Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Compromission d'un compte de messagerie

Endiguement

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 compromission est suspectée ou confirmée sur un compte de messagerie.

À quoi sert-elle ?

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

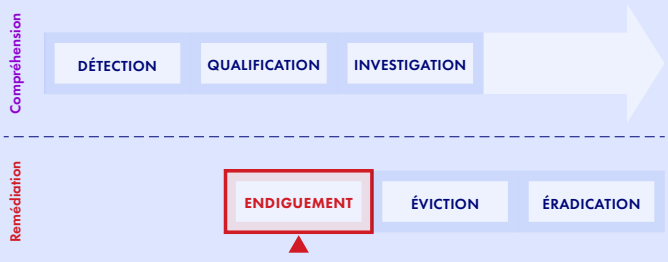
Comment l'utiliser ?

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 différents 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.

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.

Avoir qualifié l'incident

Avoir *qualifié* que l'incident en cours sur mon système d'information est bien une compromission d'un compte de messagerie et en avoir évalué la gravité :
Fiche précédente conseillée : Fiche réflexe - Compromission de compte de messagerie - 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.

Avoir les capacités d'administration

S'assurer que les personnes qui mettront en œuvre les actions d'endiguement aient les *droits d'accès* au système d'administration de la messagerie, l'accès aux comptes affectés si possible avec les personnes qui en sont victimes, et les accès aux journaux des solutions liées à la messagerie.
Vous pouvez également conduire certaines des mesures avec l'utilisateur concerné ; cependant si la personne n'est pas volontaire, il vous sera nécessaire de disposer l'accès à l'administration de la messagerie.
Si le système d'information est infogéré, s'assurer de la capacité à mobiliser l'infogérant 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*.

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.

IMPORTANT

Lorsque l'incident couvre plusieurs fuseaux horaires, il est conseillé de choisir un fuseau pour le traitement de l'incident.

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.

ACTIONS D'ENDIGUEMENT PAR PRIORITÉS

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

Actions principales	Priorité
Reprendre le contrôle du compte compromis *(Mesure 1)*	P0
Nettoyer les emprises restantes sur le compte compromis *(Mesure 2)*	P0
Protéger le poste de l'utilisateur compromis *(Mesure 3)*	P1
Protéger les autres accès à l'organisation de l'utilisateur compromis *(Mesure 4)*	P1
Préserver les traces *(Mesure 5)*	P1

Cette fiche propose également des actions complémentaires qui vont au-delà de l'endiguement, pour permettre d'approfondir les investigations :

Actions supplémentaires	Priorité
Limiter la propagation depuis la messagerie compromise *(Mesure 6)*	P2
Superviser les actions de l'attaquant *(Mesure 7)*	P2
Investiguer le système d'information *(Mesure 8)*	P3
Sécuriser la solution de messagerie *(Mesure 9)*	P4
Sensibiliser et communiquer *(Mesure 10)*	P4

ACTIONS D'ENDIGUEMENT PAR THÈMES

Une compromission d'un compte de messagerie indique certes qu'il y a eu une action malveillante sur le compte en question, mais l'incident a pu s'étendre à d'autres comptes ou systèmes. La remédiation ne doit donc pas être limitée à un simple changement de mot de passe, mais doit faire l'objet de mesures complémentaires pour limiter la progression de la compromission.
Lors d'une compromission d'un compte de messagerie, il peut être complexe de déterminer l'ampleur de l'incident qui en a résulté. Il peut être limité à de l'espionnage et de l'exfiltration de données du compte compromis, mais également servir d'accès initial pour attaquer d'autres comptes, réaliser des escroqueries comme l'arnaque au président, attaquer des systèmes, etc.
Cette partie détaille les différentes mesures d'endiguement possibles selon quatre axes thématiques. Chaque *mesure* est ensuite scindée en *actions unitaires* :

- Endiguement de la compromission de messagerie
  - Protéger la messagerie
    - Mesure 1 - Reprendre le contrôle du compte compromis
    - Mesure 2 - Nettoyer les emprises restantes sur le compte compromis
  - Protéger l'environnement de l'utilisateur compromis
    - Mesure 3 - Protéger les autres accès à l'organisation de l'utilisateur compromis
    - Mesure 4 - Protéger le poste de l'utilisateur compromis
  - Préparer l'investigation
    - Mesure 5 - Préserver les traces
- Approfondissement de l'investigation
  - Limiter l'extension de la compromission
    - Mesure 6 - Limiter la propagation depuis la messagerie compromise
    - Mesure 7 - Superviser les actions de l'attaquant
    - Mesure 8 - Approfondir les recherches sur le système d'information
  - Sécuriser l'organisation
    - Mesure 9 - Sécuriser la solution de messagerie
    - Mesure 10 - Sensibiliser et communiquer

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.

