PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 11/08/2025
N° CERTFR-2024-RFX-008

Défiguration de site web - Endiguement

Fiche Réflexe

ANSSI/SDO
11/08/2025

Version : 2
Nombre de pages : 18

Table des matières

1 Présentation de la fiche

1.1 À qui s'adresse-t-elle ?

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

1.2 Quand l'utiliser ?

Utiliser cette fiche lorsqu'une défiguration (ou défacement) est détectée sur un site web de l'organisation.

1.3 À quoi sert-elle ?

L'objectif de cette fiche est de proposer les premières actions d'*endiguement* face à une défiguration de site web. Elles viseront à figer la situation pour *limiter les dommages potentiels* et à *préserver la réputation de l'organisation*.

1.4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie Actions d'endiguement par priorités pointe l'ordre chronologique et prioritaire des actions détaillées dans la partie suivante.
- La partie Actions d'endiguement par thèmes détaille les différentes actions d'endiguement possibles selon 4 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.

2 Prérequis

2.1 Avoir qualifié l'incident

Avoir *qualifié* que l'incident en cours sur mon système d'information soit bien une *défiguration de site web* causée par la *compromission du serveur web*, et en avoir évalué la gravité :

Fiche précédente conseillée : Fiche réflexe - Défiguration de site web - 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.

2.2 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*, ou si le site web est *hébergé* chez un tiers, s'assurer de la capacité à mobiliser leur support technique dans l'urgence. Il aura non seulement les capacités opérationnelles pour agir, et pourra sans doute faire bénéficier de son expérience sur ce type d'incident.

2.3 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.

3 Actions d'endiguement par priorités

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

Actions	Priorité
Mettre hors-ligne le site web *(Mesure 1)*	P0
Préserver les sauvegardes *(Mesure 2)*	P0
Préserver le contenu du site web affecté *(Mesure 3)*	P1
Préserver les journaux *(Mesure 4)*	P1
Mettre en ligne une page de maintenance *(Mesure 5)*	P2
Communiquer *(Mesure 6)*	P2
Limiter la propagation sur le reste du système d'information *(Mesure 7)*	P3
Limiter la propagation sur les machines hôtes *(Mesure 8)*	P3

4 Actions d'endiguement par thèmes

Pour rappel, une *défiguration de site web* a principalement 7 causes :

- **Compromission du site web** :
    1. Usurpation d'un compte de gestion du site web ou d'un compte d'administration de son serveur hôte
    2. Sabotage délibéré d'un employé interne
    3. Exploitation d'une vulnérabilité (XSS, injection SQL, etc.), affectant le site web lui-même, un de ces composants (plugin, bibliothèque tierce), ou son moteur de gestion
- **Compromission d'un système tiers** :
    4. Compromission d'un site tiers, dont la page web importe du contenu (par exemple, javascript)
    5. Compromission des enregistrements DNS qui redirigent le trafic vers un serveur contrôlé par l'attaquant
    6. Compromission d'un équipement en amont du serveur web
    7. Compromission globale du système d'information, du tenant cloud ou de l'hébergeur

Les mesures d'endiguement qui seront présentées dans cette partie cibleront principalement **une défiguration** causée par la **compromission du site web**. Si la qualification a déterminé que la défiguration était due à une **compromission d'un système tiers**, certaines mesures d'endiguement ont été recommandées à la fin de la fiche de qualification, mais elles ne figurent pas dans cette fiche.

Endiguer une défiguration de site web consiste principalement à **figer la situation** en *limitant l'extension des dommages* contre le système d'information et en *préservant l'image de l'organisation*.

