code ou d'un acteur malveillant sur une machine du système d'information, résultant en sa prise de contrôle.
Faute de pouvoir qualifier précisément la prise de contrôle, dans de nombreux cas, toute activité adverse sur le système pouvant avoir donné lieu à une escalade de privilège est considérée comme une compromission. Une compromission entraîne généralement une forme de communication entre la machine compromise et un attaquant y exécutant des actions.

Degrés de gravité

- *Anomalie courante* (gravité faible) : Une anomalie courante est un incident de sécurité ne représentant pour l'instant pas de menace sérieuse pour la sécurité du système d'information et n'entraînant pas d'impact significatif sur l'activité métier. Elle nécessite tout de même d'être correctement qualifiée pour confirmer son faible degré de gravité.
- *Incident mineur* (gravité modérée) : Un incident mineur est un incident de sécurité représentant une menace limitée pour le système d'information et entraînant - ou risquant d'entraîner - un impact modéré sur l'activité métier.

- *Incident majeur* (gravité élevée) : Un incident majeur est un incident de sécurité représentant une menace sérieuse pour le système d'information et entraînant - ou risquant d'entraîner - un impact fort sur l'activité métier.
- *Crise cyber* (gravité critique) : Une crise cyber représente un incident de sécurité ayant un *périmètre étendu* sur le système d'information, un *impact fort* sur l'activité métier et nécessitant une *résolution urgente*.

Endiguer un incident

L'endiguement désigne l'ensemble des actions prises au début d'un incident de sécurité informatique destinées à en contenir l'ampleur. Elles n'ont généralement pas vocation à être prolongées durablement.

Fuite de données

Une *fuite de données*, également appelée *violation de données*, désigne un incident au cours duquel des informations confidentielles, sensibles ou protégées sont consultées, divulguées ou volées par une personne non autorisée. Cela peut concerner divers types de données, notamment des informations personnelles, financières, médicales, ou des secrets commerciaux.
Les fuites de données peuvent résulter de cyberattaques, comme le piratage ou le phishing, mais aussi d'erreurs humaines, telles que l'envoi d'informations à la mauvaise adresse e-mail ou la perte de dispositifs contenant des données sensibles. Les conséquences d'une fuite de données peuvent être graves, allant de pertes financières et d'atteintes à la réputation de l'entreprise à des problèmes juridiques et à la compromission de la vie privée des individus concernés.

Qualifier un incident

Qualifier un incident signifie :

- *Confirmer* qu'un incident de sécurité est bien en cours et si oui, déterminer précisément sa *nature*.
- *Évaluer la gravité/priorité de l'incident* en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

La qualification permettra de prendre des décisions éclairées sur la réponse à l'incident et d'allouer les ressources appropriées pour le résoudre.

FICHE RÉFLEXE

L'InterCERT France fédère aujourd'hui plus de 100 CERTs sur le territoire national, constituant ainsi la 1ère communauté de CERTs en France.

Cette fiche réflexe est issue de la coopération et du partage d'expérience de plusieurs de ces CERTs. Elle a pour objectif d'être un outil efficace lors des premières étapes de gestion de l'incident en cours, en proposant des actions concrètes pour débuter le processus de remédiation.

Vous pouvez trouver l'ensemble de ces fiches au lien suivant :
`https://www.intercert-france.fr/publications/fiches-reflexes/`

Votre expérience dans le traitement d'un incident et l'utilisation de cette fiche est précieuse. Dans le but d'améliorer sa qualité, nous vous invitons à partager vos commentaires et suggestions d'amélioration, en nous contactant à l'adresse suivante :
fichesreflexes-remediation@intercert-france.fr