ENDIGUEMENT DE LA COMPROMISSION DE MESSAGERIE

Protéger la messagerie

Mesure 1 - Reprendre le contrôle du compte compromis

Pour tout compte de messagerie compromis, les informations d'authentification doivent être réinitialisées et les emprises nettoyées, afin de supprimer les accès illégitimes de l'attaquant :

Action 1.a : Bloquer le compte de messagerie

- ☐ Bloquer le compte, si possible, en attendant une levée de doute avec l'utilisateur victime
- ☐ Ne débloquer le compte qu'au moment de sa réinitialisation

> IMPACT
>
> **Selon les solutions de messagerie, cette action peut empêcher de recevoir des courriels et avoir des impacts sur l'utilisation d'autres services accédés par le compte.**

Action 1.b : Réinitialiser le compte de messagerie compromis

- ☐ Révoquer les *sessions actives/tokens* du compte
- ☐ Forcer la réinitialisation du *mot de passe* du compte via un système sûr avec un mot de passe solide
- ☐ Si le compte utilise un *MFA*, forcer son réenregistrement
  - ☐ Si non encore utilisé, activer le *MFA* en mode *Enforce* (et non en mode *Audit*)

Action 1.c : Nettoyer les persistances et accès illégitimes sur le compte compromis

- ☐ Supprimer les *MFA* illégitimement ajoutés au compte
- ☐ Supprimer les accès des appareils pouvant accéder à la messagerie sans MFA

> IMPORTANT
>
> **En cas d'envoi de messages frauduleux à d'autres utilisateurs, il faudra au plus vite faire une communication pour prévenir et empêcher une diffusion de l'attaque.**

Mesure 2 - Nettoyer les emprises restantes sur le compte compromis

Action 2.a : Nettoyer les règles de gestion sur le compte compromis

- ☐ Supprimer ou modifier les *délégations* illégitimes sur la boîte aux lettres du compte
- ☐ Désactiver les règles de *transfert automatique* illégitimes à un compte tiers
- ☐ Désactiver d'autres règles de gestion qui sembleraient illégitimes (par exemple, des permissions, modification des listes de diffusion, copies cachées, etc.)

Action 2.b : Nettoyer les accès d'applications tierces au compte compromis

- ☐ Détecter un accès frauduleux via une extension logicielle (plugin) ou une application tierce

Action 2.c : Nettoyer les actions d'administration illégitimes

Si le compte avait des droits d'administration, investiguer les journaux et nettoyer ses actions illégitimes :

- ☐ Supprimer ou suspendre les comptes utilisateurs illégitimement créés
- ☐ Supprimer ou suspendre les privilèges suspects ajoutés à d'autres comptes utilisateurs, puis effectuer une levée de doute sur ces comptes

REMARQUE

Attention également aux listes de diffusion qui peuvent être un vecteur de diffusion de contenu malveillant.

Protéger l'environnement de l'utilisateur compromis

Mesure 3 - Protéger le poste de l'utilisateur compromis

Action 3 : Protéger le poste utilisateur

- ☐ Surveillez de potentielles notifications antivirales sur le poste
- ☐ Si des éléments vous amènent à soupçonner une compromission du poste (hameçonnage, vol d'identifiants, etc.), vous pouvez basculer sur la procédure adéquate
- ☐ Dans le doute, faire une analyse antivirale complète du poste ou le réinstaller

Mesure 4 - Protéger les autres accès à l'organisation de l'utilisateur compromis et les autres utilisateurs

Action 4.a : Réinitialiser les accès de l'utilisateur aux autres applications de l'organisation

- ☐ Forcer la réinitialisation des *mots de passe* de tous les comptes de l'organisation associés à la victime, en priorité des applications accessibles depuis Internet
- ☐ Révoquer les *sessions actives/tokens* de tous les comptes de l'organisation associés à la victime, en priorité des applications accessibles depuis Internet
  - ☐ Ne pas oublier le VPN, les autres accès à distance et services cloud

IMPORTANT

- ► **Un phishing ou autre vol de données n'a pu extraire qu'un seul couple login/mot de passe, mais qui peuvent potentiellement être réutilisables sur d'autres applications.**
- ► **Un info stealer a pu extraire du navigateur de l'utilisateur compromis non seulement plusieurs couples login/mot de passe, mais également des tokens de sessions actives.**
- ► **Si le compte appartient à un administrateur / personnel de DSI, soyez attentifs à la récupération de secrets d'authentification qui permettent de se connecter sur le SI avec des droits privilégiés.**

Action 4.b : Protéger les autres utilisateurs affectés

- ☐ Procéder à une communication auprès des utilisateurs ayant été susceptibles d'être contactés par le compte compromis

Préparer l'investigation

Mesure 5 - Préserver les traces

Action 5.a : Augmenter la verbosité et la rétention des journaux

- ☐ Il convient d'augmenter autant que possible la verbosité et la rétention des données sur les comptes compromis (logs SMTP, utilisateurs, proxy, solutions de sécurité)
- ☐ Il est également possible de demander l'augmentation des journaux disponibles au fournisseur de la solution de messagerie, selon son contrat

Action 5.b : Préserver les journaux du compte compromis

- ☐ Exporter les journaux, si possible centrés sur le compte compromis, pour ne pas supprimer des traces utiles à l'investigation
- ☐ Mettre de côté la dernière sauvegarde et mettre en rétention le compte si nécessaire

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. Parmi ces éléments de preuve, veillez à bien exporter et conserver les mails originaux (mail avec en-têtes) qui ont été détectés comme suspects ou envoyés par l'attaquant.

APPROFONDISSEMENT DE L'INVESTIGATION

> **REMARQUE**
>
> Ces mesures vont au-delà d'un endiguement classique et doivent être considérées comme des actions propres à un début d'investigation plus poussée.

Limiter l'extension de la compromission

Mesure 6 - Limiter la propagation depuis la messagerie compromise

Action 6.a : Vérifier les courriels du compte compromis

- ☐ Détection de courriels frauduleux envoyés vers l'externe ou interne (voire sur la même boite)
- ☐ Détection de courriels frauduleux supprimés dans la corbeille ou dans les brouillons
- ☐ Détection de création de templates ou signatures frauduleux
- ☐ Détection de courriels placés dans le dossier SPAM ou dans la quarantaine
- ☐ Détection de courriels indiquant des réinitialisations de mot de passe ou d'appareils de confiance
- ☐ Détection de courriels contenant des identifiants (mots de passe, clés SSH, QR Code, clés d'API, tokens, etc.), qui seront tous à considérer compromis car potentiellement accédés par l'attaquant
- ☐ Détection de règles de suppression et lecture automatique de messages reçus (utilisée pour cacher les retours de mail de personnes contactées durant l'usurpation)

> **REMARQUE**
>
> Par mail frauduleux, on entend tout message illégitime, comme par exemple une fraude au fournisseur, au président, au salaire, demande de changement de RIB, envoi de liens malveillants, etc.

Action 6.b : Vérifier les fichiers sensibles accessibles par le compte compromis

- ☐ Détecter des fichiers sensibles dans la boîte de messagerie du compte compromis
- ☐ Détecter des fichiers sensibles auxquels peut accéder le compte via des partages de fichiers liés à la messagerie (par exemple pour *Microsoft 365* : *SharePoint, Teams*, etc.)
  - ☐ Vérifier dans les journaux si l'attaquant a effectivement accédé à ces fichiers

> **IMPORTANT**
>
> **Dans le cadre d'une interconnexion entre la messagerie et des partages de fichiers (par exemple, configuration O365, OneDrive, Sharepoint, etc.), une vigilance particulière devra être portée à l'exfiltration de données par ce biais.**

Mesure 7 - Superviser les actions de l'attaquant

Action 7.a : Mettre en détection les adresses IP identifiées

- ☐ Identifier les adresses IP sources avec lesquelles le compte a été illégitimement accédé
- ☐ Mettre en détection ces adresses IP sources, pour pouvoir voir quels autres comptes l'attaquant a obtenu, et avec lesquels il tente de se connecter
  - ☐ Il sera plus efficace de mettre ces adresses IP en détection plutôt que de les bloquer, car cela donnera plus d'informations sur l'étendue de la compromission