Cet objectif peut être atteint en suivant les mesures ci-dessous réparties selon 4 axes thématiques. Chaque *mesure* sera ensuite scindée en *actions unitaires* :

- Limiter l'extension des dommages

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

4.1 Limiter l'extension des dommages

4.1.1 Mesure 1 - Mettre le site web hors-ligne

Action 1.a : Mettre le site web hors-ligne

☐ Si possible, mettre le site web en *mode maintenance*
☐ Sinon, *arrêter le service du site web* (mais le serveur hôte peut rester allumé)

Cette mesure d'isolation a pour objectifs de :

- *Limiter les dommages* contre le site web
- *Limiter la fuite de données* et les conséquences légales et réglementaires potentielles
- *Préserver l'image* de l'organisation
- *Limiter la propagation de la compromission* contre le serveur hôte ou d'autres systèmes et applications accessibles

Action 1.b : Préserver les serveurs hôtes

Pour prévenir la compromission des serveurs hôtes et l'éventuelle propagation de l'attaque, il est également possible de :

☐ Si ce sont des *machines virtuelles* :
    ☐ Mettre ces serveurs en *pause*

  - ☐ Déconnecter les interfaces réseaux virtuelles
  - ☐ Créer un instantané des serveurs (disque et mémoire)
  - ☐ Renommer la machine `MACHINE_SOUS_INVESTIGATION`
- ☐ Si ce sont des *machines physiques Windows*, les mettre en *veille prolongée*
- ☐ Sinon, si possible, *isoler les machines du réseau* tout en gardant un accès d'administration physique, virtuel ou hors-bande :
  - ☐ Désactiver tous les flux entrants depuis Internet vers les serveurs hôtes
  - ☐ Désactiver tous les flux sortants depuis les serveurs hôtes vers Internet
- ☐ Sinon, en dernier recours, *éteindre* la machine

4.1.2 Mesure 2 - Préserver les sauvegardes

Les *sauvegardes* sont primordiales pour rétablir le site web en cas de défiguration ou d'incident destructif.

Action 2 : Préserver les sauvegardes du site web

- ☐ Identifier les ressources sauvegardées à préserver :
  - Configuration
  - Code
  - Fichiers métiers
  - Base de données
- ☐ Préserver ces sauvegardes en les mettant *hors-ligne* ou en les *exportant*.

Attention

Si le site web a été compromis, ses sauvegardes peuvent également l'avoir été. Elles ne devront donc pas être restaurées en production avant qu'une investigation ait été menée.

4.2 Préserver les traces

4.2.1 Mesure 3 - Préserver le contenu du site web affecté

Si les serveurs hôtes n'ont pas été *éteints* ou mis en *pause*, enlever de la portée de l'attaquant tout accès à ses fichiers téléversés sur les serveurs compromis :

Action 3 : Préserver le contenu du site web affecté

- ☐ Déplacer le contenu du site web affecté dans un nouveau dossier préfixé par *INCIDENT* hors de portée du service web

4.2.2 Mesure 4 - Préserver les journaux

Préserver les journaux avant leur rotation pour pouvoir investiguer les empreintes laissées par l'attaquant et éradiquer son accès initial et ses moyens de persistance :

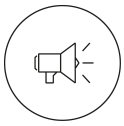
Action 4.a : Préserver les journaux sur les systèmes tiers

- ☐ Journaux des équipements en amont :
  - ☐ pare-feu
  - ☐ répartiteur de charge
  - ☐ mandataire inverse (*reverse-proxy*)
  - ☐ pare-feu applicatif (*WAF*)
  - ☐ etc.
- ☐ Journaux de la console antivirus et/ou de l'EDR

Si les serveurs hôtes n'ont pas été *éteints* ou qu'un *instantané* n'a pas été réalisé, préserver alors leurs propres journaux :

Action 4.b : Préserver les journaux des serveurs hôtes

- ☐ Journaux de l'interface de gestion
- ☐ Journaux du site web
  - ☐ Ne pas oublier les journaux des plugins et bibliothèques tierces
- ☐ Journaux du système



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.

Action 4.c : Augmenter la traçabilité

- ☐ Augmenter la durée de rétention des journaux
- ☐ Augmenter la verbosité des journaux
- ☐ Mettre en place un export des journaux en temps réel vers un puits de logs

4.3 Préserver l'image de l'organisation

4.3.1 Mesure 5 - Mettre en ligne une page de maintenance

Action 5.a : Mettre en ligne une page de maintenance

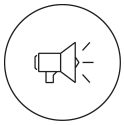
- Utiliser une simple page de maintenance HTML avec uniquement du texte et des images locales (sans aucun lien externe, sans JavaScript, et dans le doute, sans aucun fichier CSS)
- Si possible, indiquer quelques informations essentielles, dûment validées pour être communiquées vers l'extérieur

Attention

La version défigurée du site peut encore être visible à cause des fonctionnalités de *cache* du CDN ou du mandataire inverse (*reverse-proxy*). Dans un tel cas, demander aux administrateurs de ces solutions de réinitialiser leur cache.

