



**PREMIÈRE
MINISTRE**

*Liberté
Égalité
Fraternité*

*Agence nationale de la sécurité des
systèmes d'information*

**Secrétariat général de la défense
et de la sécurité nationale**

Paris, le 15/07/2024
N° CERTFR-2024-RFX-002

Chiffrement ou effacement en cours - Endiguement

Fiche Réflexe

ANSSI/SDO
15/07/2024



Version : 1
Nombre de pages : 18

Table des matières

1 A qui s'adresse-t-elle?	3
2 Quand l'utiliser?	3
3 A quoi sert-elle?	3
4 Comment l'utiliser?	3
5 Avoir qualifié l'incident	4
6 Avoir les capacités d'administration	4
7 Ouvrir une main courante	4
8 Contenir la propagation de l'attaque	5
9 Préserver les biens essentiels de l'organisation	9
10 Préserver les traces	12
11 Définitions	14
12 Contacter le CERT-FR	15
12.1 Important	15
12.2 Par Téléphone	15
12.3 Par Internet	15
12.4 Clé PGP du CERT-FR	15
13 Contacts	16
14 Déclarations	16
15 Préparation	17
16 Licence	17

1 A qui s'adresse-t-elle ?

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

2 Quand l'utiliser ?

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

3 A quoi sert-elle ?

L'objectif de cette fiche est de proposer les premières actions d'*endiguement* ayant pour objectif de circonscrire l'attaque. Elles tenteront de *limiter son extension et son impact* et de donner du temps aux défenseurs pour s'organiser et reprendre l'initiative.

4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie *Actions d'endiguement par priorités* pointe l'ordre prioritaire des actions détaillées dans la partie suivante.
- La partie *Actions d'endiguement par thèmes* détaille les différentes actions d'endiguement possibles selon 3 axes thématiques.

Si l'organisation estime avoir besoin d'aide pour réaliser ces actions d'endiguement, elle peut contacter des équipes spécialisées en réponse à incident, qu'elles soient internes ou externes : voir la partie *Contacts*.

- Prérequis
- Actions d'endiguement par priorités
- Actions d'endiguement par thèmes
 - Contenir la propagation de l'attaque
 - Préserver les biens essentiels de l'organisation
 - Préserver les traces
- Suite des actions
- Annexes

5 Avoir qualifié l'incident

Avoir *qualifié* que l'incident en cours sur le système d'information soit bien une *exécution d'un logiciel malveillant de chiffrement ou d'effacement*, par exemple de type rançongiciel, et en avoir évalué la gravité :

Fiche précédente conseillée : Fiche réflexe - Chiffrement ou effacement en cours - Qualification

Les mesures d'endiguement proposées dans cette fiche devront être appliquées en cohérence avec les conclusions de la *qualification* : le *périmètre* affecté par l'incident, son *impact* potentiel sur l'organisation, l'*urgence* à résoudre la situation, etc.

6 Avoir les capacités d'administration

S'assurer que les personnes qui mettront en œuvre les actions d'endiguement aient les *droits d'administration* du système d'information : réseau, système, sécurité opérationnelle.

Si le système d'information est infogéré, s'assurer de la capacité à mobiliser l'infogérant dans l'urgence.

7 Ouvrir une main courante

Dès le début de l'incident, ouvrir une *main courante* pour tracer toutes 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 ayant réalisé cette action ou ayant informé sur l'évènement
3. La description de l'action ou de l'évènement et les machines concernées

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.

Cette partie pointe l'ordre prioritaire des actions détaillées dans la partie suivante :

Actions	Priorité
Isoler temporairement d'Internet (<i>Mesure 1 - Action 1.a</i>)	P0
Préserver les sauvegardes (<i>Mesure 4</i>)	P0
Préserver les serveurs de fichiers non sauvegardés (<i>Mesure 5</i>)	P0
Isoler les machines infectées (<i>Mesure 2</i>)	P0
Préserver un contrôleur de domaine (Windows) (<i>Mesure 6</i>)	P1
Entraver la propagation du chiffrement (<i>Mesure 3</i>)	P2
Préserver les traces (<i>Mesure 7</i>)	P3
Rétablir progressivement les accès Internet essentiels (<i>Mesure 1 - Action 1.b</i>)	P3

Cette partie détaille les différentes mesures d'endiguement possibles selon 3 axes thématiques. Chaque *mesure* est ensuite scindée en *actions unitaires* :

