Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Défiguration de site web

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

A quoi sert-elle ?

L'objectif de cette fiche est de proposer une *aide à la qualification* d'une défiguration de site web. Les différentes actions proposées aideront à :

- *Confirmer* qu'un incident de sécurité est bien en cours, et qu'il est de type *défiguration de site web*.
- Évaluer la *gravité* de l'incident en évaluant le *périmètre* affecté, l'*impact* potentiel sur 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

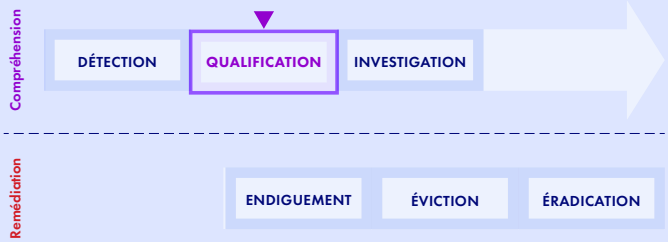
Prérequis 3

Conclusions attendues de la qualification 4

Méthode d'évaluation pas à pas 5

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.

Disposer des personnes nécessaires

S'assurer que les personnes qui effectueront la qualification de l'incident aient :

- Les *accès à l'administration* des serveurs web et des serveurs DNS.
- Les *accès aux équipements de sécurité* en amont du site web.
- Les *accès à la console d'administration* des tenants dans le cas d'un site dans le cloud.

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.

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.
La partie suivante présentera des actions détaillées pour guider pas à pas ces évaluations.

Évaluer l'incident

Mesure 1 - Confirmer l'incident de type défiguration de site web

- ☐ *L'incident de type défiguration de site web est-il confirmé, ou nécessite-il des investigations complémentaires ?*

Mesure 2 - Identifier les systèmes compromis

- ☐ *Les serveurs hôtes hébergeant le site web défiguré peuvent-ils être précisément identifiés ?*
- ☐ *Quels systèmes semblent avoir été compromis ? Les serveurs hôtes du site web eux-mêmes, ou un système tiers (fournisseur de contenu tiers, enregistrement DNS, équipement en amont) ?*
- ☐ *Les systèmes compromis sont-ils hébergés en interne, chez un prestataire externe ou au sein d'un tenant cloud ?*
- ☐ *Est-il encore nécessaire de poursuivre les investigations pour identifier et localiser les systèmes compromis ?*

Mesure 3 - Évaluer le périmètre de l'incident

- ☐ *Un compte d'administration semble-t-il avoir été usurpé ? Si oui, pourrait-il avoir d'autres accès aux interfaces de gestion ou aux accès distants de l'entreprise ? Un périmètre de compromission plus large est-il à craindre ?*
- ☐ *En plus du défacement du site web, le système de l'hôte du serveur web pourrait-il être compromis ?*
- ☐ *Une propagation de l'attaque à d'autres serveurs est-elle à possible ?*
- ☐ *Le cas échéant, le tenant cloud est-il en risque ?*
- ☐ *Existe-t-il un risque que l'incident se généralise ?*

Mesure 4 - Évaluer l'impact de l'incident

- ☐ *Quelles activités sont impactées par la défiguration ? Sont-elles vitales ?*
- ☐ *Quelles activités seraient impactées par la mise hors-ligne du site web ou du serveur hôte ? Sont-elles vitales ?*
- ☐ *L'incident a-t-il des impacts réglementaires ?*
- ☐ *Existe-t-il un risque que l'incident s'aggrave ?*

Mesure 5 - Évaluer l'urgence à résoudre l'incident

- ☐ *Quelles sont les activités vitales actuellement perturbées, ou susceptibles de l'être suite à des mises hors-ligne, pour lesquelles des mesures préventives de continuité d'activité doivent être envisagées dès maintenant ?*

Qualifier l'incident

Conclure quant à la gravité de l'incident

- ☐ La défiguration du site web est-il causé par une compromission du site web lui-même ?
- ☐ 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

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.

Cette fiche doit permettre de qualifier l'incident malgré la diversité des causes possibles.

Mesure 1 - Confirmer l'incident de type défiguration de site web

Confirmer que l'incident est de type *défiguration de site web* en évaluant différents signaux :

Action 1.a : Évaluer les signaux forts

- ☐ Changement illégitime de la page d'accueil ou d'une page d'authentification.
- ☐ Changements illégitimes dans le contenu du site (images ou messages inappropriés, informations falsifiées, liens malveillants, etc.).
- ☐ Affichage de contenus externes inappropriés (par exemple, bannière de publicité).
- ☐ Apparition du site web sur une liste noire (*Google Safe Browsing*, *Microsoft Defender SmartScreen*, etc.).
- ☐ Revendication de l'attaque au nom d'un activisme politique ou religieux.
  - ☐ Depuis quand ces premiers signaux forts sont-ils apparus ?

Action 1.b : Évaluer les signaux faibles

- ☐ Notifications des utilisateurs (sur le site web ou les réseaux sociaux).
- ☐ Augmentation soudaine de commentaires négatifs sur le site web.
- ☐ Alertes antivirales, EDR ou SIEM sur le serveur hôte.
- ☐ Baisse soudaine du trafic sur le site web (potentiellement due à son apparition dans une liste noire).

Action 1.c : (Conclure) Confirmer l'incident de type défiguration de site web

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

- ☐ *L'incident de type défiguration de site web est-il confirmé, ou nécessite-il des investigations complémentaires ?*

Mesure 2 - Identifier les systèmes compromis

> **REMARQUE**
>
> Cette partie a pour objectif d'identifier les serveurs compromis : s'agit-il des *serveurs hôtes*, des *serveurs DNS*, de *serveurs en amont*, ou de *serveurs tiers* ? **Une fois les systèmes compromis identifiés, vous pouvez clôturer cette Mesure 2 et passer directement à la Mesure 3 suivante.**

Examiner si les **serveurs hôtes** ont eux-mêmes été compromis, ou au contraire semblent être restés intègres :

Action 2.a : Identifier le site web défiguré

- ☐ Quel est le nom qualifié (*FQDN*) du site web victime de la défiguration ?
- ☐ Quelle page du site web est impactée ?
  - ☐ Y a-t-il d'autres pages également impactées ?
- ☐ La défiguration est-elle visible sur d'autres sites web de l'organisation ?

Action 2.b : Identifier les serveurs hébergeant le site défiguré

- ☐ Les serveurs hôtes hébergeant le site web défiguré sont-ils hébergés :
  - ☐ chez un hébergeur externe ?
  - ☐ chez un fournisseur de service *cloud* ? Si oui :
    - ☐ quel tenant héberge les serveurs hôtes ?
  - ☐ sur le système d'information de l'organisation ? Si oui :
    - ☐ dans une DMZ dédiée du système d'information de l'organisation ?
- ☐ Combien de serveurs hébergent le site web ? Sont-ils en *cluster* ?

Action 2.c : Identifier l'élément compromis

En analysant le code source de la page compromise (touche `F12` dans le navigateur et onglets) :

- ☐ Le code source lui-même a-t-il été modifié ?
  - Si non, quel élément référencé par ce code a été altéré ?
    - ☐ Une image
    - ☐ Une vidéo
    - ☐ Du code JavaScript
    - ☐ Une section commentaires
    - ☐ Autre élément embarqué
- ☐ **L'élément compromis est-il hébergé sur le serveur lui-même ?**
  - Si non, depuis quelle source est-il chargé (onglet "Réseau" dans la fenêtre `F12`) ?
  - ☐ **Sur un serveur backend ?** (serveur de fichiers, base de données, etc.)
  - ☐ **Chez un fournisseur externe ?** (CDN, service tiers, etc.)

Si les serveurs hôtes semblent être intègres et non compromis, la défiguration serait alors causée par la compromission d'autres serveurs, qu'il convient maintenant d'identifier...

Action 2.d : Examiner l'enregistrement DNS du site web

Vérifier si les enregistrements DNS redirigent vers un site illégitime, ce qui, en cas de réponse affirmative, confirmerait la compromission des **serveurs DNS** :

- ☐ En effectuant une résolution DNS du FQDN du site web défiguré, l'enregistrement obtenu pointe-t-il vers une adresse IP légitime (appartenant à l'organisation ou au CDN légitime) ? Si non :
  - ☐ Les enregistrements DNS de l'organisation ont-ils été modifiés peu avant la défiguration, et pointent-ils vers des adresses IP illégitimes ?
  - ☐ Les serveurs DNS sont-ils internes ou externes à l'organisation ?
    - ☐ S'ils sont internes, identifier précisément ces serveurs.
    - ☐ S'ils sont hébergés dans le *cloud*, identifier leur tenant.

Action 2.e : Trouver l'équipement à l'origine de la défiguration en amont des serveurs web

Enfin, si aucun système n'a encore été identifié comme compromis, remonter la chaîne des équipements qui transportent le flux web afin de trouver celui qui cause la défiguration.

- ☐ Procéder à des tests unitaires pour afficher la page défigurée en remontant le flux web, puis identifier l'équipement responsable de la défiguration :
  - ☐ Répartiteur de charge
  - ☐ Relais inverse (*reverse-proxy*)
  - ☐ Pare-feu
  - ☐ Autre ?
- ☐ L'équipement compromis est-il hébergé en interne, chez un prestataire externe ou au sein d'un tenant cloud ?

Action 2.f : (Conclure) Identifier les systèmes compromis

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

- ☐ *Les serveurs hôtes hébergeant le site web défiguré peuvent-ils être précisément identifiés ?*
- ☐ *Quels systèmes semblent avoir été compromis ? Les serveurs hôtes du site web eux-mêmes, ou un système tiers (fournisseur de contenu tiers, enregistrement DNS, équipement en amont) ?*
- ☐ *Les systèmes compromis sont-ils hébergés en interne, chez un prestataire externe ou au sein d'un tenant cloud ?*
- ☐ *Est-il encore nécessaire de poursuivre les investigations pour identifier et localiser les systèmes compromis ?*

> **REMARQUE**
>
> Si ce sont les *serveurs hébergeant le site web* qui ont été identifiés compromis, continuer cette fiche et passer à la Mesure 3 suivante. Sinon, si un *système tiers* semble être la cause de la défiguration (enregistrement DNS, fournisseur de contenu tiers, équipement en amont), aller directement la partie Suite des actions.

Mesure 3 - Évaluer le périmètre de l'incident

Action 3.a : Investiguer une usurpation d'accès d'administratif

- ☐ Peu avant la défiguration, un compte administrateur semble-t-il s'être authentifié de manière illégitime sur une interface de gestion exposée sur Internet ou avoir réalisé une action suspecte ?
  - Interface du CMS
  - Service d'hébergement ou service cloud
  - Service de stockage (SFTP)
  - Base de données exposées
  - Gestion des commentaires
  - Autres interfaces de gestion exposées ?
- ☐ Si oui, l'analyse des journaux permet-elle de confirmer que ce compte a effectué la modification illicite à l'origine de la défiguration ?
  - ☐ Est-ce un compte interne à l'entreprise ou celui d'un prestataire ?
- ☐ **L'utilisateur de ce compte pourrait-il avoir d'autres accès aux interfaces de gestion ou aux accès distants de l'entreprise ? Un périmètre de compromission plus large est-il à craindre ?**

Action 3.b : Évaluer la compromission système des serveurs hôtes

- ☐ Détection :
  - ☐ Des alertes antivirales ou EDR sur les serveurs hôtes ont-elles détecté un comportement ou un dépôt de code malveillant ?
  - ☐ Des alertes sur les équipements de sécurité en amont du site web (WAF, sonde de détection réseau, pare-feu, relais inverse, etc.) ont-elles détecté des tentatives d'exploitation de vulnérabilité, peu avant la défiguration ?
- ☐ Investigation :
  - ☐ À partir de l'identification des versions des composants (site web, extensions fonctionnelles ou *plugins*, bibliothèques, système d'exploitation), existe-t-il des vulnérabilités connues telles des CVE qui permettraient cette défiguration ?

- ☐ Peu avant la défiguration, une authentification avec un compte d'administration a-t-elle été réalisée illégitimement sur le serveur hôte depuis Internet (par exemple, connexion SSH) ?
- ☐ Plusieurs sites web hébergés par les mêmes serveurs hôtes sont-ils défigurés également ?
- ☐ Le serveur web est-il exécuté avec un compte privilégié sur le système ?

☐ **En plus du défacement du site web, le système de l'hôte du serveur web pourrait-il être compromis ?**

> **REMARQUE**
>
> Si la compromission système du serveur hôte est suspectée, qualifier cette hypothèse à l'aide de la fiche suivante : Fiche réflexe - Compromission système - Qualification.

Action 3.c : Évaluer la potentielle propagation de la compromission

- ☐ La défiguration est-elle visible sur d'autres sites web de l'organisation ?
- ☐ Les serveurs hôtes sont-ils cloisonnés - par exemple dans une DMZ - ou peuvent-ils communiquer avec d'autres serveurs de l'organisation ?
- ☐ Le site web contient-il des mots de passe réutilisables sur d'autres systèmes du système d'information ?
- ☐ Si des vulnérabilités ou des alertes ont été détectées sur les serveurs hôtes compromis, sont-elles également présentes sur d'autres serveurs exposés de l'organisation ?
- ☐ **Une propagation de l'attaque à d'autres serveurs est-elle possible ?**

Action 3.d : Évaluer la potentielle compromission du tenant

- ☐ Parmi les systèmes suspectés compromis identifiés dans les étapes précédentes, certains sont-ils hébergés dans un tenant *cloud* ?
  - ☐ Si oui, un compte administrateur semble-t-il s'y être authentifié de manière illégitime peu avant la défiguration ?
  - ☐ D'autres comportements anormaux ou alertes laissent-elles suspecter la compromission du tenant *cloud* ?

> **REMARQUE**
>
> Si la compromission d'un *tenant Azure* est suspectée, qualifier cette hypothèse à l'aide de la fiche suivante : Fiche réflexe - Compromission d'un tenant Azure - Qualification.

Action 3.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 :

- ☐ *Un compte d'administration semble-t-il avoir été usurpé ? Si oui, pourrait-il avoir d'autres accès aux interfaces de gestion ou aux accès distants de l'entreprise ? Un périmètre de compromission plus large est-il à craindre ?*
- ☐ *En plus du défacement du site web, le système de l'hôte du serveur web pourrait-il être compromis ?*
- ☐ *Une propagation de l'attaque à d'autres serveurs est-elle à possible ?*
- ☐ *Le cas échéant, le tenant cloud est-il en risque ?*
- ☐ *Existe-t-il un risque que l'incident se généralise ?*

Mesure 4 - Évaluer l'impact de l'incident

> **REMARQUE**
>
> Pour évaluer les impacts métiers liés à l'application web défigurée, il peut être pertinent de contacter le référent de l'application (chef de projet, *application owner*, etc.).

Action 4.a : Évaluer les impacts sur l'activité

- ☐ La défiguration a-t-elle un impact sur l'activité de l'organisation en ce qui concerne :
  - ☐ une interruption de l'activité métier ?
  - ☐ une atteinte à l'image de marque ?

- ☐ une perte financière ?

☐ Une *activité vitale* pour l'organisation est-elle liée au site web ou au serveur hôte ?

- ☐ Si votre organisation possède une analyse d'impact métier (Business Impact Analysis ou *BIA*), cette activité perturbée en fait-elle partie ?

☐ Y aurait-il un fort impact sur une activité vitale :

- ☐ Si le *site web* devait être mis hors-ligne ?
- ☐ Si le *serveur hôte* hébergeant le site web devait être isolé d'Internet ou éteint ?
  - ☐ D'autres sites web ou d'autres services seraient-ils alors impactés ?

☐ En fonction du périmètre de compromission évalué, existe-t-il un risque que l'incident ne s'aggrave ?

Action 4.b : Évaluer les impacts réglementaires

☐ Les serveurs hôtes compromis sont-ils reliés à un système d'information soumis à une *réglementation particulière* (LPM, NIS2, etc.) ?
☐ Peut-on savoir si les serveurs hôtes compromis hébergent des données sensibles dans leurs fichiers ou leurs bases de données ?

- ☐ données classifiées
- ☐ données personnelles
- ☐ données à statut protégé (santé, financière, etc.)
- ☐ données soumises à engagement contractuel ou réglementaire autre

☐ Informer les responsables de ces données afin qu'ils puissent entreprendre les actions nécessaires (déclarations réglementaires, etc.).

Action 4.c : (Conclure) Évaluer l'impact de l'incident

☐ *Quelles activités sont impactées par la défiguration ? Sont-elles vitales ?*
☐ *Quelles activités seraient impactées par la mise hors-ligne du site web ou du serveur hôte ? Sont-elles vitales ?*
☐ *L'incident a-t-il des impacts réglementaires ?*
☐ *Existe-t-il un risque que l'incident s'aggrave ?*

Mesure 5 - Évaluer l'urgence à résoudre l'incident

Action 5.a : Évaluer l'urgence à résoudre l'incident

Pour chacune des activités vitales perturbées, ou susceptibles de l'être suite à des mises hors-ligne :

☐ 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 5.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 actuellement perturbées, ou susceptibles de l'être suite à des mises hors-ligne, pour lesquelles des mesures préventives de continuité d'activité doivent être envisagées dès maintenant ?*

Qualifier l'incident

Conclure quant à la gravité de l'incident

☐ La défiguration du site web est-il causé par une compromission du site web lui-même ?
☐ L'incident est-il *circonscrit* sur mon système d'information, ou est-il potentiellement plus étendu ?

- ☐ L'incident est 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

Si la défiguration du site web est causée par la compromission du site web lui-même :

- Mettre en œuvre des mesures d'endiguement à l'aide de la fiche Fiche réflexe - Défiguration de site web - Endiguement.

Dans toutes les autres situations, des exemples de mesures d'endiguement sont suggérés ci-dessous :

Si les enregistrements DNS ont été compromis :

- Si le service DNS est externalisé, réinitialiser tous les accès d'administration et reconfigurer les enregistrements DNS légitimes.
- Si le serveur DNS est interne à l'organisation, utiliser en plus la fiche suivante : Fiche réflexe - Compromission système - Qualification.

Si le contenu illégitime provient d'un fournisseur tiers identifié :

- Rendre inopérants tous les liens vers ce fournisseur dans les pages du site (supprimer, commenter ou renommer) et prévenir que le site fonctionne en mode dégradé. Entre-temps, une page de maintenance peut être affichée.
- Prendre en compte que cette mesure ne sera pas efficace tout de suite à cause de la mise en *cache* des pages web.
- Tenter de contacter le fournisseur tiers pour le prévenir de la compromission semble lui être attribuée.

Si un système en amont des serveurs web est suspecté compromis :

- Mettre en ligne une page de maintenance sur un autre serveur et y rediriger les résolutions DNS.
- Utiliser en plus la fiche suivante sur le système suspecté compromis : Fiche réflexe - Compromission système - Qualification.

Si un système suspecté compromis est hébergé sur un tenant Azure :

- Qualifier la compromission éventuelle du tenant avec la fiche suivante : Fiche réflexe - Compromission d'un tenant Azure - Qualification.

Parallèlement, piloter la suite du traitement de cet incident et demander 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*.

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 - Défiguration de site web - Endiguement
- 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