

FICHE RÉFLEXE

Compromission d'un équipement de bordure réseau

Endiguement

InterCERT FRANCE



CC BY-NC-SA 4.0



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 lorsque :

- la compromission d'un équipement de bordure réseau de l'organisation a été confirmée ;
- un équipement 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 de router 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 SOHO ou box internet pour de petites organisations

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 ?

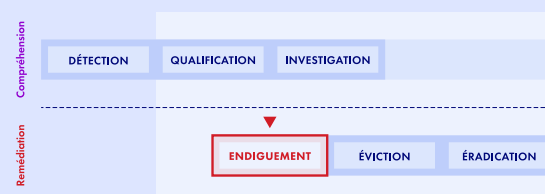
Deux parties principales composent cette fiche :

- 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 4 axes thématiques.

Si l'organisation estime avoir besoin d'aide pour réaliser ces actions d'endiguement, elle peut contacter des équipes spécialisées en réponse à incident, qu'elles soient internes ou externes : voir la partie Contacts.

SOMMAIRE

Prérequis	3
Actions d'endiguement par priorités	4
Actions d'endiguement par thèmes	6
Suite des actions	10
Annexes	11





PRÉREQUIS

Avoir qualifié l'incident

Avoir *qualifié* que l'incident en cours sur le système d'information soit bien une compromission d'équipement de bordure réseau, et en avoir évalué la gravité. Nous vous recommandons de consulter la fiche réflexe : *Compromission d'un équipement de bordure réseau - Qualification* (cf. la section Liens utiles)

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'administration* du système d'information : réseau, système, sécurité opérationnelle.

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*.

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.



ACTIONS D'ENDIGUEMENT PAR PRIORITÉS

Cette partie pointe l'ordre chronologique et prioritaire des actions détaillées dans la partie suivante. Plusieurs cas de figure se présentent qui demanderont des actions différentes, ils sont résumés dans le diagramme suivant :