- Contenir la propagation de l'attaque
 - Mesure 1 - Isoler temporairement d'Internet
 - Mesure 2 - Isoler les machines infectées
 - Mesure 3 - Entraver la propagation du chiffrement
- Préserver les biens essentiels de l'organisation
 - Mesure 4 - Préserver les sauvegardes
 - Mesure 4.1 - Préserver les serveurs de gestion des sauvegardes
 - Mesure 4.2 - Préserver les supports de stockage des sauvegardes
 - Mesure 4.3 - Préserver les serveurs de sauvegarde sur hyperviseur
 - Mesure 4.4 - Préserver les serveurs de sauvegarde dans le cloud
 - Mesure 5 - Préserver les serveurs de fichiers non sauvegardés
 - Mesure 6 - Préserver un seul contrôleur de domaine (Windows)
- Préserver les traces
 - Mesure 7 - Préserver les traces

Les actions présentées dans cette partie sont regroupées par thèmes, et non par priorités! Pour cela, se référer à la précédente partie Actions d'endiguement par priorités.

8 Contenir la propagation de l'attaque

Mesure 1 - Isoler temporairement d'Internet

Avant d'essayer d'isoler une par une les machines chiffrées par le rançongiciel, il est possible dans un premier temps de couper temporairement les communications avec Internet :

- [] **Action 1.a : Couper les communications Internet sur les pare-feux périphériques**
 - [] Désactiver tous les *flux entrants* Internet vers toutes les zones internes
 - [] Ne pas oublier de désactiver notamment les *accès VPN* depuis Internet
 - [] Désactiver tous les *flux sortants* Internet depuis toutes les zones internes
 - [] Pour les *flux WAN* entre différents sites de l'organisation, arbitrer entre :
 - [] Maintenir les accès WAN essentiels pour préserver les flux métiers internes
 - [] Couper les accès WAN pour isoler le périmètre compromis du reste du système d'information
 - [] Vérifier par des tests l'isolation d'Internet en entrée et en sortie (test de navigation Internet, test de *ping*, supervision du monitoring réseau, ou autres tests simples)

Cette mesure d'isolation a pour objectif de priver le rançongiciel de son serveur de contrôle, et ainsi :

- *Empêcher le rançongiciel de recevoir de nouveaux ordres* de chiffrement et de latéralisation, d'exfiltration de données sensibles, d'installation de nouvelles portes dérobées et persistances.
- *Empêcher l'attaquant d'observer les actions des défenseurs* et d'entraver la remédiation en cours.
- *Donner du temps aux défenseurs* pour analyser la situation et se concentrer sur la suite de l'endiguement de la propagation et des investigations.

Remarque : Priver l'entreprise d'Internet peut engendrer un *coût*, mais celui-ci est à comparer au coût de la perte des données métiers en cours de chiffrement et au coût de la remédiation et de la reconstruction qui s'ensuivra (prestation de réponse à incident, prestation de reconstruction, service détérioré, coût RH - business - juridique, etc.).

Impacts : Cette action d'isolation d'Internet va temporairement saturer le service d'assistance HelpDesk, bloquer les télémaintenances, perturber les services essentiels, bloquer les mises à jour (y compris des antivirus et autres solutions de sécurité), bloquer les liens avec les applications cloud (y compris de sécurité), bloquer l'accès à des services tiers, etc.

Globalement, tant que l'investigation n'est pas terminée et que les moyens de communication de l'adversaire ne sont pas identifiés, il est déconseillé de permettre des communications non contrôlées par une *liste blanche* et non essentielles, que ce soit pendant la remédiation ou une reconstruction trop hâtive :

- [] **Action 1.b : Rétablir progressivement les accès Internet nécessaires au traitement de l'incident ou à la survie de fonctions essentielles**
 - [] *Flux entrant* : Un flux entrant essentiel peut être rétabli à condition d'ajouter un second facteur d'authentification en plus du simple mot de passe (adresse IP source en *liste blanche*, MFA, etc.) aux acteurs suivants :
 - [] Acteurs de services de réponse à incident
 - [] Acteurs essentiels au maintien d'activité et à l'infogérance (avec prudence car ils sont potentiellement vecteurs de la compromission)

- *Flux sortant* : Un flux sortant essentiel peut être rétabli à condition de restreindre l'adresse IP ou le domaine de destination avec une *liste blanche* (en utilisant un équipement de type proxy ou pare-feu) aux services suivants :
 - Services de sécurité : SOC, mises à jour et accès à la console de l'antivirus/EDR, supervision
 - Services essentiels au maintien d'activité

Mesure 2 - Isoler les machines infectées

Préserver une machine infectée par un rançongiciel permettra d'éviter sa propagation depuis cette machine vers le reste du système d'information :

- **Action 2.a : Préserver les machines infectées du reste du système d'information**
 - Si ce sont des *machines virtuelles*, mettre ces serveurs en *pause*
 - Si ce sont des *machines physiques Windows*, les mettre en *veille prolongée*
 - Sinon, arbitrer entre :
 - *Éteindre* la machine si elle n'est pas complètement chiffrée, pour arrêter le chiffrement (mais cela purgera la mémoire)
 - *Isoler* la machine du réseau pour ne pas purger la mémoire, par exemple en débranchant le câble réseau et en désactivant le Wifi (mais cela n'arrêtera pas le chiffrement s'il était encore en cours)

Remarque : Autant que possible, *éviter d'éteindre électriquement* une machine chiffrée car cela purgerait la mémoire RAM. Or, préserver la mémoire pourrait être utile aux *investigations* et concourir à retrouver des *clés de déchiffrement* nécessaire au recouvrement des données par des entreprises spécialisées.

Si les zones infectées sont identifiées et peuvent être concrètement isolées au niveau réseau, isoler ces zones peut éviter à l'incident de s'étendre davantage :

- **Action 2.b : Isoler les zones infectées du reste du système d'information**
 - *Isoler* au niveau du réseau les zones infectées (réseau physique ou virtualisé)

Impacts : Une telle action peut avoir de grands impacts sur les applications métiers dont les interdépendances pourraient ne plus être accessibles. Si jamais cette action est réalisée, il faudra être vigilant aux remontées de dysfonctionnements de la part des équipes internes et avoir la capacité d'effectuer un retour arrière ou de filtrer finement les flux réseaux strictement nécessaires.

Mesure 3 - Entraver la propagation du chiffrement

Si vous observez que la propagation du chiffrement semble continuer malgré les mesures précédentes, il est alors probable qu'un système central d'administration ait été compromis

(exemple : GPO) ou que le rançongiciel chiffre les partages réseaux qui lui sont accessibles. Dans de tels cas, seules des équipes spécialisées pourront investiguer et donner des contre-mesures ciblées et efficaces. En attendant l'intervention de ces équipes, quelques actions complémentaires et génériques peuvent être tentées...

Lorsqu'on est probablement en présence d'un chiffrement des partages réseaux avec des comptes privilégiés :

- **Action 3.a : Neutraliser les comptes à privilèges suspectés compromis** Si des comptes à privilèges sont suspectés d'être utilisés pour le chiffrement des partages réseaux, certaines actions peuvent être tentées, tout en prenant garde aux effets de bords qu'elles pourraient entraîner :
 - Réinitialiser ces comptes (*efficace uniquement si la latéralisation s'effectue par une authentification par mot de passe*)
 - Désactiver ces comptes (*efficace immédiatement si authentification par mot de passe et avec un peu de latence pour une authentification Kerberos*)

Si on ne sait pas quel compte à privilèges est utilisé pour le chiffrement des partages réseaux, on peut vouloir neutraliser tous les comptes à privilèges avec les mêmes leviers précédents :

- **Action 3.b : Réinitialiser tous les comptes à privilèges**
 - Créer un nouveau compte *Administrateur de domaine* dit *bris de glace*
 - Réinitialiser tous les comptes à privilèges sans oublier les comptes *administrateurs du domaine* (en utilisant le compte *bris de glace* précédent)

Impacts : *Agir sur les comptes à privilèges peut avoir de gros impacts en production et cela doit être fait avec précaution. Généralement, on peut rarement arrêter une propagation d'un maliciel sans causer des dommages sur la production, et le pilotage par une équipe spécialisée devient nécessaire.*

Remarques :

- Sur un parc Active Directory, une modification sur un compte utilisateur effectuée sur un contrôleur de domaine peut prendre du temps à être synchronisée avec les autres contrôleurs de domaine.
- Un simple compte utilisateur, même sans privilège, peut chiffrer tout un serveur de fichiers si les droits d'accès aux fichiers sont trop larges.
- La latéralisation par rebond est également possible (exemple : ver informatique), mais pour un rançongiciel, cette méthode de propagation est moins probable. Dans ce cas, les actions d'endiguement précédentes restent valables.