☐ Si cela n'est pas possible, ou si vous souhaitez limiter le périmètre de la compromission, vous pouvez bloquer l'adresse IP

REMARQUE

Certains attaquants sont en capacité de changer fréquemment d'adresse IP. Si l'attaquant dispose d'une persistance sur la messagerie, le blocage de l'adresse IP n'aurait donc pas d'impact. Si les connexions se font depuis une adresse interne, vous pouvez également investiguer la possibilité d'un *acteur malveillant interne*.

Action 7.b : Investiguer l'accès initial

☐ *Hameçonnage* : Investiguer des *courriels suspects* pouvant donner lieu à une compromission (URL de phishing, ...)
☐ *Infostealer* : Investiguer les *pièces jointes suspectes* pouvant donner lieu à une compromission (logiciel malveillant, ...)

Action 7.c : Bloquer toute tentative d'accès initial

Si l'accès initial de la compromission a pu être identifié précédemment :

☐ Mettre en quarantaine ou bloquer les messages entrants de l'expéditeur ou de tout le domaine source de messagerie malveillant
☐ Bloquer les mails entrants contenant des indicateurs identifiés (IP, URL, pièces jointes, etc.)
☐ Bloquer les requêtes web vers l'URL identifiée comme malveillante
☐ Bloquer des types de fichiers identifiés (exécutable, archive avec un mot de passe, etc.)
☐ Bloquer tous les partages mis en place par l'attaquant (sharelink, OneDrive etc.)
☐ Activer ou paramétrer correctement le SPF/DKIM/DMARC si nécessaire

De plus, si l'origine de la compromission est un tiers de confiance :

☐ Contacter le tiers de confiance pour l'alerter de la probable compromission du compte expéditeur

IMPACT

Bloquer un domaine source, surtout s'il est de confiance, peut avoir des effets importants sur l'activité et la relation avec le tiers. Il est nécessaire d'anticiper les conséquences de cette action et de prévenir le service d'assistance HelpDesk. Cet impact peut être relativisé si votre solution de messagerie propose des blocages temporaires des indicateurs (par exemple, blocage de l'expéditeur pendant 7 jours).

Sur l'application de messagerie (si cela est possible), à la place de bloquer l'adresse IP, il est possible de la placer en détection/supervision afin de pouvoir voir quels autres comptes l'attaquant a obtenu et avec lesquels il tente de se connecter.

Mesure 8 - Approfondir les recherches sur le système d'information

Action 8.a : Détecter les événements inhabituels liés à la messagerie

☐ Détecter des connexions provenant de localisations, de systèmes inhabituels sur le compte compromis et/ou d'autres comptes ou systèmes
☐ Détecter des connexions provenant d'équipements de connexion inhabituels sur le compte compromis et/ou d'autres comptes ou systèmes
☐ Détecter des connexions d'adresses IP inhabituelles sur le compte compromis et/ou d'autres comptes ou systèmes
☐ Détecter des connexions à des horaires inhabituels sur le compte compromis et/ou d'autres comptes ou systèmes
☐ Détecter des alertes d'échecs de connexion suivies d'une connexion réussie suspecte sur le compte compromis et/ou d'autres comptes ou systèmes
☐ Détecter des erreurs *MFA* sur le compte compromis et/ou d'autres comptes ou systèmes
☐ Détecter des notifications de voyage impossible
☐ Détecter des comportements inhabituels sur la partie DMARC

Action 8.b : Détecter les événements inhabituels en dehors de la messagerie

☐ Détecter des connexions vers des IP/domaines rares, ou tout autre flux inhabituel
☐ Détecter des actions anormales sur le système d'information réalisées avec le compte de l'utilisateur victime

Action 8.c : Détecter des anomalies sur le poste utilisateur

- ☐ Si le login/mot de passe a été extrait par du *phishing*, inutile de suspecter une compromission du poste utilisateur
- ☐ Si aucun élément ne permet de connaître la méthode de récupération du login/mot de passe, investiguer la présence d'un *info stealer* sur le poste utilisateur en commençant par les alertes antivirales ou de l'EDR
- ☐ Si une alerte a détecté un *infostealer*, superviser si d'autres postes ont eu la même alerte
- ☐ Il est également possible d'investiguer un leak du login/mot de passe dans le cadre d'un vol de données

En fonction des détections opérées pendant cette phase, il conviendra de récupérer les indicateurs afin d'orienter les recherches sur d'autres comptes/postes potentiellement compromis et de déterminer le périmètre réel de la compromission.
Si, lors de cette phase, une compromission étendue sur le système est détectée ou suspectée, il est possible de se référer à la fiche dédiée : Fiche Réflexe - Compromission système - Qualification.

Sécuriser l'organisation

Mesure 9 - Sécuriser la solution de messagerie

> REMARQUE
> Cette partie comprend des mesures structurelles à appliquer au sein de votre organisation pour la sécuriser sur le long terme.

Action 9.a : Sécuriser les mots de passe

- ☐ Configurer une politique de mots de passe *forts*, et surtout *longs*
- ☐ Configurer des mesures permettant d'empêcher les attaques par *force brute* sur l'authentification

Action 9.b : Réinitialiser les autres comptes

- ☐ Forcer le renouvellement de *mot de passe* et du *MFA*. Si plusieurs comptes ont été compromis dans la même période, le faire pour tous les utilisateurs.

Action 9.c : Généraliser l'usage du MFA

- ☐ Imposer l'usage du *MFA* pour les comptes administrateurs, sans exception
- ☐ Tendre à imposer l'usage du *MFA* pour tous les comptes sensibles
- ☐ Généraliser le *MFA* à tous les utilisateurs, seule mesure générale vraiment efficace contre l'usurpation initiale de compte
- ☐ Encourager la différenciation des usages professionnels et personnels pour le stockage des secrets

Action 9.d : Sécuriser la solution de messagerie

- ☐ Vérifier si la solution de messagerie est à jour, et si besoin la *mettre à jour*
- ☐ Vérifier si la solution de messagerie est affectée par une vulnérabilité, et suivre les recommandations de l'éditeur et la sortie d'un *patch de sécurité*
- ☐ Activer les mesures de sécurité de base (*SPF/DKIM/DMARC...*)

Mesure 10 - Sensibiliser et communiquer

Action 10.a : Sensibiliser l'utilisateur

- ☐ Sensibiliser l'utilisateur à ne pas utiliser le même mot de passe sur les différentes applications de l'organisation et à différencier ses mots de passe des environnements professionnels et personnels
- ☐ Sensibiliser l'utilisateur sur les responsabilités et les risques d'une usurpation d'identité via une boîte de messagerie ou par un code malveillant

Action 10.b : Communiquer sur l'incident

- ☐ Si vous vous apercevez que votre organisation a été susceptible de transmettre des courriels frauduleux à des tiers, il conviendra de les prévenir. Aussi, il serait judicieux de vérifier que l'organisation ne fait pas l'objet d'un blocage auprès de ces tiers (par exemple, en vérifiant les logs des mails sortants vers ces tiers).
- ☐ Si la source du message suspect est un tiers ou un partenaire de confiance, il peut être raisonnable d'en informer l'entreprise concernée.
- ☐ Si une adresse mail identifiée comme du spam a été détectée lors de l'investigation, il est possible de la signaler auprès de Signal Spam
- ☐ Enfin, en cas de campagne étendue de *hameçonnage* ou de *spam* à destination de votre organisation, il est conseillé de réaliser une communication auprès des utilisateurs afin de les sensibiliser, de leur rappeler les bonnes pratiques, et éventuellement de relater de manière transparente l'incident.

SUITE DES ACTIONS

A la fin de ces actions d'endiguement, la compromission devrait être contenue. Cela étant, seule une analyse approfondie permettra d'appréhender les indicateurs décelés durant cette première phase de remédiation.
Pour rappel, la compromission d'un compte de messagerie n'est que très rarement l'objectif final d'une attaque (hors cas d'espionnage), et constitue plutôt une porte d'entrée et un moyen de perpétrer une attaque plus large (vol d'accès au VPN ou aux applications, arnaque au président, usurpation d'identité pour envoyer des requêtes illégitimes aux vraies cibles, réinitialisation de mot de passe d'application, etc.).
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*.

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 - Compromission de compte de messagerie - Qualification
- 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