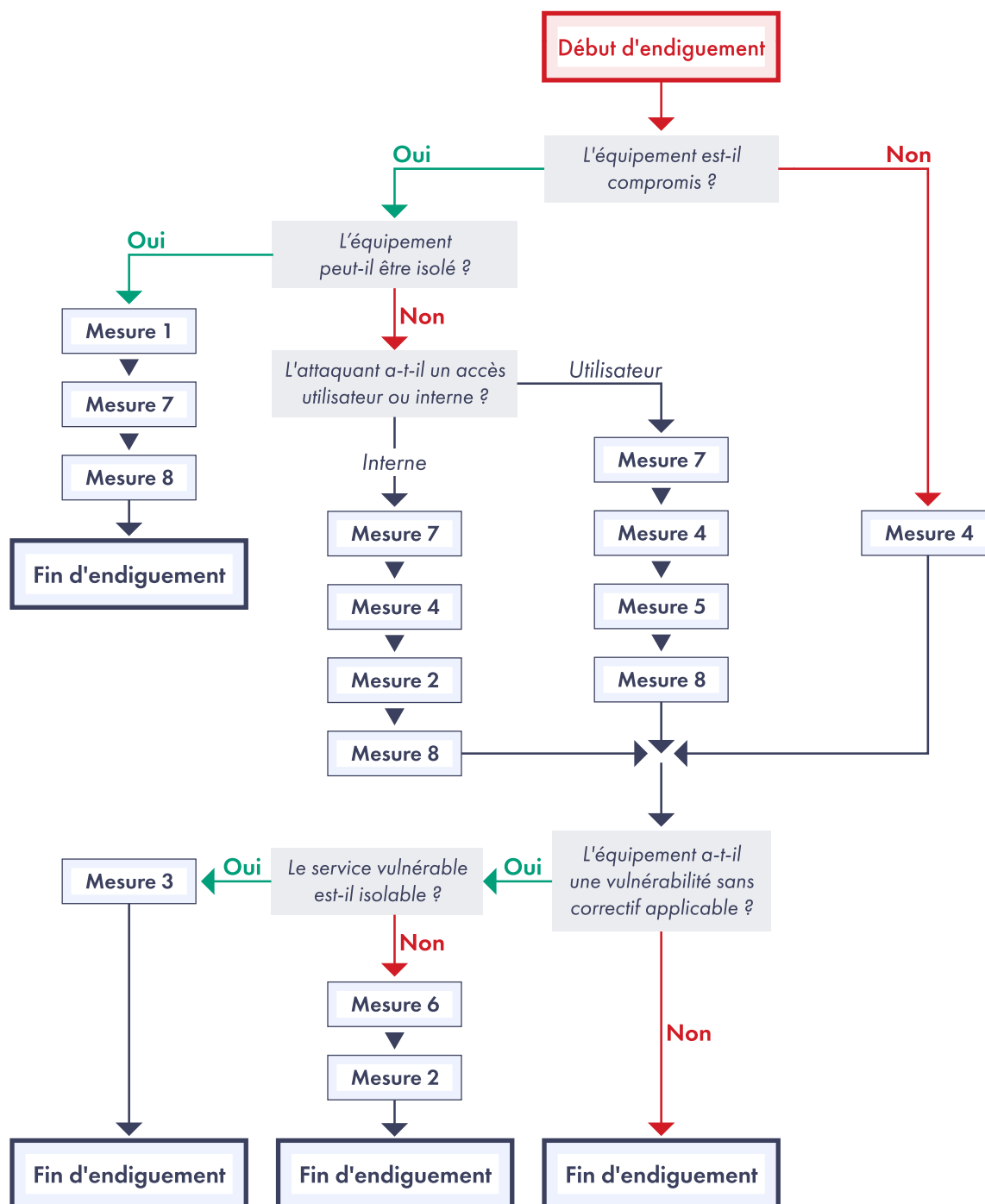


Figure 1 – Diagramme de décision de traitement

REMARQUE

Deux niveaux de compromission de l'équipement sont possibles. Le premier niveau est un accès légitime i.e. l'attaquant peut accéder à



des fonctionnalités de l'équipement normalement mises à disposition du client. 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 2 – Architecture d'équipement réseau



REMARQUE

La question d'isoler l'équipement ou certains de ses services au niveau réseau peut se poser. Il est important de déterminer rapidement si les impacts liés à une isolation sont acceptables par rapport aux risques et impacts liés à un filtrage potentiellement incomplet du trafic de cet équipement. La phase de qualification de l'incident est cruciale pour déterminer la pertinence de cette action. Il est par conséquent recommandé de consulter la fiche réflexe de qualification de compromission d'équipement de bordure réseau (cf. la section Liens utiles).



ACTIONS D'ENDIGUEMENT PAR THÈMES

Cette partie détaille les différentes mesures d'endiguement possibles selon 3 axes thématiques. Chaque mesure est ensuite scindée en actions unitaires :

- ▶ Actions réseau
 - Mesure 1 - Isoler l'équipement
 - Mesure 2 - Filtrer au maximum le trafic
 - Mesure 3 - Isoler le service vulnérable
- ▶ Actions système
 - Mesure 4 - Mettre à jour l'équipement
 - Mesure 5 - Changer les secrets compromis
 - Mesure 6 - Appliquer les mesures de mitigation du fabricant
- ▶ Préservation de traces
 - Mesure 7 - Préserver les données système
 - Mesure 8 - Préserver les journaux

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.

Actions réseau

Mesure 1 - Isoler l'équipement

Action 1.a Isoler la machine suspectée de compromission

- ☐ S'il s'agit d'une machine virtuelle, la mettre en pause
- ☐ S'il s'agit d'une machine physique :
 - ☐ privilégier une isolation via d'autres équipements réseau (switch, pare-feu,...)
 - ☐ sinon, via une déconnexion réseau physique de l'équipement
 - ☐ sinon, via sa propre configuration (désactivation d'interfaces,...)



IMPACT

Une fois cette action réalisée, votre équipement n'est plus connecté à internet et ne peut donc rendre les services pour lesquels il a été installé.



REMARQUE

Si votre équipement est une passerelle VPN, assurez-vous que les administrateurs en charge des actions suivantes de la réponse à incident disposent bien d'un accès au SI.

Mesure 2 - Filtrer au maximum le trafic

Action 2.a : Limiter la surface exposée

- ☐ Désactiver tout service non essentiel exposé par l'équipement
- ☐ Retirer de l'interface internet de l'équipement tout service qui ne le nécessite pas explicitement
- ☐ Mettre en place des listes d'accès (par plages d'adresses IP, géographie, etc.) sur les services exposés restants



IMPACT

Cette action va potentiellement impliquer une perturbation ou interruption de certains services durant la plage de temps où les accès de l'équipement compromis sont filtrés.

Action 2.b : Filtrer le trafic sortant de l'équipement

- ☐ Mettre en place du filtrage de trafic sortant vers internet initié par l'équipement de bordure réseau
- ☐ N'autoriser que les flux sortants vers les services considérés comme essentiels



IMPACT

Cette action va potentiellement impliquer une perturbation ou interruption de certains services durant la plage de temps où le trafic sortant de l'équipement compromis est filtré.



REMARQUE

Il est à noter que toutes les mesures de filtrage réseau sont à effectuer dans la mesure du possible au niveau d'équipements réseau en amont ou aval de l'équipement compromis et non sur l'équipement lui-même. Ceci permettra de limiter les risques que l'attaquant ne modifie lui-même la configuration réseau de l'équipement pour s'octroyer un accès.

Mesure 3 - Isoler le service vulnérable

Action 3.a : rendre inaccessible le service vulnérable

- ☐ Désactiver le service vulnérable
- ☐ Si impossible, filtrer le trafic entrant vers le port exposant le service vulnérable



IMPACT

Cette action va interrompre le service durant la plage de temps où il sera fixé.

Actions système

Mesure 4 - Corriger les vulnérabilités

Action 4.a : Appliquer la procédure de correction proposée par l'éditeur

- ☐ Appliquer les correctifs de l'éditeur



REMARQUE

Cette mesure n'est à effectuer que si votre équipement de bordure est affecté par une vulnérabilité pour laquelle un correctif que vous êtes en capacité d'appliquer est disponible.



IMPACT

Cette action peut perturber les services rendus par l'équipement, consultez les notes du fabricant pour déterminer les impacts potentiels.



Mesure 5 - Changer les secrets potentiellement compromis

Action 5.a : Changer les secrets utilisés par l'attaquant

- ☐ Changement tout secret dont l'usage par l'attaquant a été identifié

Action 5.b : Changer les secrets potentiellement utilisés par l'attaquant

- ☐ Identifier et renouveler les secrets rendus accessibles par la compromission (contenus dans l'équipement, ou indirectement accessibles)

REMARQUE

Certaines de ces actions peuvent prendre beaucoup de temps et avoir des impacts sur le bon fonctionnement du SI. Un arbitrage doit être fait entre les secrets renouvelables rapidement et le risque que représente leur compromission. Il est par conséquent recommandé de consulter la fiche réflexe de qualification de compromission d'équipement de bordure réseau (cf. la section Liens utiles). Les accès dont les secrets ne sont pas renouvelés doivent être étroitement surveillés durant la suite de la réponse à incident.

IMPACT

Cette action peut entraîner des pertes de tunnels VPN, une impossibilité pour certains utilisateurs de se connecter, et des indisponibilités variées en fonction des secrets changés.

Mesure 6 - Appliquer des mesures de mitigation

Action 6.a : Appliquer les mesures de réduction de risque proposées par le fabricant

- ☐ Appliquer les mesures de mitigation du fabricant pour limiter les impacts de la vulnérabilité.

IMPACT

Cette action peut perturber les services rendus par l'équipement, consultez les notes du fabricant pour déterminer les impacts potentiels.

Préservation des traces

Mesure 7 - Préserver les données système

Action 7.a : Préserver l'état du système afin de pouvoir l'analyser

Si l'équipement est une machine virtuelle dont un instantané peut être pris.

- ☐ Effectuer et exporter un instantané (*snapshot*) de l'équipement

Action 7.b : Exporter les informations de l'équipement

Si l'équipement ne permet pas de prendre des instantanés systèmes.

- ☐ Exporter la configuration de l'équipement
- ☐ Appliquer la fonctionnalité d'un export de données système (archive ou outil de diagnostic, sauvegarde, export de système de fichier, etc...) si l'équipement en dispose



Mesure 8 - Préserver les journaux de l'équipement

Action 8.a : Préserver les traces des journaux générés par l'équipement

- ☐ Exporter les journaux réseau et système de l'équipement si ces derniers ne sont pas déjà collectés



IMPACT

Cette action peut être longue en fonction de la volumétrie de journaux stockés sur l'équipement



SUITE DES ACTIONS

Une fois la situation figée par les mesures précédentes, l'endiguement est terminé.

La réponse à incident doit cependant rapidement continuer avec :

- ▶ une supervision de circonstance sur les tentatives de retour de l'attaquant
- ▶ une investigation forensique pour déterminer l'ampleur de la compromission du SI et la mise en place d'un plan de remédiation approprié.

De manière générale, un incident doit être géré jusqu'à son terme avec tous les corps de métier concernés. La réponse à incident inclut notamment des actions non exclusivement informatiques comme, par exemple, le maintien d'activité, la communication aux partenaires, les dépôts de plainte et déclarations, etc...

Pour s'assurer d'une réponse à incident efficace, il est conseillé de mettre en place une gestion d'incident cyber et de vous faire aider par des équipes spécialisées. La liste des entités auxquelles vous pouvez potentiellement demander de l'aide est disponible dans la section "Contacts" des annexes.



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 :

Document	Lien
Fiche réflexe - Compromission d'un équipement de bordure réseau - Qualification	https://www.intercert-france.fr/publications/fichereflexe-compromissionequipementbordurereseau-qualification
Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique	https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique
Cyberattaques et remédiation	https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber

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 organisations 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.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.
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.