RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
REMÉDIATION

CYBERATTAQUES ET REMÉDIATION
PILOTER LA REMÉDIATION

V.0.0 – **APPEL PUBLIC À COMMENTAIRES**

SI VOUS ÊTES AU CŒUR D'UN INCIDENT

Si vous lisez ce paragraphe, vous êtes peut-être en train de chercher comment traiter un incident, voire une crise de sécurité informatique.

Vous trouverez dans ce document un certain nombre d'éléments destinés à vous aider dans l'organisation et le pilotage des actions techniques de remédiation.

Si vous vous trouvez actuellement dans l'urgence de la gestion de l'incident, vous n'aurez probablement pas le temps de lire l'intégralité de ce document. Il vous est recommandé cependant de lire les prochaines lignes, qui font office de synthèse.

La remédiation est l'une des activités de la réponse à incident cyber, avec la gestion de crise et l'investigation. C'est un projet dont l'objectif est de **poser les fondements pour une reprise durable du contrôle du système d'information par les défenseurs.** L'exécution du projet de remédiation suit habituellement 3 étapes et une activité de fond synthétisées dans le présent document par l'acronyme E3R[1] :

1 - **ENDIGUEMENT DE L'ATTAQUANT :** pour empêcher l'aggravation de l'incident.

2 - **ÉVICTION DE L'INTRUS DU CŒUR DU SI :** pour recréer une base de confiance d'où mener la reconstruction.

3 - **ÉRADICATION DES EMPRISES DE L'ADVERSAIRE :** pour éliminer les capacités de retour de l'attaquant par des portes dérobées laissées lors de l'intrusion.

1. Voir Partie I - Élaboration du plan de remédiation, section 1. Définitions : la remédiation et la séquence « ER3 ».

Parallèlement à ces étapes, la **reconstruction** recrée l'infrastructure compromise ou détruite par l'attaque.

Afin d'exécuter efficacement les étapes sus-citées, une organisation est nécessaire :

1. Identifier et prioriser les objectifs stratégiques avec la direction (I.2.)
2. Décliner les objectifs stratégiques en objectifs opérationnels (I.3.)
3. Mobiliser les moyens au service des objectifs opérationnels (II.4.)
   a. Équipes internes
   b. Matériels et logiciels
   c. Supports externes
4. Identifier les porteurs, prioriser et initier les sous-projets de réalisation des objectifs opérationnels (II.2.)
5. Suivre et coordonner la réalisation des sous-projets de réalisation des objectifs opérationnels (II.2.a.)
6. Tout au long du plan, communiquer régulièrement vers les décideurs et vers les exécutants l'état d'avancement global du projet de remédiation (II.2.b)
7. S'appuyer sur des prestataires, en cas de besoin, en mesure de soutenir le pilotage et la mise en œuvre de la remédiation (III.)

La Partie IV – Plans types de ce document présente des check-lists correspondant aux trois scénarios types de l'activité de remédiation :

SCÉNARIO 1 : « Restaurer au plus vite des services vitaux »

SCÉNARIO 2 : « Reprendre le contrôle du SI »

SCÉNARIO 3 : « Saisir l'opportunité pour préparer une maîtrise durable du SI »

V.0.0 – **APPEL PUBLIC À COMMENTAIRES**

Ces scenarios sont des archétypes des orientations les plus fréquemment rencontrées. Ils nécessitent une adaptation à chaque situation. Cependant, ces plans-types ont l'atout de proposer des exemples opérationnels de pilotage et de mise en œuvre de la remédiation.

Ménagez-vous et ménagez vos équipes. La remédiation est un marathon qui peut s'étendre sur plusieurs mois. Tous les efforts des équipes ne peuvent pas transformer des mois en jours et un rythme exceptionnel n'est pas soutenable durablement. Gérez la durée dès le début : la capacité à soutenir le plan d'action dans la durée est plus importante que son rythme d'exécution.

Pour des éléments complémentaires davantage focalisés sur la gestion de crise cyber, vous pouvez vous référer aux bonnes pratiques et aux recommandations issues du guide *Crises d'origine cyber, les clés d'une gestion opérationnelle et stratégique*. Il est à noter qu'**un projet de remédiation sans investigation de l'incident risque de ne pas être pertinent**[2]**.**

2. Voir Partie II - Exécution de la remédiation, section 6. La prise en compte de l'adversaire.

TABLE DES MATIÈRES

SI VOUS ÊTES AU CŒUR D'UN INCIDENT 1
INTRODUCTION 7

1 – OBJECTIFS DU DOCUMENT 8

2 – DESTINATAIRES DU DOCUMENT 10

3 – ORGANISATION DU DOCUMENT 10

PARTIE I – ÉLABORATION DU PLAN DE REMÉDIATION 12

1 – DÉFINITIONS : LA REMÉDIATION ET LA SÉQUENCE « E3R » 14

2 – STRUCTURATION DU PLAN AUTOUR D'OBJECTIFS STRATÉGIQUES 16
- a. Contrôle et validation du plan de remédiation 16
- b. Structuration du plan de remédiation 17
- c. Identification des objectifs stratégiques 18

3 – DÉCLINAISON DES OBJECTIFS STRATÉGIQUES EN OBJECTIFS OPÉRATIONNELS DE REMÉDIATION 20
- a. Principes 20
- b. Nature des objectifs opérationnels 21
- c. Élaboration des objectifs opérationnels 22
- d. Considérations métier 28

PARTIE II – EXÉCUTION DU PLAN DE REMÉDIATION 30

1 – LA REMÉDIATION DANS LA GESTION D'INCIDENT 31

2 – PHASES DE LA REMÉDIATION 33
- a. Phase d'endiguement 33
- b. Phase d'éviction 35
- c. Phase d'éradication 38
- d. Stratégie de reconstruction 42

V.0.0 – APPEL PUBLIC À COMMENTAIRES

3 – PILOTER LA REMÉDIATION 42
- a. Responsabilités 43
- b. Communication 43

4 – SORTIE DE LA REMÉDIATION 45
- a. Définition des conditions de sortie 45
- b. Temporalité de la sortie 46
- c. Le risque de démobilisation précoce 47
- d. Après la fin de la remédiation 48
- e. Problèmes courants du redémarrage métier 48

5 – LOGISTIQUE DE LA REMÉDIATION 51
- a. Limites des capacités internes 51
- b. Traitement du matériel informatique dans la remédiation 52
- c. Identification des besoins 53
- d. Planification des moyens dans la durée 54
- e. Mobiliser les aides extérieures 54

6 – LA PRISE EN COMPTE DE L'ADVERSAIRE 56
- a. Le besoin de compréhension de l'attaque pour la remédiation 57
- b. Les sources de connaissance externe 63
- c. La sélection des mesures de sécurité et de supervision 64

PARTIE III – LES PRESTATAIRES DANS LA REMÉDIATION 70

1 – LA FORMULATION DES BESOINS 71

2 – LA SÉLECTION DES PRESTATAIRES 72

3 – LE PILOTAGE DE LA PRESTATION 73

4 – LA FIN DE PRESTATION 75

PARTIE IV – PLANS TYPES 76

1 – « RESTAURER AU PLUS VITE DES SERVICES VITAUX » 77
- a. Description 77
- b. Objectif stratégique 77

c. Objectifs opérationnels 78
d. Déroulement 78
e. Risques résiduels 79

2 – « REPRENDRE LE CONTRÔLE DU SI » 80
a. Description 80
b. Objectif stratégique 80
c. Objectifs opérationnels 80
d. Déroulement 80
e. Risques résiduels 81

3 – « SAISIR L'OPPORTUNITÉ POUR PRÉPARER UNE MAÎTRISE DURABLE DU SI » 81
a. Description 81
b. Objectif stratégique 82
c. Objectifs opérationnels 82
d. Déroulement 82
e. Risques résiduels 83

ANNEXES 84

A – STRUCTURE DU CORPUS DOCUMENTAIRE 85

B – GLOSSAIRE 86

INTRODUCTION

1 OBJECTIFS DU DOCUMENT

Cette publication propose un cadre conceptuel aux opérations de remédiation qui succèdent aux incidents majeurs[3] de sécurité informatique portant atteinte à l'intégrité du système d'information. La remédiation telle que considérée dans le présent document est la **reprise de contrôle d'un système d'information compromis** lors d'un tel incident.

Ce document s'inscrit dans le corpus documentaire[4] de l'ANSSI consacré à la remédiation et y constitue une référence médiane entre le volet stratégique destiné aux dirigeants et les documents du volet technique détaillant l'exécution des opérations de remédiation. Plus précisément, ce document est destiné à **assister la conception et le déroulement du projet de remédiation au niveau opérationnel.**

⚠ **Attention :** Ce document ne permet pas de saisir toutes les dimensions de la gestion de l'incident. Il est consacré à la réalisation du projet de remédiation au sein du traitement d'un incident de sécurité. Cette activité vient compléter la gestion de crise[5], la communication de crise et l'investigation[6]. Le lecteur est invité à se référer aux publications de l'ANSSI relatives à ces activités pour des recommandations sur leur mise en place[7]. Ce document vise à donner des clés d'organisation et de décision dans un temps chaud, mais il ne se substitue pas aux guides techniques de l'ANSSI, qui seuls donnent une vision en profondeur des sujets abordés.

3. Voir la définition dans le glossaire en annexe.
4. Voir l'annexe A « Structure du corpus documentaire ».
5. Voir la définition dans le glossaire en annexe.
6. *Idem.*
7. Pour en savoir plus, consultez le guide de l'ANSSI : *Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique*.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

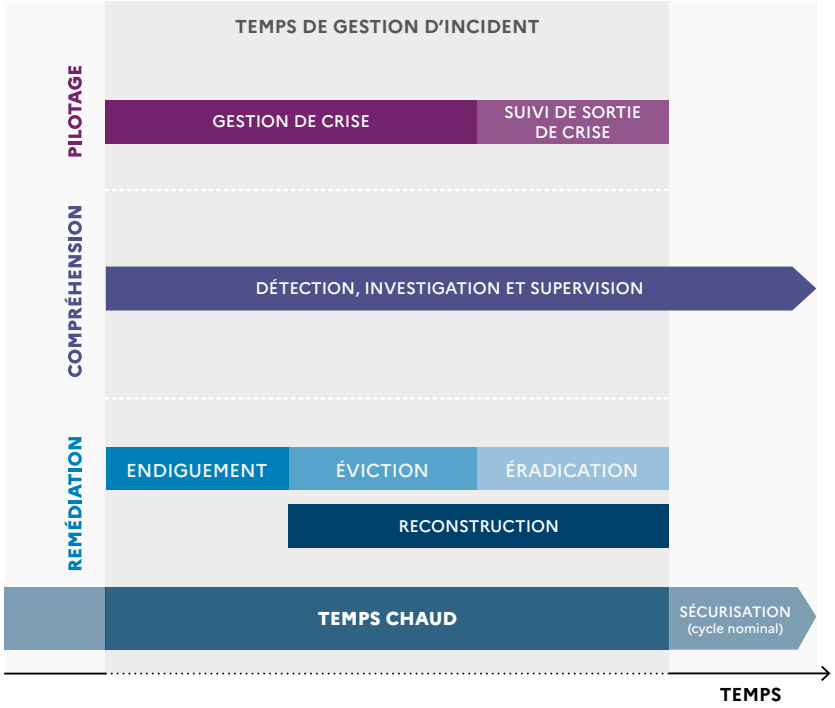


Figure 1 - La remédiation dans le contexte de l'incident

La remédiation est une action exceptionnelle. Elle s'inscrit dans un temps de rupture par rapport au cycle normal d'amélioration continue de la sécurité du système d'information et suppose que celui-ci reprenne dès la sortie de l'incident. La remédiation telle que considérée dans ce document correspond aux activités décrites au chapitre 11 de la norme ISO 27035 « *Incident containment, eradication and recovery operations* »[8].

8. Norme ISO/IEC 27035 : 2011, https://www.iso.org/standard/44379.html

Ce document n'est pas un référentiel fixant un processus à suivre impérativement ou des catégories de prestataires prédéterminés à même de soutenir la remédiation. Au contraire, il tente de présenter les options que chaque responsable pourra mettre en œuvre selon la spécificité de son cas.

2 DESTINATAIRES DU DOCUMENT

Ce document s'adresse aux responsables amenés à piloter les opérations de remédiation consécutives à un incident de sécurité des systèmes d'information. Il est également destiné à leurs interlocuteurs consultants et prestataires de services intervenant dans les opérations de remédiation. Il doit permettre aux pilotes opérationnels de se faire les relais des enjeux de la remédiation auprès des dirigeants et du COMEX de leur organisation.

3 ORGANISATION DU DOCUMENT

Ce document est structuré en quatre parties :

PARTIE I - ÉLABORATION DU PLAN DE REMÉDIATION

Cette section est le cœur du document. Elle propose une démarche de structuration du plan de remédiation autour des objectifs de niveau décisionnel, et un découpage des objectifs opérationnels.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

PARTIE II - EXÉCUTION DE LA REMÉDIATION

Ce chapitre propose un parcours des points sensibles en termes de sécurité informatique à prendre en compte lors d'opérations de remédiation sur les parties les plus couramment rencontrées dans les systèmes d'information actuels. Ce survol se veut une introduction pour les guides techniques relatifs à ces parties publiés séparément.

PARTIE III - PRESTATIONS DE REMÉDIATION

Cette section apporte un soutien dans la sélection et le pilotage des prestations contribuant aux opérations de remédiation, ainsi que dans la formulation des appels d'offre et des étapes clés de la réalisation.

PARTIE IV - PLANS TYPES

La déclinaison opérationnelle de trois scénarios décisionnels types est proposée dans ce chapitre. Ces plans proposent un modèle d'articulation entre les niveaux décisionnel, opérationnel et technique.

PARTIE I

ÉLABORATION DU PLAN DE REMÉDIATION

La réussite d'une remédiation nécessite de concevoir et de dérouler un plan. La formalisation du plan de remédiation est d'autant plus importante que cette activité commence dans le feu de l'incident et peut s'étendre longtemps après celui-ci[9]. Suivant la phase de remédiation, un plan d'action de sécurisation dans la durée doit la prolonger et reprendre un cycle d'amélioration continue de la sécurité du SI.

Le plan de remédiation est donc découpé en un ou plusieurs objectifs stratégiques. Chacun de ces objectifs est décliné en objectifs opérationnels. L'atteinte des objectifs opérationnels nécessitera l'exécution d'un sous-projet.

Il est crucial de séquencer les objectifs de tous niveaux et de les classer par priorité pour gérer cette exécution dans la durée. En effet, les rythmes, les acteurs et les moyens d'exécution de ce plan varient, non seulement suivant la phase de son avancement, mais aussi en fonction du niveau de préparation de l'organisation, et de la maîtrise du système avant l'incident.

Si la remédiation est une activité de nature technique, c'est bien le risque sur le métier qui doit l'orienter. La gravité de l'incident est caractérisée par l'ampleur de ses impacts sur les métiers. Si la perturbation ou la menace sur le métier est vitale, cet incident peut être qualifié de crise.