Plus tard, une fois les actions d'endiguement terminées, il sera également possible de rétablir un service dégradé en mettant en ligne une *version statique* du site. Pour ce faire, les principales étapes seraient les suivantes :

1. Vérifier si un *export statique du site web* est réalisable par les équipes techniques (certains éditeurs de CMS mettent à disposition des outils ou plugins pour convertir un site dans une version statique).
2. Créer la version du site statique sans la défiguration (attention aux codes de l'attaquant présents sur le serveur compromis).
3. Déterminer le serveur qui hébergera le site statique : utiliser un serveur de maintenance temporaire (en interne ou hébergé chez un tiers) ou garder le même serveur.
4. Durcir autant que possible le serveur web qui hébergera le site statique :
    - Mettre à jour tous les correctifs de sécurité du serveur hôte et du serveur web
    - Désactiver tous les plugins du serveur web inutiles pour afficher du contenu statique HTML
    - Activer les fonctionnalités de sécurité disponibles sur le serveur hôte (antivirus, EDR, etc.) et les équipements en amont (pare-feu applicatif ou *WAF*, sonde réseau, IPS, etc.)
    - Effectuer un scan antivirus complet du serveur hôte
    - Renouveler les identifiants du site web et du serveur hôte (voir la partie Mesure 9 - Limiter la propagation sur les machines hôtes)



Remarque

- Mettre en ligne une version statique uniquement avec des pages HTML empêcherait l'attaquant d'exploiter une vulnérabilité applicative du site. (Attention, cela n'empêcherait tout de même pas l'exploitation de vulnérabilités du système d'exploitation du serveur hôte, du service web ou de ses plugins installés).

- Ne pas remettre en ligne le site web sans avoir fait investiguer et éradiquer l'accès initial et les moyens de persistance, par des équipes spécialisées.

4.3.2 Mesure 6 - Communiquer

La défiguration d'un site web porte généralement atteinte à la réputation de l'organisation en affichant une revendication politique ou idéologique illégitime. Il est donc nécessaire de communiquer publiquement pour la désapprouver.

Action 6.a : Communiquer

☐ Communiquer publiquement pour désapprouver l'affichage illégitime

4.4 Limiter la propagation de l'attaque sur le système d'information

Une fois la situation figée, et avant de reconstruire le site web, prendre en considération que l'attaque a pu être plus grave que la défiguration : l'attaquant a pu se propager sur le serveur hôte et même se latéraliser sur le système d'information.

4.4.1 Mesure 7 - Limiter la propagation sur le reste du système d'information

Si un compte de gestion a été usurpé (identifié lors de l'étape de qualification), l'empêcher de se connecter sur d'autres machines du système d'information :

Action 7.a : Examiner tous les accès du compte de gestion usurpé

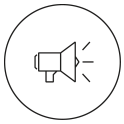
☐ Examiner tous les accès que peut avoir le compte de gestion usurpé sur le système d'information :

  ☐ Autres sites web accessibles à partir de la même interface de gestion
  ☐ Interfaces d'administration du système d'information ou du tenant cloud, le cas échéant
  ☐ Accès distant
  ☐ VPN

☐ Réinitialiser tous ces accès distants et configurer l'authentification forte si possible
☐ Investiguer si des connexions réussies illégitimes ont eu lieu sur ces accès

Action 7.b : Investiguer la propagation de l'attaque sur le reste du système d'information

- ☐ Investiguer des connexions anormales depuis le serveur hôte vers le reste du système d'information
- ☐ Investiguer des connexions sortantes Internet anormales depuis le serveur hôte



Remarque

En cas de doute sur une potentielle propagation de l'attaque à d'autres systèmes d'information, utiliser la fiche : Fiche réflexe - Compromission système - Qualification

4.4.2 Mesure 8 - Limiter la propagation sur les machines hôtes

Si les serveurs hôtes n'ont pas été préservés et que seul le site web a été mis hors-ligne à la Mesure 1, se protéger d'une propagation de l'attaque avec les actions suivantes.

