RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
REMÉDIATION

CYBERATTAQUES ET REMÉDIATION

PRÉPARER LA REMÉDIATION

Table des matières

PARTIE I

INTRODUCTION

a Objectifs du document

Les incidents de sécurité informatique surviennent rarement au meilleur moment pour les défenseurs.

Beaucoup d'organisations ont développé des plans de continuité et de reprise d'activité. Malheureusement, l'expérience montre qu'au moment de la publication de ce texte, ces plans sont encore rarement adaptés à des évènements de cybersécurité d'ampleur.

Face à de telles attaques, les organisations victimes et les experts qui les assistent doivent travailler avec les éléments à leur disposition tels qu'ils les trouvent.

Leur objectif va être de reprendre le contrôle du système d'information et d'y établir un niveau de fonctionnement suffisant pour un retour à la normalité.

La remédiation est un projet éminemment pragmatique : il s'exécute à un moment subi, avec les moyens disponibles sur l'instant, et des priorités dictées par la survie de l'organisation victime de la cyberattaque.

Le présent document s'appuie sur des retours opérationnels de l'ANSSI. Il est aussi issu d'ateliers avec des prestataires en réponse à incident qui ont bien voulu partager leurs expériences.

Il ne vise pas à définir un système de gestion ou un référentiel de conformité. Les listes d'actions qui y sont citées prennent en compte les besoins concrets d'équipes amenées à opérer des remédiations.

Á terme, les éléments pointés ici devraient être intégrés dans la gestion de la continuité et de la reprise d'activité, ainsi que dans la préparation à la crise. Un des objectifs du présent document est de devenir obsolète.

Ce document vise à fournir une liste de points dont la préparation, ou simplement l'identification, permet de faciliter l'élaboration et l'exécution d'un plan de remédiation.

Il vise aussi à fluidifier les conditions d'interventions de prestataires en charge des activités de remédiation chez leurs clients victimes de cyberattaques.

b Concepts et vocabulaire

Ce document vient compléter les guides de l'ANSSI de la collection « Cyberattaques et remédiation »[1].

En particulier, le vocabulaire spécifique est défini en annexe du guide « Piloter la remédiation ».

Sur les aspects relatifs à la gestion de crise, les guides de la collection « Anticiper et gérer une crise Cyber » de l'ANSSI sont la référence considérée dans le présent document.

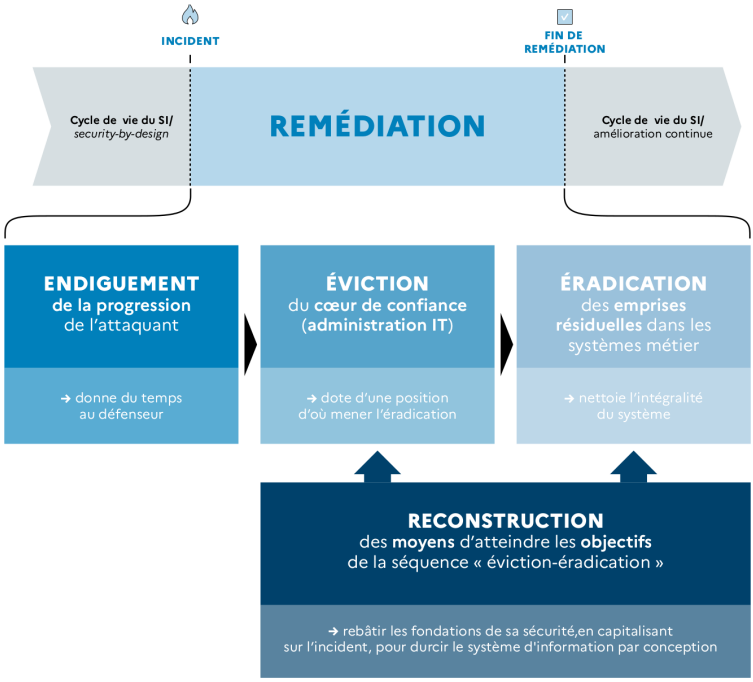
Les références et liens vers les documents cités sont disponibles en annexe. Il est recommandé de s'y référer pour approfondir le sujet.

c Rappels sur la remédiation aux cyberattaques

Les guides sur la remédiation des incidents *cyber* définissent quelques concepts clés repris ci-dessous :

- **La remédiation** aux incidents *cyber* est définie comme le **projet de reprise de contrôle** d'un système d'information compromis et du **rétablissement d'un état de fonctionnement suffisant**;
- **La remédiation aux incidents de sécurité informatique est un projet** : c'est une séquence d'actions qui peut être complexe et s'étendre sur plusieurs mois.
- **Les objectifs de la remédiation doivent être alignés sur les objectifs métiers de l'organisation** : les incidents majeurs affectent les activités métiers et parfois la survivabilité de l'organisation. Ces priorités de l'organisation définissent les objectifs stratégiques du projet de remédiation.
- **Le projet de remédiation n'est qu'une des activités de réponse aux incidents** : la gestion de crise, les activités d'investigation et de supervision de sécurité, les aspects non informatiques de la continuité d'activité fonctionnent en parallèle du projet de remédiation.

1. Voir https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber.



- Le projet de remédiation est **constitué de 4 activités** : l'**Endiguement**, l'**Éviction**, l'**Éradication** et la **Reconstruction**.

d Destinataires du document

Ce document s'adresse aux personnes qui sont en charge de préparer et piloter la remédiation d'un incident de cybersécurité.

Ces destinataires peuvent aussi bien être des membres d'une équipe de gestion de la sécurité informatique interne, d'une DSI ou d'une équipe de réponse à incident.

