Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Compromission d'un équipement de bordure réseau

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 ?

Cette fiche peut être employée dans deux cas de figure :

- en cas de suspicion ou détection de compromission d'équipement de bordure réseau ;
- si un de vos équipements de bordure réseau est affecté par une vulnérabilité

Est désigné comme *équipement de bordure réseau* dans une organisation un équipement, physique ou virtuel, pouvant recevoir du trafic depuis internet et dont le rôle est d'acheminer du trafic entre le SI de l'organisation et internet. Ce type d'équipement inclut donc :

- les pare-feu en périmètre d'organisation,
- les passerelles VPN,
- les routeurs d'entreprises ou box internet pour de petites organisations.

A quoi sert-elle ?

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

- *Confirmer* qu'un incident de sécurité est bien en cours, et qu'il s'agit bien de la compromission d'un équipement de bordure réseau.
- Évaluer la *gravité* de l'incident en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

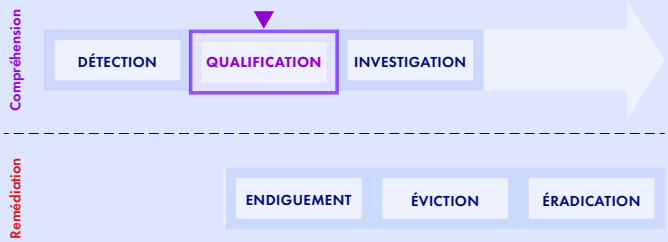
Comment l'utiliser ?

Deux parties principales composent cette fiche :

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

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

SOMMAIRE



PRÉREQUIS

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 nécessaires au système d'information :

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

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

Ouvrir une main courante

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

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

Ce document sera utile pour :

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

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

Avoir pris connaissance des actions déjà entreprises

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

CONCLUSIONS ATTENDUES DE LA QUALIFICATION

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

Évaluer l'incident

Mesure 1 - Confirmer la compromission de l'équipement réseau

- ☐ *L'incident est-il confirmé ou nécessite-t-il des investigations complémentaires ?*
- ☐ *Quel est le niveau de compromission de l'équipement ?*
- ☐ *La compromission est-elle récente ? Date-t-elle de plus de quelques heures ?*
- ☐ *Y a-t-il des traces de latéralisation de l'attaquant vers d'autres machines ?*

Mesure 2 - Évaluer le périmètre de l'incident

- ☐ *L'incident est-il circonscrit à une partie du système d'information identifiable ?*
- ☐ *Quels secrets ont été compromis ? Donnent-ils accès à d'autres parties du SI ?*
- ☐ *D'autres systèmes d'information interconnectés avec celui de l'organisation sont-ils à risque ?*

Mesure 3 - Évaluer l'impact de l'incident

- ☐ *Des activités vitales sont-elles perturbées ?*
- ☐ *Y a-t-il des chaînes d'activité impactées dont la défaillance peut causer des perturbations graves ?*
- ☐ *L'attaquant dispose-t-il de droits étendus sur le SI ?*
- ☐ *La DSI a-t-elle les compétences en interne pour réinstaller l'équipement ou installer ses correctifs ?*
- ☐ *La DSI a-t-elle les compétences en interne pour maintenir les activités vitales ?*

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

- ☐ *Les impacts sont-ils élevés ?*
- ☐ *Quelles sont les activités vitales menacées par cette compromission ? L'attaquant est-il en position de les perturber facilement ?*

Qualifier l'incident

Conclure quant à la gravité de l'incident

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

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

MÉTHODE D'ÉVALUATION PAS À PAS

Évaluer l'incident

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

Mesure 1 - Confirmer l'incident

Évaluer les détections et les dysfonctionnements sur son système d'information permet d'acquérir de la connaissance sur le type de malveillance qui le menace et, dans le cas présent, de *confirmer ou infirmer une compromission* :

Action 1.a : Identifier l'équipement suspect

- ☐ *Si le signalement provient d'une alerte interne (SIEM, EDR, Antivirus,...), disposez-vous de suffisamment d'informations dans le signalement pour identifier l'équipement ?*
- ☐ *Si le signalement provient d'une alerte externe, et identifie l'équipement de bordure réseau par une adresse IP publique ou un nom de domaine*
  - ☐ *L'adresse IP appartient-elle bien à votre SI ?*
  - ☐ *L'adresse IP publique ou le nom de domaine signalé correspond-il directement à l'équipement réseau suspect ou à un relais ?*
    - ☐ *Disposez-vous de suffisamment d'informations complémentaires dans le signalement pour identifier l'équipement ?*
    - ☐ *Y a-t-il des journaux accessibles qui vous permettent d'identifier l'équipement compromis (journaux de répartiteur de charge,...) ?*
- ☐ *En cas de vulnérabilité annoncée, êtes vous en capacité de lister rapidement les versions de vos différents équipements de bordure réseau ?*