Dès lors, le plan de remédiation s'accomplit en coopération avec la plupart des acteurs de l'organisation. Les incidents majeurs et les crises nécessitent la mise en place de cellules de gestion dédiées et temporaires. Le travail dans un mode exceptionnel est coûteux. Les ressources de l'organisation sont mobilisées au détriment des activités de long terme, ce qui interrompt les cycles d'amélioration continue de la qualité et de la sécurité. La sortie de ce mode doit donc se faire le plus tôt possible, et généralement avant le terme des activités de

9. Il faut néanmoins distinguer le moment où le plan de remédiation se termine pour retourner sur des activités « normales » de durcissement du système d'information. Le point de commutation entre les deux étapes est généralement atteint quand les activités techniques peuvent s'effectuer avec un niveau de précaution normal vis-à-vis de la présence adverse sur les systèmes et les réseaux.

remédiation[10], afin d'assurer une transition vers les actions de sécurité de long terme et un retour à la normale.

1 DÉFINITIONS : LA REMÉDIATION ET LA SÉQUENCE « E3R »

La remédiation est définie comme le projet de reprise de contrôle d'un système d'information compromis. Elle débute avec l'identification de l'incident et ne se termine que quand les objectifs stratégiques ont été atteints, ce qui consiste généralement au rétablissement des services et à l'éviction de l'adversaire.

Il est possible de résumer les étapes d'un projet de remédiation suivant l'acronyme « E3R », une séquence des trois « E » accompagnée d'actions de reconstruction.

1. ENDIGUEMENT : Freiner l'attaquant au sein du système d'information, en introduisant de la friction dans son activité afin de donner du temps et de la visibilité aux défenseurs.

2. ÉVICTION : Éliminer durablement l'adversaire du cœur de confiance, depuis lequel le reste du système d'information est géré.

3. ÉRADICATION : Nettoyer le système d'information de toute emprise, même mineure, de l'attaquant.

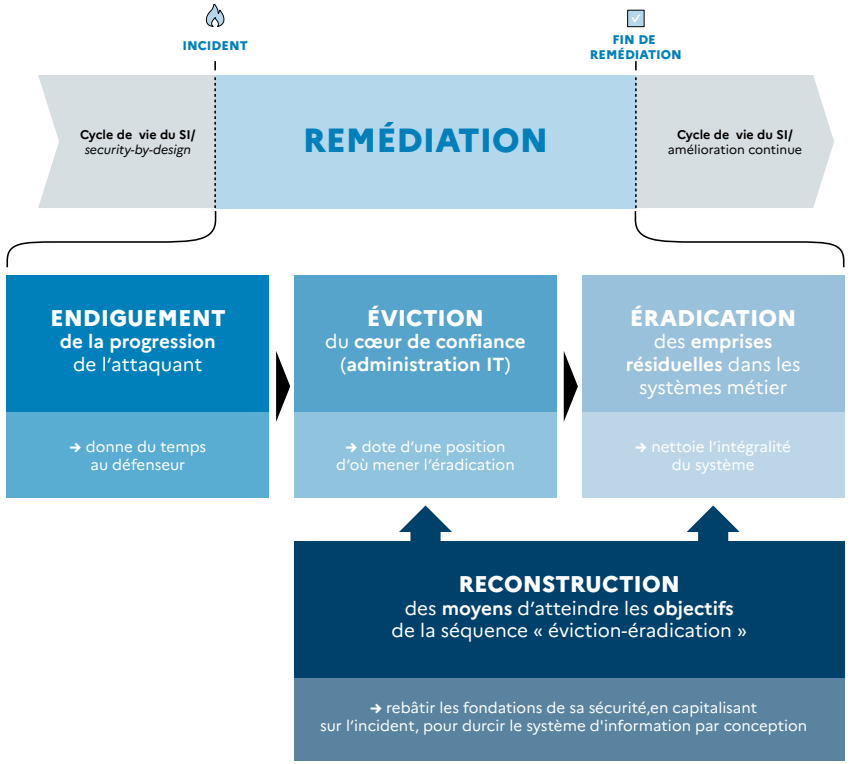
RECONSTRUCTION : Cette activité, dont l'objectif est la remise en fonction et en condition de sécurité des services informatiques sous la forme d'un cœur de confiance, est parallèle aux trois étapes en « E ».

10. Lors d'incidents destructifs, la remise en place de services essentiels se compte en semaines ou en mois. La reconstruction durable d'un système d'information contrôlé prend des mois, et souvent plus d'un an.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

En réponse à une attaque destructrice (sabotage, rançongiciel), elle est un objectif majeur de la remédiation. Dans les intrusions à visée d'espionnage, la reconstruction est plutôt un moyen au service des activités d'éviction et d'éradication. La reconstruction commence dès l'éviction et peut s'étendre durant toute la phase d'éradication. À terme, les activités de reconstruction devraient se poursuivre au travers du cycle normal de sécurisation du système d'information.

Le bon accomplissement de la séquence E3R vise à doter les défenseurs d'un système d'information maîtrisé, sur lequel les tentatives de retour de l'attaquant sont détectées et neutralisées. Le séquencement des actions est organisé de manière à minimiser les risques de retour arrière (re-compromission), et à limiter les capacités de nuisance de l'attaquant.



L'éviction est indispensable au projet de remédiation. En recréant un cœur de confiance de SI, sécurisé et exempt de contrôle adverse, elle dote le défenseur d'une position d'où mener l'éradication.

L'échec de cette étape conduit généralement à un cycle de compromission/remédiation qui peut s'étendre sur des mois, voire des années. Ce type de « guérilla numérique » n'est jamais gagnant pour les défenseurs : les équipes s'épuisent et se démoralisent, la DSI est durablement paralysée, et ce au prix d'efforts minimes pour l'attaquant

2 STRUCTURATION DU PLAN AUTOUR D'OBJECTIFS STRATÉGIQUES

a – Contrôle et validation du plan de remédiation

Dans le temps chaud de l'incident, c'est sous le contrôle de structures d'exception que la remédiation commence, à laquelle contribuent les directions métiers, la DSI et la direction chargée de la sécurité. Par la suite, l'organisation normale de l'entité doit reprendre progressivement le pilotage de la remédiation.

La remédiation n'est donc pas juste l'accomplissement d'une suite de tâches techniques isolées. C'est un processus complexe qui inclut une forte part de communication et de coordination, et une sensibilité aux enjeux métier.

En particulier, **la réussite de la remise en œuvre d'un service et d'une fonction se mesure au fait que le métier puisse en valider le fonctionnement attendu**, pas seulement au redémarrage de l'infrastructure.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

b – Structuration du plan de remédiation

Le plan de remédiation est un projet qui décline des objectifs stratégiques en objectifs opérationnels et les objectifs opérationnels en actions techniques.

Par exemple, l'objectif stratégique « verser la paie à la fin du mois » peut se décliner en plusieurs objectifs opérationnels : « restaurer les sauvegardes de l'application RH dans la semaine », « réinstaller l'application RH », « mettre en place des postes pour la saisie des temps », etc. Ensuite, si l'on regarde de plus près, l'objectif opérationnel « restaurer les sauvegardes de l'application RH dans la semaine » peut se décliner en actions techniques telles que « installer un serveur de restauration », « réindexer les bandes de sauvegarde », « restaurer les bandes contenant les données de l'application RH », etc.

NIVEAU	DÉCIDEUR	MISE EN ŒUVRE	DESCRIPTION
Objectif stratégique	Direction de l'organisation	Directions techniques et métier	Objectifs pour l'organisation
Objectif opérationnel	Direction technique et métiers	Direction technique	Objectifs pour les services informatiques
Actions techniques	Responsable de sous-projet	Intervenants techniques	Actions sur le système d'information

La conception du plan de remédiation peut donc être schématisée comme suit :

1. identifier les objectifs stratégiques ;
2. pour chaque objectif stratégique, décliner les objectifs opérationnels ;
3. pour chaque objectif opérationnel, décliner les actions techniques.

c – Identification des objectifs stratégiques

Les objectifs stratégiques sont des choix de la direction de l'organisation connaissant les priorités métier.

Ils sont formulés en termes non techniques et permettent de décliner les objectifs de la remédiation. Ces objectifs doivent être **priorisés** et associés à des **échéances précises**.

Les objectifs stratégiques **doivent être peu nombreux**. Un trop grand nombre d'objectifs différents cause une dispersion des moyens et conduit à l'échec.

Il est parfois tentant de changer des objectifs stratégiques en cours de traitement. Or, ces changements ont un impact catastrophique sur l'organisation de la remédiation. Il convient donc de ne changer de cap que dans des circonstances exceptionnelles.

Peu nombreux, priorisés, inscrits dans le temps, soutenus dans la durée, les objectifs stratégiques sont l'horizon des équipes qui travaillent à les atteindre.

Ces éléments sont indispensables aux décideurs techniques pour piloter leurs actions. L'absence de tels objectifs est un problème majeur. Dans la durée d'un incident, la DSI risque de se retrouver en porte-à-faux vis-à-vis des métiers et de la direction. De plus, le fonctionnement de l'organisation peut être affecté par des priorités mal définies.

Les objectifs stratégiques sont élaborés avec les responsables des processus métier de l'organisation, et validés par la direction de l'organisation. Il peut être utile de s'appuyer sur les études de risques, de continuité ou de reprise d'activité préexistantes pour les identifier[11].

11. En particulier l'identification d'actifs primordiaux en analyse de risque ou les Analyses d'Impact sur l'Activité (BIA – Business Impact Analysis) en continuité, qui ont normalement déjà effectué le travail de priorisation des actifs.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

Exemples d'objectifs stratégiques :

- « Payer les salaires à la fin du mois. »
- « Rouvrir les accès partenaires en sécurité sous deux mois. »
- « Redémarrer des livraisons sous quinze jours. »

Le présent document propose, dans la partie IV, trois scénarios types avec des priorités stratégiques différentes. Celles-ci vont se décliner en objectifs spécifiques à chaque organisation :

Scénario 1 : « Restaurer au plus vite des services vitaux ».

Il désigne le rétablissement prioritaire des services avec une sécurisation réduite au strict minimum pour redémarrer le cœur de service. Dans ce cas, le reste du système d'information est momentanément sacrifié. Ce scénario n'est à privilégier qu'en cas d'extrême urgence : mise en péril de la survie de l'organisation, menace immédiate des intérêts vitaux de la nation ou risque sur les personnes.

Scénario 2 : « Reprendre le contrôle du SI ».

Il désigne un retour protégé à l'état antérieur du système d'information avant la compromission. Ce scénario se caractérise par un investissement moyen sur la sortie de temps, mais la diminution durable des risques est reportée intégralement sur l'amélioration continue.

Scénario 3 : « Saisir l'opportunité pour préparer une maîtrise durable du SI ».

Il désigne une remédiation consistant en un pivot vers une sécurisation durable du système d'information. Cette approche mise sur un investissement plus important lors de l'incident pour réformer les architectures et les pratiques avant le retour à la normale et redémarrer sur une organisation durablement contrôlée.

Chacun de ces scénarios illustre des arbitrages distincts dont chaque organisation doit peser les facteurs et se les approprier. Ces trois approches ne sont qu'illustratives et il convient d'adapter les objectifs du plan de remédiation aux priorités de l'organisation.

Dans le cas d'incidents destructeurs, les activités de remédiation peuvent s'appuyer sur les Plans de Continuité d'Activité (PCA) et les Plans de Reprise d'Activité (PRA), en particulier dans l'analyse des priorités métier. Le PCA commence dès la phase d'endiguement et le PRA peut correspondre aux activités d'éviction et d'éradication. Idéalement, la remédiation s'inscrit dans l'exécution des PCA et PRA.

En revanche, la plupart de ces plans ne sont pas encore prévus pour des cas de malveillance informatique à large échelle. Il convient donc de considérer avec prudence l'usage des procédures sur un système compromis et de les amender pour tenir compte de l'adversaire.

3 DÉCLINAISON DES OBJECTIFS STRATÉGIQUES EN OBJECTIFS OPÉRATIONNELS DE REMÉDIATION

a – Principes

La réalisation des objectifs opérationnels vise à atteindre les objectifs stratégiques.

Ce principe permet de sélectionner et de prioriser les objectifs opérationnels : la priorité des objectifs stratégiques se reportera sur les objectifs opérationnels à leur service.

Dans un projet de remédiation, chaque objectif opérationnel peut être considéré comme un sous-projet, avec ses propres échéances et ses propres moyens.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Tableau 1 - Exemples de déclinaisons d'objectifs

OBJECTIF STRATÉGIQUE	OBJECTIF OPÉRATIONNEL
Être capable de payer les salaires dès le mois courant.	▪ Réinstallation du logiciel de paie sous une semaine. ▪ Réinstallation d'une plateforme de restauration dans la semaine. ▪ Réindexation des bandes de sauvegarde sous dix jours. ▪ Restauration des dernières données saines de l'application de gestion de paies avant la dernière semaine du mois.
Rouvrir les accès partenaires.	▪ Passage en authentification multi-facteur sur tous les accès à distance d'ici deux semaines. ▪ Mise en place d'une supervision de circonstance renforcée. ▪ Ouverture sélective de flux dans les pares-feux.

b – Nature des objectifs opérationnels

La plupart des objectifs opérationnels sont orientés vers la mise en œuvre de mesures de sécurité. Dans ce cas, l'effet dans la durée de leur réalisation est un aspect important à prendre en compte pour décider des objectifs opérationnels à mener. Par exemple, les compétences nécessaires à la maintenance de nouveaux équipements de sécurité doivent être identifiées.

Néanmoins, certains objectifs sont d'une autre nature et ne concernent pas directement la sécurisation. Par exemple, des actions telles la mise à jour d'une cartographie des services ou la restauration d'une sauvegarde correspondent à des objectifs opérationnels sans être des mesures de sécurité.

Les initiatives qui ne servent pas d'objectif stratégique ne sont pas des objectifs opérationnels de remédiation. Il est fréquent dans une remédiation que de telles actions soient poussées parce qu'elles préexistaient, ou par volonté de bien faire. Dans un temps chaud de gestion d'un incident majeur, les ressources, en particulier humaines sont sous tension. Les actions qui ne servent pas les objectifs du plan de remédiation vont donc en détourner de précieuses ressources. Il est recommandé de revoir régulièrement les listes d'actions pour en expurger celles qui ne servent pas le plan stratégique.

c – Élaboration des objectifs opérationnels

CHOIX DES OBJECTIFS OPÉRATIONNELS

Le choix des objectifs opérationnels doit se faire suivant plusieurs axes :

- effet sur l'avancement en direction d'un ou de plusieurs objectifs stratégiques ;
- complexité et coût de mise en œuvre ;
- capacité à être maintenus dans la durée.

Idéalement un bon objectif opérationnel devrait avancer significativement en direction d'un objectif stratégique. Il devrait être aussi d'un coût supportable. Enfin, dans la mesure du possible, il devrait être pérenne de manière à pouvoir être repris dans le cadre du cycle de plan d'amélioration continue post-incident. Néanmoins, dans la plupart des cas, un arbitrage entre ces axes est nécessaire.

Les objectifs opérationnels doivent répondre aux critères S.M.A.R.T :

Spécifique : l'objectif doit être défini sans ambiguïté et compris de manière identique entre toutes les parties.

Mesurable : il doit être possible de déterminer si l'objectif est atteint ou pas.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

Accepté : toutes les parties prenantes doivent adhérer à l'objectif. En particulier, il est nécessaire que les différentes directions impliquées soient en accord.

Réaliste : l'objectif doit être réalisable dans le temps de la crise et avec les moyens réellement disponibles.

Limité dans le Temps : l'objectif doit être borné en durée.

En substance, la définition d'objectifs opérationnels de remédiation relève d'une gestion de projet dans un cadre particulièrement contraint par le temps et les moyens. Toutes les bonnes pratiques classiques en la matière s'appliquent.

Les circonstances d'une gestion d'incident sont sujettes à de nombreux aléas et les opérations s'effectuent dans un contexte d'incertitude forte. Il n'est pas rare que la réalisation d'un objectif opérationnel se heurte à un obstacle imprévu. Dans ce cas, il faut que le dispositif de gestion soit attentif à l'avancement, à ses freins et reste souple dans l'adaptation, voire la redéfinition des objectifs. Afin de fournir cette flexibilité, le suivi des activités de remédiation doit être effectué finement et en permanence par la direction de l'entité.

ÉCUEILS À ÉVITER DANS LA DÉFINITION DES OBJECTIFS OPÉRATIONNELS

Au plus haut de l'intensité d'un incident, il arrive de confondre vitesse et précipitation. Or, la définition des objectifs opérationnels est déterminante pour la réussite des objectifs stratégiques.

La liste ci-dessous n'est évidemment pas exhaustive, mais elle propose un certain nombre de cas notables.

Tableau 2 - Exemples de problèmes d'objectifs opérationnels souvent rencontrés

ÉCUEIL	DESCRIPTION
Miser sur la mise en place de la solution de sécurité « miracle ».	Cet écueil est particulièrement fréquent. Bien que souvent nécessaire, la mise en place d'une solution de sécurité (ex. EDR) ne peut en soi suffire à sortir de l'incident. Elle ne devrait pas monopoliser tous les moyens et l'attention.
La définition d'objectifs irréalistes.	Les décisions prises dans le traitement d'un incident sont souvent marquées par une volonté d'empêcher la récidive de façon définitive. Il est alors tentant de fixer des objectifs excessivement élevés et de s'épuiser à tenter de les atteindre. Il est conseillé de s'appuyer sur les experts[12] bénéficiant d'une expérience de ce type de situation et de privilégier des objectifs conservateurs.
Définir des objectifs à partir de ce qu'on sait faire plutôt que ce qui est nécessaire.	Dans le stress d'une crise, il est naturel de se reposer sur les procédures et les pratiques existantes. Cependant, les actions de remédiation doivent être guidées par des objectifs plutôt que par des habitudes. Ainsi, les DSI, qui sont censées mettre en œuvre, lors d'une remédiation, le durcissement des accès dans l'Active Directory ou la configuration des politiques d'audit, peuvent avoir tendance à poursuivre l'exécution de leurs tâches de routine, telle la gestion des EDR et du réseau.
Éparpillement des objectifs.	Faute d'un plan centralisé et priorisé, chaque équipe peut avoir tendance à accomplir des actions simultanées sans coordination mutuelle. Il en résulte des défauts de couverture, des problèmes d'ordonnancement et de synchronisation, ainsi qu'une incapacité à finaliser les actions, faute de concentration des moyens. Ce type de problème peut être aggravé par un manque de communication entre équipes en temps normal et l'intervention exceptionnelle de personnel externe à l'organisation. Le pilotage de la remédiation porte un travail de coordination des objectifs et d'actions techniques dès leur définition afin de minimiser ce risque.
Viser des actions techniques trop complexes.	En temps normal, la définition des échéances d'un projet informatique est souvent difficile. Dans le feu d'un incident, cela l'est doublement. Les équipes tendent à surestimer la capacité à accomplir des actions complexes dans un environnement dégradé et sont susceptibles de se retrouver bloquées dans leur réalisation. Il est nécessaire de privilégier les actions les plus simples et les plus précises possibles, y compris lorsqu'il semble possible de les complexifier.

12. Voir Partie III – Les prestataires dans la remédiation.

Garder des objectifs inflexibles face à un obstacle.	La réalisation des objectifs doit être suivie attentivement afin de détecter les actions bloquées. Les blocages peuvent avoir des sources diverses : inter-blocage entre sous-projets, inadéquation des choix face à la réalité du système d'information, problème d'implémentation avec une technologie, manque de compétence ou de disponibilité d'un personnel clé, actions de l'attaquant, découverte d'éléments nouveaux sur le système d'information ou sur l'attaque. Il est normal d'abandonner ou de redéfinir des actions en cours de remédiation. Les pilotes et les exécutants doivent également y être sensibilisés afin d'être capables de se coordonner autour de ces problématiques.
Faire porter des objectifs durables exclusivement par des équipes temporaires.	Certaines actions nécessitent des expertises précises : durcissement Active Directory, mise en place de segmentation réseau, configuration de politique d'audit… Ces mesures ont besoin de vivre dans le temps. Si une passation entre les équipes intervenant en urgence et celles qui doivent les porter dans la durée n'est pas prévue, le niveau de sécurité tend à chuter dès la fin de la remédiation, parfois très rapidement.
Valider les réouvertures de service en termes purement techniques.	Les porteurs d'actions techniques ne sont que rarement en mesure de vérifier qu'un processus métier est possible de bout en bout. Le problème est exacerbé par l'intervention d'informaticiens externes pendant un incident qui ont une faible connaissance du métier de l'organisation. Il arrive alors que l'équipe technique considère que les services soient repassés dans un état nominal alors que les métiers ne peuvent toujours pas travailler. Une validation par les directions métiers du bon redémarrage d'une fonction permet d'éviter un tel écueil. Cette étape doit être prévue dès la planification des objectifs opérationnels.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Faire reposer des objectifs concurrents sur des ressources limitées.	L'atteinte de plusieurs objectifs opérationnels concurrents peut reposer sur un groupe de personnes limité ou des outils informatiques ayant une capacité de traitement limitée. Dans ce cas, il conviendra d'identifier précocement ces points pour prioriser la réalisation de ces objectifs et éventuellement identifier des alternatives. Par exemple, les besoins de restauration peuvent être importants et sont limités en débit. Il peut donc être opportun de cibler uniquement la partie applicative ou les données, et les appliquer sur des systèmes neufs, ou commencer l'activité avec une base de données vierge.
Restreindre ses options à des options seulement techniques ou pérennes.	L'atteinte d'objectifs stratégiques à très court terme requiert généralement de mettre en place des solutions temporaires, tels une bulle métier isolée, un système de coursier interne ou un plan de communication papier. Ces options ne doivent pas être oubliées, même si elles ont vocation à disparaître après le traitement de l'incident.

d – Considérations métier

Au-delà des ressources de la DSI, la mise en œuvre d'un plan de remédiation contribuant à la gestion d'un incident majeur de sécurité informatique affecte également les métiers de l'entité. Si l'incident perturbe directement la capacité de production (rançongiciel par exemple), les opérations de remédiation sont même susceptibles d'interrompre tout ou partie de l'activité des métiers. Ces derniers sont généralement les seuls à pouvoir indiquer les conséquences des changements techniques ou organisationnels sur leur capacité à travailler, ainsi que le caractère prioritaire de la reprise de leur activité. Ils doivent donc être inclus dans l'organisation et le suivi de la remédiation. Si une gestion de crise est mise en place, celle-ci prend généralement en charge l'organisation de la communication interne. Pour le responsable de la remédiation, un certain nombre de motifs imposent des échanges étroits avec les métiers :

→ **Identifier les impacts et les priorités métier :** Travailler avec les responsables des activités pour identifier les actifs à protéger prioritairement et pour déterminer l'ordre de redémarrage des processus. Ces priorités sont définies en fonction de leur importance pour l'exécution des processus métier. Ces informations orientent la stratégie.

→ **Partager les objectifs :** Les objectifs opérationnels du plan de remédiation sont publiés dans des synthèses d'information et d'arbitrages. Les responsables des métiers doivent être informés de ces choix afin de pouvoir s'y adapter au mieux, voire de faire corriger des erreurs avant l'exécution des actions.

→ **Impliquer les métiers dans le rythme de la reconstruction :** Pendant toute la durée d'un incident majeur, les métiers peuvent subir des perturbations fortes. La remédiation devrait prévoir d'assister à résoudre les problèmes les plus prioritaires par des solutions ad hoc de manière à minimiser l'impact de ces perturbations.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

→ **Valider et coordonner la reprise :** À un moment, les services des principaux métiers vont pouvoir reprendre dans un environnement sécurisé. Cette reprise doit se faire après validation par les métiers du bon fonctionnement de leurs outils. Elle doit être planifiée, de manière à ce que les aspects humains, commerciaux et logistiques soient gérés en accord avec ce que permet le calendrier de la remédiation.

PARTIE II

EXÉCUTION DU PLAN DE REMÉDIATION

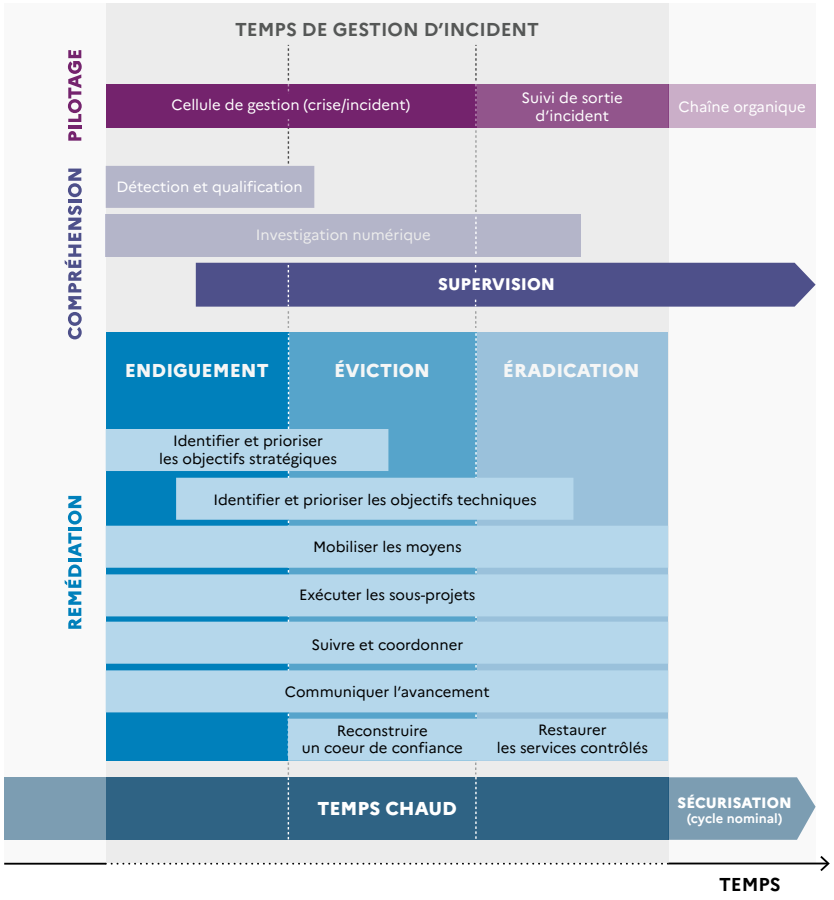
1 LA REMÉDIATION DANS LA GESTION D'INCIDENT

La remédiation ne s'exécute pas dans un contexte isolé. Le projet de remédiation s'inscrit dans une organisation de réponse à incident ou de gestion de crise, dont l'avancement est rythmé par des instances de pilotage et des temporalités parfois distinctes.

Néanmoins, le fonctionnement dans un mode exceptionnel est couteux et complexe à tenir dans la durée. Les dernières étapes de la remédiation s'exécutent alors généralement sous le contrôle de la DSI et des directions métiers ordinaires.

La bonne articulation de ces composantes, et leur inscription dans une séquence complexe nécessite une bonne vision de l'avancement des différents traitements, mais aussi une communication importante entre les intervenants.

Figure 2 - Articulation de la gestion d'incident et de la remédiation



V.0.0 – APPEL PUBLIC
À COMMENTAIRES

2 PHASES DE LA REMÉDIATION

Le projet de remédiation est séquencé en trois phases successives : l'endiguement, l'éviction et l'éradication. Il convient de ne pas traiter hâtivement l'une de ces étapes : échouer à une étape compromet généralement la suivante et force à reprendre tout ou partie des étapes antérieures.

a – Phase d'endiguement

Très tôt dans un incident, il est possible de prendre des mesures qui limitent la liberté de l'attaquant. Ces mesures n'ont pas vocation à expulser durablement l'intrus, mais à limiter l'impact de l'incident, tout du moins d'en limiter l'aggravation, tout en donnant du temps aux défenseurs pour s'organiser et reprendre l'initiative.

OBJECTIFS DE L'ENDIGUEMENT

→ **Préserver les traces :**

- en sauvegardant les éléments de preuve utiles à la compréhension de l'incident.

→ **Limiter l'extension des dommages :**

- en empêchant l'adversaire de détruire des traces ;
- en limitant l'extension d'un chiffrement ou d'une destruction d'information ;
- en empêchant l'extension de l'attaque à d'autres systèmes.

→ **Limiter les impacts métiers :**

- en mettant hors de portée de l'attaquant des services ou des données du système compromis ;
- en protégeant des informations sensibles ou nécessaires à la reconstruction du système.

→ **Limiter la liberté de l'attaquant :**

- en limitant les canaux de communication possibles ;
- en isolant les ressources compromises identifiées.

→ **Augmenter la connaissance sur l'attaque :**

- en supervisant les moyens d'attaque identifiés ou probables ;
- en contraignant l'adversaire à utiliser des moyens de communication détectables.

POINTS D'ATTENTION

Les actions sur un système d'information compromis sont une forme de communication vis-à-vis d'adversaires qui peuvent être encore présents. Toute action coercitive peut être perçue par l'adversaire et entraîner une réaction.

Par conséquent, il est nécessaire de sélectionner avec prudence les mesures d'endiguement. Une telle approche permet d'atteindre les objectifs fixés, tout en gardant le plus possible l'attaquant dans le doute quant à la connaissance par les défenseurs de ses moyens et de ses actions.

Lorsque des actions graves imminentes ne sont pas à craindre, il peut être prudent de mettre sous surveillance un moyen de l'attaquant identifié, plutôt que de le désactiver hâtivement et le forcer à utiliser d'autres moyens qui n'ont pas encore été identifiés.

Les mesures d'endiguement sont souvent l'une des causes directes des dysfonctionnements du système d'information. Une traçabilité forte des actions prises (typiquement par une main courante) doit être assurée. Ceci permet de tracer l'origine d'un dysfonctionnement immédiat ou futur. Ces notes visent aussi à ne pas oublier de mettre en place des mesures potentiellement perturbatrices lors du retour à la normale. Aussi, les notes et les mains courantes sont souvent utiles lors des démarches auprès de la justice et des assureurs.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

EXEMPLES D'ACTIONS D'ENDIGUEMENT

- Coupure de l'accès Internet par filtrage sur le pare-feu extérieur.
- Mise en sécurité des sauvegardes par déconnexion du réseau.
- Segmentation du réseau au niveau 2 sur les commutateurs Ethernet.
- Extinction de machines sensibles.
- Sauvegarde d'instantanés de machines virtuelles.
- Désassociation de services avec le Domaine Active Directory.

b – Phase d'éviction

L'éviction vise à recréer une enclave sous contrôle des défenseurs depuis laquelle mener les actions de reconstruction et d'éradication des emprises adverses. Ce cœur de confiance[13] est celui sur lequel est construite la sécurité de tout le système d'information. Si l'opération d'éviction est imparfaite, l'adversaire est susceptible de contourner les mesures mises en place pour compromettre le système une nouvelle fois. La reconstruction d'un cœur de confiance fiable est indispensable pour sécuriser le système, mais ce n'est que le début de la démarche.

Quoique souvent relativement brèves, les opérations d'éviction doivent faire l'objet d'une préparation et d'une précision d'exécution particulières. En cas d'échec de ces actions, la remédiation est à reprendre depuis l'endiguement.

13. Voir la définition dans le glossaire en annexe.

OBJECTIFS DE L'ÉVICTION

- Créer un socle système et réseau hors de portée de l'attaquant.
- Mettre en place des moyens d'administration fiables.
- Concilier le besoin d'assurance sur les éléments importés du système compromis (typiquement les annuaires et une partie des informations d'authentification), et la minimisation des travaux de reconstruction.
- Construire les services d'authentification et de gestion système de confiance sur lesquels appuyer la remise en production du système d'information.

EXEMPLES D'ACTIONS D'ÉVICTION

- Recréation d'une infrastructure de virtualisation.
- Création d'une compartimentation réseau isolant les composants sensibles.
- Bascule d'un annuaire Active Directory compromis à un annuaire sain.
- Mise en place de stations d'administration dédiées et renforcées.

MISE EN ŒUVRE DE L'ÉVICTION

Les opérations d'éviction doivent faire l'objet d'une préparation minutieuse : identification du cœur minimal, architecture de la nouvelle infrastructure, acquisition et installation de serveurs et de postes d'administration, planification des changements d'identifiants.

En revanche, il est recommandé qu'un moment de bascule brutale du système compromis vers un système sain soit planifié. La soudaineté du changement vise à réduire les opportunités pour l'attaquant de

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

compromettre le nouveau cœur de confiance lors de son passage en production.

Suivant le rythme d'un incident, la préparation de ce moment pivot s'étend sur plusieurs jours voire des semaines et l'exécution se fait en quelques heures.

Étant donné que l'éviction touche au cœur de l'infrastructure d'un système d'information, même bien préparée, ses impacts se répercutent sur les services en dehors du périmètre recréé. Des opérations de résolution de problèmes sur le SI liées à l'éviction sont donc à prévoir et peuvent durer plusieurs semaines[14]. Il est impératif d'avoir préparé l'après « bascule » avec les équipes d'administration, qui devront régler les dysfonctionnements induits par ces changements.

POINTS D'ATTENTION

Il peut être tentant de créer un cœur de confiance protégé à travers une accumulation de mesures de sécurité. Cependant, chaque mesure importée dans le cœur de confiance doit être contrôlée depuis celui-ci. Sinon, une telle action constitue potentiellement une source de compromission de la zone de confiance. Par exemple, le déploiement d'un EDR dans un cœur de confiance implique que sa console soit incluse dans cette zone. De même, l'usage de la virtualisation dans le cœur de confiance suppose que l'administration des hyperviseurs y soit incluse. Par ailleurs, la multiplication de mesures se recouvrant imparfaitement n'offre souvent qu'un gain minime en sécurité, pour un coût significatif en complexité de gestion et en performances. L'expérience montre qu'il est préférable de réduire au minimum les éléments inclus dans le cœur de confiance et de gérer la sécurité de celui-ci spécifiquement par rapport à celle du reste du système d'information.

14. Ces impacts sont moindres si le système d'information a été en grande partie détruit. Mais il existe toujours des comptes inclus dans des scripts, des machines mal gérées ou des services éteints et rallumés dans une mauvaise temporalité qui doivent être traités manuellement.

Par ailleurs, il est risqué de tenter des évictions partielles à travers des mesures de nettoyage de systèmes compromis, sans création d'un environnement de confiance. Dans certains cas, rares, cette approche est la seule possible. Cependant, le nettoyage d'un environnement compromis par un adversaire compétent est très difficile, et les cas de re-compromissions ne sont pas rares. Placer la barre haut dans l'éviction vise à éviter des cycles « tentative d'éviction »/« re-compromission », qui épuisent et démoralisent les équipes avec des résultats souvent médiocres. Une stratégie de simple nettoyage du cœur de confiance n'est donc recommandée que si on a une très forte assurance d'avoir identifié tous les points de persistance adverse.

Enfin, il est parfois tentant de recréer l'intégralité d'un système d'information, sans réimporter aucun élément du système compromis. Il est observé que si l'essentiel des fonctions centrales d'un système de taille modérée peuvent assez facilement être reconstituées ainsi, le retour à la normale se heurte rapidement à de nombreux obstacles difficiles à surmonter. Cette approche est particulièrement problématique dans les systèmes d'identité centralisée[15]. Dans cette configuration, les droits appliqués au niveau des ressources réparties dans la totalité du système (fichiers, boîtes aux lettres, accès à des services) dépendent d'identifiants centralisés. Ces identifiants changeant dans une reconstruction depuis zéro, ils devront être adaptés partout. Il est recommandé de n'entreprendre ce type de reconstruction que dans des systèmes de taille limitée ou très maîtrisés.

c – Phase d'éradication

L'éradication est la dernière étape avant le retour à la normale. Lors de cette phase, les défenseurs cherchent à éliminer toute persistance de l'attaquant dans le système d'information. Pour ce faire, ils opèrent depuis le cœur de confiance construit lors de l'éviction.

15. Classiquement, mais pas exclusivement, dans les environnements Microsoft Active Directory.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

En pratique, il n'est jamais possible d'avoir une certitude d'éviction totale. La mise en place d'une supervision de sécurité est nécessaire afin de détecter les tentatives de retour qui n'auraient pas été anticipées.

Sur la plupart des systèmes d'information, l'éradication ne peut pas être conduite brutalement. Le processus est généralement phasé par secteur du SI et le processus ramène progressivement l'intégralité des zones dans un état contrôlé.

OBJECTIFS DE L'ÉRADICATION

- Supprimer les accès de l'adversaire.
- Éliminer les voies de retour possible pour l'attaquant.
- Acquérir une visibilité sur les tentatives de retour.

EXEMPLES D'ACTIONS D'ÉRADICATION

- Déploiement d'un EDR et d'une supervision sur les postes de travail.
- Découpage du SI en sous-systèmes[16] et, pour chacune de ces zones, migration dans une architecture contrôlée avec inspection ou réinstallation des machines.
- Mise en place d'une collecte d'évènements détaillés (Events Windows, Syslog, *traps*) et campagne de recherche de compromission dans les journaux collectés.
- Passage systématique d'outils de recherche de compromission portant des marqueurs associés à l'attaquant.
- Migration des données vers de nouvelles instances des services.

16. Suivant des découpages qui peuvent être : par zone géographique, par métier, par priorité du service porté…

POINTS D'ATTENTION

L'étape d'éradication peut être très longue. Les possibilités de persistance d'un attaquant sur un système d'information sont multiples[17]. La plupart n'en mettent en œuvre qu'un faible nombre mais une éradication ne peut jamais garantir de les avoir toutes découvertes. Il peut être observé que des objectifs trop ambitieux soient abandonnés en cours d'exécution, par épuisement des ressources. Il est donc préférable de viser un niveau d'assurance moindre sur l'exhaustivité de l'éradication, tout en le complétant par des capacités de détection et de réaction.

L'objectif de la remédiation est d'aboutir à un système sur lequel les activités adverses éventuelles sont détectées et neutralisées avant de devenir critiques. Au contraire, son but n'est pas de tendre vers un système étanche.

Il est généralement impossible, à grande échelle, d'obtenir la certitude qu'aucune porte dérobée, aucune faille ni aucun changement de configuration ne sont passés inaperçus. Il est préférable de prioriser les efforts d'éradication sur les points sensibles, de compartimenter le système d'information et d'adapter le niveau d'inspection à la criticité de la zone.

Par ailleurs, lors de l'éradication, il est tentant de se contenter de se focaliser sur les systèmes technologiquement maîtrisés : les postes et les serveurs sous système Windows, voire Linux. Si l'attaquant a compromis le système d'information, il peut avoir compromis des composants moins surveillés[18], tels :

- **Les équipements réseaux :** routeurs, commutateurs, pare-feu, terminateurs VPN.

17. Les persistances peuvent être par l'installation d'implants, par changements de configuration, par modification de droits, par création ou altération de comptes locaux ou transverses…

18. Souvent, ceux-ci contiennent des socles systèmes anciens, des logiciels peu mis à jour, et des mots de passe par défaut. Changer leur configuration peut compromettre la sécurité, mais pour l'attaquant sont simplement des systèmes où personne ne surveille ses actions.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

- **Les systèmes plus rares :** mainframe, mini-ordinateurs, systèmes UNIX moins communs.
- **Les équipements reliés au réseau :** imprimantes, baies de stockage, caméras, téléphonie, automates industriels[19].

Bien qu'il soit rarement possible d'analyser tous ces équipements, l'hypothèse de leur compromission doit être considérée lors de l'éradication. Des mesures d'inspection, d'isolation, de réinstallation, ou de supervision de ces appareils doivent être étudiées.

d – Stratégie de reconstruction

Afin de faciliter l'endiguement et de reconstruire progressivement le SI, deux approches alternatives dominent :

→ Par isolement : le SI est coupé en sous-réseaux isolés entre eux, les services portés par chacun d'eux faisant l'objet d'un assainissement dédié pouvant être effectué de manière distincte. Les flux rouverts entre ces réseaux sont progressifs et très précis. Une telle démarche requiert de connaître finement les flux réseaux applicatifs et d'être en capacité de les identifier rapidement.

→ Par sanctuarisation : un nouveau réseau sain est créé, dans lequel les services assainis sont réinstallés ou réintégrés progressivement. Une telle démarche se heurte généralement à des problématiques liées au changement d'adressage et de configuration réseau codée en dur.

Ces deux démarches engendrent des sollicitations importantes des équipes techniques qui ne doivent pas être négligées et requiert d'avoir validé la confiance dans l'infrastructure réseau[20].

19. Notablement, même hors domaine industriel, les automates de gestion technique bâtimentaire.

20. Les attaquants avancés vont fréquemment s'implanter sur les équipements réseau : routeurs, pare-feu. Une stratégie de remédiation ne doit se reposer sur de tels équipements que si un bon niveau d'assurance quant à leur non compromission est atteint.

3 PILOTER LA REMÉDIATION

Le pilotage de la remédiation est une activité à part entière. Cette tâche s'apparente avant tout à de la gestion de projet et à du suivi d'action.

Ce pilotage est un projet particulier, qui nécessite de nombreux arbitrages et des interactions avec un large spectre de personnes, dans des circonstances contraintes.

En particulier, il convient de distinguer[21] **:**

- la gestion de crise ou d'incident qui organise le niveau stratégique de l'organisation face à l'attaque ;
- le pilotage de l'investigation qui vise à établir l'historique de l'attaque ;
- le pilotage du projet de remédiation, qui consiste à organiser et à suivre la réalisation des actions de remédiation.

Le cumul de ces rôles par une même personne est rarement efficace pour tout incident d'ampleur. Non seulement la charge de travail est généralement excessive pour être portée par un individu, mais les compétences requises pour chacun de ces travaux sont différentes.

a – Responsabilités

Le ou les pilotes de la remédiation sont chargés de l'établissement du plan de remédiation, du suivi de l'exécution des tâches, et de la qualification de leurs changements.

Ils s'appuient sur des experts pour les choix techniques complexes.

21. Le tableau décrivant l'articulation entre la remédiation et les autres activités dans l'incident se trouve dans la partie II - Exécution de la remédiation, section 1. La remédiation dans la gestion d'incident.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Ils présentent et font arbitrer par la direction de crise, ou les porteurs de processus métier, les choix et les modifications de priorités.

Un rôle important du pilotage de la remédiation consiste à surveiller que les plans soient bien suivis, ainsi qu'à s'assurer que les problèmes rencontrés soient bien partagés et, au besoin, arbitrés au plus tôt. En particulier, les nouvelles informations issues de l'investigation doivent être prises en compte dans le pilotage, et parfois amener à surseoir ou à abandonner des actions, voire des objectifs opérationnels.

b – Communication

La communication sur la remédiation s'inscrit dans le cadre plus vaste de la communication de crise[22].

Plusieurs grands destinataires de communication sur la remédiation peuvent être identifiés :

→ **Les décideurs** doivent être informés de l'avancement, des besoins et des problèmes rencontrés, sans être noyés dans les détails. Afin d'éviter les communications trop techniques, et les effets tunnels où le projet n'informe pas sur son avancement, il est prudent de définir un format synthétique de communication fréquemment remis à jour. Les points cruciaux sont : le calendrier de remédiation et ses éventuels délais, ainsi que le suivi des risques liés à chaque étape.

→ **Les équipes** de remédiation doivent bénéficier d'une vision fréquemment mise à jour sur l'avancement du projet et sur les étapes critiques de celui-ci. Plusieurs groupes travaillant en parallèle, il est important de faire redescendre vers toutes les équipes les informations sur l'avancement de chacune. En effet, même lorsque chaque tâche est découpée par équipe, garder une vision d'ensemble pour s'assurer de la cohérence des mesures est essentiel. Il est recommandé de privilégier des équipes pluridisciplinaires plutôt que de spécialistes

22. Pour en savoir plus, consultez le guide de l'ANSSI : *Anticiper et gérer sa communication de crise cyber*.

afin de conserver le contexte des actions lors de leur réalisation. Des documents de suivi d'actions et des points multi-hebdomadaires sont généralement les vecteurs de cette communication.

→ **Les directions métiers** sont affectées en tout ou partie par la remédiation. Elles ne seront pas totalement parties prenantes de certaines étapes de reconstruction technique, mais il convient de leur donner une vision de la remédiation tout au long de son exécution. Les points importants sont le calendrier de la remédiation et les changements dans les processus métier. Une telle communication n'a pas forcément besoin d'être fréquente. En revanche, elle doit être tenue à jour au fur et à mesure des évolutions de l'opération. L'implication des directions métiers ainsi que le partage des réussites et des échecs de la remédiation contribuent grandement au maintien de la cohésion de l'organisation durant l'incident. C'est aussi avec les métiers que les arbitrages complexes sur la reconstitution des fonctions de l'organisation doivent être faits. Cette communication est généralement faite sous forme de points hebdomadaires.

→ **Le reste de l'organisation :** Pour des raisons de sécurité opérationnelle, le détail de la remédiation ne peut généralement être partagé avec l'intégralité de l'organisation. Néanmoins, il est nécessaire d'accompagner les changements induits par la remédiation. Pour ce faire, les principaux messages portent généralement sur la communication de l'existence du projet de sécurisation et surtout sur la préparation et l'accompagnement des mesures de sécurisation. Ces communications sont généralement effectuées par voie de messagerie, mais aussi par la mise en place de documents, de « foires aux questions » et de points de contacts.

→ **Les partenaires extérieurs :** La communication publique n'est pas du ressort de l'équipe de remédiation. En revanche, les changements effectués sur le système d'information se répercutent sur les clients et les fournisseurs. En particulier, la mise en place de mesures de sécurité, telles que l'activation d'authentifications multi-facteurs, requiert des communications particulières à leur destination.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

Il convient donc de synchroniser les messages liés à ces changements avec la communication de crise, afin d'éviter que les messages ne soient désynchronisés par rapport aux faits observables.

4 SORTIE DE LA REMÉDIATION

a – Définition des conditions de sortie

La fin du projet de remédiation est atteinte lorsque **tous les objectifs stratégiques ont été satisfaits**. Le niveau des réalisations attendues doit être fixé de manière réaliste, sous peine d'échec.

L'éradication des emprises adverses sur un système informatique étendu est une tache laborieuse. Le système reprend vie dès le début du rétablissement des services, et de nouvelles contaminations surviennent fréquemment. Les objectifs de l'éradication doivent être ciblés en fonction de la criticité des systèmes ou de la capacité de retour. Il n'est pas réaliste de viser, en dehors des cas les plus simples, une certitude totale d'éradication. En revanche, il est possible d'éliminer les présences sensibles et de traiter les reliquats au fil de l'eau lors de leur détection ultérieure.

Il en est de même pour le rétablissement de services après une attaque destructive. L'attaque aura changé les pratiques, ainsi que l'organisation et les systèmes qui la supportent. Certains services peuvent être définitivement abandonnés ou réformés. Dans certains cas, l'accélération d'un plan de migration est provoquée par l'attaque. Dans les cas les plus extrêmes, le rétablissement de certains services est simplement impossible à cause des données perdues. Il peut être également jugé tout simplement trop couteux vis-à-vis de l'intérêt qu'il présente. La définition des niveaux de service attendus en fin de remédiation est donc cruciale.

Dans l'évaluation de l'atteinte des objectifs, un équilibre doit être recherché entre le niveau attendu et la durée d'engagement dans la remédiation. Ces critères sont normalement explicités dans la définition des objectifs opérationnels. Cependant, ils sont souvent réévalués en cours d'opération. En effet, l'atteinte de ces objectifs, les difficultés associées et les coûts de remédiation de certains sous-systèmes tendent à être mieux identifiés au fil de l'opération. Lorsque les niveaux d'atteinte sont modifiés, ceux-ci doivent être validés par les différents échelons de pilotage et rapidement communiqués aux parties prenantes.

b – Temporalité de la sortie

Si le plan de remédiation est efficace, une première forme de retour à la normalité peut s'effectuer avant la fin de son exécution.

Ce point de sortie de temps chaud est essentiellement caractérisé par une capacité à rendre aux métiers l'essentiel de leurs capacités antérieures à l'incident.

À ce stade, un cœur de confiance autour des actes d'administration permet de s'assurer de la protection des comptes privilégiés. Les principales applications métier sont restaurées dans un environnement plus sécurisé.

Bien qu'il n'y ait quasiment jamais à cette période de reconstitution totale des capacités métier, pour le moment, l'activité vitale de l'organisation est restaurée dans un environnement protégé.

La fin effective de la remédiation peut avoir lieu assez longtemps après ce redémarrage. Les transitions réussies ne le sont que grâce au soutien de la direction. Par conséquent, seule la coordination entre l'équipe de remédiation et les décideurs stratégiques de l'organisation permet de porter l'effort dans la durée.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Pour cela, il est indispensable :

- de continuer à communiquer périodiquement l'avancement de la remédiation avec l'organe décisionnel ;
- d'accompagner les utilisateurs à privilèges (administrateurs, développeurs) dans une transition de leurs pratiques ;
- de faire un retour à l'ensemble de l'organisation sur la remédiation et ses objectifs afin de minimiser le contre-coup de la sortie de crise.

c – Le risque de démobilisation précoce

La sortie de la crise est aussi le moment où l'on démantèle la plupart des dispositifs exceptionnels d'ordre organisationnel et technique.

Néanmoins, cette phase est psychologiquement complexe :

- Dans la crise, une partie conséquente de l'organisation, voire sa totalité, vit au rythme de l'incident.
- En sortie de crise, les équipes impliquées dans la remédiation ont encore un travail conséquent à accomplir, alors que le reste se démobilise.
- Pour les utilisateurs privilégiés du système d'information, c'est aussi un moment critique où la justification des mesures exceptionnelles s'estompe. Les pratiques d'administration sécurisée ne sont généralement pas devenues un réflexe et pèsent sur le travail des usagers.
- Il existe alors un risque d'abandonner la remédiation à mi-chemin et de retourner, par praticité, vers des pratiques d'exploitation non sécurisées.

À ce stade, le coût de l'incident est présent dans tous les esprits, et l'impact d'une rechute généralement bien compris. Mais cette sensibilité peut vite s'émousser dans la reprise d'activité.

d – Après la fin de la remédiation

Comme toutes les activités inclues dans une gestion d'incident, la remédiation doit faire l'objet d'un recueil de retours d'expérience.

Les incidents de sécurité, et les opérations de reconstruction sont des expériences uniques pour mettre en évidence les forces et les faiblesses d'un système d'information et d'une organisation. Ces retours peuvent non seulement aider à la préparation aux éventuels futurs incidents, mais aussi à irriguer les processus d'amélioration de la sécurité dans la durée. Notamment, le retour d'expérience de la remédiation doit aider à établir un plan d'action de sécurisation post-incident.

Une partie considérable des équipes intervenant sur les remédiations sont des spécialistes externes aux organisations victimes des attaques. Il est donc conseillé de procéder à des phases de recueil de retours d'expérience « à chaud » afin d'y inclure des interlocuteurs qui risquent d'être plus tard indisponibles.

Les autres aspects du retour d'expérience sur la remédiation se fondent dans les différentes pratiques pilotées dans le cadre de la gestion de crise ou d'un incident de sécurité.

e – Problèmes courants du redémarrage métier

Un système d'information n'est quasiment jamais redémarré dans son intégralité. Lorsque cela a lieu durant un incident, de nombreux problèmes sont susceptibles d'apparaître. Les conséquences pour les métiers d'une reprise mal gérée peuvent aller d'un délai de reprise excessif à des pertes ou à des corruptions d'information irrécupérables.

Afin de minimiser les risques de ce type de dysfonctionnements, il convient de planifier scrupuleusement l'ordre de redémarrage des services de l'organisation, d'identifier les tests permettant de valider la bonne réalisation de chaque étape et de prévoir des points de « go/no-go » pour l'avancement des opérations de restauration.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Un certain nombre de problèmes sont récurrents lorsque des changements à grande échelle ou des redémarrages de système d'information ont lieu. Ils doivent faire l'objet d'une attention particulière.

Tableau 4 - Problèmes courants lors du redémarrage des services

OBJECTIF STRATÉGIQUE	OBJECTIF OPÉRATIONNEL
Dépendances circulaires.	L'ordonnancement du redémarrage requiert non seulement d'identifier les dépendances techniques (celle d'une application sur sa base de données), mais aussi organisationnelles (par exemple le besoin d'un service d'e-mail pour recevoir des données traitées dans une application).
Remise en production des données antérieures.	La restauration de données applicatives est une opération souvent délicate que les plans ne prévoient pas. Tout d'abord, il faut disposer d'assez d'espace disque pour les stocker souvent au moins deux fois, puisque la copie remise en production nécessite souvent une conversion dans un autre format. Parfois, il est même nécessaire d'être en mesure de stocker plusieurs fois la taille des données, du fait des fichiers temporaires générés pendant un ré-import de masse. En outre, si les données sont sensibles pour le métier ou pour la sécurité du système d'information, le choix de la date à restaurer représente une décision importante, souvent arbitrée au plus haut niveau. Des données trop anciennes perdent de leur valeur et requièrent fréquemment des travaux intensifs de mise à jour. Des données récentes peuvent avoir été piégées par l'attaquant afin de produire un effet néfaste ou de pérenniser ses accès. La connaissance de l'ancienneté de la compromission sera déterminante dans ce choix.

Synchronisation avec les services externes.	Des restaurations ou des interruptions créent un décalage entre deux services. Il est toujours possible que des désynchronisations surviennent. Les plus courantes sont les expirations de données d'identification ou la perte de rotation d'informations cryptographiques. Il arrive aussi que certains services attendent une continuité de séquence chronologique ou numérique, et qu'un saut ou un retour arrière créent des dysfonctionnements. La prévention de ces problèmes nécessite d'identifier les dépendances externes des applications, si besoin de recréer des associations ou des synchronisations. Il peut être nécessaire de forcer certains compteurs, voire de créer des données synthétiques pour combler des écarts.
Reprise des données métier générées pendant la crise.	Suivant la complexité des applications, la réconciliation des données générées pendant la crise avec celles antérieures peut être très complexe. Un incident de sécurité informatique s'étend généralement sur plusieurs semaines, parfois plusieurs mois. En général, des instances des applications critiques sont redémarrées dans des configurations temporaires pour couvrir cette période. Ces applications vont générer des données avant de pouvoir être réintégrées sur une instance reconstruite. Les opérations de fusion peuvent forcer des arbitrages sur des pertes d'information, ou des opérations d'export, de filtrage et de réimport sensibles. Une réflexion préalable sur le sujet est déterminante dans la résolution de ce type de problématiques.

V.0.0 – **APPEL PUBLIC À COMMENTAIRES**

Corruption d'états du fait de redémarrages partiels.	Les redémarrages dans un temps chaud, même bien préparés, échouent fréquemment. Des éléments inconnus sont découverts, des mesures d'endiguement viennent bloquer des communications ou des exécutions ; des scripts enfouis appelés indirectement ont été perdus… Ces incidents peuvent vite devenir bloquants s'ils ne sont pas anticipés. Une procédure de retour à l'état antérieur doit donc être prévue à ce stade de redémarrage, afin de pouvoir corriger le problème et de nettoyer les reliquats de la tentative échouée. Pour chaque étape, une validation des résultats doit être mise en place par le métier.

5 LOGISTIQUE DE LA REMÉDIATION

a – Limites des capacités internes

La remédiation d'un système d'information compromis est un projet lourd.

Les équipes en charge de l'informatique au jour le jour voient leurs priorités changer et sont soumises à une charge de travail importante sur un temps court. Même en abandonnant les tâches courantes, les équipes internes sont rarement en mesure de soutenir un tel surcroît de travail sans aide externe.

Par ailleurs, le travail de remédiation nécessite des expertises particulières : en technologie Active Directory, en configuration d'hyperviseurs, en restauration d'applications complexes. Ces compétences sont rarement toutes disponibles à l'intérieur de l'organisation.

Au contraire, il convient de s'assurer de garder en interne le savoir acquis lors de l'incident et de ne pas s'appuyer exclusivement sur des prestataires externes.

Enfin, la mise en œuvre de moyens exceptionnels nécessite l'acquisition de matériels, de comptes et de licences qui ne sont généralement pas disponibles avant l'incident au sein de l'organisation.

La mobilisation de ressources en début de remédiation est capitale afin de faire face à l'ampleur et à la complexité des tâches. Le financement de la remédiation est dimensionnant et doit être déterminé le plus tôt possible au niveau stratégique.

b – Traitement du matériel informatique dans la remédiation

La restauration d'informations sauvegardées, la création de nouveaux services sécurisés ou leur simple rotation nécessitent du matériel.

Si l'organisation ne dispose pas de stocks de serveurs et de moyens de stockage suffisants, plusieurs approches sont possibles :

- **→ Effectuer une réutilisation par rotation rapide du matériel préexistant** limite les coûts et les délais de livraison du matériel. Néanmoins, cette solution provoque des pertes d'informations et de preuves, voire de données métier. Dans le cas d'attaques avancées, le risque de persistance dans les *firmwares* rend précaire la réutilisation, dans le cœur de confiance, de matériels potentiellement compromis.

- **→ Acquérir par achat, location ou prêt, du nouveau matériel**, permet d'absorber le pic de besoin lors de la remédiation. Il est possible de lisser les coûts dans la durée en redistribuant les équipements après la remédiation. Cette stratégie peut être très efficace, mais elle suppose un budget significatif et un lien fort avec les fournisseurs. Les livraisons doivent se faire dans des délais très courts.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

- **→ Externaliser totalement certaines fonctions chez des prestataires externes** est aussi possible. Une bascule totale ou partielle dans le *cloud* du SI est souvent envisagée lors des remédiations. Mais cette solution constitue généralement un facteur structurant pour l'organisation. Or, le temps chaud laisse peu de place à l'étude du changement de posture en termes de risques et de coûts. Lorsque ce changement est envisagé, ses impacts dans la durée doivent donc être considérés.

Généralement, un panachage de plusieurs de ces options est retenu, souvent en accélérant des projets de refonte déjà envisagés.

c – Identification des besoins

Le surcroît d'activité lors d'un incident important nécessite de mobiliser des moyens externes. Même en bénéficiant d'un afflux temporaire d'aide, les équipes internes vont être fortement sollicitées par les opérations.

Les conséquences de cette mobilisation temporaire doivent également être prises en compte : horaires exceptionnels à compenser, blocages de jours de congé et mise en œuvre de moyens d'accueil (bureaux, connectique, prises électriques, sanitaire, nourriture).

Le pilotage de l'incident ou de la crise nécessite d'anticiper le plus exactement possible ces besoins et ces dépenses associées.

Un rôle clé du pilotage de la remédiation réside donc dans l'identification des ressources nécessaires à chaque étape et le provisionnement de ces moyens. Malheureusement, la disponibilité de moyens humains ou techniques en délais très court est souvent un problème. Les pilotes de remédiation peuvent être amenés à changer entre des plans alternatifs pour remplir leurs objectifs en fonction de cette disponibilité.

d – Planification des moyens dans la durée

Dès le début d'une opération de remédiation, il convient de s'inscrire dans un temps long. Même quand cette durée est considérée, elle est, en pratique, presque toujours sous-estimée.

La prise en compte du temps long implique de mettre en place une gestion durable des ressources humaines mobilisées, mais aussi de prendre en compte cette durée dans le budget alloué aux intervenants externes, quitte à en modérer l'ampleur initiale.

De nombreuses opérations de remédiation tendent à se terminer à une date arbitraire après avoir épuisé la totalité du budget alloué, sans avoir évincé l'attaquant.

Tableau 5 - Échelles de durée des étapes de remédiation

	PRÉPARATION	EXÉCUTION
ENDIGUEMENT	Heures	Jours à semaines
ÉVICTION	Jours à semaines	Heures à jours
ÉRADICATION	Semaines	Semaines à mois
RETOUR À LA NORMALE	Mois à année	

e – Mobiliser les aides extérieures

Évincer un attaquant installé sur un système d'information est un métier différent de l'infogérance en temps normal. Les opérations de remédiation requièrent de s'appuyer sur un panel varié de spécialistes en reconstruction post-incident, d'experts en technologies particulières et de généralistes pour réaliser les nombreuses actions techniques planifiées.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Outre ces intervenants[23], plusieurs entités peuvent assister l'organisation dans la préparation de sa remédiation. Certaines peuvent directement assister au traitement, mais la plupart vont plutôt rediriger vers des prestataires à même d'assister l'organisation.

On peut citer :

- Les CERTs[24] sectoriels, territoriaux, nationaux ou privés peuvent fournir directement une assistance ou indiquer des prestataires compétents.
- Les autorités de tutelles de nombreux secteurs disposent de plus en plus de capacités de suivi des incidents de sécurité informatique et peuvent diriger vers des prestataires adéquats.
- Les assureurs, outre leur rôle de couverture financière, maintiennent souvent des listes de prestataires, voire disposent avec eux de conditions négociées à l'avance.
- Dans les groupes d'entreprises, il n'est pas rare qu'une capacité interne au groupe puisse être sollicitée.
- Dans les ministères, les FSSI[25] peuvent aussi rediriger vers les services à même d'assister au traitement de l'incident.

23. Concernant les prestataires, voir la Partie III – Les prestataires dans la remédiation.
24. *Computer Emergency Response Team.*
25. Fonctionnaires de Sécurité des Systèmes d'Information.

6 LA PRISE EN COMPTE DE L'ADVERSAIRE

Un incident de sécurité informatique diffère d'un incident de production ordinaire. Cet événement implique l'action d'un adversaire actif et hostile. Quelle que soit la motivation de l'intrusion, l'attaquant a des raisons de s'opposer à la remédiation.

Les actions de remédiation doivent s'effectuer en tenant compte de cette présence et s'assurer que l'intrusion ne puisse se reproduire.

Cela implique en particulier :

- de bloquer les chemins de compromission utilisés par l'adversaire ;
- d'éradiquer les moyens d'accès que l'attaquant aurait conservés sur le système d'information ;
- de s'assurer de l'intégrité des systèmes nouveaux ou réinstallés lors de leur acquisition, de leur configuration et de leur mise en œuvre ;
- de protéger les échanges entre intervenants sur la remédiation contre les actions de l'adversaire.

Suivant les cibles, les pratiques et les moyens techniques de l'attaquant, celui-ci peut quitter le système d'information dès l'incident détecté, ou au contraire y rester en s'adaptant activement aux actions des défenseurs. Tout au long de la remédiation, il convient de garder à l'esprit que toute action visible par l'attaquant est une potentielle communication implicite à son égard et peut provoquer une réaction, ou une adaptation.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

a – Le besoin de compréhension de l'attaque pour la remédiation

Suite aux constats de l'intrusion, une investigation sur les actions de l'attaquant doit être diligentée. Le pilotage de la remédiation est informé par les résultats de ces analyses.

Celle-ci peut s'étendre sur plusieurs semaines, mais dès les premiers jours elle peut fournir un certain nombre d'éléments cruciaux : comptes utilisés par l'attaquant, failles exploitées, outils déployés. Le déploiement ou le renforcement de moyens de supervision de sécurité vient donner une vue sur les actions hostiles en cours.

Si l'attaquant est toujours actif sur le système d'information, il est souvent intéressant de l'observer, tant que les risques d'aggravation sont maîtrisés, afin de comprendre ses objectifs et ses moyens.

Au fur et à mesure des progrès de l'investigation, les découvertes peuvent amener à changer les objectifs opérationnels ou à en réévaluer la priorité.

Avec l'avancée du projet de remédiation, la connaissance de l'attaque est de moins en moins nourrie par l'investigation et de plus en plus par les mesures de supervision du système d'information. Au terme de la remédiation, seules restent les mesures de supervision.

POINTS CRUCIAUX POUR LA REMÉDIATION

Pour l'équipe de remédiation, les principales questions techniques à poser à l'équipe d'investigation sont les suivantes :

→ **Question n°1 : Quels moyens l'attaquant a-t-il utilisés pour communiquer lors de l'attaque ?**

La plupart des attaques ne sont pas le fait de codes autonomes[26]. Si l'attaquant pilote les actions à distance, il utilise des moyens de com-

26. À noter aussi que la plupart des codes autonomes rendent également compte de leurs actions via des communications dirigées vers l'extérieur qui sont détectables.

munication et souvent une infrastructure complexes. L'identification des moyens de contrôle de l'attaquant permet de bloquer les canaux de communication et de superviser d'éventuelles tentatives de retour.

Cette connaissance permet de durcir ces canaux vis-à-vis de leur usage par l'attaquant et de positionner les moyens de supervision. La connaissance des communications adverses permet de suivre son activité avant l'éradication et de détecter des persistances oubliées après son terme.

Quand des canaux de communication actifs sont identifiés, le choix de les laisser en place est à étudier. Le blocage des canaux connus informe l'adversaire qu'il est détecté. Cette action peut le pousser à utiliser des chemins que les défenseurs ne connaissent pas. Il peut en résulter une perte de visibilité sur les activités de l'attaquant..

Exemples :

- adresses IP et nom d'hôtes de serveurs[27];
- noms de domaines ;
- protocoles spécifiques ;
- motifs protocolaires[28].

→ Question n°2 : Quels moyens ont été utilisés par l'attaquant pour se déplacer dans le système d'information ?

L'accès initial d'un attaquant lui donne rarement un accès direct à son objectif avec les privilèges dont il a besoin.

Pour accéder aux ressources qui l'intéressent, l'attaquant doit se déplacer au sein du système d'information. Ce mouvement est couramment appelé la latéralisation. L'attaquant va aussi chercher les moyens

27. On parle généralement de serveur de Commande et Contrôle ou C².

28. Par exemple des entêtes HTTP particuliers utilisés par l'attaquant.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

d'acquérir les droits d'accès nécessaires à l'accomplissement de ses objectifs. Ces mouvements et cette acquisition de droits se font en exploitant des vulnérabilités du SI.

La connaissance des moyens utilisés permet de neutraliser ceux qui sont illégitimes et de sécuriser (par supervision, ou par contrôle d'accès renforcé) ceux qui sont légitimes. L'identification d'exploitation de failles permet de définir les priorités de déploiement de correctifs. Ces informations permettent à la supervision de sécurité de détecter les moments où un adversaire revenu au sein du système d'information s'y déplace.

Exemples :

- connexions RDP ou SSH ;
- exécution à distance par PSExec ou WMI ;
- exploitation de failles applicatives ou système ;
- utilisation d'outils d'administration à distance déployés sur le parc ;
- utilisation de comptes légitimes.

→ Question n°3 : Quels sont les moyens de persistance identifiés ?

Dans la plupart des cas, l'attaquant cherche à garder un accès sur le système d'information compromis. Si l'objectif de l'intrus est l'espionnage, la persistance lui permet de revenir ultérieurement chercher davantage d'informations. En revanche, si son but est l'entrave ou le sabotage criminel, l'attaquant cherche à rester dans le SI afin d'observer la façon dont se déroule la réponse à incident. Des cas où les attaquants sabotent la remédiation ont déjà été observés, de même que des re-chiffrements de victimes de rançongiciels.

Pour maintenir leurs accès, les attaquants modifient les configurations de sécurité, ou déploient des outils, plus ou moins furtifs, permettant de reprendre pied après une éviction.

Ces moyens de persistance vont être recherchés et neutralisés systématiquement lors de la phase d'éradication. Leur connaissance permet à la supervision de sécurité de détecter les tentatives de retour de l'attaquant.

Exemples :

- usurpation[29] de comptes, préexistants, créés, voire modifiés par l'attaquant ;
- implants logiciels ;
- reconfiguration d'équipements de filtrage ;
- accès *Cloud* ;
- services d'accès à distance[30].

LIMITES DE L'INVESTIGATION

L'enquête sur l'incident a ses propres objectifs. Ses étapes sont indépendantes de la remédiation. Il convient de faire attention à bien synchroniser ces deux activités : il n'est recommandé ni de bloquer la remédiation en l'attente d'une information peu utile, ni de la brusquer avant de détenir suffisamment d'informations.

Dans les investigations, il convient en particulier de porter attention à certaines tendances, décrites ci-dessous, qui ne servent pas la remédiation.

→ L'obsession du point d'entrée initial

Souvent, le point d'entrée initial peut être identifié rapidement : un poste compromis au moyen d'une pièce jointe piégée, ou un accès VPN dont le mot de passe était disponible sur Internet.

29. On peut observer des attaquants usurpant, créant ou changeant les droits de comptes sur les SSO, ou locaux aux systèmes. Ce peut être le cas aussi bien sur les serveurs, les postes de travail que sur les équipements d'infrastructure : VPN, pare-feu, hyperviseurs, systèmes sans fils.

30. Les VPNs et bastions sont des points d'entrée naturels, mais il faut penser aussi à des services comme ConnectWise Control, TeamViewer ou LogMeIn qui sont souvent utilisés par les services de support.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

Cependant, il arrive que ce point d'intrusion soit moins clair, en particulier quand l'intrusion est ancienne. Avec certains attaquants il n'est pas rare qu'il y ait eu une campagne initiale qui ait donné à l'attaquant plusieurs points d'entrée.

Il est déconseillé de concentrer tous les moyens de la remédiation sur la couverture du point d'entrée.

Dans la plupart des cas, il est possible de réduire la fenêtre exploitable par l'attaquant mais pas de la fermer totalement : le métier a besoin d'échanger des documents avec le monde extérieur, les mots de passe sont réutilisés et il existe toujours, sur une surface suffisamment large, au moins un service vulnérable.

Il faut donc considérer comme probable l'existence en permanence d'au moins un équipement compromis dans le SI.

Une stratégie plus efficace consiste à :

- remédier aux vulnérabilités identifiées ;
- réinstaller les équipements compromis ;
- désactiver les comptes compromis ;
- définir une procédure de réintégration dans le système d'information d'un équipement au statut de compromission indéterminé (mise à jour, intégration dans la supervision).

La limitation des possibilités de latéralisation ou d'escalade de privilèges représentent souvent les mesures de sécurité les plus efficaces, sur lesquelles il est recommandé de concentrer les plus gros efforts.

→ L'imputation[31] de l'incident

L'identification du mode opératoire de l'attaquant est souvent possible, au moins partiellement, grâce à l'investigation. En revanche, l'identification des auteurs de l'attaque est complexe et réservée aux autorités compétentes. De nombreux attaquants utilisent un répertoire technique très large.

En pratique, cette information est rarement très utile dans le cadre de la remédiation et fait souvent l'objet d'une attention démesurée par rapport à sa praticité.

La remédiation ne devrait pas attendre une éventuelle imputation pour choisir la définition et l'exécution de ses objectifs.

→ La concentration sur les vecteurs d'attaque connus

Quand l'investigation détermine un chemin précis de l'attaque, il est tentant de se concentrer sur les points exploités par l'attaquant. Ces informations sont souvent utilisées pour concentrer les mesures de sécurité en fonction de ce qui a été vu. La connaissance de l'attaque aide effectivement à l'éradication des accès de l'attaquant et à la détection d'éventuelles tentatives de retour.

Cependant, les recherches ne sont malheureusement jamais exhaustives. Il faut donc se garder d'un faux sentiment de sûreté dans l'éviction de l'attaquant. Une attention particulière doit être maintenue sur d'éventuelles activités anormales signalant un angle mort oublié.

Pour éviter de tomber dans ce piège, il est souvent utile de compléter l'étude de l'attaque par une recherche de vulnérabilités dans le système d'information, pour découvrir les failles résiduelles et les combler.

31. Identification du mode opératoire attaquant grâce à des preuves techniques.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

b – Les sources de connaissance externe

La connaissance des moyens mis en œuvre par l'attaquant est importante dans le choix des mesures d'endiguement, mais surtout vitale à l'éradication de ses accès sur le système d'information.

Les résultats de l'investigation permettent souvent de pivoter sur des informations externes et d'élargir les recherches.

Exemple : le mode opératoire de l'attaquant est de voler des informations sur des serveurs de fichiers, d'en faire des archives au format RAR et de les exfiltrer par un serveur web. Une recherche en source ouverte permet d'indiquer que ces activités sont souvent associées au déploiement d'un type d'outil de contrôle à distance particulier que les équipes de remédiation pourront chercher lors de l'éradication.

Ce type d'information peut être trouvé dans les publications des éditeurs de solutions de sécurité, des CERTs et des autorités de sécurité informatique. Ces informations peuvent également être fournies par des services d'information sur la menace[32].

Dans le feu d'une crise, il est possible d'oublier cet élargissement d'horizon, qui est pourtant important.

c – La sélection des mesures de sécurité et de supervision

L'investigation fournit des informations sur les activités de l'attaquant, mais aussi sur les faiblesses du système d'information. Cette information permet de réévaluer sa sécurité, et d'ajuster les mesures à prendre.

Les actions passées de l'attaquant ne sont pas déterminantes de celles qu'il entreprendra dans le futur. La défense du SI ne doit donc pas se limiter à la prévention de ce qui s'est déjà produit.

32. Ces services sont couramment commercialisés sous l'appellation CTI, pour *Counter Threat Intelligence*.

En revanche, les zones d'ombre dans lesquelles l'attaquant a initialement échappé à la détection doivent être couvertes.

On cherchera notablement à prévenir et à détecter :

- les escalades de privilèges locales ou globales ;
- les explorations et latéralisations ;
- les persistances et leurs communications.

Ces mesures sont généralement mises en place au cours de l'incident pour soutenir les actions de remédiation. Il est recommandé de considérer leur pérennité dès leur mise en place. En particulier, la question de l'adéquation des mesures au niveau de mobilisation des équipes doit être posée. Ce niveau ne peut généralement pas être identique pendant et après l'incident.

d – Sécurité opérationnelle dans la remédiation

La sécurité opérationnelle désigne la protection des actions de défense contre l'attaquant. Ces mesures de protection devraient être appliquées à toutes les équipes opérant dans le cadre de la réponse à l'incident : gestion stratégique, investigation et remédiation. Une remédiation n'est pas un projet d'intégration ordinaire. Cette section présente des rappels sur les mesures de sécurité à prendre en compte. Les opérations effectuées en présence d'un adversaire intelligent et hostile, qui observe et réagit, nécessitent des précautions particulières. La plupart des intervenants non spécialistes n'en sont pas familiers.

CONTEXTE

De nombreux attaquants ne partent pas du SI compromis une fois leurs objectifs atteints ou lorsqu'ils ont été détectés. En particulier, il est fréquent qu'ils suivent les actions de réponse à incident et de remédiation, afin d'y réagir. Pour ce faire, ils surveillent les échanges des défenseurs, récupèrent les documents générés par les équipes

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

travaillant sur l'incident et tentent de collecter les nouveaux mots de passe au fur et à mesure de leurs changements…

Les équipes de remédiation ne peuvent pas se reposer sur une infrastructure qui a été compromise pour travailler sans risque. Une telle situation nécessite la mise en place de moyens spécifiques jusqu'à ce que la confiance ait pu être rétablie dans le système d'information.

Par ailleurs, l'incident informatique peut être la source directe d'une dégradation des moyens de travail. Ainsi, une attaque par rançongiciel rend généralement la messagerie, les partages de fichiers et même souvent le réseau interne indisponibles ou utilisables uniquement en mode dégradé.

Dans ces circonstances, des moyens improvisés sont généralement mis en place : postes de travail d'usage temporaire, baies de disques, infrastructure info-nuagique. Ces systèmes vont contenir des informations sensibles. Or, ces moyens sont souvent exempts de mesures de sécurité adéquats et sont donc très exposés au risque de compromissions.

Une sécurité parfaite dans la remédiation est impossible à obtenir et à conserver dans la durée pour un coût acceptable. Les mesures de protection du projet de remédiation doivent être choisies en conscience des compromis, en acceptant certains risques, mais en évitant la paralysie due à un excès de prudence.

ÉCHANGES AU SEIN DE L'ÉQUIPE DE REMÉDIATION

Les actions prises à son égard représentent la priorité de l'attaquant. Ses droits sont souvent étendus lors de la découverte d'une compromission. Il n'est donc pas rare de constater que les comptes de messagerie des administrateurs, des RSSI, des DSI ou des équipes de réponse à incident soient espionnés. Parfois, les attaquants sont en mesure de suivre les réunions de crise en ligne[33].

33. Plusieurs groupes de rançongiciel ont ainsi publié des copies d'écran de sessions Teams et de discussions Slack des équipes de réponse à incident.

Les intrus essaient aussi de récupérer les documents relatifs à la défense du système d'information : plans d'action, nouvelles configurations, listes de marqueurs. Ils tentent aussi d'accéder aux forums de discussion internes et aux Wiki. Dans certains cas, des attaquants utilisent des outils de contrôle des mobiles (MDM) pour suivre les activités de réponse sur les téléphones de l'organisation.

Dans le cas d'attaques avancées, l'usage de moyens de renseignement peut inclure une veille plus large : par exemple, vérifier que les maliciels ne sont pas déposés sur un service comme VirusTotal, espionner les communications de l'organisation à destination des spécialistes de réponse à incident ou des forces de l'ordre.

Il est donc impératif que le travail de remédiation soit totalement dissocié du système faisant l'objet de l'intrusion. Cela inclut l'usage de stockage et de moyens d'échange externes au système compromis[34]. Les postes utilisés doivent aussi être protégés. Idéalement, des postes neufs ou réinstallés, non liés au système d'information, devraient être utilisés. Si cela n'est pas possible, une protection particulière doit être mise en place : EDR spécifique, durcissement de configuration, restriction des communications.

Les données échangées en dehors des postes protégés doivent être chiffrées en transit et de préférence en stockage, afin de ne pas être interceptées.

Dans la plupart des organisations, la téléphonie a été portée sur IP. Ce mode de communication représente donc également un système informatique ciblé par les attaquants. Il faudra généralement préférer des échanges par téléphonie cellulaire, ou par application chiffrant de bout en bout l'usage de la téléphonie interne, de préférence certifiées par l'ANSSI[35].

34. Il convient de prêter attention à la transitivité des accès. Ainsi l'utilisation d'un service de communication infonuagique appuyé sur le domaine Active Directory compromis n'est pas sûr.

35. Voir la liste sur le site de l'ANSSI : https://www.ssi.gouv.fr/administration/produits-certifies/

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

Si des applications et des services nuagiciels sont utilisés pour la remédiation, l'usage d'authentifications multi-facteurs est impératif.

Un équilibre doit être trouvé entre les mesures de sécurité opérationnelles raisonnables et la capacité à travailler. Cet ajustement résulte toujours d'un compromis entre praticité et sécurité. Néanmoins, ces compromis doivent être faits en conscience et en étant accompagnés. En outre, ils doivent éventuellement faire l'objet de mesures compensatoires.

COMMUNIQUER AVEC LE RESTE DE L'ORGANISATION

La remédiation affecte nécessairement le reste de l'organisation. Il est donc nécessaire de communiquer.

Ne rien dire génère toujours une anxiété nuisible. Cependant, il faut considérer que toute communication interne est lue par l'attaquant, et souvent communiquée à l'extérieur[36].

Il est généralement prudent de ne pas inclure d'éléments trop précis sur les actions en cours dans les communications internes, avant que celles-ci ne soient terminées.

L'équilibre entre la transmission d'informations fournies et la préservation de la confiance est difficile à trouver. Ces décisions doivent être coordonnées au plus haut niveau.

SE COORDONNER AVEC L'EXTÉRIEUR DE L'ORGANISATION

Souvent, en cours de traitement de l'incident, les échanges avec l'extérieur sont affectés : coupure de liaison, fermeture d'accès distants, activation d'options de sécurité. Les partenaires de l'organisation vont inévitablement découvrir ces changements. Par ailleurs, ces interlocuteurs peuvent être des cibles secondaires, ou le point d'entrée, de l'attaquant.

36. Pour en savoir plus, consultez le guide de l'ANSSI *Anticiper et gérer sa communication de crise cyber*.

Les communications avec les partenaires doivent donc se faire en considérant que l'attaquant a une vue sur les moyens habituels de communication. Généralement, cela implique la mise en place de moyens dédiés pour échanger, le temps de l'incident, avec les partenaires informés.

Les échanges avec les prestataires ou avec les entités externes impliquées dans la remédiation doivent être protégés au même niveau que les échanges internes à l'équipe de remédiation. Un système d'information dédié, des solutions de chiffrement et l'utilisation d'authentifications multi-facteurs sont fortement recommandés. Un point d'attention particulier sera porté sur l'enrôlement des participants dans les systèmes de la remédiation. Faute de précautions suffisantes, les attaquants récupèrent les identifiants et peuvent se connecter à la place de l'usager légitime.

Face à des attaquants avancés, même quand les échanges sont chiffrés, la connaissance des destinataires d'échanges peut être une information sensible. Par exemple, si un RSSI se met subitement à échanger avec des adresses de courriel d'une entreprise de réponse à incident, ou à téléphoner à un numéro associé à l'ANSSI, c'est probablement indicateur qu'une gestion d'incident est en cours.

DÉCOMMISSIONNEMENT DES MOYENS EXCEPTIONNELS

Lors du traitement de l'incident, de nombreuses informations sensibles sont échangées sur des systèmes inhabituels. Des accès exceptionnels sont également mis en place.

Il faut éviter que ces éléments ne constituent, après la remédiation, un risque de fuite d'information ou d'accès incontrôlés. Pour ce faire, une attention particulière doit être portée à la destruction des données hors système d'information sécurisé (typiquement sur une instance d'espace de travail nuagique), et à la suppression des accès depuis des postes hors système d'information.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

Si des postes dédiés à la remédiation ont été utilisés, le plus prudent est de les effacer et de les réinstaller. Une telle action est facilitée par l'usage du chiffrement de disque lors de l'incident.

De même, les médias portables doivent être décommissionnés, notamment les clés et les disques USB pouvant contenir des éléments sensibles.

Afin de mener cette tâche à bien, une comptabilité de tous ces éléments doit être maintenue pendant la remédiation.

PARTIE III

LES PRESTATAIRES DANS LA REMÉDIATION

Un projet de remédiation consécutif à un incident majeur de sécurité informatique requiert une mobilisation importante des équipes techniques et l'intervention d'expertises variées. Peu d'organisations disposent d'effectifs suffisants et la diversité de compétences nécessaires pour couvrir ces besoins. La plupart des prestations de remédiation incluent donc une part importante de sous-traitance.

1 LA FORMULATION DES BESOINS

La formulation des besoins doit être la plus spécifique possible.

Malheureusement, les termes du domaine de la remédiation sont interprétés de façon très diverse.

Il ne faut pas hésiter à dresser une liste explicite des actions attendues du prestataire.

En particulier, il est nécessaire de bien distinguer, parmi les prestations lors d'une réponse à incident, celles relevant de la remédiation et celles qui n'en relèvent pas.

→ Prestations de remédiation :

- Les prestations de pilotage de la remédiation, qui viennent assister la direction de l'organisation dans la reprise en main de son système d'information.
- Les interventions techniques d'expertise au service de la remédiation, qui peuvent aller du nettoyage et la remédiation d'un Active Directory à la réorganisation d'un réseau ou la récupération de données endommagées. Ces interventions sont menées par des experts, qui savent intervenir sur un système d'information compromis.

- Les prestations d'administration de matériel, de logiciel et d'applicatif sont souvent nécessaires à la restauration, la réinstallation, ou la reconfiguration de composants du système d'information, voire à l'exécution de tâches d'éradication centralement planifiées. En revanche, ces interventions ne sont pas menées par des spécialistes d'interventions sur des systèmes compromis. Elles doivent être accompagnées pour limiter les risques de mauvaises pratiques.

→ Autres activités de la réponse à incident :

- Les prestations d'investigation numérique, qui visent à retrouver les traces de l'attaquant, à établir la façon dont celui-ci s'est introduit dans le système d'information et dont il s'est déplacé dans celui-ci, ainsi qu'à repérer les accès encore présents.
- Les prestations de pilotage de crise qui viennent assister la direction de l'organisme dans la gestion de l'incident, en particulier dans la coordination des actions, la gestion des impacts et la communication.

2 LA SÉLECTION DES PRESTATAIRES

Idéalement, les relations avec des prestataires devant intervenir dans l'urgence sont contractualisées dans le cadre de la préparation aux incidents de sécurité informatique.

S'il n'existe pas de cadre contractuel préexistant à l'incident, il est préférable de s'appuyer sur des relations déjà établies, via des assureurs ou des organisations sectorielles.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

L'ANSSI délivre le Visa de sécurité[37] à un certain nombre de prestataires, dont des Prestataires de Réponse aux Incidents de Sécurité[38] (PRIS). Il est donc possible de s'appuyer sur des prestataires de confiance dont le niveau de compétence a été vérifié. Néanmoins, il est important de noter que cette qualification PRIS n'intègre pas actuellement les prestations de pilotage et de mise en œuvre de la remédiation, de même qu'il n'existe pas encore de schéma de qualification englobant tous les types d'interventions de la remédiation.

Le présent guide peut ainsi servir de base afin de formuler les exigences des bénéficiaires et d'identifier les prestations à assurer.

Lors de la sélection des prestataires, il est important d'identifier les jalons de la prestation qui permettront d'en mesurer l'avancement. Ces jalons devraient être déterminés dès la contractualisation.

3 LE PILOTAGE DE LA PRESTATION

La particularité des prestations dans le cadre d'une remédiation consiste en leur succession rapide.

En effet, plusieurs intervenants aux expertises spécifiques pointues (restauration de fichier, configuration Active-Directory, configuration de pare-feu ou de virtualisation, etc.), travaillent sur des périodes courtes. Leurs actions doivent s'intégrer à des activités plus longues de restructuration du système d'information.

37. Visa de sécurité sur le site de l'ANSSI : https://www.ssi.gouv.fr/entreprise/visa-de-securite/

38. La liste des PRIS peut être trouvée sur le site de l'ANSSI : https://www.ssi.gouv.fr/administration/qualification/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/

Afin de limiter les pertes d'information et de capacité, il convient d'apporter une attention particulière :

- aux interventions qui se bloquent mutuellement, à ordonnancer avec prudence et en incluant des marges ;
- au bon recueil des livrables de chaque intervenant et à leur mise à disposition des autres acteurs, internes ou externes qui en auront besoin ;
- au format des livrables, qui doit permettre à ceux qui les consomment d'en faire un usage le plus direct possible (en évitant des ressaisies, ou des conversions sources d'erreur fréquentes) ;
- à la bonne définition les conditions de fin d'intervention et leur validation afin de ne pas recevoir des livrables partiels ou des configurations incomplètes.

La coordination entre intervenants est complexe et indispensable. L'organisation d'ateliers entre ces acteurs peut être particulièrement pertinente afin de s'assurer de la bonne compréhension entre les spécialistes et la continuité entre les différentes étapes de la remédiation. Le travail en binôme entre les membres de la DSI et les intervenants externes au long de la remédiation est une façon efficace de limiter les pertes d'informations.

Enfin, il convient de détecter au plus vite les points bloquants susceptibles d'être rencontrés par un intervenant, afin d'éviter une paralysie de toute la remédiation. Pour ce faire, des points d'avancement fréquents sont une bonne solution.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

4 LA FIN DE PRESTATION

La prestation est terminée lorsque tous les jalons ont été atteints.

Il convient de s'assurer de récupérer tous les livrables, même s'ils ont déjà été transmis à un autre intervenant.

Par ailleurs, il est fréquent d'avoir besoin de recontacter un intervenant afin de préciser certains paramétrages. Ces points post-intervention doivent être prévus en amont afin d'éviter des indisponibilités ou des coûts imprévus.

PARTIE IV

PLANS TYPES

Cette partie étudie trois scénarios-types. Leur but est de décrire la façon dont les priorités décisionnelles de l'organisation sont articulées avec les objectifs opérationnels et les moyens à mettre en œuvre. Ces scénarios sont des archétypes qui ne doivent pas être exécutés tels quels, mais qui requièrent d'être adaptés à l'organisation qui en bénéficie.

Si ces scénarios peuvent couvrir une remédiation simple, ils sont souvent utilisés comme des phases successives, dans des plans de remédiation plus complexes.

1 « RESTAURER AU PLUS VITE DES SERVICES VITAUX »

a – Description

Ce scénario s'applique dans une situation où la perturbation de l'activité de l'organisation produit un impact majeur sur sa survie ou sur un service essentiel ou vital.

Dans ces circonstances, il peut être nécessaire d'effectuer une remédiation centrée sur le ou les services concernés, avant de pouvoir traiter des problèmes structurels. Ce scénario suppose que les services vitaux puissent être décorrélés du reste du système d'information.

La remédiation décrite ci-dessous présente les phases nécessaires à une réouverture de services après une compromission majeure.

b – Objectif stratégique

- Assurer la continuité ou le redémarrage d'un service vital pour l'organisation dans un délais bref.

c – Objectifs opérationnels

- Création d'un socle de confiance restreint pour le service vital (réseau, virtualisation, identification).
- Restauration sécurisée du service vital (réinstallation ou nettoyage).
- Suppression des accès résiduels de l'attaquant dans la bulle des services critiques.
- Préparation d'une sécurisation du SI vital sur la durée.
- Remédiation minimale aux vulnérabilités exploitées par l'attaquant sur le reste du SI.

d – Déroulement

Un cœur de confiance minimal est restauré autour duquel une bulle de redémarrage est construite. Ce cœur de confiance n'est pas nécessairement une infrastructure d'authentification complète mais plutôt un socle système, réseau et d'identité strictement nécessaire.

Les dépendances du service critique sont inspectées, nettoyées et importées dans la bulle de redémarrage.

Les serveurs supportant le service peuvent être réinstallés ou importés, et nettoyés. Si une réinstallation offre de meilleures garanties, celle-ci n'est pas toujours possible (temps de reconstitution des configurations, ou simplement disponibilité des médias d'installation).

La bulle est mise sous supervision de sécurité serrée et le service est redémarré au plus vite.

Sur le reste du système d'information, hors bulle, une campagne minimale d'éradication des vulnérabilités exploitées et des portes dérobées positionnées par l'attaquant est menée après redémarrage du service.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Toute montée en niveau de sécurité sur le reste du système d'information sera traité dans un plan ultérieur. Celui-ci peut être une étape du plan de remédiation. Autrement, si le risque est accepté, ces actions peuvent s'inscrire dans l'amélioration continue du système d'information.

Par ailleurs, la séparation forte d'un service essentiel du reste de l'organisation est rarement pérenne. À terme, la réintégration de ce service dans le système d'information sécurisé est nécessaire. L'objet du scénario consiste à se donner le temps de traiter cette réintégration hors de l'urgence.

e – Risques résiduels

La priorité donnée à la vitesse de rétablissement du service ne permet pas de créer ou de recréer une organisation résiliente de la sécurité du SI.

Si un projet de montée en maturité de la sécurité du système considéré n'est pas mené dans un second temps, le risque d'apparition de nouveaux incidents significatifs est élevé. En pratique, il est constaté que même si l'activité essentielle a été sauvegardée, la récurrence d'incidents dans le reste du SI affecte durablement l'organisation. Le plan de sécurité du SI dans la durée doit prendre en compte les actions repoussées hors du temps chaud.

Quand un chantier de sécurisation en profondeur n'est pas mené après un incident, l'ANSSI note que le coût de la récurrence d'incidents affectant les métiers peut rapidement dépasser ceux d'une remédiation plus complète.

2 « REPRENDRE LE CONTRÔLE DU SI »

a – Description

Dans ce scénario, l'organisation vise à recréer un système d'information dans un état proche de l'état initial sans viser de transformations profondes.

Les objectifs de ce scénario sont alignés vers un renforcement de l'existant en minimisant les changements.

b – Objectifs stratégiques

- Retrouver dans un délai raisonnable un fonctionnement et une activité de production nominaux au sein de l'entreprise.
- Reprendre le contrôle du système d'information.

c – Objectifs opérationnels

- Création d'un cœur de confiance dur et maîtrisable dans la durée.
- Restauration du niveau de sécurité antérieure du SI en dehors du cœur de confiance.
- Remédiation aux vulnérabilités spécifiques exploitées par l'attaquant hors du cœur de confiance.
- Suppression des accès de l'attaquant dans tout le système d'information.

d – Déroulement

Un cœur de confiance est reconstruit contenant une infrastructure de gestion complète et sécurisée. L'architecture de cette bulle est reconstruite entièrement à l'état de l'art.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Une supervision de sécurité forte est mise en place sur le cœur de confiance avant sa mise en service et est maintenue durablement.

Les serveurs et les postes terminaux font l'objet d'une campagne de remédiation des vulnérabilités identifiées et d'éradication des portes dérobées de l'attaquant. Aucun changement d'architecture ou de processus de gestion n'est effectué hors du cœur de confiance.

Une supervision de sécurité forte mais temporaire est mise en place hors du cœur de confiance pour s'assurer de l'efficacité de l'éradication. Ce niveau de supervision en dehors du cœur de confiance est progressivement ramené à un état moins élevé mais durablement supportable.

e – Risques résiduels

Dans ce scénario, la priorité est accordée à la vitesse de sortie de crise et au retour à un rythme normal de fonctionnement. Il en résulte que des travaux de sécurisation en profondeur en dehors du cœur de confiance ne peuvent être menés et que les risques de future compromission et d'escalade de privilège restent élevés.

3 « SAISIR L'OPPORTUNITÉ POUR PRÉPARER UNE MAÎTRISE DURABLE DU SI »

a – Description

Dans ce scénario, l'incident est utilisé comme point de départ d'une restructuration de la sécurité du système d'information.

Les objectifs stratégiques visent à réduire durablement les risques de perturbations majeures liées à la sécurité informatique, au prix d'un rétablissement plus long et d'un investissement initial plus important.

Les objectifs opérationnels concernent des mesures durables et une sécurité intégrée.

b – Objectifs stratégiques

- Retrouver un fonctionnement et une activité de production nominaux au sein de l'entreprise.
- Mettre en place une protection durable pour éviter de reproduire une situation comparable.

c – Objectifs opérationnels

- Création d'un cœur de confiance durci et maîtrisable dans la durée.
- Création d'un niveau de sécurité maitrisé et durable sur les pratiques d'administration des serveurs et des applications.
- Remédiation aux vulnérabilités exploitées par l'attaquant sur les terminaux.
- Mise en place d'une capacité durable de détection/réaction/correction sur la totalité du SI.
- Suppression des accès de l'attaquant dans tout le système d'information.

d – Déroulement

Un cœur de confiance est reconstruit contenant un socle de service très complet. Pour ce faire, l'architecture du cœur de confiance est reconstruite entièrement.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Une supervision de sécurité forte est mise en place sur le cœur de confiance avant redémarrage et est maintenue durablement.

L'architecture des services hors cœur de confiance est découpée en secteurs à traiter successivement. Par défaut, tous les secteurs sont considérés compromis.

Chaque secteur est revu à son tour :

- les vulnérabilités identifiées y sont corrigées ;
- les portes dérobées de l'attaquant y sont supprimées ;
- son architecture et l'organisation de sa gestion sont revues et modifiées si nécessaire ;
- sa supervision de sécurité est intégrée avec celle du cœur de confiance.

Les secteurs remédiés constituent le SI sain, avec pour objectif d'y inclure tout le SI. Les secteurs non encore traités sont considérés compromis et font l'objet de mesures d'isolation et de supervision de sécurité serrées.

Les postes terminaux font l'objet d'une campagne de remédiation des vulnérabilités identifiées et d'éradication des portes dérobées. Ils sont soumis à une supervision de sécurité moindre que sur les serveurs et le cœur de confiance.

e – Risques résiduels

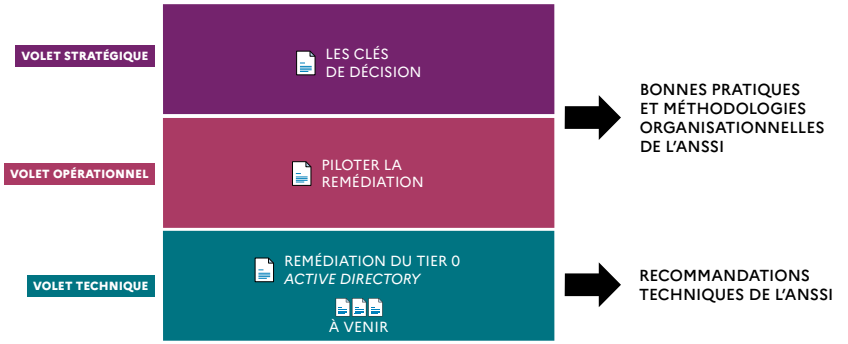
Aucun système d'information moderne ne peut assurer une protection forte de tous les segments du système d'information. En particulier, parmi les postes terminaux, il est accepté que certains restent compromis. Les efforts sont concentrés sur la limitation des escalades et des impacts, afin que les incidents de faible gravité n'escaladent pas.

La construction du cœur de confiance assure que, même en cas d'incident grave, il soit possible de reprendre la main sur le système d'information sans opérations de grande ampleur.

ANNEXES

A STRUCTURE DU CORPUS DOCUMENTAIRE

Ce corpus se compose de trois documents, reprenant en détails les trois volets de la remédiation : la partie stratégique, la partie opérationnelle et la partie technique.



B GLOSSAIRE

CŒUR DE CONFIANCE

Le cœur de confiance est la partie d'un système d'information sur laquelle repose la sécurité de la totalité du système d'information. La compromission d'un composant du cœur de confiance permet celle de la totalité du système d'information. Dans la plupart des systèmes d'information, le cœur de confiance inclut : la gestion des identités, la virtualisation, l'administration et les composants assurant la supervision de sécurité. Les architectures sécurisées visent à minimiser la taille et la complexité du cœur de confiance, afin d'en rendre la sécurisation la plus simple possible. Ce caractère minimal du cœur de confiance est particulièrement important dans un incident où chaque partie peut avoir fait l'objet d'une compromission.

CRISE D'ORIGINE CYBER

Une crise « d'origine cyber » se définit par la déstabilisation immédiate et majeure du fonctionnement courant ou futur d'une organisation (pertes de marchés, arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes, perte d'intégrité majeure, etc.) en raison d'une ou de plusieurs actions malveillantes sur ses services et ses outils numériques (cyberattaques de type rançongiciel, déni de service, etc.). C'est donc un évènement à fort impact, qui ne saurait être traité par les processus habituels et dans le cadre du fonctionnement normal de l'organisation.

Les événements accidentels, c'est-à-dire ne résultant pas d'une activité malveillante sur les SI, et les actions malveillantes n'entraînant pas l'interruption immédiate et majeure des services essentiels de l'organisation sont par conséquent exclus du périmètre de définition.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

ENDIGUEMENT

L'endiguement (*containment* en anglais) désigne l'ensemble des actions prises au début d'un incident de sécurité informatique destinées à en contenir l'ampleur. La plupart des mesures d'endiguement sont perturbatrices des fonctionnements habituels du système d'information, ou consommatrices anormales de ressources. En tant que telles, elles n'ont généralement pas vocation à être prolongées durablement. L'exécution du plan de remédiation doit permettre de lever les mesures d'endiguement vers une posture soutenable dans la durée.

ÉVICTION

La reprise de contrôle d'un système d'information requiert la création, ou la recréation d'un cœur de confiance. Ce sous-système, maintenu hors de portée de l'attaquant par des mesures fortes est le socle des actions de reconquête. Depuis ce cœur de confiance, les défenseurs vont pouvoir intervenir sur le reste du système d'information hors de portée de l'attaquant.

L'éviction consiste donc en la recréation d'un cœur de confiance à partir des informations du système qui a été compromis. Dans certains cas, l'éviction est une recréation sans réutilisation d'anciens éléments du système d'information. Dans la plupart des cas, l'éviction est plutôt une combinaison de filtrage et de nettoyage des informations du système compromis avant de les utiliser sur des systèmes réinstallés.

ÉRADICATION

L'éradication désigne à la fois la recherche et la neutralisation des emprises résiduelles ou potentielles de l'attaquant dans le système d'information autour du cœur de confiance.

L'éradication sur un grand système peut représenter un travail de grande ampleur. Pour cette raison, les opérations d'éradication sont souvent phasées par service, par métier, ou par secteur du système d'information.

GESTION DE CRISE[39]

Processus de gestion qui identifie les impacts potentiels qui menacent une organisation et fournit un cadre pour renforcer la résilience, avec la capacité d'une réponse efficace qui préserve les intérêts des principales parties prenantes de l'organisation, sa réputation, sa marque et ses activités créatrices de valeur, et qui rétablit efficacement les capacités opérationnelles.

INCIDENT DE SÉCURITÉ MAJEUR

Un incident majeur d'origine cyber est une séquence d'évènements techniques impactant ou risquant d'impacter sévèrement un ou des métiers identifiés comme essentiels à l'activité de l'organisation.

C'est l'impact et non la nature d'un incident cyber qui détermine sa gravité. L'impact est toujours à considérer vis-à-vis des métiers supportés par l'informatique. L'incident majeur est caractérisé par le potentiel de dégénérer en crise s'il n'est pas convenablement circonscrit et traité.

INVESTIGATION[40]

Procédé visant à collecter et à analyser tout élément technique, fonctionnel ou organisationnel du système d'information permettant de qualifier une situation suspecte en incident de sécurité et de comprendre le mode opératoire et l'étendue d'un incident de sécurité sur un système d'information.

39. D'après le référentiel d'exigences pour les prestataires d'accompagnement et de conseil en sécurité des systèmes d'information (PACS), https://www.ssi.gouv.fr/uploads/2022/10/referentiel-pacs_v0.3.2.pdf

40. D'après le référentiel d'exigences pour les prestataires de réponse aux incidents de sécurité (PRIS), https://www.ssi.gouv.fr/uploads/2014/12/pris_referentiel_v2.0.pdf

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

NIVEAUX DE GESTION D'UN INCIDENT MAJEUR DE SÉCURITÉ INFORMATIQUE

Un incident de sécurité et sa gestion peuvent être considérés suivant trois plans distincts :

- **Le niveau décisionnel** est responsable de la prise en compte de l'incident et de ses impacts sur les activités dans le pilotage de l'organisation. À ce niveau, porté par les cadres dirigeants, sont décidées les grandes orientations de la gestion et de la sortie de crise, en fonction des priorités de l'organisation et de ses parties prenantes.
- **Le niveau opérationnel** est géré par les responsables du système d'information et de sa sécurité. Les choix de ce niveau sont généralement portés par les responsables techniques, les directeurs de système d'information et les responsables de sécurité des systèmes d'information. Dans l'incident, c'est à ce niveau qu'est décidé comment décliner en plan d'actions techniques macroscopiques les directions décidées au niveau décisionnel.
- **Le niveau technique** est celui auquel les actions techniques sont organisées, exécutées et effectuées.

OBJECTIFS STRATÉGIQUES DE REMÉDIATION

Les objectifs stratégiques de remédiation sont une description des états cibles formulés par la direction. Ils décrivent les états de fonctionnement et de sécurité de l'organisation visés pendant et en sortie de remédiation.

Ce sont les objectifs pilotés au niveau décisionnel.

La direction de l'organisation est celle qui détermine et priorise les objectifs stratégiques de remédiation.

OBJECTIFS OPÉRATIONNELS DE REMÉDIATION

Un objectif de remédiation est un état mesurable de niveau de sécurité ou de niveau fonctionnel du système d'information. Ces objectifs sont la déclinaison technique des objectifs stratégiques de remédiation. Ces objectifs sont détaillés sous forme d'actions concrètes dans le plan de remédiation.

PLAN DE REMÉDIATION

Le plan de remédiation est la liste des actions à mener pour mettre le système d'information en conformité avec les objectifs opérationnels de remédiation.

Ce plan peut être découpé en sous-projets par objectif opérationnel de remédiation.

REMÉDIATION

La remédiation est définie comme le projet de reprise de contrôle d'un système d'information compromis. Elle correspond à une séquence d'actions qui mène d'un état subi vers un état désiré. Dans le cadre d'un incident de sécurité informatique, c'est un travail qui commence dès l'endiguement de l'action adverse et qui peut s'étendre sur plusieurs mois.

Quand une gestion de crise est mise en place, celle-ci se termine souvent alors que la remédiation n'en est qu'à ses premières phases.

La remédiation ne se termine que lorsque les niveaux fonctionnel et sécuritaire du système d'information répondent aux objectifs stratégiques. Le terme de la remédiation est également un retour au cycle d'amélioration continue de la sécurité.

TEMPS CHAUD

Le terme « temps chaud » est utilisé dans le présent document pour désigner la période entre la détection d'un incident majeur et la sortie des dispositifs exceptionnels de sa gestion (ou d'une gestion de crise).

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

Le « temps chaud » s'oppose au « temps froid » pendant lequel les processus de gestion de l'organisation ne sont pas mobilisés pour faire face spécifiquement à l'incident.

Dans la plupart des cas, la remédiation commence en temps chaud, mais se termine en temps froid.

La remédiation consiste en la reprise de contrôle d'un système d'information compromis. Le volet opérationnel en constitue un pilier essentiel : l'élaboration, l'exécution, la logistique ou encore la sortie de la remédiation sont des étapes clés qu'il est nécessaire de maîtriser. Bien piloté, l'incident subi devient une opportunité d'amélioration significative.

La remédiation est l'une des dimensions majeures de la reprise de contrôle suite à une attaque cyber, avec l'investigation, la communication et la gestion de crise. C'est un travail qui commence dès l'endiguement de l'action adverse et qui peut s'étendre sur plusieurs mois.

Fruit d'une riche expérience dans l'accompagnement d'organisations victimes d'incidents de sécurité, l'ANSSI publie un corpus de guides sur la remédiation, décrivant les principes de son pilotage et de sa bonne mise en œuvre : le volet stratégique, le volet opérationnel et le volet technique.

Ce volet opérationnel assistera la conception et le déroulement du projet de remédiation au travers de scénarios types et d'un accompagnement étape par étape.

Version 0.0 – Avril 2023
Dépot légal : avril 2023
ISBN papier : 978-2-11-167138-6
ISBN numérique : 978-2-11-167139-3

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