Sans être destinataires directs du document, d'autres parties prenantes sont concernées par certains des points listés (ex. : direction, équipes de communication).

e Temporalité

Dans ce document, les actions listées peuvent s'inscrire dans deux temporalités distinctes :

- **La préparation en anticipation ou à froid** s'effectue avant que la détection de l'incident n'ait eu lieu, quand les équipes ne sont pas spécifiquement mobilisées. Ces activités viennent compléter les travaux de durcissement du système d'information et de préparation aux incidents de cybersécurité ou aux crises.
  Ce document fournit au lecteur des points de vérification de la capacité d'une organisation à gérer des opérations de remédiation sur incident ***cyber*** avant d'être dans l'urgence. Idéalement, les activités de préparation à la remédiation à froid devraient faire partie de la gestion de la continuité d'activité et de la vie ordinaire du système d'information.
- **La préparation lors de la réaction** s'exécute après que l'incident a été détecté. Cette activité vise à préparer, en temps et en ressources contraints, l'amorce de la remédiation et l'éventuelle intervention de spécialistes. Cette préparation, de dernière minute, est un travail de mobilisation des ressources préparées, et souvent d'improvisation avec celles disponibles. Cette préparation dans l'incident tente de minimiser les frictions matérielles et organisationnelles et permettre d'entamer au plus vite et dans les meilleures conditions possibles le projet de remédiation. En cours d'incident, certaines ressources identifiées dans le présent document vont manquer. Il convient d'identifier au cas par cas si ce manque justifie des démarches supplémentaires pour les acquérir ou si le coût, en temps, humain ou financier, ne se justifie pas.

f Organisation du document

Ce document est découpé en grandes sections thématiques, chacune contenant des listes organisées par sujet, des éléments à prendre en compte pour préparer un projet de remédiation à un incident de ***cyber***.

Ces sections sont structurées du point de vue de l'organisateur de la remédiation, et non en fonction du porteur du sujet. Il revient au lecteur d'identifier qui, dans son organisation, est en mesure d'apporter les réponses aux questions soulevées dans le document.

Pour chaque entrée, il est indiqué si elle est à considérer en ***Anticipation***, en ***Réaction*** ou dans les deux cas.

Un tableau récapitulatif, disponible sur le site de l'ANSSI, reprend de façon synthétique les entrées de toutes les sections.

⚠ Pendant une réponse à incident, un adversaire est potentiellement toujours actif sur le système d'information de la victime. Les informations rassemblées en réaction à un incident sont sensibles. **Elles doivent être stockées dans des espaces sûrs**, inaccessibles à l'attaquant. Souvent, le traitement sur papier des informations relative à l'incident reste encore le plus simple et le plus sécurisé.

PARTIE II

LA SITUATION

Une bonne compréhension de la situation est indispensable au pilotage. A froid, cette vision est acquise par les activités de pilotage et de supervision du système d'information. A chaud, de nouvelles informations sont à prendre en compte et la connaissance de la situation doit être complétée d'éléments propres à l'incident.

Le croisement de ces informations donne une situation technique de l'incident permettant de prendre des décisions éclairées.

a Éléments de qualification et réactions initiales

Que s'est-il passé ? De prime abord, répondre à cette question pourtant fondamentale n'est pas aisé, les évènements de sécurité ayant conduit à l'incident étant parfois dispersés.

Rassembler ces informations est crucial pour diriger et éclairer le pilotage de l'incident et de la remédiation.

Ces informations sont rares et donc encore plus précieuses dans les premiers temps de l'incident, en phase d'Endiguement.

- *En réaction*
  - Identifier les événements de sécurité liés à l'incident ;
  - Lister les tickets SOC liés à l'incident ;
  - Établir une chronologie des symptômes initiaux et constats des utilisateurs et des administrateurs.

b Actions entreprises

Les actions entreprises en début d'incident sont rarement tracées correctement. Or, elles sont souvent très importantes sur la suite des opérations : liaisons coupées, actions à distinguer de celles de l'attaquant, postes et serveurs éteints…

Il est primordial de rassembler ces éléments, identifier les porteurs de ces informations et formaliser les actions dans une main courante.

- *En réaction*
  - Retranscrire la connaissance informelle des actions entreprises ;
  - Recenser les mains courantes métiers et techniques ;
  - Identifier les plans et documents de suivi d'actions ;
  - Lister les tickets DSI liés à l'incident.

c Pilotage

La préparation du pilotage de la remédiation s'inscrit dans la préparation aux incidents majeurs et aux crises. Il est recommandé de se référer au guide ANSSI/CDSE de pilotage de crise[1]. Les priorités de l'organisation doivent guider le projet de remédiation. Pour ce faire, un certain nombre éléments de connaissance sont requis dans la formulation des objectifs stratégiques.

- *En anticipation*
  - Identifier et documenter les modes de sollicitation aux décideurs ;
  - Définir les priorités métier.

- *En réaction*
  - Définir les objectifs stratégiques ;
  - Définir le périmètre et les limites des interventions ;
  - Valider et ajuster les priorités métier.

1. Se référer à l'annexe 1 pour les références exactes

d Moyens de supervision

Les moyens de supervision technique permettent de situer les événements de l'incident et d'observer leur déroulement.

Ces moyens nourrissent la connaissance de l'adversaire et permettent d'en comprendre les actions.

- *En anticipation*
  - Identifier et documenter les accès aux services de supervision de production et les journaux ;
  - Mettre en place des collectes de journaux systèmes et applicatifs (puits de logs et d'événements) ;
  - Déployer une infrastructure de supervision de sécurité : EDR, XDR, SIEM.

- *En réaction*
  - Mettre les principaux journaux systèmes, applicatifs et réseau sous séquestre ;
  - Allonger les politiques de rétention de journaux par défaut, voire en arrêter temporairement la rotation ;
  - Isoler les moyens d'administration de la supervision de sécurité : EDR, XDR, SIEM, par du filtrage réseau, du filtrage applicatif ou du contrôle d'accès au niveau des utilisateurs.

PARTIE III

LES PLANS

La majorité des organisations disposent de plans de continuité et de reprise d'activité. Cependant, ceux-ci ne prennent que rarement en compte les enjeux de sécurité informatique.

a Plans de continuité et de reprise d'activité

Les Plans de Continuité d'Activité (PCA) et les Plans de Reprise d'Activité (PRA) constituent la dimension métier de la continuité. Ils sont soutenus par les Plans de Continuité Informatique (PCI) et Plans de Reprise informatique (PRI). Les plans de continuité d'activité sont souvent uniquement prévus face à des sinistres traditionnels (incendies, inondations…) et la dimension ***cyber*** doit y être incluse sous plusieurs angles.

- *En anticipation*
  - Prendre en compte la sécurité informatique dans la continuité d'activité ;
  - Préparer la continuité face à un incident ***cyber*** ;
  - Établir les objectifs de temps de reprise (RTO) et de points de reprise (RPO) ;
  - Collecter les retours des exercices de PCI et PRI.