Action 1.b : Trouver des traces de compromission

- ☐ *En cas de vulnérabilité annoncée sur la marque de l'équipement, la version logicielle de l'équipement est-elle affectée ?*
- ☐ *Si vous disposez d'un dispositif de supervision, y a-t-il d'autres alertes liées à ce signalement, à propos de la même machine ou à des horodatages proches par exemple ?*
- ☐ *Si le signalement indique des connexions réseau malveillantes vers l'équipement*
  - ☐ *Retrouvez-vous dans vos journaux réseau des traces de ces connexions ?*
  - ☐ *Retrouvez-vous dans les journaux système de l'équipement des actions malveillantes (connexions illégitimes à un compte, modifications malveillantes de configuration,...)*
- ☐ *Si le signalement mentionne l'exploitation d'une vulnérabilité spécifique*
  - ☐ *Retrouvez-vous des traces spécifiques à cette exploitation mentionnées dans les différents bulletins de sécurité à votre disposition ? Dans ceux du CERT-FR (cf la section Liens utiles) ? Dans vos abonnements sur la cyber-menace ?*
- ☐ *Trouvez-vous dans vos différents journaux des traces de connexions illégitimes initiées par l'équipement suspect à la période indiquée par le signalement ? Entre cette période et maintenant ?*
- ☐ *Si des traces de compromission sont bien présentes :*
  - ☐ *A quand remontent-elles ? Quelques heures ? Plus ?*
  - ☐ *Laissent-elles penser que l'attaquant s'est intéressé à d'autres machines du parc ?*

Action 1.c : Déterminer le niveau de compromission de l'équipement

Pour comprendre les deux niveaux de compromission possibles, vous pouvez consulter la section Niveau de compromission de l'équipement.

- ☐ *L'attaquant a-t-il un accès utilisateur ?*
  - ☐ *L'attaquant dispose-t-il de secrets d'authentification valides pour utiliser des fonctions de l'équipement ?*
  - ☐ *L'attaquant a-t-il accès à des fonctionnalités de l'équipement qui devraient être protégées par authentification ?*
- ☐ *Y a-t-il des soupçons d'un accès interne i.e. l'attaquant peut-il exécuter du code arbitraire sur l'équipement ?*

- ☐ *Les actions malveillantes observées sont-elles irréalisables via les fonctions d'administration de l'équipement accessibles à un utilisateur légitime ?*
- ☐ *Si vous retrouvez des traces d'exploitation de vulnérabilité sur votre équipement, la vulnérabilité en question était-elle de type "exécution de code à distance" (RCE) ?*
- ☐ *Y a-t-il eu récemment des bulletins d'alerte sur l'équipement à propos de vulnérabilités de type RCE ? Y a-t-il eu un bulletin d'alerte CERT-FR sur le sujet (cf la section Liens utiles) ?*

REMARQUE

En cas de doute sur cette question, considérer que le niveau de compromission le plus grave i.e. accès interne est atteint.

Action 1.d : (Conclure) Confirmer la compromission de l'équipement réseau

- ☐ *L'incident est-il confirmé ou nécessite-t-il des investigations complémentaires ?*
- ☐ *Quel est le niveau de compromission de l'équipement ?*

REMARQUE

Si la conclusion est que l'équipement n'est pas compromis mais est affecté par une vulnérabilité non corrigée, il est recommandé de continuer à répondre aux questions de cette fiche et d'appliquer les mesures correspondantes de la fiche d'endiguement (cf la section Liens utiles).

Mesure 2 - Évaluer le périmètre de l'incident

Action 2.a : Déterminer les accès réseau de l'attaquant

- ☐ *A quels LAN internes l'équipement compromis a-t-il accès ?*
- ☐ *Y a-t-il un filtrage mis en place pour limiter les flux réseau transitant par l'équipement ?*
  - ☐ *Si l'équipement a une fonction de passerelle VPN, un filtrage s'applique-t-il aux adresses IP assignées lors de connexions VPN ?*
- ☐ *Y a-t-il un filtrage mis en place pour limiter les flux réseau initiés par l'équipement ?*
- ☐ *S'il y a du filtrage en place, est-il effectué par l'équipement soupçonné compromis ?*
  - ☐ *Si oui, l'attaquant est-il en mesure de le désactiver/modifier ?*
- ☐ *L'attaquant dispose-t-il d'un accès à des SI appartenant à des tiers via son accès ?*
  - ☐ *Les tiers joignables via cet équipement réseau peuvent-ils être facilement listés ?*

Action 2.b : Déterminer les secrets hébergés par l'équipement réseau permettant un accès direct au SI

- ☐ *Cela inclut mais ne se limite pas à*
  - ☐ *Des mots de passe de comptes locaux à l'équipement, notamment ayant des droits administrateur*
  - ☐ *Des secrets LDAP ou de comptes Active Directory, notamment privilégiés (administrateur de domaine,...)*
  - ☐ *Des secrets de tunnels VPN tels que des mots de passe, certificats et clés*
  - ☐ *Des secrets d'infrastructure de gestion de clés (clés privées de certificats, d'autorité de certification,...)*
  - ☐ *Des communautés et clés SNMP*
  - ☐ *Des secrets de MFA, comme des graines TOTP*

Action 2.c : Déterminer si d'autres équipements sont à risque

- ☐ *L'organisation a-t-elle d'autres équipements de bordure réseau ?*
- ☐ *Sont-ils du même fabricant et sont-ils à jour ?*
- ☐ *Les secrets de l'équipement soupçonné compromis sont-ils partagés sur ces autres équipements ?*

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

- ☐ *L'incident est-il circonscrit à une partie du système d'information identifiable ?*
- ☐ *Les ressources compromises permettent-elles à l'attaquant d'accéder à d'autres parties du parc ?*
- ☐ *D'autres systèmes d'information interconnectés avec celui de l'organisation sont-ils à risque ?*

Mesure 3 - Évaluer l'impact de l'incident

Action 3.a : Évaluer les impacts sur le SI

- ☐ *Les secrets de l'équipement considérés comme compromis donnent-ils des accès privilégiés au SI ?*
- ☐ *Quels seraient les impacts de la réutilisation de ces secrets ?*
- ☐ *Ces secrets compromis peuvent-ils être rapidement renouvelés ?*
- ☐ *L'équipement est-il toujours maintenu par son éditeur ?*
- ☐ *Un équipement de secours est-il disponible ?*
- ☐ *La DSI a-t-elle les compétences en interne pour réinstaller l'équipement ou installer ses correctifs ?*
- ☐ *L'entité affectée a-t-elle des capacités de supervision suffisantes pour déterminer de potentielles activités supplémentaires de l'attaquant ?*
- ☐ *L'entité affectée a-t-elle des capacités d'administration et de réponses suffisantes pour entraver de potentielles activités supplémentaires de l'attaquant ?*

Action 3.b : Évaluer les impacts sur les activités métier

- ☐ *Des données sensibles transitent-elles par cet équipement ?*
- ☐ *Y a-t-il des applications ou serveurs portant des activités métier essentielles pour votre entité joignables par cet équipement ?*
  - ☐ *L'attaquant a-t-il accès à des données sensibles (partage de fichier, interface web, etc...) ?*
  - ☐ *L'attaquant a-t-il accès à des interfaces d'administration d'équipements critiques ?*
- ☐ *Vos activités essentielles peuvent-elles fonctionner en cas d'indisponibilité de l'équipement réseau ?*
  - ☐ *Fonctionneront-elles en mode dégradé ?*
  - ☐ *Ces activités sont-elles prises en compte dans un Plan de Continuité d'Activité ou un Plan de Reprise d'Activité ?*
- ☐ *L'entité a-t-elle les compétences en interne pour maintenir les activités vitales ? avec quel niveau de dégradation dans l'activité ?*

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

- ☐ *L'attaquant dispose-t-il de droits étendus sur le SI ?*
- ☐ *Des activités vitales sont-elles perturbées ?*
- ☐ *Ces perturbations peuvent-elles être compensées par un plan de continuité d'activité ?*

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

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

- ☐ *Les impacts de cette compromission sont-ils élevés ?*
- ☐ *Quelles sont les autres activités vitales menacées par cette compromission, au-delà de celles déjà identifiées comme compromises ?*
  - ☐ *L'attaquant est-il en position de les compromettre facilement (en disponibilité, intégrité ou confidentialité) ?*

Qualifier l'incident

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

- ☐ La compromission de l'équipement de bordure réseau est-elle *confirmée* ?
- ☐ 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 ? La situation peut-elle se dégrader rapidement ?
- ☐ 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 l'incident est confirmé et qu'il s'agit bien d'une compromission d'équipement réseau alors, en cohérence avec le *périmètre de compromission* évalué :

- Mettre en œuvre des **mesures d'endiguement** pour contenir l'attaque.
  - Fiche suivante conseillée : *Fiche réflexe - Compromission d'un équipement de bordure réseau - Endiguement* (cf la section Liens utiles)

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*.

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* (cf la section Liens utiles)

ANNEXES

Niveau de compromission de l'équipement

Deux niveaux de compromission de l'équipement sont possibles. Le premier niveau est un accès utilisateur i.e. l'attaquant peut accéder à des fonctionnalités de l'équipement normalement mises à disposition d'un administrateur. Cela peut avoir lieu si l'attaquant dispose d'identifiants de comptes locaux à l'équipement par exemple, ou peut contourner les mécanismes d'authentification de l'équipement. Le deuxième est un accès interne à l'équipement, où l'attaquant est capable d'exécuter du code arbitraire sur l'équipement. Un accès interne est généralement plus grave qu'un accès légitime car il donne à l'attaquant une grande liberté d'action sur l'équipement et rend difficile son expulsion.

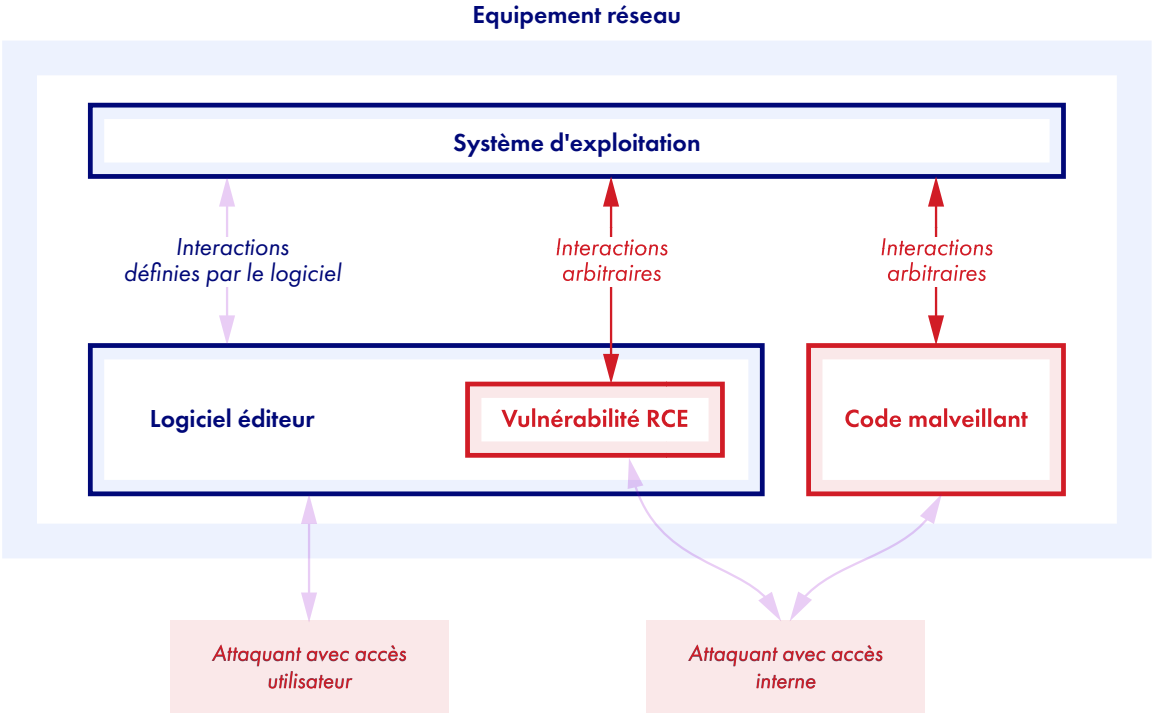


Figure 1 – Architecture d'équipement réseau

> **REMARQUE**
>
> Certains équipements réseau donnent directement un accès système privilégié aux administrateurs. Une compromission utilisateur et interne sont alors identiques et il faudra considérer le niveau de compromission comme le plus grave i.e. interne.

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 :

Document	Lien
Fiche réflexe - Compromission d'un équipement de bordure réseau - Endiguement	https ://www.intercert-france.fr/publications/fichereflexe-compromissionequipementbordurereseau-endiguement
Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique	https ://messervices.cyber.gouv.fr/guides/crise-cyber-les-cles-dune-gestion-operationnelle-et-strategique
Guides ANSSI cyberattaques et remédiation	https ://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber
Bulletins d'alerte du CERT-FR	https ://www.cert.ssi.gouv.fr/alerte/

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.
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.

Qui ?	Comment ?	Pourquoi ?
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