Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Compromission d'un Tiers

Qualification

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 entité tierce en relation avec votre organisation est victime d'une compromission.

A quoi sert-elle ?

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

- *Confirmer* qu'un incident de sécurité est bien en cours, et qu'il est de type compromission d'un Tiers.
- Évaluer la *gravité* de l'incident en identifiant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

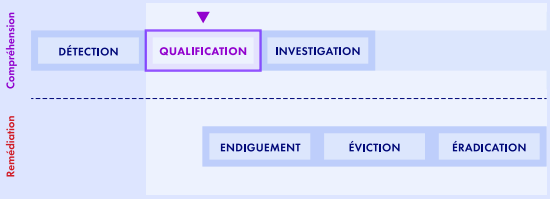
Comment l'utiliser ?

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) 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

Avoir à disposition les ressources nécessaires

Il est préférable pour mener efficacement la qualification de s'entourer des personnes disposant des connaissances et accès nécessaires au système d'information, et notamment :

- Les *accès à l'administration et à la surveillance* du système d'information
- Les *accès aux équipements de sécurité* du système d'information
- Une bonne connaissance des *processus et priorités métier* de l'organisation
- L'annuaire de contacts d'urgence
- Une connaissance de l'écosystème de l'entreprise ou accès à un référentiel de Tiers (cf. Définition d'un Tiers plus haut)

Ces personnes peuvent être internes ou externes à votre organisation, surtout concernant le périmètre du Tiers. 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 évènements survenus sur le système d'information dans un *ordre chronologique*.
Chaque ligne de ce document doit représenter une action avec au minimum les trois informations suivantes :

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 :

- Garder 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 effets de bord non anticipés

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 partie résume les conclusions auxquelles doivent mener les évaluations, qui aboutiront à la qualification de l'incident.
La partie suivante détaillera justement des actions détaillées qui aideront à conduire pas à pas ces évaluations.

Différents types possibles de Tiers

Le concept de Tiers peut couvrir des réalités différentes. Ci-dessous une liste non exhaustive des différents types de Tiers auxquels ce document peut faire référence :

1. Fournisseur (notamment IT)
2. Client
3. Prestataire (notamment Freelance)
4. Partenaire (par exemple dans le cadre d'une coentreprise ou "joint venture")
5. Filiale (notamment dans les cas d'achat ou de vente récent(e), et surtout si les systèmes d'informations sont gérés séparément)

Tous ces cas de figure ne seront pas forcément pertinents dans votre contexte. Mais identifier le type de tiers sera important par la suite car il pourra le cas échéant avoir un impact différent en termes de risques. Dans la suite de cette fiche, nous décrirons ces différents cas par le terme générique **"TIERS" par** opposition au terme **"ENTREPRISE"** qui définit votre propre périmètre.
Dans le cas particulier où le Tiers est un fournisseur de services IT (tel qu'un prestataire SaaS ou PaaS), sa compromission peut représenter une porte d'entrée supplémentaire pour un attaquant lui permettant de se latéraliser sur votre système d'information. Elle constitue alors une première étape – intentionnelle ou opportuniste – vers une intrusion dans le système d'information de votre entreprise. Ce scénario correspond à ce que l'on appelle une attaque sur la chaîne d'approvisionnement, ou *supply chain*. Dans cette fiche, nous ne traiterons pas des motivations de l'attaquant, mais nous concentrerons sur la qualification de l'évènement, en vue d'une réaction rapide.

Évaluer l'incident

Mesure 1 - Confirmer l'incident de type compromission d'un Tiers

- ☐ *L'incident de type compromission d'un Tiers est-il confirmé ?*
- ☐ *Sinon, la compromission en question semble-t-elle réaliste ? Nécessite-t-elle des investigations complémentaires ?*

Mesure 2 - Évaluer le périmètre de l'incident et ouvrir un canal de communication avec le Tiers

- ☐ Si La compromission du Tiers est confirmée, définir la nature de compromission impliquant le Tiers et ses caractéristiques :
  - ☐ Quel est le type d'attaque que le Tiers a subi (rançongiciel, compromission de messagerie, intrusion dans son système d'information...) ?
  - ☐ *L'incident est-il circonscrit à une partie identifiable de son système d'information ?*
  - ☐ *Les ressources d'administration ont-elles été compromises (comptes, postes, serveurs) ? Un compte à haut niveau de privilège semble-t-il avoir été compromis ?*
  - ☐ *Existe-t-il un risque pour d'autres systèmes d'information, éventuellement interconnectés avec celui de mon organisation ?*
- ☐ Identifier le type de Tiers
  - ☐ Définir le périmètre d'interaction entre le Tiers et le système d'information de mon entreprise.
- ☐ Établir la communication avec le Tiers.

Mesure 3 - Évaluer en parallèle l'impact de l'incident et l'urgence à intervenir

- ☐ La compromission du Tiers a-t-elle impacté mon système d'information ?
  - ☐ Sinon, mon système d'information est-il en risque et dois-je prendre des mesures d'endiguement ?
- ☐ La compromission du Tiers a-t-elle impacté mon activité métier ? Si oui :
  - ☐ Quelles sont les activités critiques liées au Tiers et qui sont à l'arrêt, pour lesquelles un rétablissement d'urgence doit être opéré ?

- ☐ Quelles sont les activités critiques liées au Tiers et maintenues en mode dégradé, pour lesquelles il faut préparer dès maintenant un rétablissement ?
- ☐ En l'absence d'impact immédiats importants, quels seraient les risques métiers à anticiper à moyen ou long terme ?

☐ Prendre en compte deux facteurs pour estimer l'urgence :

- ☐ Le type d'incident subi par le Tiers.
- ☐ Le niveau d'interaction entre votre entreprise et le Tiers.

Objectif : Conclure sur le cas de figure dans lequel l'entreprise se trouve

à l'issue de l'évaluation précédente (ou de l'analyse pas à pas décrite ci-après), l'entreprise doit se trouver dans l'un des 4 cas de figure suivants :

- ☐ Cas I - Aucune compromission n'est confirmée : ni celle du Tiers, ni celle de l'entreprise ne sont avérées.
- ☐ Cas II - La compromission du Tiers est confirmée, mais aucun impact identifié au sein de l'entreprise.
- ☐ Cas III - Détection d'un comportement anormal de la part du Tiers : La compromission du Tiers n'est pas forcément confirmée (il peut s'agir d'un incident de production non lié à un incident de sécurité dans le système d'information du Tiers) mais un incident de sécurité est suspecté au sein de l'entreprise.
- ☐ Cas IV - Détection d'un comportement malveillant provenant du Tiers : La compromission du Tiers est confirmée ou fortement suspectée et un incident a également été détecté au sein de votre entreprise.

MÉTHODE D'ÉVALUATION PAS À PAS

Cette section détaillera les actions à mener pour aboutir de manière structurée et progressive à la qualification de l'incident.

Évaluer l'incident de manière détaillée

Mesure 1 - Confirmer l'incident de type compromission d'un Tiers

Action 1.a : Identifier la source du signalement

- ☐ Le Tiers lui-même.
- ☐ Un partenaire externe.
- ☐ Une source interne.
- ☐ Une source publique (CTI, Presse, Infos partenaire/humaines).

Action 1.b : Identifier le type du signalement

- ☐ Article de presse, billet de blog public.
- ☐ Simple signalement (mail, appel téléphonique, via SMS ou messagerie...).
- ☐ Rapport technique (fourni par le Tiers, par un régulateur...).
- ☐ Publication par l'attaquant.
- ☐ Détection d'un incident interne (Détection par un équipement de sécurité de l'entreprise (antispam, SIEM, solution de CTI...)).
  - ☐ Détection par l'entreprise d'un comportement malveillant de la part du Tiers ou lié au Tiers (usurpation/personification...).

Action 1.c : Évaluer la fiabilité du signalement

- ☐ La compromission en question semble-t-elle crédible au regard du contexte, de la source et de son niveau de confiance, du type de l'information ?
  - ☐ Source fiable, information fiable.
  - ☐ Source fiable, mais information non confirmée.
  - ☐ Source non fiable, information peu fiable.