Lorsqu'un système central d'administration a probablement été compromis :

- **Action 3.c : Analyser avec un antivirus le dossier SYSVOL du domaine Active Directory**

- Analyser le dossier SYSVOL du domaine Active Directory avec un antivirus à jour, depuis un ordinateur sain
- **Action 3.d : Inspecter certains moyens de propagation usuels**
 - Inspecter si des scripts ou exécutables inconnus sont présents dans le dossier SYSVOL du domaine Active Directory (exemple : \SYSVOL\\scripts)
 - Inspecter si une tâche planifiée inconnue est créée sur les machines compromises et exécute du code inconnu
 - Inspecter si une GPO a été illégitimement modifiée ou créée pour exécuter du code inconnu (exécution de tâche planifiée, lancement de script au démarrage, déploiement d'un logiciel, etc.)

Remarque : Des mesures de *durcissement* permettent également d'entraver une latéralisation d'attaque, mais il est difficile de les mettre en œuvre dans le *temps chaud* d'un incident. Leur mise en œuvre sera généralement plus tard dans la remédiation, lorsque les défenseurs auront repris le contrôle de leur système d'information et pourront s'atteler à son durcissement. On peut citer comme telles mesures :

- Retirer les droits d'administration locale de tous les utilisateurs (pour entraver une élévation de privilèges locale des machines infectées).
- Activer LAPS (pour entraver la latéralisation avec un compte administrateur local compromis).
- etc.

9 Préserver les biens essentiels de l'organisation

Mesure 4 - Préserver les sauvegardes

Les *sauvegardes* ne doivent pas être chiffrées car elles seront primordiales pour rétablir les services du système d'information après l'incident : il faut donc les préserver au plus tôt.

Mesure 4.1 - Préserver les serveurs de gestion des sauvegardes

- **Action 4.1.a : Identifier les différents types de sauvegarde du système d'information**
 - Identifier la solution de sauvegarde des machines virtuelles
 - Identifier la solution de sauvegarde des fichiers
- **Action 4.1.b : Identifier les serveurs de gestion des sauvegardes**
 - Identifier les serveurs physiques
 - Identifier les serveurs virtuels (et l'hyperviseur qui les héberge)
- **Action 4.1.c : Préserver les serveurs de gestion des sauvegardes**

- Si ce sont des *machines virtuelles*, mettre ces serveurs en *pause*
- Si ce sont des *machines physiques Windows*, les mettre en *veille prolongée*
- Dans le cas contraire, *éteindre* ces serveurs

D'autres actions sont possibles pour préserver un serveur, mais contrairement aux actions ci-dessus, elles ne permettent pas d'arrêter le chiffrement du serveur s'il était déjà en cours, ou seraient plus compliquées à réaliser sans réelle plus-value de sécurité dans le cas présent :

- *Isoler du réseau*, tout en gardant un accès d'administration physique, virtuel ou hors-bande
- *Confiner* dans un VLAN ayant des flux extrêmement limités
- *Sortir le compte d'administration du domaine Active Directory compromis*

Remarque : Les sauvegardes ne doivent pas être restaurées tant que l'analyse de l'équipe de réponse à incident n'a pas conclu une *date de restauration sûre*.

Remarque : Arrêter les processus de sauvegarde des clients (*agent*) depuis la console de gestion protégera les sauvegardes des clients mais pas le serveur de sauvegarde lui-même. Cette action est donc également faisable mais a été jugée moins efficace.

Impacts : *Impossibilité de réaliser de nouvelles sauvegardes jusqu'à leur remise en service.*

Mesure 4.2 - Préserver les supports de stockage des sauvegardes

- **Action 4.2.a : Identifier les supports de stockage des sauvegardes, accessibles depuis le réseau**
 - NAS
 - SAN
 - Robots de sauvegardes
 - Lecteurs de bandes, etc.
- **Action 4.2.b : Préserver les supports de stockage des sauvegardes, accessibles depuis le réseau**
 - *Éteindre* ces supports ou les *isoler* du réseau, au plus efficace

D'autres actions sont possibles pour préserver un serveur, mais contrairement aux actions ci-dessus, elles ne permettent pas d'arrêter le chiffrement du serveur s'il était déjà en cours, ou seraient plus compliquées à réaliser sans réelle plus-value de sécurité dans le cas présent :

- *Isoler du réseau*, tout en gardant un accès d'administration physique, virtuel ou hors-bande
- *Confiner* dans un VLAN ayant des flux extrêmement limités
- *Sortir le compte d'administration du domaine Active Directory compromis*

Remarque : Les serveurs de gestion des sauvegardes ayant déjà été préservés par la mesure précédente :

- Les supports de stockage des sauvegardes sont donc normalement sans activité et peuvent être simplement éteints.
- Les supports de stockage des sauvegardes hors-ligne ou uniquement accessibles en back-end des serveurs de gestion ne sont pas accessibles par le réseau et sont considérés comme déjà préservés : disques locaux, DAS, SAN, etc. Ils n'ont donc pas besoin d'être éteints.

Impacts : *Aucun impact ne résulterait de cette mesure si ces supports ne stockent que des sauvegardes. Mais s'ils stockent des fichiers d'applications métiers, des effets de bords d'indisponibilité seront à gérer.*

Mesure 4.3 - Préserver les serveurs de sauvegarde sur hyperviseur

Si le *serveur de gestion des sauvegardes* est une *machine virtuelle* éteinte précédemment, il faut alors le préserver en l'exportant de l'hyperviseur qui l'héberge :

- **Action 4.3 : Exporter la machine virtuelle de gestion des sauvegardes**
 - Prendre un instantané de la machine virtuelle (déjà mise en pause) puis l'exporter sur un disque dédié hors ligne

Remarque : Cette mesure peut ne pas être prioritaire si les serveurs hyperviseurs semblent non ciblés par le chiffrement.

Remarque : En parallèle de cette mesure de préservation, des mesures pour restreindre l'accès aux hyperviseurs peuvent être étudiées, comme les sortir du domaine Active Directory (s'ils y étaient) et n'utiliser que des comptes d'administration locaux.

Mesure 4.4 - Préserver les serveurs de sauvegarde dans le cloud

Des serveurs de gestion ou de stockage des sauvegardes peuvent être hébergés dans le *cloud*. Pour de tels serveurs, effectuer les mêmes actions que précédemment en considérant que ce sont des machines virtuelles :

- **Action 4.4 : Préserver les serveurs de sauvegarde dans le cloud**
 - Identifier les serveurs de sauvegarde dans le cloud
 - *Mettre en pause, sinon éteindre* ces serveurs

Impacts : *Impossibilité de réaliser de nouvelles sauvegardes jusqu'à leur remise en service.*

Mesure 5 - Préserver les serveurs de fichiers non sauvegardés

Si des serveurs de fichiers ne sont pas sauvegardés, alors ils doivent être préservés au même titre que les sauvegardes, car ils sont susceptibles de contenir des données nécessaires à la reprise d'activité de l'organisation :

- **Action 5.a : Identifier les serveurs de fichiers non sauvegardés**
- **Action 5.b : Préserver les serveurs de fichiers non sauvegardés**
 - Si possible, *éteindre* ces serveurs immédiatement et attendre l'éradication de l'adversaire avant de les rallumer
 - Sinon, pour le maintien des activités vitales, il est envisageable de les confiner dans une nouvelle bulle réseau avec les applications critiques qui en dépendent

Impacts : Malheureusement, préserver un serveur de fichiers aura plus d'impacts que de préserver un serveur de stockage de sauvegardes car ils sont accessibles directement par les utilisateurs et les applications. Cette mesure engendrera sûrement une indisponibilité de service.

Mesure 6 - Préserver un seul contrôleur de domaine (Windows)

Si le système d'information utilise un domaine Active Directory et si on craint la compromission de compte à privilège, on peut dès à présent préserver un contrôleur de domaine en prévision de la restauration du système d'information :

- **Action 6 : Préserver un seul contrôleur de domaine**
 - De préférence choisir un contrôleur de domaine *physique* et *l'éteindre*
 - Sinon, préserver un contrôleur de domaine virtuel en le *mettant en pause* et en *l'exportant* de l'hyperviseur sur un disque dédié hors ligne

Impact : Normalement, les services rendus par les contrôleurs de domaine sont redondants par clusterisation, et l'un d'eux peut donc être mis à l'écart sans coupure de service. Des effets de bords peuvent toutefois survenir si le contrôleur de domaine est le premier contacté dans la liste des DNS reçus par les clients (dont les résolutions DNS peuvent résulter en timeout) ou si le FQDN ou l'IP du contrôleur de domaine a été renseigné en dur dans un service.

10 Préserver les traces

Mesure 7 - Préserver les traces

Pour soutenir la réponse à incident dans son objectif d'investigation, il faut prioritairement préserver les logs les plus anciens possibles, augmenter leur rétention et leur verbosité. Plus les équipes d'investigation auront les traces d'activité de l'adversaire, plus efficace sera son éradication :

- **Action 7.a : Préserver les traces dans les journaux d'équipements**

- Identifier les équipements de sécurité du système d'information :
 - pare-feux
 - passerelles VPN
 - proxy
 - console antivirus et EDR, etc.
- Exporter les logs
- Augmenter la rétention des logs
- Configurer les logs les plus complets possibles

Remarque : Les journaux des machines compromises sont normalement déjà préservés puisqu'elles sont soit en veille soit éteintes.

- **Action 7.b : Préserver les traces dans les journaux d'authentification**

- Identifier la solution de stockage des journaux d'identification sur le réseau interne, comme le domaine Active Directory
- Exporter ces logs
- Augmenter la rétention de ces logs

Si les logs sont déjà exportés dans un SIEM ou un centralisateur de logs, il est alors inutile de les exporter et d'augmenter leur rétention sur les machines sources, mais il faut néanmoins augmenter leur verbosité lorsque cela est possible.

Remarque : En plus d'être indispensable à la compréhension de l'incident, sauvegarder les éléments de preuve pourra être nécessaire pour répondre aux forces de l'ordre lors d'éventuelles poursuites judiciaires.

A la fin de ces actions d'endiguement, la compromission devrait être contenue. Pour autant, l'incident a très probablement impacté l'organisation au-delà de son système d'information et il reste encore beaucoup à faire.

De manière générale, un incident doit être géré jusqu'à son terme avec tous les corps de métier concernés : *investigation forensique et remédiation par une équipe spécialisée, maintien d'activité, communication interne aux partenaires, dépôt de plainte et déclarations, etc.*

Pour ce faire, il est conseillé de piloter la suite de la résolution de l'incident en cohérence avec les *impacts* identifiés et demander de l'aide :

- 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 mis à disposition par le CERT Santé, en collaboration avec le CSIRT-PJ : <https://cyberveille-sante.gouv.fr/dossier-thematique/aide-au-depot-de-plainte-en-cas-dattaque-par-rancongiel>. 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.

11 Définitions

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.

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.

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.

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*.

12 Contacter le CERT-FR

12.1 Important

Quand vous effectuez un signalement auprès du CERT-FR, un numéro de référence vous est attribué. Pensez à rappeler ce numéro quand vous nous recontactez, ou dans l'entête de vos messages afin de simplifier le suivi du cas.

12.2 Par Téléphone

Le CERT-FR est joignable 7J/7, 24H/24 :

- depuis la France métropolitaine au **3218** (service gratuit + prix d'un appel) ou 09 70 83 32 18
- depuis certaines collectivités territoriales situées en Outre-mer ou depuis l'étranger au +33 9 70 83 32 18

12.3 Par Internet

- **mèl** : cert-fr@ssi.gouv.fr
- **site** : <https://cert.ssi.gouv.fr/contact/>

12.4 Clé PGP du CERT-FR

Pour vérifier l'intégrité des informations fournies ci-dessous, veuillez contacter le CERT-FR.

Identifiant de la clé : 0x1B45CF2A

Empreinte de la clé : 7F4C 8FA6 A356 D1CC 2E5C AB09 5416 33B8 1B45 CF2A

Télécharger la clé publique : https://cert.ssi.gouv.fr/Images/public_key_2024.asc

13 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		
CERT/CSIRT externe en prestation de réponse à incident	https://www.cybermalveillance.gouv.fr/diagnostic/accueil https://cyber.gouv.fr/produits-services-qualifies	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.

14 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.
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-notifier-une-violation-de-donnees-personnelles	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.

15 Préparation

En *prévention* d'un incident, une fiche réflexe sera d'autant plus efficace si elle a pu être 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. # 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 - Qualification
- Comment réagir en cas d'incident rançongiciel
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- Cyberattaques et remédiation

16 Licence

Ce document est dérivé des les travaux du GT Fiches Réflexes de remédiation de l'InterCERT FRANCE

Les documents originaux peuvent être consultés sur le site de l'InterCERT-France (<https://www.intercert-france.fr/>).

Le présent document est publié sous licence CC BY-NC-SA 4.0.

ANSSI/SDO
Version 1- UNDEF

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr

