PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 11/08/2025
N° CERTFR-2025-RFX-006

Compromission d'un tiers - Endiguement

Fiche Réflexe

ANSSI/SDO
11/08/2025

Version : 1
Nombre de pages : 16

Table des matières

1 Présentation de la fiche **3**
- 1.1 À qui s'adresse-t-elle ? 3
- 1.2 Quand l'utiliser ? 3
- 1.3 À quoi sert-elle ? 3
- 1.4 Comment l'utiliser ? 3

2 Prérequis **3**
- 2.1 Avoir qualifié l'incident 3
- 2.2 Avoir les capacités d'administration 4
- 2.3 Ouvrir une main courante 4

3 Actions d'endiguement par priorités **5**
- 3.1 I - Ni la compromission du Tiers, ni celle de l'entreprise ne sont en l'état confirmées. 5
- 3.2 II - La compromission du Tiers est confirmée, mais pas celle de l'entreprise. 5
- 3.3 III et IV Détection d'un incident au sein de l'entreprise liée à la compromission d'un Tiers 5

4 Actions d'endiguement par thèmes **6**
- 4.1 Sommaire 6
- 4.2 Theme 1 - Continuité d'activité 6
- 4.3 Theme 2 - Endiguement de l'incident 8

5 Suite des actions **10**
- 5.1 Remarques générales 10
- 5.2 Retour d'expérience et capitalisation sur la gestion de l'incident 10

6 Annexes **11**
- 6.1 Liens utiles 11
- 6.2 Définitions 11
- 6.3 Contacts 13
- 6.4 Déclarations 13
- 6.5 Préparation 14
- 6.6 Contacter le CERT-FR 14
- 6.7 Licence 15

1 Présentation de la fiche

1.1 À qui s'adresse-t-elle ?

- Responsables de la sécurité des systèmes d'information (RSSI)
- Administrateurs du système d'information
- Centre Opérationnels de Sécurité (SOC)

1.2 Quand l'utiliser ?

Utiliser cette fiche lorsqu'une entité tierce en relation avec votre organisation est victime d'une compromission et que la qualification a été réalisée (confirmation de la typologie d'incident).

1.3 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.

1.4 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 2 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.

2 Prérequis

2.1 Avoir qualifié l'incident

Il faut avoir *qualifié* qu'il y a bien une compromission d'un Tiers, et en avoir évalué le type et la gravité :

CC BY-NC-SA 4.0

- Fiche précédente conseillée : Fiche réflexe - Compromission d'un tiers - 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.

2.2 Avoir les capacités d'administration

S'assurer que les personnes qui mettront en œuvre les actions d'endiguement ont 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.

Il peut également être utile d'inclure assez tôt dans les échanges des personnes ayant la connaissance des relations avec le Tiers ou déjà en relation avec lui et autorisée à suivre l'incident.

2.3 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 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.

CC BY-NC-SA 4.0

3 Actions d'endiguement par priorités

Cette partie pointe l'ordre chronologique et prioritaire des actions détaillées dans la partie suivante selon le cas de figure identifié lors de la qualification, à savoir :

- 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.

3.1 I - Ni la compromission du Tiers, ni celle de l'entreprise ne sont en l'état confirmées.

Ce cas s'applique si la confirmation n'est confirmée ni sur l'organisation ni chez le tiers, ou si la compromission confirmée pour un tiers ayant très peu ou pas de liens avec l'entreprise.

Actions	Priorité
Sensibiliser les effectifs sur les potentiels risques actuels *(Mesure 1)*	P0
Maintenir un canal de communication avec le Tiers pour suivre l'évolution de la situation *(Mesure 2)*	P1

3.2 II - La compromission du Tiers est confirmée, mais pas celle de l'entreprise.

Ce cas s'applique si la compromission du tiers est confirmée, mais que rien ne permet de considérer l'organisation défendue comme compromise. Le tiers a potentiellement de forts liens avec l'organisation.

Actions	Priorité
Premières remédiations d'urgence selon la pertinence *(Mesure 4)*	P0
Surveillance et Threat Hunting *(Mesure 5)*	P1
Maintenir la communication avec le Tiers pour suivre l'évolution de la situation *(Mesure 2)*	P1
Sensibiliser les effectifs sur le risque actuel *(Mesure 1)*	P2
Plan de Continuité et de Reprise d'Activité (PCA/PRA) *(Mesure 3)*	P3

3.3 III et IV Détection d'un incident au sein de l'entreprise liée à la compromission d'un Tiers

CC BY-NC-SA 4.0

Actions	Priorité
Premières remédiations d'urgence selon la pertinence *(Mesure 4)*	P0
Traiter l'incident interne selon la fiche réflexe correspondant au type d'incident identifié *(Mesure 6)*	P0
Surveillance et Threat Hunting *(Mesure 5)*	P1
Maintenir la communication avec le Tiers pour suivre l'évolution de la situation *(Mesure 2)*	P1
Sensibiliser les effectifs sur le risque actuel *(Mesure 1)*	P2
Plan de Continuité et de Reprise d'Activité (PCA/PRA) *(Mesure 3)*	P3

4 Actions d'endiguement par thèmes

4.1 Sommaire

Cette partie détaille les différentes mesures d'endiguement possibles selon 2 axes thématiques. Chaque *mesure* est ensuite scindée en *actions unitaires* :

Les actions présentées dans cette partie sont regroupées par thèmes, et non par priorités ! Pour comprendre quelles mesures et dans quel ordre effectuer ces actions, se référer à la précédente partie Actions d'endiguement par priorités.

- Thème 1 : Continuité d'activité
  - Mesure 1 - Sensibiliser les équipes en interne
  - Mesure 2 - Maintenir la communication avec le Tiers pour suivre l'évolution de la situation
  - Mesure 6 - Mettre en place des mesures de continuité d'activité
- Thème 2 : Endiguement de l'incident
  - Mesure 3 - Limiter l'exposition au tiers compromis
  - Mesure 4 - Mettre en place une surveillance de circonstance (Surveillance et Threat Hunting)
  - Mesure 5 - Traiter l'incident en interne

4.2 Theme 1 - Continuité d'activité

4.2.1 Mesure 1 - Sensibiliser les effectifs sur le risque actuel

- ☐ Définir une posture de communication (prestataire, effectifs en lien avec le prestataire…) en fonction :
  - ☐ du niveau de risque et
  - ☐ du niveau de sensibilisation des collaborateurs
  - ☐ de la sensibilité de l'incident
- ☐ Informer les collaborateurs sensibilisés en relation avec le Tiers ou couper les liens + notification du Tiers

CC BY-NC-SA 4.0

- ☐ Communiquer plus largement sur les éléments à disposition concernant la compromission si décidé ainsi.
- ☐ Définir une conduite à tenir vis-à-vis du Tiers (nouveau processus de travail et/ou d'interactions…)

☐ Mettre en place un processus de signalement de comportements suspects

- ☐ Liste de diffusion temporaire pour les employés

☐ Processus de traitement des signalements internes afin qu'ils puissent être pris en compte dans les actions d'endiguement et de qualification

4.2.2 Mesure 2 - Maintenir la communication avec le Tiers pour suivre l'évolution de la situation

☐ Prévoir, selon les disponibilités des parties prenantes et l'impact, un point plus ou moins régulier.
☐ Suivre éventuellement les remédiations côté Tiers à l'aide des fiches endiguement correspondant à l'incident identifié chez le Tiers (voir Mesure 6)

4.2.3 Mesure 3 - Plan de Continuité et de Reprise d'Activité (PCA/PRA)

Action 3.a : Consulter les procédures de PCA existantes

☐ Vérifier la documentation et les protocoles en place.
☐ Identifier les contacts clés et les ressources nécessaires.

Action 3.b : Définir un plan de PCA avec le tiers

☐ Élaborer un plan d'action pour les actifs IT indisponibles en coopération avec les métiers.
☐ Établir un niveau minimum de sécurité pour reprendre partiellement l'activité.

Action 3.c : Définir un plan de reprise d'activité sur la base de pré-requis de sécurité avec le tiers

☐ Documenter les exigences et mesures de sécurité pour assurer la reprise d'activité.
☐ Par exemple :

- ☐ Partage d'un rapport d'investigation sur l'attaque incluant les actions de remédiation
- ☐ Rotation des identifiants de connexion

CC BY-NC-SA 4.0

4.3 Theme 2 - Endiguement de l'incident

4.3.1 Mesure 4 - Premières remédiations d'urgence

- ☐ Étudier au cas par cas les actions à entreprendre (par exemple en cas de compromission d'un compte de messagerie, il ne sera pas forcément utile de couper tous les accès VPN) sur la base des deux critères :
  - ☐ Étendue de l'interconnexion (plus l'interconnexion est grande, plus la surface d'attaque l'est également, justifiant de vouloir couper les accès)
  - ☐ Gravité de l'incident (plus l'incident chez le Tiers est important, plus la coupure sera justifiée)
- ☐ Désactiver/couper les accès (IT) selon la typologie de l'incident identifiée chez le Tiers.
  - ☐ Interconnexions de machines (firewall, proxy, VPN)
  - ☐ Accès à une ou plusieurs applications (ou désactivation de compte)
  - ☐ Blocage de mails (Antispam/Passerelle mail/Parefeu)
  - ☐ Mise en quarantaine de logiciel, d'applications ou de matériel fournis par le Tiers
- ☐ Notifier le Tiers des actions entreprises.

4.3.2 Mesure 5 - Surveillance et Threat Hunting

Action 5.a : Surveillance

- ☐ Sensibilisation des équipes de surveillance et mise en place de monitoring pour une attention particulière sur les activités liées à ce tiers

Action 5.b : Investigations et Threat Hunting

- ☐ Recherche dans l'infrastructure de l'entreprise des IOCs semblables à ceux observés chez le tiers .

4.3.3 Mesure 6 - Traiter l'incident interne selon la fiche réflexe correspondant au type d'incident identifié

Action 6.a : Dans le cadre d'une Compromission d'un Système

- ☐ Traiter l'incident comme une compromission système : 'Fiche réflexe - Compromission Système - Endiguement'

CC BY-NC-SA 4.0

Action 6.b : Dans le cadre d'une Compromission de Messagerie

☐ Traiter l'incident comme une compromission de messagerie : 'Fiche réflexe - Compromission Messagerie - Endiguement'

Action 6.c : Dans le cadre du déploiement d'un logiciel de chiffrement ou d'effacement

☐ Traiter l'incident comme un déploiement de logiciel de chiffrement en cours ou imminent : 'Fiche réflexe - Chiffrement - Endiguement'

Action 6.d : Dans le cadre d'une Compromission de Tenant Azure

☐ Traiter l'incident comme une compromission d'un tenant Azure : 'Fiche réflexe - Tenant Cloud - Endiguement'

Action 6.e : Dans le cadre d'une Défiguration Web

☐ Traiter l'incident comme une défiguration de site web : 'Fiche réflexe - Défiguration Web - Endiguement'

Action 6.f : Dans le cadre d'une Compromission d'un Equipement Réseau de Bordure

☐ Traiter l'incident comme une compromission d'un équipement réseau de bordure : 'Fiche réflexe - Équipement de bordure Réseau - Endiguement'

Action 6.g : Dans le cadre d'un Déni de Service

☐ Traiter l'incident comme un déni de service : 'Fiche réflexe - Déni de Service - Endiguement'

Action 6.h : Dans le cadre d'une Fuite de Données

☐ Traiter l'incident comme une fuite de données : 'Fiche réflexe - Fuite de données - Endiguement'

CC BY-NC-SA 4.0

5 Suite des actions

5.1 Remarques générales

À la fin de ces actions d'endiguement, la compromission devrait être contenue. Pour autant, l'incident a très probablement impacté l'organisation au-delà de son système d'information et il reste encore beaucoup à faire.

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*.

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

Remarque : Dans le cas d'une compromission de Tiers, il pourra s'avérer utile de calquer le suivi interne aux points organisés avec le Tiers pour s'assurer de la bonne circulation de l'information et que le tempo est adéquate pour des mises à jour régulières.

5.2 Retour d'expérience et capitalisation sur la gestion de l'incident

Une fois l'incident terminé, il pourra être utile de documenter et capitaliser la gestion de cet incident, en termes de processus et de standard

☐ Enrichir l'analyse de la menace par la rédaction de rapport d'investigation en cas d'incident
  ☐ Analyser la source de l'attaque et les TTP de l'attaquant ainsi que ses motivations.
  ☐ Mettre en place des actions de remédiation.

☐ Évaluer le besoin d'appliquer de nouveaux standards de sécurité, ou de les adapter au contexte
  ☐ Estimer la conformité aux normes de sécurité pertinentes.
  ☐ Intégrer ces standards dans le plan de PCA/PRA.

CC BY-NC-SA 4.0

6 Annexes

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

6.2 Définitions

6.2.1 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.

6.2.2 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.

6.2.3 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.

CC BY-NC-SA 4.0

6.2.4 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*.

6.2.5 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.

6.2.6 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.

6.2.7 Qualifier un incident

Qualifier un incident signifie :

- *Confirmer* qu'un incident de sécurité est bien en cours et si oui, déterminer précisément sa *nature*.

CC BY-NC-SA 4.0

- *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.

6.3 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.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	Consulter la section Contacter le CERT-FR	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.

6.4 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.

CC BY-NC-SA 4.0

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.

6.5 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.

6.6 Contacter le CERT-FR

Attention

Quand vous effectuez un signalement auprès du CERT-FR, un numéro de référence vous est attribué. Pensez à rappeler ce numéro quand vous nous recontactez, ou dans l'entête de vos messages afin de simplifier le suivi du cas.

6.6.1 Par Téléphone

Le CERT-FR est joignable 7J/7, 24H/24 :

- depuis la France métropolitaine au **3218** (service gratuit + prix d'un appel) ou 09 70 83 32 18
- depuis certaines collectivités territoriales situées en Outre-mer ou depuis l'étranger au +33 9 70 83 32 18

CC BY-NC-SA 4.0

6.6.2 Par Internet

- mèl : cert-fr@ssi.gouv.fr
- site : https://cert.ssi.gouv.fr/contact/

6.6.3 Clé PGP du CERT-FR

Pour vérifier l'intégrité des informations fournies ci-dessous, veuillez contacter le CERT-FR.

Identifiant de la clé : 0x1B45CF2A

Empreinte de la clé : 7F4C 8FA6 A356 D1CC 2E5C AB09 5416 33B8 1B45 CF2A

Télécharger la clé publique : https://cert.ssi.gouv.fr/uploads/public_key_2024.asc

6.7 Licence

Ce document est dérivé des travaux du GT Fiches Réflexes de remédiation de l'InterCERT FRANCE

Les documents originaux peuvent être consultés sur le site de l'InterCERT-France (https://www.intercert-france.fr/publications/fiches-reflexes/).

Le présent document est publié sous licence CC BY-NC-SA 4.0.

ANSSI/SDO
Version 1- UNDEF

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

cyber.gouv.fr