Action 1.d : (Conclure) Confirmer l'incident de type compromission d'un Tiers

- ☐ *L'incident de type compromission d'un Tiers est-il confirmé ?*
- ☐ *Sinon, la compromission en question semble-t-elle réaliste ? Nécessite-t-elle des investigations complémentaires ?*

Mesure 2 - Évaluer le périmètre de l'incident et ouvrir la communication avec le Tiers

Action 2.a : Définir le périmètre de la compromission du Tiers

Définir le périmètre de la compromission du Tiers afin de préparer l'évaluation des interactions IT entre les deux parties. La priorité est d'identifier les actifs à risque et le niveau de risque pour l'entreprise si la compromission se propage.

- ☐ Quel est le type de compromission du Tiers ?
  - ☐ Défiguration Web
  - ☐ Déni de Service (DDoS, Sabotage...)
  - ☐ Rançongiciel
  - ☐ Compromission d'un compte de messagerie professionel ou BEC (*Business Email Compromise*)
  - ☐ Compromission d'un système (ex : serveur interne, applicatif...)
  - ☐ Compromission d'un équipement de bordure réseau

- ☐ Fuite de données
- ☐ Autre... (préciser) :

☐ L'attaque touche-t-elle tout ou juste une partie du système d'information du Tiers ?

Action 2.b : Définir le périmètre d'interaction entre le Tiers et le système d'information de mon entreprise.

☐ Définir quel est le type de Tiers dont il est question :

- ☐ Fournisseur
- ☐ Client
- ☐ Prestataire
- ☐ Partenaire
- ☐ Filiale
- ☐ Autre

☐ Définir le type de liens entre l'entreprise et le Tiers :

- ☐ Moyens de communication
  - ☐ Messagerie (Outlook, Gmail...)
  - ☐ Plateformes collaboratives (Teams, Slack ...)
  - ☐ Appels téléphoniques
- ☐ Ressources d'infrastructure ou d'administration
  - ☐ Comptes utilisateur
    - ☐ avec droits d'administration ou non
  - ☐ Accès (application, VPN, données internes de l'entreprise)
  - ☐ Postes de travail
  - ☐ Serveurs
  - ☐ Tenant / Ressource cloud
- ☐ Établir les interactions entre ces éléments (accès utilisateur, connexions...)
- ☐ Lister les personnels ayant l'habitude ou pouvant interagir avec la ou les éventuelles boîtes mail compromises.
- ☐ Lister les accès aux applications utilisées par les comptes du Tiers :
  - ☐ Cloud partagé
  - ☐ Applications tierces ou de l'entreprise
  - ☐ Accès VPN
- ☐ Dresser le contexte réglementaire (RGPD, autre protection des données, etc.) et contractuel (SLA, NDA, pénalités, clauses d'indicent déjà prévues...)

☐ Estimer si le périmètre compromis inclut :

- ☐ des données de mon entreprise.
- ☐ des données (personnelles, sensibles, financières, classifiées ...) et/ou soumises à des cadres réglementaires particuliers.

Action 2.c : Etablir la communication avec le Tiers (le canal dépendra de la nature de la relation avec le Tiers).

☐ Permettre la prise de contact en identifiant les bons interlocuteurs (techniques ou métier) chez le Tiers :

- ☐ Vérifier les contacts existants au sein de l'entreprise.
- ☐ Consulter le référentiel des personnes en interne ayant un lien ou étant déjà en contact avec le Tiers (technique ou non).
- ☐ Vérifier auprès d'une personne dans l'entreprise qui communique régulièrement avec le Tiers si des informations ne sont pas déjà disponibles.
- ☐ Estimer la sensibilité de l'incident - valider que les contacts identifiés peuvent être informés de l'incident.
- ☐ Possiblement, identifier si le Tiers possède une équipe de réponse à Incident de référence (CERT, CSIRT...) ou un autre prestataire l'accompagnant sur l'incident ("Incident Retainer", éditeur de sécurité...) et entrer en contact avec lui.
- ☐ Respecter les clauses contractuelles (création d'un ticket, communication formelle...)
- ☐ Si nécessaire, utiliser un canal indépendant :
  - ☐ Appel
  - ☐ Messagerie personnelle
  - ☐ Rencontre présentielle