Action 8.a : Réinitialiser les comptes de gestion du serveur

Si un compte de gestion a été usurpé (identifié lors de l'étape de qualification), supprimer tous les moyens d'accès illégitimes que l'attaquant aurait pu configurer :

- ☐ Identifier les interfaces de gestion exposées du site web exposée sur Internet.
- ☐ Puis, pour chacune de ces interfaces de gestion, réinitialiser les comptes de gestion :
  - ☐ Réinitialiser les identifiants des comptes administratifs du site web, avec un *mot de passe fort*
  - ☐ Configurer un *double facteur d'authentification* (MFA), pour entraver l'usurpation de compte
  - ☐ Révoquer leurs *sessions actives* / *jetons*

Action 8.b : Investiguer la propagation de l'attaque sur le système hôte

- ☐ Investiguer une latéralisation de l'attaque à d'autres sites web du serveur hôte
- ☐ Investiguer les alertes antivirales ou EDR sur le serveur d'hôte
  - ☐ webshell
  - ☐ RAT
  - ☐ etc.
- ☐ Investiguer une élévation de privilège vers le serveur hôte, à commencer par la recherche d'actions de reconnaissance (*whoami*, etc.) et de persistance (*tâches planifiées*, *run keys*, etc.)
- ☐ Investiguer des modifications ou ajouts de fichiers sur le système hôte

Attention

Ne pas écarter la possibilité que le compte d'administration n'ait pas été usurpé et que l'administrateur lui-même ait réalisé ces actions frauduleuses.

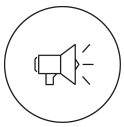
Dans le doute d'une compromission du serveur hôte, réinitialiser tous les secrets d'authentification auxquels aurait pu accéder l'attaquant :

Action 8.c : Réinitialiser les secrets d'authentification présents sur le serveur hôte

- ☐ Réinitialiser les identifiants des comptes d'administration local du serveur hôte (avec un *mot de passe fort*)
- ☐ Réinitialiser les identifiants des comptes d'administration du domaine qui se sont connectés sur le serveur hôte depuis son dernier redémarrage (avec un *mot de passe fort*)
- ☐ Réinitialiser les identifiants des comptes dont le mot de passe était présent en clair dans les fichiers de configuration du site web ou du serveur
- ☐ Révoquer et réinitialiser les clés privées présentes sur le serveur (clés privées TLS, clés privées SSH, clés d'API, etc.)

Impact

- *Réinitialiser les identifiants des comptes d'administration aura un impact sur tous les systèmes d'information administrés par ces comptes. Réaliser cette mesure avec prudence.*
- *Si les certificats TLS révoqués sont des certificats Wildcard, tous les serveurs qui les utilisent doivent renouveler les leurs avant la révocation des anciens.*



Remarque

Dans le doute d'une propagation de l'attaque au système hôte, utiliser la fiche : Fiche réflexe - Compromission système - Qualification

5 Suite des actions

Une fois la situation figée par les mesures précédentes, l'endiguement est terminé.

La suite de la remédiation devra faire appel à des équipes spécialisées. Elle suivra globalement le processus suivant :

- Investigation puis éradication de l'accès initial et des emprises laissées par l'attaquant
- Durcissement du serveur
- Restauration des sauvegardes

- Rétablissement du service

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*.

6 Annexes

6.1 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 - Défiguration de site web - Qualification
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- Cyberattaques et remédiation

6.2 Définitions

6.2.1 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.

6.2.2 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.

6.2.3 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.

6.2.4 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*.

6.2.5 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.

6.2.6 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.

6.2.7 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.

6.3 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-incidents-de-securite-pris`	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	Consulter la section Contacter le CERT-FR	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.

6.4 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	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.

6.5 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.

6.6 Contacter le CERT-FR

Attention

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.

6.6.1 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

6.6.2 Par Internet

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

6.6.3 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/uploads/public_key_2024.asc

6.7 Licence

Ce document est dérivé des 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/publications/fiches-reflexes/).

ANSSI/SDO
Version 2- UNDEF

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

cyber.gouv.fr