PREMIÈRE 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 15/07/2024
N° CERTFR-2024-RFX-008

Défiguration de site web - Endiguement

Fiche Réflexe

ANSSI/SDO
15/07/2024

Version : 1
Nombre de pages : 17

Table des matières

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'une défiguration est détectée sur un site web de l'organisation.

3 A 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*.

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 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.

5 Avoir qualifié l'incident

Avoir *qualifié* que l'incident en cours sur mon système d'information soit bien une *défiguration de site web* causé 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.

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*, 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.

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
Mettre hors-ligne le site web *(Mesure 1)*	P0
Reprendre le contrôle de l'administration *(Mesure 2)*	P0
Préserver les traces *(Mesure 9)*	P0
Préserver le contenu du site web affecté *(Mesure 3)*	P1
Mettre en ligne une version statique *(Mesure 5)*	P1
Communiquer *(Mesure 6)*	P2
Préserver les sauvegardes *(Mesure 4)*	P2
Limiter les impacts liés aux données sensibles *(Mesure 7)*	P3
Limiter la propagation sur le système d'information *(Mesure 8)*	P3

Rappel : 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 (javascript, etc.) 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 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.

Endiguer une *défiguration de site web* consiste principalement à figer la situation en *limitant les dommages potentiels* 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* :

- Préserver le serveur web affecté
  - Mesure 1 - Mettre hors-ligne le site web
  - Mesure 2 - Reprendre le contrôle de l'administration
  - Mesure 3 - Préserver le contenu du site web affecté
  - Mesure 4 - Préserver les sauvegardes
- Préserver l'image de l'organisation
  - Mesure 5 - Mettre en ligne une version statique
  - Mesure 6 - Communiquer
- Limiter les impacts de l'attaque contre l'organisation

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 Préserver le serveur web affecté

Mesure 1 - Mettre hors-ligne le site web

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

Pour prévenir la compromission du serveur hôte et l'éventuelle propagation de l'attaque, il est également possible de :

- [ ] **Action 1.b : Isoler le serveur hôte d'Internet**
    - [ ] Désactiver tous les flux entrants depuis Internet vers le serveur hôte
    - [ ] Désactiver tous les flux sortants depuis le serveur hôte vers Internet
    - [ ] Si le serveur est une machine virtuelle, déconnecter les interfaces réseaux virtuelles

Certains actions suivantes, comme la réinitialisation des mots de passe, nécessiteront que le serveur web soit accessible des administrateurs… tout en restant isolé d'Internet :

- [ ] **Action 1.c : Rétablir les accès administratifs** Tout en laissant le site web isolé d'Internet, permettre l'accès aux administrateurs :
    - [ ] à l'interface de gestion du site web
    - [ ] au serveur hôte

Mesure 2 - Reprendre le contrôle de l'administration

- [ ] **Action 2.a : Identifier les interfaces de gestion exposées du site web**

Puis, pour chacune de ces interfaces de gestion, réinitialiser les comptes administratifs :

- [ ] **Action 2.b : Réinitialiser les comptes administratifs du site web**
  - [ ] 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*

Si un compte d'administration a été usurpé (identifié lors de la qualification en prérequis), nettoyer tous les moyens d'accès illégitimes que l'attaquant aurait pu configurer :

- [ ] **Action 2.c : Nettoyer les moyens d'accès administratifs illégitimes**
  - [ ] Création de comptes d'administration illégitimes
  - [ ] Ajout de moyens d'authentification (MFA) ou d'enrôlement d'appareils illégitimes
  - [ ] Modification illégitime d'adresses de récupération de mot de passe

Attention : La possibilité que le compte d'administration n'ait pas été usurpé et que l'administrateur lui-même ait réalisé ces actions frauduleuses n'est pas à écarter.

Mesure 3 - Préserver le contenu du site web affecté

Pour enlever de la portée de l'attaquant tout accès à ses fichiers téléversés sur le serveur compromis et pour préserver ses traces :

- [ ] **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

Mesure 4 - Préserver les sauvegardes

Les *sauvegardes* sont primordiales pour rétablir le site web en cas de défiguration ou d'incident destructif. Il faut donc préserver ces sauvegardes, par exemple en les mettant hors-ligne ou en les exportant.

- [ ] **Action 4 : Préserver les sauvegardes du site web**

- [ ] Configuration
- [ ] Code
- [ ] Fichiers
- [ ] Base de données

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.

9 Préserver l'image de l'organisation

Mesure 5 - Mettre en ligne une version statique

Une fois les accès de l'attaquant coupés, préserver l'image de l'organisation en mettant temporairement en ligne une version statique du site web, en attendant sa reconstruction…

- [ ] **Action 5.a : Créer le site statique**
  - [ ] Vérifier si un *export statique du site web* est réalisable par les équipes techniques
  - [ ] Choisir avec la direction de l'organisation et l'équipe de communication, le type de site statique à exposer temporairement :
    - [ ] Une *version statique du site web* (ce qui signifie mettre en ligne une *version dégradée* du site web)
    - [ ] Une simple *page de maintenance*
  - [ ] Créer le site statique

Remarques :

- Certains éditeurs de CMS mettent à disposition des outils ou plugins pour convertir un site dans une version statique.
- Mettre en ligne une version statique uniquement avec des pages HTML empêche l'attaquant d'exploiter une vulnérabilité applicative du site.
- [ ] **Action 5.b : Déterminer le serveur qui hébergera le site statique** Plusieurs méthodes, au choix :
  - [ ] Utiliser un serveur de maintenance temporaire, en interne ou hébergé chez un tiers (le trafic web sera redirigé vers celui-ci)
  - [ ] Garder le même serveur (la version statique sera copiée à la racine du site web initial, dont le contenu affecté a déjà été déplacé précédemment)
- [ ] **Action 5.c : Durcir a minima le serveur web qui hébergera le site statique**
  - [ ] Mettre à jour tous les correctifs de sécurité du :

    - [ ] serveur hôte
    - [ ] 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, etc.)
    - [ ] équipement en amont (WAF, IPS, etc.)
  - [ ] Effectuer un scan antivirus complet du serveur hôte
  - [ ] Effectuer un scan de vulnérabilités complet sur le service web et corriger les vulnérabilités remontées
  - [ ] Renouveler les identifiants précédemment utilisés pour le site web et le serveur hôte
- [ ] **Action 5.d : Mettre en ligne la version statique**

Attention :

- La version défacée du site peut encore être visible à cause d'une fonctionnalité de *cache* du CDN ou du reverse-proxy. Dans un tel cas, appeler les administrateurs de ces solutions afin de réinitialiser leur cache.
- **Si malgré la mise en ligne d'une version statique du site une nouvelle défiguration a lieu**, 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).
- 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.

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 : Communiquer**
  - [ ] Communiquer publiquement pour désapprouver l'affichage illégitime

10 Limiter les impacts de l'attaque contre l'organisation

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 accéder à des données sensibles et se propager en dehors du site web. Il conviendra autant que possible d'en examiner les potentiels impacts et de limiter leur gravité.

Mesure 7 - Limiter les impacts liés aux données sensibles

- [ ] **Action 7.a : Examiner les données sensibles potentiellement accédées**
  - [ ] Examiner les données sensibles du site web affecté
  - [ ] Examiner les données sensibles accessibles via le compte usurpé (si avéré) à partir de l'interface de gestion
  - [ ] Prendre en considération :
    - [ ] Fichiers et données métiers sensibles
    - [ ] Bases de données
    - [ ] Identifiants de connexion
- [ ] **Action 7.b : Limiter les impacts liés aux données sensibles potentiellement accédées**
  - [ ] Déterminer les accès ayant potentiellement eu lieu sur les données sensibles :
    - [ ] Accès en lecture (vol de données, perte de confidentialité)
    - [ ] Accès en écriture (perte d'intégrité)
    - [ ] Suppression
  - [ ] Informer les responsables de ces données afin qu'ils puissent entreprendre les actions nécessaires.

Mesure 8 - Limiter la propagation sur le système d'information

- [ ] **Action 8.a : Examiner tous les accès du compte de gestion usurpé (si avéré)**
  - [ ] 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
    - [ ] Accès distant
    - [ ] VPN
  - [ ] Réinitialiser tous ses accès distants et configurer l'authentification forte si possible
  - [ ] Investiguer si des connexions réussies illégitimes ont eu lieu sur ces accès
- [ ] **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 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

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 privée TLS, clés privée SSH, etc.)

Impacts : *- 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.*

- [ ] **Action 8.d : 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 : Dans le doute d'une propagation de l'attaque au système hôte ou à d'autres systèmes d'information, utiliser la fiche : Fiche réflexe - Compromission système - Qualification

11 Préserver les traces

Mesure 9 - Préserver les traces

Préserver les journaux avant leur rotation pour pouvoir investiguer et éradiquer l'accès initial et les emprises laissées par l'attaquant :

- [ ] **Action 9.a : Préserver les traces de l'incident**
  - [ ] Journaux de l'interface de gestion
  - [ ] Journaux du site web
    - [ ] Ne pas oublier les journaux des plugins et bibliothèques tierces
  - [ ] Journaux du serveur hôte
  - [ ] Si le serveur hôte est virtualisé :

    - [ ] Réaliser un *snapshot* du serveur hôte (avec toutes les traces au plus proche de l'incident)
    - [ ] Nommer le snapshot clairement avec un nom explicite (exemple : AAAAMMJJ_SNAPSHOT_DEFACE)
- [ ] Journaux des équipements en amont (pare-feu, répartiteur de charge, reverse-proxy, WAF, etc.)
- [ ] Journaux de la console antivirus

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 9.b : Augmenter la traçabilité**
    - [ ] Augmenter la rétention des journaux
    - [ ] Augmenter la verbosité des journaux
    - [ ] Mettre en place un export des journaux en temps réel vers un puits de logs

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*.

12 Définitions

Qualifier un incident

Qualifier un incident signifie :

- *Confirmer* qu'un incident de sécurité est bien en cours et si oui, déterminer 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*.

13 Contacter le CERT-FR

13.1 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.

13.2 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

13.3 Par Internet

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

13.4 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.frImages/public_key_2024.asc`

14 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/newline%7B%7D%3Chttps://www.m-cert.fr/newline%7B%7D%3Chttps://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.

15 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.

16 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.

17 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

18 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/`).

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