- ☐ Contacter le Tiers :
  - ☐ L'informer des activités remarquées ou suspectées.
  - ☐ Organiser si possible une réunion pour permettre un échange et de pouvoir poser des questions.
  - ☐ Proposer de l'aide si le Tiers n'a pas les moyens de gérer (dépend ici aussi de la nature de la relation avec le Tiers.)
    - ☐ Mise en contacts vers des spécialistes
    - ☐ Proposer l'intervention de l'équipe CERT de l'entreprise (si la relation entre l'entreprise et le Tiers est très importante - Cela est notamment possible dans une relation groupe-filiale où le CERT ne couvre pas forcément tous les périmètres)

Action 2.d : (Conclure) Évaluer le périmètre de l'incident et ouvrir la communication avec le Tiers

- ☐ Si la compromission du Tiers est confirmée, définir la nature de compromission impliquant le Tiers et ses caractéristiques :
  - ☐ Quel est le type d'attaque que le Tiers a subi (rançongiciel, compromission de courriel, intrusion dans son système d'information...) ?
  - ☐ *L'incident est-il circonscrit à une partie du système d'information identifiable chez le Tiers ?*
  - ☐ *Les ressources d'administration ont-elles été compromises (comptes, postes, serveurs) ? Un compte à haut niveau de privilège semble-t-il avoir été compromis ?*
  - ☐ *D'autres systèmes d'information interconnectés avec celui de l'organisation sont-ils en risque ?*
- ☐ Définir le périmètre d'interaction entre le Tiers et le système d'information de mon entreprise.
- ☐ Établir la communication avec le Tiers.

Mesure 3 - Évaluer l'impact de l'incident et l'urgence à résoudre l'incident

Action 3.a : Investigation ciblée pour vérifier si la compromission de l'entreprise est confirmée (ou non) ?

- ☐ Vérifier s'il existe une détection corrélée en interne de l'entreprise.
  - ☐ Si oui, quelle partie de l'entreprise semble avoir été affectée ?
- ☐ Récupérer dès que possible une liste des identifiants techniques ou marqueurs liés à la compromission du Tiers (adresse mail, adresse IP, comptes spécifiques, Connexions VPN...)
- ☐ En fonction de l'incident, chercher des signes de compromission similaires
  - ☐ Connexions compte de messageries inhabituels (heures, localisation)
  - ☐ Actions d'administration
    - ☐ Ajout d'utilisateurs
    - ☐ Modification de politiques de sécurité
    - ☐ Ajout de règles de redirection
  - ☐ Interactions avec des plateformes/espaces de partage (ex : Sharepoint, Cloud partagé, FTP, ...)
    - ☐ Téléchargement massif
      - ☐ Suppression massive ou supecte
      - ☐ Consultation par des comptes suspectés d'être compromis
    - ☐ Consulations des outils/équipes de surveillance de l'entreprise.
  - ☐ Recherche des IoC :
    - ☐ Mettre ces éléments en détection dans les équipements idoines (SIEM, ...)
    - ☐ Rechercher ces IoC de manière proactive sur les équipements de sécurité (EDR, Proxies...)

Action 3.b : (Conclure) Évaluer en parallèle l'impact de l'incident et l'urgence à intervenir

- ☐ La compromission du Tiers a-t-elle impacté mon système d'information ?
  - ☐ Sinon, mon système d'information est-il en risque et dois-je prendre des mesures d'endiguement ?
- ☐ L'incident a-t-il impacté mon activité métier ? Si oui :
  - ☐ Quelles sont les activités critiques liées au Tiers et qui sont à l'arrêt, pour lesquelles un rétablissement d'urgence doit être opéré ?
  - ☐ Quelles sont les activités critiques liées au Tiers et maintenues en mode dégradé, pour lesquelles il faut préparer dès maintenant un rétablissement ?
  - ☐ Sinon, quels seraient les impacts métiers à craindre à long terme ?
- ☐ Considérer deux facteurs pour estimer l'urgence :
  - ☐ Le type d'incident chez le Tiers.
  - ☐ Le niveau d'interaction entre votre entreprise et le Tiers.

Qualifier l'incident

Résumer les résultats de l'évaluation

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. Voici les questions à se poser :

- ☐ L'incident de type compromission d'un Tiers est-il *confirmé* ?
- ☐ L'incident est-il *circonscrit* [sur mon système d'information et sur celui du Tiers], ou est-il étendu et quelle est sa nature ?
- ☐ L'incident présente-t-il un *impact fort* pour mon *activité métier* et le fonctionnement de mon *système d'information* ?
- ☐ L'incident nécessite-t-il une intervention *urgente*, ou les activités critiques ont-elles réussi à être maintenues ?

Conclure quant à la gravité de l'incident

- ☐ Au final, quelle *gravité* représente cet incident de sécurité ?
  - ☐ Anomalie courante : incident sans impact significatif
  - ☐ Incident mineur : impact limité, sans menace ultérieure immédiate
  - ☐ Incident majeur : impact fort sur le système d'information ou l'activité métier
  - ☐ Crise cyber :

Conclure quant au cas de figure de l'incident

- ☐ Cas I - Aucune compromission n'est confirmée : ni celle du Tiers, ni celle de l'entreprise ne sont avérées.
- ☐ Cas II - La compromission du Tiers est confirmée, mais aucun impact identifié au sein de l'entreprise.
- ☐ Cas III - Détection d'un comportement anormal de la part du Tiers : La compromission du Tiers n'est pas forcément confirmée (il peut s'agir d'un incident de production non lié à un incident de sécurité dans le système d'information du Tiers) mais un incident de sécurité est suspecté au sein de l'entreprise.
- ☐ Cas IV - Détection d'un comportement malveillant provenant du Tiers : La compromission du Tiers est confirmée ou fortement suspectée et un incident a également été détecté au sein de votre entreprise.

SUITE DES ACTIONS

Agir selon le cas dans lequel l'entreprise se trouve

A l'issue de la qualification, voici les actions à entreprendre selon le cas dans lequel vous vous trouvez :

- ► Cas I - Aucune compromission n'est confirmée : ni celle du Tiers, ni celle de l'entreprise ne sont avérées.
  - ☐ Actions : Commencer à identifier les liens de votre entreprise avec le Tiers et attendre de nouvelles informations (provenant du Tiers, des investigations lancées...) liées à la compromission.
- ► Cas II - La compromission du Tiers est confirmée, mais aucun impact identifié au sein de l'entreprise.
  - ☐ Actions : Poursuivre l'analyse de cette fiche et la mettre à jour régulièrement pour mieux estimer l'impact.
  - ☐ Actions : Renforcer la veille concernant le Tiers concerné (médias, CTI, etc.)
- ► Cas III - Détection d'un comportement anormal de la part du Tiers : La compromission du Tiers n'est pas forcément confirmée (il peut s'agir d'un incident de production non lié à un incident de sécurité dans le système d'information du Tiers) mais un incident de sécurité est suspecté au sein de l'entreprise. OU BIEN
- ► Cas IV - Détection d'un comportement malveillant provenant du Tiers : La compromission du Tiers est confirmée ou fortement suspectée et un incident a également été détecté au sein de votre entreprise.
  - ☐ Actions 1 : Consulter la ou les fiche(s) réflexe correspondante(s) et traiter l'incident sur votre périmètre (Qualification puis Endiguement).
  - ☐ Actions 2 : Poursuivre en parallèle le déroulé de cette fiche.

Si l'incident est bien confirmé et qu'il est de type compromission d'un Tiers, 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 Tiers - Endiguement

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

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 :

- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- Cyberattaques et remédiation

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.

Contacts

La gestion d'un incident cyber implique de faire appel à des équipes spécialisées au sein de CERT/CSIRT, qui appuieront les équipes internes dans la réalisation de leurs actions de défense.

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation	Se référer aux procédures internes.	Pour les organisation disposant d'une équipe de réponse à incident interne.
CERT/CSIRT externe en prestation de réponse à incident	`https://www.cybermalveillance.gouv.fr/diagnostic/accueil` `https://cyber.gouv.fr/prestataires-de-reponse-aux-incidents-de-securite-pris`	Pour les petites organisations : consulter le registre des prestataires spécialisés sur Cybermalveillance Pour les organisations opérant un système d'information complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS)
CSIRT régional	`https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux`	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations
CERT sectoriel	`https://www.cert-aviation.frhttps://www.m-cert.frhttps://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.