- *En réaction*
  - Actualiser les objectifs de temps de reprise (RTO) et de points de reprise (RPO) ;
  - Inspecter les PCA/PRA comme potentielle ressource pour le plan de remédiation ;
  - Utiliser les retours des exercices de PCI et PRI pour identifier les points d'attention ;
  - Adapter le PCI/PCA face à l'incident.

b Plans de restauration de données

Les données sauvegardées sont une des bases de la reconstitution des services. Cependant, déplacer une information depuis des bandes vers des disques ne constitue que la première étape d'une restauration. Les étapes menant de l'information restaurée à la donnée en production devraient être anticipées et préparées.

Il est recommandé de se référer aux documents de l'ANSSI : « Les essentiels - Sauvegarde des systèmes d'information » et « Les Fondamentaux de la sauvegarde des systèmes d'information » référencés en annexe pour approfondir le sujet.

- *En anticipation*
  - S'assurer de la protection des serveurs de sauvegarde et en particulier du filtrage des accès vers ces systèmes.
  - Planifier la remise en production :
    - de l'infrastructure de restauration ,
    - des systèmes (machines physiques ou virtuelles) ,
    - des équipements réseau et sécurité ,
    - des fichiers de configurations ,
    - des données.
  - Planifier le déplacement des données du point de restauration vers la production.

- *En réaction*
  - Protéger les sauvegardes :
    - Mettre hors ligne le ou les serveurs de sauvegarde ou de leurs stockages ;
    - Dissocier les identités utilisées sur la sauvegarde du domaine ***ActiveDirectory*** ;
    - Changer des mots de passe des opérateurs de sauvegarde sur le système et l'application.
  - Gérer le déplacement des données :
    - Identifier les points de restauration ;
    - Identifier et allouer l'espace libre ;

- Planifier le mode de transfert vers la remise en production.

– Planifier la remise en production :
  - de l'infrastructure de restauration ,
  - des systèmes (machines physiques ou virtuelles) ,
  - des équipements réseau et sécurité ,
  - des fichiers de configurations ,
  - des données.

– Planifier la resynchronisation des données sauvegardées avec celles générées pendant la crise.

c Kits de continuité

Beaucoup d'organisations ne déploient pas un système complet de gestion de la continuité, mais ont constitué des kits de continuité. Ces kits regroupent des documents et des moyens à utiliser pour assurer la continuité d'activité de l'organisation dans le cas d'un incident majeur. Parfois ces kits sont aussi nommés ***mallettes de continuité***. Ces kits devraient au moins contenir les éléments listés dans le présent document.

▪ *En anticipation*
  – Valider l'adéquation du kit de continuité aux incidents de sécurité informatique ;
  – Identifier les porteurs des actions de constitution et maintien ;
  – Constituer et maintenir le kit ;
  – Identifier et maintenir une copie des éléments du kit de continuité hors système d'information (clé USB, impression, ordinateur hors-ligne…) ;
  – Assurer un maintien du kit dans la durée.

▪ *En réaction*
  – Identifier les moyens du kit effectivement disponibles ;
  – Distribuer les moyens et accès aux intervenants.

PARTIE IV

COMMUNICATION

Choisir un niveau de communication pendant un incident grave influe fortement sur le déroulement et les impacts de la crise.

Il est recommandé de se référer au guide ANSSI « Anticiper et gérer sa communication de crise cyber »[1] pour un développement dédié à ce sujet.

Les éléments détaillés ci-dessous viennent apporter des compléments sur les aspects plus spécifiques à la remédiation.

a Posture de discrétion

Réagir face à une cyberattaque, c'est entamer une interaction avec un adversaire : les actions des défenseurs et leurs effets sont observés et interprétés par l'attaquant. Selon son niveau de compétence, de persistance et d'agressivité, sa réaction aux opérations de remédiation est variable. Les communications, qu'elles soient entre participant à la gestion de l'incident, avec les équipes de l'organisation ou avec des entités externes sont aussi des sources d'information potentielles pour l'attaquant.

La réussite du projet de remédiation à un incident ***cyber*** nécessite de contrôler les informations perceptibles par l'attaquant afin de limiter ses possibilités d'adaptation.

Cacher son jeu à l'attaquant est encore plus important dans les attaques à visées d'espionnage où la compromission peut être découverte sans que l'attaquant ne le réalise.

Une posture est définie par le niveau de précautions employées dans la communication de l'organisation attaquée, que cette communication soit publique ou interne. Mais elle définit aussi le niveau de précaution à prendre dans les actions de remédiation pour les protéger de la vue de l'adversaire.

Plus le niveau de discrétion est élevé, plus les actions courantes nécessitent des précautions et moins elles sont rapides et simples.

1. Voir les références précises en annexe 1

La posture de discrétion doit être donc pensée à un instant donné, et doit être considérée comme évolutive selon la situation de l'incident afin de conserver un bon équilibre entre efficacité des actions et échanges et discrétion.

Il est proposé de considérer trois postures de discrétion de niveau croissant [2] :

- ***Posture de discrétion faible :*** privilégier la transparence, en acceptant le risque d'informer l'attaquant ;
- ***Posture de discrétion moyenne :*** opter pour une communication ciblée, limitant les détails publics ;
- ***Posture de discrétion élevée :*** privilégier le secret pour priver l'adversaire d'information, quitte à accepter de ne pas informer employés, partenaires et public.

- *En anticipation*
  - Préparer les postures de discrétion et leurs supports :
    - Identifier les facteurs permettant de choisir les points d'équilibre entre le risque de donner des informations et le besoin d'agir et communiquer pour chaque niveau de discrétion. [3] ;
    - Identifier et préparer les porteurs d'actions, les moyens et des procédures pour chaque niveau de discrétion ;
    - Identifier les acteurs informés et leur niveau d'information acceptable pour chaque posture.

- *En réaction*
  - Sélectionner et communiquer une posture de discrétion aux acteurs concernés ;
  - Compléter la préparation des moyens ad-hoc si nécessaire (par exemple : installation de postes hors domaine, acquisition d'ordiphones…) ;
  - Identifier les éléments pertinents pour la cellule de gestion de crise dans la préparation des communications publiques.

2. Ces niveaux sont définis plus en détail dans le référentiel PRIS référencé en annexe.

3. D'autres facteurs vont dicter le choix de cette posture au delà de l'interaction avec l'attaquant. On peut notamment penser à certaines obligations de déclarations publiques ou les contraintes contractuelles vis à vis de partenaires.

b La communication avec l'écosystème de l'organisation

Dans la plupart des incidents de sécurité informatique significatifs, une communication avec les clients, usagers, partenaires et fournisseurs est nécessaire. Celle-ci est d'autant plus importante si des interconnexions réseaux sont en place.

Les points ci-après s'ajoutent aux recommandations générales de communication qu'il est possible de retrouver dans les guides ANSSI relatifs à la communication de crise.

- *En anticipation :*
  - Catégoriser les partenaires et leur besoin d'information ;
  - Identifier des scénarios types nécessitant une coordination ou une communication (par exemple : coupures et rétablissements d'accès partenaires) ;
  - Préparer des conditions contractuelles propices : identifier et faire inclure dans les contrats des clauses d'incidents et des accords de confidentialité couvrant les incidents de cybersécurité ;
  - Identifier les obligations contractuelles et réglementaires de communication.

- *En réaction :*
  - Catégoriser les partenaires ou mettre à jour les différentes catégories et leurs besoins d'information ;
  - Les modes de communication : sélectionner des modes de communication adaptés à la posture de discrétion et au partenaire ;
  - Maintenir les protections contractuelles : vérifier la présence de clauses de confidentialité dans les contrats des intervenants sur l'incident.

PARTIE V

LA CONNAISSANCE DU SI ET DES ACTIFS MÉTIER

Protéger requiert de connaître. Dérouler des opérations de remédiation sur un système d'information connu et maîtrisé sera bien moins difficile. A l'inverse, découvrir un système d'information dans l'urgence au moment d'y déployer un projet de remédiation viendra aggraver la confusion de la crise.

a Cartographies métiers

L'identification des différentes activités affectées, les métiers associés et les liens avec les actifs supports du système d'information est indispensable pour prioriser les actions de remédiation.

Certains documents communs sont précieux dans l'acquisition de connaissance métier.

- *En anticipation*
  - Identifier ou préparer une analyse d'impact métiers[1] ;
  - Collecter les analyses de risques applicatives ;
  - Identifier les principales applications et leurs porteurs métiers[2] ;
  - Constituer une cartographie des dépendances entre applications et leurs actifs supports ;
  - Rassembler les retours d'exercices de continuité (PCA/PRA, PCI/PRI).

- *En réaction*
  - Mettre à disposition les documents des analyses d'impacts métier et les analyses de risques applicatives ;
  - Mettre à disposition ou constituer une cartographie applicative sommaire incluant des porteurs métiers ;
  - Mettre à disposition ou constituer une cartographie sommaire des dépendances entre applications et autres actifs supports.

1. Aussi appelée ***Business Impact Assessment*** (BIA), l'analyse d'impact métiers permet d'identifier les priorités de continuité de l'organisation

2. Idéalement cartographier toutes les applications serait souhaitable. Mais dès qu'une organisation atteint une certaine complexité, cela est rarement tenable. Du point de vue de la remédiation aux incidents ***cyber***, l'important est d'avoir identifié les applications critiques pour l'organisation.

b Cartographies techniques

Les équipes impliquées dans le projet de remédiation ont besoin de connaitre le terrain pour le défendre. Elles auront besoin de s'appuyer sur une documentation existante et souvent de la mettre à jour. Cette création de cartographie pourra s'appuyer sur le guide de cartographie du système d'information de l'ANSSI (référencé en annexe).

La constitution et le maintien de cartographies techniques peut être une tache considérable. Dans le cadre d'une remédiation à un incident ***cyber***, une connaissance exhaustive et à jour est rarement réaliste. En revanche, avoir travaillé sur les points listés ci-dessous, même sans atteinte l'exhaustivité, fait une grande différence lors de la survenue d'un incident majeur.

- *En anticipation*
  - Recenser et/ou documenter les procédures opérationnelles du système d'information ;
  - Constituer un catalogue d'applications (serveurs et postes clients) et leurs dépendances internes et externes ;
  - Collecter les analyses ***ActiveDirectory*** (relations d'approbation, comptes et groupes à privilèges…) ;
  - Maintenir un recensement des connexions Internet et des adresses IP publiques associées ;
  - Recenser les adresses IP de services exposés sur Internet, localement ou dans le cloud ;
  - Constituer et maintenir des matrices de flux ;
  - Constituer et maintenir une cartographie du zonage réseau et de la segmentation au niveaux des couches liaison [3] et réseau [4] ;
  - Documenter les conventions de nommage de machines (DNS, LDAP ou ***ActiveDirectory***) ;
  - Maintenir une base de données des actifs du système [5] ;
  - Collecter les rapports d'audit et d'incident précédents.

5. Topologie de couche 2, Ethernet, WiFi ou autre
5. Topologie de couche 3, segmentation en sous-réseaux avec leur adressage IP
5. La CMDB pour ***Configuration Management DataBase***, voir une définition précise en annexe.

- *En réaction*
  - Mettre à disposition les catalogues d'application et de leurs dépendances techniques ou en constituer un sommaire (identification des principaux serveurs, des applicatifs et des logiciels utilisés, des dépendances techniques de chacun) ;
  - Mettre à disposition la cartographie du zonage réseau et de la segmentation au niveau des couches liaison et réseau ;
  - Mettre à disposition la matrice de flux ou constituer un schéma sommaire des principaux axes de communication au sein du SI (principes de filtrage entre les zones, passage ou non par des *proxy*. principaux flux applicatifs) ;
  - Documenter les conventions de nommage des machines (DNS et *ActiveDirectory*) ;
  - Recenser les connexions Internet et les adresses IP publiques associées ;
  - Recenser les adresses IP de services exposés sur Internet, localement ou dans le cloud ;
  - Mettre à disposition les procédures opérationnelles du système d'information, si disponibles ;
  - Mettre à disposition les analyses *ActiveDirectory* récentes quand elles existent (relations d'approbation, comptes et groupes à privilèges…)
  - Mettre à disposition les rapports d'audit et d'incident précédents.

⚠ Dans le traitement d'un incident, il est courant de découvrir des parties non documentées du système d'information. Ce peuvent être des éléments mis en place sans consultation avec la direction informatique (***Shadow IT***). Certains sous systèmes peuvent être considérés hors périmètre de l'informatique bien que raccordé à ses réseaux : les systèmes de gestion de bâtiment, le contrôle d'accès, la vidéo-surveillance, les systèmes industriels ou les réseaux téléphoniques. Enfin, il arrive que des composants restent présents alors qu'ils sont supposés avoir été décommissionnés. La mise à jour des cartographies technique lors d'un incident de sécurité est donc souvent nécessaire.

c Localisation

Les systèmes d'information ont une composante physique. La connaissance de la localisation de ces systèmes est souvent nécessaire dans la remédiation.

- *En anticipation ou en réaction*
  - Recenser la localisation des actifs du SI, pièces, centres de données (adresses géographiques des bâtiments), baies techniques ;
  - Identifier les extensions du système d'information dans les filiales ou chez des partenaires (par exemple : où sont les routeurs et pare-feu ?) ;
  - Identifier et documenter les contraintes d'accès (physiques et logiques) et de transport.

d Interconnexions et accès partenaires

Les organisations modernes sont très interconnectées.

Des fournisseurs et des partenaires divers accèdent à leur système d'information à distance. La généralisation du nomadisme numérique et du télétravail a aussi multiplié les modes d'accès aux infrastructures. Ces accès peuvent être une source de menace, mais aussi des canaux de propagation ou de retour de l'attaque. Leur connaissance est donc vitale à une remédiation réussie.

- *En anticipation ou en réaction*
  - Recenser et documenter les accès de télémaintenance interne ou tierce (y compris les équipements en ***leasing***, le support applicatif, l'OT…) ;
  - Recenser et documenter les accès en nomadisme et télétravail ;
  - Recenser et documenter les accès des tiers mainteneurs hors informatique : chaufferie, sécurité physique, gestion bâtimentaire… ;
  - Recenser et documenter les accès à des services de tiers hébergés sur le système d'information (par exemple : boitiers réseaux, ou équipements en leasing).

PARTIE VI

LES MOYENS DE COORDINATION DANS LA CRISE

a Moyens de communication

Les moyens de communication de la plupart des organisations modernes dépendent du système d'information. Cette dépendance peut être directe, comme lorsque les serveurs et les services de communication font partie du système d'information, ou indirecte, lorsqu'il s'agit d'infrastructures info-nuagiques ou de terminaux gérés par les mêmes annuaires[1]. Quand le système d'information est compromis, les moyens de communication utilisés habituellement pour se coordonner le sont aussi.

- *En anticipation*
  - Préparer des moyens de messagerie dissociés du système d'information.

- *En réaction*
  - Identifier des moyens d'échanges de fichiers indépendant du système d'information ;
  - Planifier la gestion des enrôlements et activations de comptes.

b Moyens de chiffrement

En temps normal, la capacité à échanger de façon protégée par des moyens cryptographiques est précieuse. Dans un incident majeur, elle devient vitale. Malheureusement, déployer des moyens cryptographiques s'improvise mal et la préparation est cruciale.

- *En anticipation*
  - Sélectionner des moyens de chiffrement ;
  - Planifier et documenter la gestion des identités et des clés cryptographiques dans la crise.

1. Tels que les appareils gérés par un système de gestion de mobiles (*Mobile Device Management* ou MDM)

- *En réaction*
  - Gérer le cycle de vie des clés cryptographiques et secrets : génération, distribution, révocation ;
  - Enrôler les participants aux échanges et désactiver les accès des sortants de la gestion de l'incident ;
  - Gérer le cycle de vie des données chiffrées dans la durée : gestion des copies, sauvegardes et éventuelle destruction.

c Accès Internet

Les moyens d'accès Internet nominaux sont souvent dégradés ou inutilisables pendant les incidents majeurs. Pourtant, l'usage de l'Internet y est particulièrement important : coordination, export de données à analyser ou à récupérer, téléchargement d'outils et de documentation.

- *En anticipation*
  - Définir des postures d'accès Internet en cours d'incident : limitations et coupures d'accès, moyens de secours ;
  - Planifier et éventuellement acquérir des moyens d'accès Internet hors infrastructure fixe (routeurs cellulaires, abonnements).

- *En réaction*
  - Ajuster l'accès Internet de l'infrastructure permanente : limitations d'accès, coupures, filtrages ;
  - Activer ou acquérir les moyens d'accès Internet hors infrastructure fixe (routeurs cellulaires, clés 4G/5G) ;
  - Gérer les moyens d'accès Internet hors infrastructure fixe (distribution, récupération, suivi des consommations).

d Carnet d'adresses des intervenants de crise

Dans la crise, la multiplication des intervenants peut rendre la gestion des contacts plus difficile que d'habitude. Quand les moyens habituels

sont soit indisponibles, soit compromis, cette gestion devient une préocupation majeure.

Gérer les contacts, collecter et distribuer ces informations dans un environnement dégradé est un travail significatif qui gagne à être préparé.

- *En anticipation*
  - Planifier les rôles et responsabilités de la gestion de contacts ;
  - Définir les moyens de collecte et d'échange des contacts ;
  - Maintenir les listes de contacts permanents.

- *En réaction*
  - Désigner les responsables de la gestion de contacts ;
  - Maintenir les listes de contacts au jour le jour ;
  - Diffuser les listes de contacts.

PARTIE VII

LES PARTIES PRENANTES EXTERNES À L'ORGANISATION

a Assurance

Les polices d'assurance ***cyber*** incluent généralement des services de mise à disposition de prestataires voire désignent des partenaires spécifiques auxquels faire appelen cas d'incident.

La mobilisation des services de l'assureur impose de suivre des étapes particulières dans des délais contraints contractuellement. Il est important de connaitre et de respecter la procédure de l'assureur pour bénéficier de la couverture souscrite.

⚠ Même en l'absence de couverture spécifique des incidents de sécurité informatique, les assureurs peuvent souvent assister leurs assurés dans une recherche de prestataires de gestion de crise ou d'incident. Il est donc pertinent de contacter l'assureur de l'organisation dans la recherche de prestataires susceptibles d'assister à la gestion de l'incident.

- *En anticipation*
  - Cataloguer les services disponibles/souscrits ;
  - Identifier le niveau de couverture de chaque périmètre ;
  - Identifier les points et moyens de contacts assurantiels.

- *En réaction*
  - Identifier et transmettre les procédures de signalement et documentations ;
  - Initier le contact avec l'assureur.

b Prestataires

La remédiation d'un incident ***cyber*** crée un surcroît d'activité ponctuel mais considérable. Par ailleurs, un certain nombre d'actions nécessite des compétences spécialisées dont peu d'organisations disposent en propre. Identifier des prestataires capables d'intervenir et

préparer leur intervention en amont de l'incident est un facteur de réussite.

Les incidents interviennent à des moments non choisis. Qui plus est, beaucoup de spécialités techniques ou du monde de la sécurité informatique sont sous tension. Il en résulte que beaucoup de prestataires ne peuvent pas intervenir dans un délai court sans contractualisation et préparation. Faute de contacts préalablement établis, les délais d'intervention peuvent être importants. La disponibilité d'un prestataire sera souvent déterminante dans la sélection de celui-ci.

Les prestataires à considérer peuvent être :

- Prestataires de réponse à incident, en particulier les prestataires qualifiés par l'ANSSI [1] ;
- Spécialistes en systèmes de stockage ;
- Spécialistes en systèmes d'exploitation ;
- Spécialistes en infrastructure réseau ;
- Spécialistes des équipements et logiciels de sécurité ;
- Experts ***ActiveDirectory*** ;
- Spécialistes dans les logiciels structurants de l'organisation ;
- Experts en récupération de données ;
- ESN [2] pouvant fournir sur quelques semaines ou mois une aide en administrateurs systèmes et réseaux pour assister les équipes internes.
- *En anticipation*
  - Identifier les prestataires potentiels ;
  - Établir un annuaire des prestataires sélectionnés incluant leurs modes de contact privilégiés et les limites de sollicitations (jours et heures non-ouvrées, délais d'intervention) ;
  - Si pertinent, contractualiser avec un prestataire sélectionné.

- *En anticipation et en réaction*
  - Identifier les prestataires nécessaires à la gestion de l'incident ;
  - Les contacter et valider les conditions d'intervention ;
  - Commander les interventions.

2. Les Prestataires de Réponse aux Incidents de Sécurité (PRIS) sont des spécialistes qualifiés par l'ANSSI pour la réponse aux incidents de sécurité informatique. La liste des PRIS est disponible à l'adresse `https://cyber.gouv.fr/sites/default/files/document/catalogue-produits-services-qualifies-agrees-certifies-anssi.pdf`

2. Entreprise de Services Numériques

c Contacts externes

Au-delà de l'organisation victime de l'attaque, certaines entités doivent être informées de l'incident. Suivant les contextes juridiques, réglementaires et contractuels, celles-ci peuvent varier. Il est très utile d'identifier les déclarations à effectuer, le processus de chacune et les porteurs d'actions en amont de l'incident.

⚠ En plus du CERT-FR de l'ANSSI, il existe aujourd'hui un maillage de CSIRT territoriaux et sectoriels qui ont pour vocation à accompagner les organisations publiques et privées dans la gestion des incidents. Ceux-ci offrent une réponse de premier niveau aux incidents d'origine ***cyber*** et surtout une réponse de proximité. Dans l'incident, ils sont de bon conseil sur l'identification des procédures adéquates et dans l'identification des contacts locaux ou spécialisés. [3]

- *En anticipation*
  - Identifier les contacts des autorités réglementaires ;
  - Identifier les partenaires, fournisseurs et clients avec lesquels une coordination pourrait être nécessaire ;
  - Identifier les engagements, contraintes réglementaires et contractuelles applicables en cas d'incident ***cyber*** ;
  - Identifier les procédures de dépôt de plainte et de notifications réglementaires.

- *En Réaction*
  - Identifier les contraintes réglementaires imposant une déclaration et les moyens de le faire ;
  - Identifier les partenaires, fournisseurs et clients avec lesquels les actions sont à coordonner ;
  - Préparer un dépôt de plainte.

3. La liste des CSIRT territoriaux peut être trouvée à l'adresse `https://www.cert.ssi.gouv.fr/csirt/csirt-territoriaux/`.

PARTIE VIII

LES MOYENS D'ACCÈS

a Accès physiques

Même si les accès à distance sont privilégiés, les opérations de remédiation requièrent souvent un accès physique aux serveurs et équipements d'infrastructure. Ceux-ci peuvent être d'autant plus complexes si les gestions d'accès sont interconnectées avec le système d'information compromis.

- *En anticipation*
  - Identifier les procédures d'accès ;
  - Identifier les niveaux de dégradation des moyens d'accès si les systèmes supports sont compromis [1] ;
  - Identifier les autorisations et éventuelles habilitations spécifiques [2] pour les intervenants.

- *En réaction*
  - Planifier les moyens d'identification dans la crise et leur vérification ;
  - Choisir le niveau de dégradation des contrôles d'accès ;
  - Identifier les autorisations et les habilitations spécifiques pour les intervenants ;
  - Identifier les personnes amenées à intervenir physiquement sur les équipements.

b Accès logiques

Lors d'un incident de sécurité informatique, certains accès logiques sont indispensables.

Avoir préalablement établi un catalogue des bases d'identités, réalisé des exports hors ligne des plus critiques (voire sur papier pour certains comptes), peut faire une grande différence dans une crise.

2. De nombreux systèmes de contrôle d'accès et d'identification s'appuyant sur le système d'information, un incident nécessite la mise en œuvre de contournements.

2. Par exemple, une habilitation électrique est nécessaire pour accéder dans certaines zones de centres de données.

Ces informations étant très sensibles, elles doivent être protégées avec un haut niveau de sécurisation.

- *En anticipation et en réaction*
  - Identifier et assurer un accès d'urgence :
    - aux comptes administrateurs systèmes locaux et LAPS ;
    - aux comptes maîtres de services cloud [3] ;
    - aux comptes administrateurs et aux mots de passe d'***appliances*** et équipements spécifiques (par exemple : industriels ou d'infrastructure réseau) ;
    - aux mots de passes et aux clés cryptographiques des sauvegardes ;
    - aux clés cryptographiques de recouvrement de médias chiffrés ;
    - aux clés maîtresses de PKI, de VPN…

c Cas des identifiants « bris de glace »

Certains comptes sont destinés à n'être utilisés qu'en cas d'incidents graves ou pour des opérations rares de reconfiguration du système d'information.

Ces comptes « bris de glace » ont généralement des droits étendus et sont normalement conservés hors ligne (dans un coffre, sous scellé…).

Ces comptes doivent être identifiés et leur accès d'urgence préparé et documenté :

- *En anticipation et en réaction*
  - Compte ***RID-500*** dans un domaine ***ActiveDirectory*** ;
  - Compte ***root*** des hyperviseurs ;
  - Comptes ***root*** d'infrastructures UNIX ;
  - Comptes « super-administrateur » de services cloud.

3. comptes contrôlant d'autres comptes privilégiés sur le service

PARTIE IX

LES INDISPENSABLES TECHNIQUES

a Médias d'installation

Dans beaucoup d'incidents, il est nécessaire de réinstaller des logiciels.

Il est d'ailleurs fréquent qu'il faille réinstaller le logiciel de gestion des sauvegardes avant de pouvoir restaurer quelque service que ce soit. Ces médias d'installation sont souvent négligés, mais peuvent constituer un point bloquant pour le projet de remédiation. Ces situations sont agravées quand les versions utilisées ne sont plus officiellement supportées ou, pire, que l'éditeur n'existe plus.

Il est donc important d'identifier les composants logiciels et leurs médias d'installation pour :

- *En anticipation et en réaction*
  - les logiciels nécessaires à redémarrer le socle du système d'information (gestion des sauvegardes en particulier),
  - les applications d'infrastructure,
  - les applications métiers,
  - les composants des systèmes industriels.

b Licences

Les médias d'installation ne suffisent pas toujours à rétablir un service. Des numéros de licence, voire des processus complexes d'activation peuvent être requis. Ceux-ci devraient être collectés et documentés afin d'éviter de devoir les rechercher dans des circonstances précaires.

- *En anticipation et en réaction*
  - Identifier et collecter :
    - les licences de systèmes d'exploitation et logiciels d'infrastructure,
    - les licences de logiciels métiers,
    - les dispositifs physiques d'activation (***Dongles***).
  - Documenter :
    - l'installation de serveurs d'enregistrement de licence,
    - les processus d'activation.

c Matériel informatique

La gestion de l'incident nécessite souvent du matériel informatique immédiatement disponible : remplacement de serveurs, mise en place de nouvelles infrastructures ou infrastructures temporaires. Souvent, l'enquête nécessite de figer des machines qui ne pourront pas être immédiatement réinstallées, rendant indisponible une partie du parc.

Une visibilité sur la disponibilité des stocks de matériel est indispensable dans l'incident. Avoir préparé les moyens de suivi de matériel avant l'incident permet des gains de temps considérables dans les opérations de remédiation.

- *En anticipation*
  - Maintenir un inventaire des serveurs et des équipements d'infrastructure réseau disponibles ou utilisables en urgence ;
  - Maintenir un stock de supports de stockage ou identifier un processus d'acquisition rapide ;
  - Conserver et sauvegarder hors ligne une copie à jour des masters des postes et des serveurs.

- *En réaction*
  - Identifier les serveurs et les équipements d'infrastructure réseau disponibles pouvant être mobilisés dans l'incident ;
  - Identifier, si nécessaire, des sources d'approvisionnement en matériel disponible rapidement ;
  - Provisionner des supports de stockage pour les échanges hors ligne ;
  - Stocker hors ligne une copîe des masters de postes et serveurs.

PARTIE X

LA DIMENSION HUMAINE

Dans un incident majeur, la gestion des éléments humains sera généralement assurée par la cellule de crise ou une équipe dédiée.

Néanmoins, les organisateurs des actions de remédiation doivent être conscients des paramètres à prendre en compte et se coordonner avec les porteurs du sujet.

a Identification des acteurs

Les intervenants sur un projet de remédiation mêlent les partenaires habituels de l'organisation et des personnels dont l'aide est exceptionnelle.

Il est judicieux d'identifier les personnels susceptibles d'intervenir sur un incident en amont de sa survenue.

Le cas échéant, cela permet aussi d'initier des relations avant la crise. Ces liens pré-établis offrent des gains de réactivité considérables lorsqu'une crise survient.

- *En anticipation*
  - Identifier les partenaires habituels qui seraient mobilisables dans un incident ***cyber*** ;
  - Identifier des partenaires exceptionnels, et de leurs fonctionnements d'intervention : heures non ouvrables, week-end, conditions de déplacement, et modes de contractualisation…
  - Si approprié, souscrire un contrat de services (souvent appelé ***retainer***).
  - Mettre en place un carnet de contacts ;
  - Identifier et mettre à disposition des porteurs d'expertise interne : infrastructures sensibles, applications clés, technologies, architecture.

b Préparation des Ressources Humaines

Durant l'incident, des heures inhabituelles de travail sont pratiquées. Ce mode de travail exceptionnel devrait être préparé avec les départements des ressources humaines et des finances de l'organisation.

- *En anticipation*
  - Identifier les règles et les limites des heures supplémentaires et du travail en heures non ouvrables dans la crise ;
  - Identifier les relais décideurs RH dans la criseé ;
  - Documenter les règles d'indemnisation, les primes, les récupérations et les compensations ;
  - Former et sensibiliser les équipes aux scénarios et aux procédures de gestion d'incident et de continuité ;
  - Utiliser des exercices pour identifier les limitations des plans de continuité et de rétablissement d'activité [1].

- *En réaction*
  - Payer les salaires et les primes en mode dégradé si les systèmes de paie et suivi des temps sont atteints ;
  - Identifier les relais décideurs RH dans la crise ;
  - Documenter et communiquer les règles d'indemnisation, de récupération, les primes et les compensations.

c Logistique des personnes

Un projet de remédiation nécessite de déplacer et de faire travailler sur une période soutenue un nombre inhabituel de personnes [2]. Accueillir ces personnels supplémentaires va requérir la mobilisation de moyens inhabituels : locaux, moyens de bureau, mais aussi moyens de transport, nourriture, et parfois des moyens de couchage.

1. Il est, en particulier, d'impliquer dans ce type d'exercice les fonctions de ressources humaines et finances qui rarement impliquées mais vitales dans l'incident.

2. Ce qui inclut non seulement les spécialistes en gestion d'incident mais aussi tous les intervenants auxquels la situation ne permet plus de travailler à distance

- *En anticipation*
  - Estimer différents paliers d'engagement et pour chacun évaluer les moyens logistiques ;
  - Prendre contact avec les prestataires logistiques potentiels (logement, alimentaire…) pour valider les capacités disponibles.

- *En réaction*
  - Préparer et maintenir les contacts ;
  - Déplacer, nourrir et loger les intervenants en déplacement ;
  - Fournir un espace de travail ;
  - Établir les procédures d'entrées/sorties, de suivi des présences et gestion de la fatigue [3] ;
  - Remonter les besoins de financement de la gestion de l'incident aux cellules de gestion de crise.

.

3. notablement le contrôle de la bonne prise de repos et de récupération prenant en compte les temps de transports

PARTIE XI

ANNEXES

Acronymes

AD ***Windows Active Directory*** - Annuaire et infrastructure d'authentification Microsoft Windows

BIA ***Business Impact Assessment*** -

CMDB ***Configuration Management DataBase*** - Base de connaissance des composantes et configuration des composants du SI

DNS ***Domain Name Service*** - Système de gestion de noms de domaines (RFC-1035)

DSI Direction des Systèmes d'Information

EDR ***Endpoint Detection and Response*** - Agent de supervision de sécurité

ESN Entreprise de Services du Numérique

IT ***Information Technologies*** - Systèmes bureautiques

LAPS ***Local Administrator Password Solution*** - Système de gestion des comptes d'administration locaux en environnement Windows

MDM ***Mobile Device Management*** - Solution de gestion de terminaux mobiles

OT ***Operational Technologies*** - Systèmes industriels

PCA Plan de Continuité d'Activité

PCI Plan de Continuité Informatique

PDIS Prestataire de Détection d'Incidents de Sécurité informatique

PKI ***Public Key Infractructure*** - Infrastructure de gestion de clés publiques

PRA Plan de Reprise d'Activité

PRIS Prestataire de Réponse aux Incidents de Sécurité informatique

PRI Plan de Reprise Informatique

RH Ressources Humaines

RPO ***Recovery Point Objective*** - Objectif de points de reprise d'activité

RTO ***Recovey Time Objective*** - Objectif de temps de reprise d'activité

SIEM ***Security Information and Events Management*** - Système de gestion des événements de sécurité

SI Système d'Information

SOC ***Security Operations Center*** - Centre de supervision de sécurité

VPN ***Virtual Private Network*** - Réseau privé virtuel

XDR ***eXtended Detection and Response*** - Système intégré de détection et réponse à incident de sécurité informatique

Références

GESTION DE CRISE

- Collection « Anticiper et gérer une crise Cyber »
  https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber
- Crise d'Origine Cyber - Les clés d'une gestion opérationelle et stratégique
  https://messervices.cyber.gouv.fr/guides/crise-cyber-les-cles-dune-gestion-operationnelle-et-strategique
- Anticiper et gérer une crise d'origine cyber
  https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber
- Organiser un exercice de gestion de crise cyber
  https://cyber.gouv.fr/publications/organiser-un-exercice-de-gestion-de-crise-cyber

CYBERATTAQUES ET REMÉDIATION

- Collection « Remédiation d'un incident cyber »
  https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber
- Cyberattaques et remédiation, les clés de la décision
  https://messervices.cyber.gouv.fr/guides/cyberattaques-et-remediation-les-cles-de-decision
- Cyberattaques et remédiation, piloter la remédiation
  https://messervices.cyber.gouv.fr/guides/cyberattaques-et-remediation-piloter-la-remediation
- Cyberattaques et remédiation, la remédiation du tier 0 Active Directory
  https://messervices.cyber.gouv.fr/guides/cyberattaques-et-remediation-la-remediation-du-tier-0-active-directory

FONDAMENTAUX DE LA SÉCURITÉ INFORMATIQUE

- Guide d'hygiène informatique
  https://cyber.gouv.fr/hygiene-informatique

- Recommandations sur l'administration sécurisée des systèmes reposant sur l'Active Directory
  https://cyber.gouv.fr/guide-admin-si-ad
- Fondamentaux de la sauvegarde des systèmes d'information
  https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation
- Les essentiels - Sauvegarde des systèmes d'information
  https://cyber.gouv.fr/publications/sauvegarde-des-systemes-dinformation

RÉFÉRENTIELS DE PRESTATAIRES QUALIFIÉS

- Référentiels d'exigences pour la qualification https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/comprendre-levaluation-de-securite/qualification-de-produit-et-services/referentiels-qualification/
- Liste des prestataires qualifiés ou en cours de qualification
  https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/services-de-securite-evalue/solutions-en-cours-de-qualification/pris/

CONNAISSANCE ET SUPERVISION DU SYSTÈME D'INFORMATION

- Cartographie du système d'information
  https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation
- Recommandation de sécurité pour l'architecture d'un système d'information
  https://cyber.gouv.fr/publications/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation
- Sécuriser la journalisation dans un environnement Microsoft Active Directory
  https://cyber.gouv.fr/publications/securiser-la-journalisation-dans-un-environnement-microsoft-active-directory
- Doctrine de détection pour les systèmes industriels
  https://cyber.gouv.fr/publications/doctrine-de-detection-pour-les-systemes-industriels

CONTINUITÉ D'ACTIVITÉ

- SGDSN - Guide pour réaliser un plan de continuité d'activité
  `https://www.sgdsn.gouv.fr/files/files/Nos_missions/guide-pca-sgdsn-110613-normal.pdf`

COLLECTION
REMÉDIATION

La préparation à la remédiation permet de faciliter l'élaboration et l'exécution de la réponse à un incident de sécurité et fluidifie les conditions d'interventions d'équipe en charge de remédier à l'attaque. Cette préparation peut se faire en anticipation, avant que la détection d'un incident n'ait lieu et quand les équipes ne sont pas spécifiquement mobilisées; ou elle peut se faire lors de la réaction d'un incident détecté, dans un temps contraint et en amorce de la remédiation.

Une préparation à la remédiation augmente l'efficacité de la réponse puisqu'un incident de sécurité informatiques survient à un moment subi par le défenseur qui doit répondre à l'attaque avec les moyens disponibles sur l'instant.

Le présent document s'appuie sur des retours opérationnels de l'ANSSI. Il est aussi issu d'ateliers avec des prestataires en réponse à incident qui ont bien voulu partager leurs expériences.

Cette publication vient compléter le volet opérationnel de la remédiation. La mise en œuvre ou l'identification des actions listées précèdent les activités du guide « Piloter la remédiation » de cette même collection.

Version 1.0 – Janvier 2026

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr