AFNOR SPEC 2208

NOVEMBRE 2022

www.afnor.org

Contacter :
AFNOR – Norm'Info
11, rue Francis de Pressensé
93571 La Plaine Saint-Denis Cedex
Tél : 01 41 62 76 44
Fax : 01 49 17 92 02
E-mail : norminfo@afnor.org

AFNOR

AFNOR SPEC 2208

CYBER-RÉSILIENCE

RECONSTRUCTION DU SI
ET CONTINUITÉ D'ACTIVITÉ
MÉTIERS EN CAS
DE CYBERATTAQUE
PARALYSANTE

NOVEMBRE 2022

afnor

SOMMAIRE

Avant-propos

Le présent document représente le consensus obtenu par un groupe d'acteurs individuels ou collectifs, identifiés dans ce document. Ce document, présenté, rédigé et mis au point à l'initiative d'AFNOR, constitue une œuvre collective au sens du Code de la Propriété Intellectuelle.

Le présent document bénéficie de la protection des dispositions du Livre 1er du Code de la Propriété Intellectuelle relatif à la propriété littéraire et artistique. Toute reproduction sous quelque forme que ce soit est une contrefaçon et toute contrefaçon est un délit.

Ce document n'a pas été soumis à la procédure d'homologation et ne peut être en aucun cas assimilé à une norme française. Son utilisation est volontaire.

ONT PARTICIPÉ À L'ÉLABORATION COLLECTIVE DE CETTE AFNOR SPEC :

PARTICIPANTS	ORGANISME
M ALLAOUA, Mehdi	ORANGE
MME ATAKOU GAUTHIEROT, Sarah	CAP GEMINI
M BAYLIS, Thomas	AIRBUS CYBERSECURITY SAS
MME BELLEC, Nora	MINISTERE EUROPE ET AFFAIRES ETRANGERES
M BENOIST, Christophe	LEADER INTERIM
MME BERARD, Béatrice	FEDERATION HOSPITALIERE FRANCE
M BERTHEL, Julien	FEDERATION HOSPITALIERE FRANCE
M BIGOT, David	ORANGE CYBERDEFENSE FRANCE
M BRESSON, Stéphane	AD NORMANDIE
M BURY, Hervé	FRAMATOME
M CAMOIN, Edouard	3DS OUTSCALE
M CAPRAI, Adrien	CNC EXPERTISE
M CARTAU, Cédric	FEDERATION HOSPITALIERE FRANCE
M CHENUT, Hubert	CNC EXPERTISE
MME DELFOSSE, Aurélia	ADVENS
M DELILLE, Gil	CREDIT AGRICOLE S.A
M DESMOUCELLES, Thomas	HABITAT 76
M DUMOUSSAUD, Laurent	ORANGE FRANCE
M DURANT, Aubert	THALES SIX GTS FRANCE SAS
M FERAY, Nicolas	HABITAT 76
M FERTALA, Mathieu	MINISTERE DE L'INTERIEUR SG / DNUM
M GILBERT, Brice	AFNOR CERTIFICATION

M GIRARDIN, Laurent	ORANGE
M HARTOUT, Xavier	ADENIUM - BE RESILIENT GROUP (BRG)
M HECTOR, François	SECINFRA
MME JEAN, Mélissa	AFNOR
MME KADRI, Hakima	CERCLE DES FEMMES DE LA CYBERSECURITE - CEFCYS
M KOUM, René	LA FRANCE MUTUALISTE
M LE BERRE, Stephan	EXATRACK
M LECONTE, Frédéric	AFNOR DEVELOPPEMENT
M LEFEVRE, Bruno	FRAMATOME
M LEPERRIER, François	FRAMATOME
M LEROUX, Benjamin	ADVENS
M MAIRA, Christophe	MUTEX
M MERIAN, Yves	IMDR - INSTITUT POUR LA MAITRISE DES RISQUES
M MERIC DE BELLEFON, Vincent	CREDIT AGRICOLE-GROUP INFRASTRUCTURE PLATFORM
MME MONTI, Anna	ADENIUM - BE RESILIENT GROUP (BRG)
M MULLOT, Cédric	AIRBUS CYBERSECURITY SAS
M OBER, Bruno	CGI FRANCE
M PANARDIE, Philippe	SDIS - SCE DEPT INCENDIE SECOURS
MME REDON, Céline	CERCLE DES FEMMES DE LA CYBERSECURITE - CEFCYS
M ROUAULT, Clément	EXATRACK
M SAUVAGE, Olivier	COOPERL ARC ATLANTIQUE
M SCUTO, Nicolas	IHEMI
M SERRE, Benjamin	ORANGE CYBERDEFENSE FRANCE
MME SINNO, Dahlia	THALES SIX GTS FRANCE SAS
M ZAMORA, François	ORANGE

REMERCIEMENTS

À tous les experts pour leurs contributions et la qualité des échanges lors des travaux

Aux co-animateurs du projet David Bigot et Xavier Hartout avec le support de Anna Monti

Aux équipes de l'AFNOR avec le support de Mélissa Jean

Introduction

Les cyberattaques se sont fortement multipliées ces dernières années. Les états et leurs agences nationales dédiées à la sécurité des systèmes d'information alertent sur une menace toujours plus élevée. Tous les organismes, de toute taille, de tout secteur sont concernés et leur exposition aux menaces est en augmentation permanente.

Les experts réunis autour de ce projet ont tous vécu des cyberattaques directement ou indirectement :

- au sein de leur propre organisme en tant que victime ;
- en tant que parties prenantes internes ou externes ;
- en tant qu'experts pour aider les organismes à faire face à ce type de menaces.

Ces expériences ont d'autant plus incité les membres du groupe à participer activement à ces travaux pour réduire l'impact des cyberattaques, plus particulièrement celle dites « paralysantes ».

Dans ce document, nous avons défini la « cyberattaque paralysante » comme étant une crise d'origine cyber, un acte malveillant envers un système d'information qui va le rendre indisponible pour une durée prolongée (plusieurs jours, voire plusieurs semaines ou mois) et qui va perdurer voire paralyser l'activité. Une cyberattaque paralysante peut émaner de personnes isolées, d'un groupe de « pirates » ou de vastes organismes ayant des objectifs géopolitiques.

Les cyberattaques paralysantes deviennent un scénario de crise dont la probabilité de survenance est élevée voire très élevée. En effet, les typologies de cyberattaques récentes (rançongiciels, intrusions directes ou par rebond, acquisition illégitime de domaines, phishing, etc.), leur fréquence et leur multiplication dans tous les domaines sociétaux (entreprises de toutes tailles, hôpitaux, collectivités) ont montré que les organismes pouvaient se retrouver perturbés durablement, sans perspective claire de retour à une situation normale avant plusieurs semaines voire plusieurs mois. La résolution est également rendue délicate en raison de la sophistication et de la virulence des cyberattaques.

Ce constat préoccupant a motivé la rédaction du présent document. Celui-ci n'a pas pour ambition de définir une doctrine universelle. Un panel d'experts y propose à tout un chacun, en joignant ensemble leurs expériences et leurs spécialités quelles qu'elles soient (technologie, continuité d'activité, management, etc.), un ensemble de pratiques à considérer, que ce soit avant l'incident ou postérieurement. La gestion de crise et la continuité des activités permettent de limiter l'impact de l'incident, réduire le risque de sur-accident et accélérer le retour à la normale tout en assurant la continuité des activités, y compris en mode dégradé, de l'organisme contribuant à une meilleure cyber-résilience.

Chacun puisera, dans cette AFNOR SPEC, des éléments de compréhension et des préconisations, en fonction de la nature de l'activité, de la maturité et des moyens de l'organisme qu'il défend. Nous souhaitons que ce travail facilite la difficile tâche des personnes chargées de la prévention des crises et du pilotage de celles-ci en cas de cyberattaque.

Objet du Document

Ce document AFNOR SPEC s'adresse à tout organisme public ou privé qui souhaiterait anticiper le traitement d'une cyberattaque ou qui aurait à faire face une cyberattaque rendant son Système d'Information indisponible pour une durée prolongée, quel que soit son niveau de préparation. Il propose des lignes directrices en matière :

- d'actions à mener en cas de survenance d'une cyberattaque paralysante ;
- de spécifications techniques à suivre pour faciliter la reconstruction du SI ;
- de préconisations à mettre en œuvre pour assurer la continuité d'activité métiers ;
- de leçons et enseignements à tirer après une cyberattaque.

Ce document d'application volontaire permet aussi aux organismes d'améliorer leur niveau de préparation face à de telles menaces en leur recommandant un certain nombre de bonnes pratiques à mettre en place en amont.

Ce guide s'adresse aux parties intéressées de tous les organismes, de tous les secteurs, à savoir :

- en premier lieu, les personnes en charge de l'informatique, de la continuité d'activité, de la sécurité, de la sécurité du SI, de la sûreté, de la gestion des risques, de la gestion de crise, de la gestion des données internes ou externes, de la communication ;
- en deuxième lieu, les décideurs ;
- en troisième lieu, les fournisseurs critiques vis-à-vis de leurs donneurs d'ordre, les organismes d'audit / contrôle et les autorités.

Ce document s'adresse aux organismes disposant *a minima* d'un responsable informatique.

Pour les TPE, une synthèse spécifique se trouve en annexe C permettant d'avoir les éléments pragmatiques à mettre en place.

Ce document n'est pas une norme homologuée.

PARTIE 1
EN CAS DE SURVENANCE D'UNE CYBERATTAQUE PARALYSANTE

La crise est généralement modélisée par le graphique ci-après qui permet de se rendre compte de l'intensité croissante à laquelle une organisation est confrontée. Dans le cas d'une cyberattaque paralysante, la durée de la crise sera allongée.

Lorsque l'entrée en crise est actée, une gestion de crise est à mettre en place rapidement avec une organisation spécifique et dédiée. Dans le cas contraire, la marge de manœuvre va drastiquement se réduire notamment avec une forte augmentation de la perte d'exploitation et avec des impacts durables sur l'organisme (*exemple : perte de clientèle*). Un ensemble d'actions doit être mené, dès la survenance de la cyberattaque, pour comprendre en l'origine (cf. analyse forensique), pour la reconstruction du SI et la continuité d'activité Métiers afin d'éviter une aggravation de la crise. Les coûts vont effectivement augmenter au cours de la crise, il est toutefois possible de conserver une marge de manœuvre suffisante en menant, dès le début de la crise, des actions préventives et immédiates.

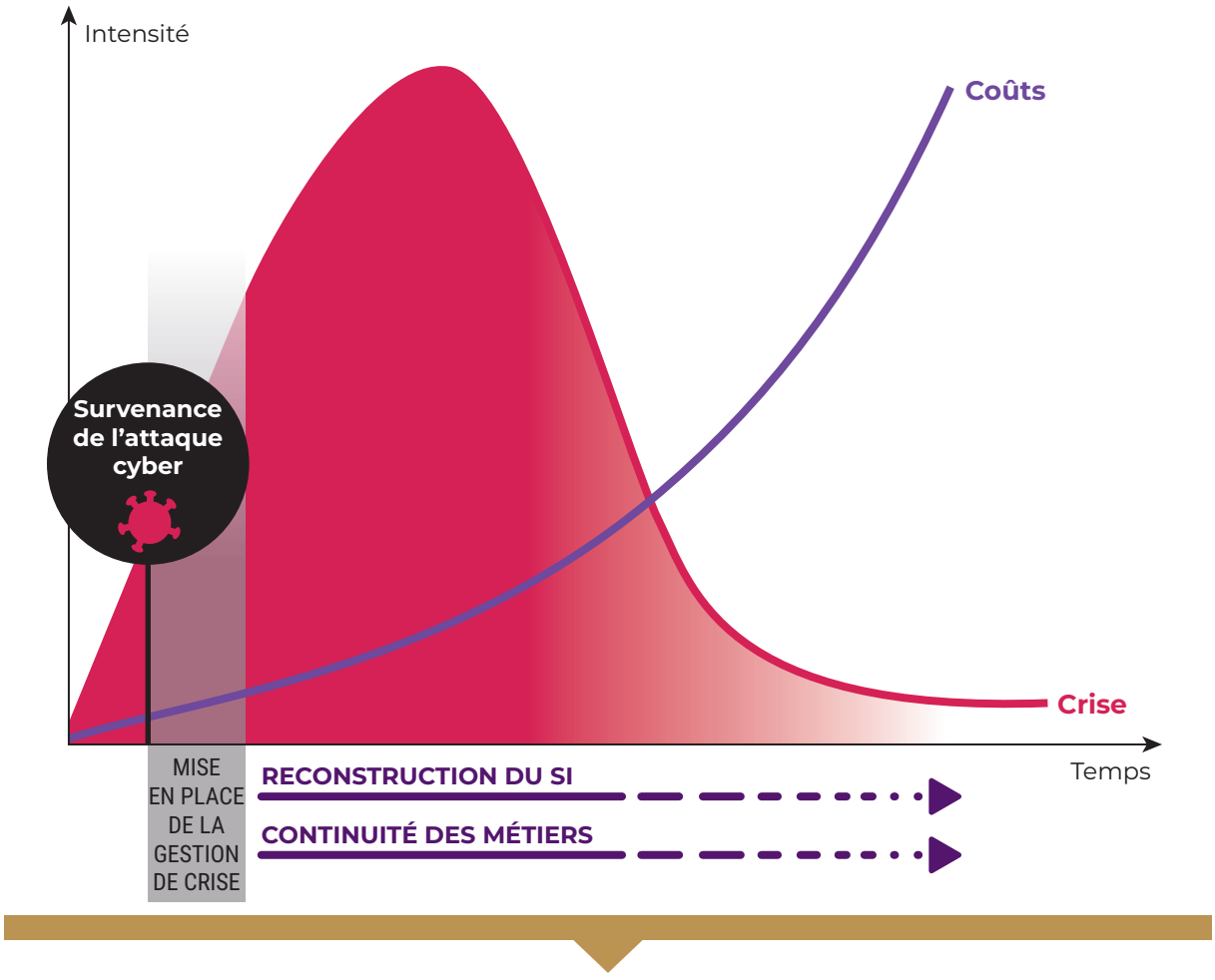


Figure 1 : Schéma de modélisation de crise (cas d'une cyberattaque paralysante)

1.1 Entrée en crise

La détection d'une situation de crise revêt un caractère essentiel et peut se faire de différentes manières. Des signaux faibles peuvent être détectés et traités grâce à des dispositifs de veille préalablement éprouvés sur des thématiques cibles et / ou des secteurs critiques.

Dans le cas des cyberattaques, l'agent de menace peut être présent dans le SI depuis plusieurs semaines, voire plusieurs mois sans être visible. Néanmoins, des signaux faibles peuvent parfois être remontés directement par :

- des utilisateurs (détection de postes de travail présentant des anomalies) ;
- des administrateurs (présence de fichiers suspects anormaux, désactivation de l'antivirus sur un large périmètre...) ;
- des systèmes de détection automatisés indiquant la présence d'un comportement suspect sur le système d'information (purge des sauvegardes, arrêt d'une partie des serveurs, séquences typiques d'une intrusion, transferts inhabituels de données, connexion à des heures insolites).

Les éléments rassemblés permettent, par exemple, d'alimenter les équipes de supervision d'un organisme en les faisant passer d'un état de vigilance à un état d'alerte. À la suite du passage en état d'alerte, une permanence visant à identifier une situation de crise et à réaliser les escalades nécessaires à la mise en place de sa gestion de crise est préconisée.

Il conviendra de déterminer une matrice d'évaluation d'un incident et du seuil à partir duquel il peut être considéré comme une crise avec la nécessité de mettre en place l'organisation adéquate. La description en amont de seuils de gravité des incidents et des crises est une aide à la décision pour le passage en crise. En effet, en cas de dépassement de ces seuils mesurant l'impact sur le fonctionnement de l'organisme, des procédures déclenchent des escalades vers des niveaux hiérarchiques. La qualification d'un incident ou d'une alerte est clé dans la décision d'entrer en crise.

Les états de vigilance et d'alerte actionnés déclenchent un suivi étroit et une analyse pointue de l'incident. Il vise également à s'assurer que l'entrée en crise n'est activée qu'à la suite d'une phase de qualification déterminante justifiant le passage en crise. Pour ce faire, il est recommandé d'avoir une cellule de vigilance en charge d'évaluer et de communiquer sur l'évolution de la situation et des risques, et peut décider du passage éventuel en état d'alerte et de l'escalade en crise si nécessaire.

Un dispositif d'information, entre les acteurs opérationnels en charge du traitement de l'incident et les acteurs internes / externes impactés par l'incident, est un élément important pour gérer un incident en cours de qualification.

La décision d'entrer en gestion de crise est une décision managériale appuyée par un exposé aussi factuel que possible de la situation et de son évolution potentielle. Bien que l'atteinte de seuils prédéfinis facilite la décision, celle-ci sera prise en considérant de nombreux facteurs tels que le caractère inconnu du problème, les accidents similaires au sein d'autres organismes, etc.

Par conséquent, une crise devient avérée dès lors qu'un incident de cybersécurité sort d'un cadre défini (criticité / périmètre métier impacté) par l'organisme et que la mise en place d'une réponse coordonnée devient nécessaire.

Type d'incident	Seuil incident mineur	Seuil incident majeur	Seuils de crise
Interruption / indisponibilité du SI x y	x minutes	x heures	y heures
Perturbation du SI x y	x minutes	x heures	y heures
Indisponibilité de Commander ou Livrer	X clients	y clients	z clients
Approvisionnement	Taux de rupture produits x	Taux de rupture produits y	Taux de rupture produits z
Atteinte à la confidentialité des données clients	X clients	y clients	z clients

Exemple de matrice d'évaluation des incidents

LES BONNES PRATIQUES

- Établir une grille de qualification des incidents de sécurité et des crises
- Définition d'une procédure de gestion des incidents de sécurité

1.2 Dispositif de crise

Le dispositif de crise lié à une cyberattaque a pour objectif de mener à bien les missions suivantes :

- identifier, alerter, mobiliser, gérer les équipes dans la durée ;
- comprendre la situation, détecter le problème et rassembler les informations ;
- maîtriser la situation, limiter les conséquences à un seuil acceptable et proposer des mesures adaptées à la situation (mise en sécurité des installations industrielles ou vitales, mesures de confinement et d'isolation des systèmes impactés...) ;
- échanger les informations, coopérer avec les pouvoirs publics et autres parties prenantes ;
- communiquer en interne et en externe ;
- sortir de la crise et gérer le post-accident ;
- organiser le fonctionnement du dispositif de crise lui-même (logistique, rotations, etc.).

LA CELLULE STRATÉGIQUE / DÉCISIONNELLE DE CRISE :

La cellule de crise est constituée d'individus aux fonctions clés (directeur de cellule de crise, adjoint, rédacteur de plan d'action, communication interne et externe, représentant IT, représentant cybersécurité, représentant métiers pour l'essentiel) ainsi que des fonctions supports (RH, juridique, finance, parties prenantes externes, etc.). Pour assurer une gestion efficace de la crise, il est conseillé d'associer à la cellule décisionnelle, des cellules opérationnelles et d'anticipation, notamment :

- une cellule intitulée « continuité d'activité » assignée à la conduite opérationnelle incluant la continuité d'activité ;
- une cellule chargée de l'investigation, la remédiation et la reconstruction du SI ;
- une cellule anticipation chargée d'identifier les possibles évolutions de la situation.

LES BONNES PRATIQUES (À PRÉPARER EN AMONT)

- Élaborer la composition des cellules de crise : sélection des fonctions métiers et supports indispensables à la gestion de crise
- Constituer des fiches missions aisées à consulter en situation d'urgence, rappelant les rôles de chacun
- Identifier les personnes intégrantes, a priori, les cellules de crise
- Identifier des salles disponibles et équipées
- Avoir un système d'alerte pour dépêcher les personnes en cellule de crise
- Déterminer les roulements des membres de la cellule de crise

EXEMPLE D'ORGANISATION DE CRISE (NIVEAU DE MATURITÉ ÉLEVÉE)

Dans le cas d'une cyberattaque paralysante, il est conseillé de former trois cellules qui seront en interaction tout au long de la crise. Toutefois, le niveau de maturité de l'organisme en matière de gestion de crise sera déterminant dans ce choix. La cellule de crise décisionnelle aura la charge de la validation et de la prise de décision, c'est elle qui donnera la ligne de conduite à adopter et qui apportera de l'ordre et de la clarté dans la gestion de crise, tant en interne qu'en externe. La cellule de crise continuité des activités prioritaires se focalisera sur les impacts métiers de la crise et se mobilisera pour permettre la continuité économique. La cellule informatique ou l'équipe d'intervention informatique analysera la cyberattaque et travaillera à la résolution de l'acte de malveillance, notamment par le remise en état du SI et de ses applications prioritaires.

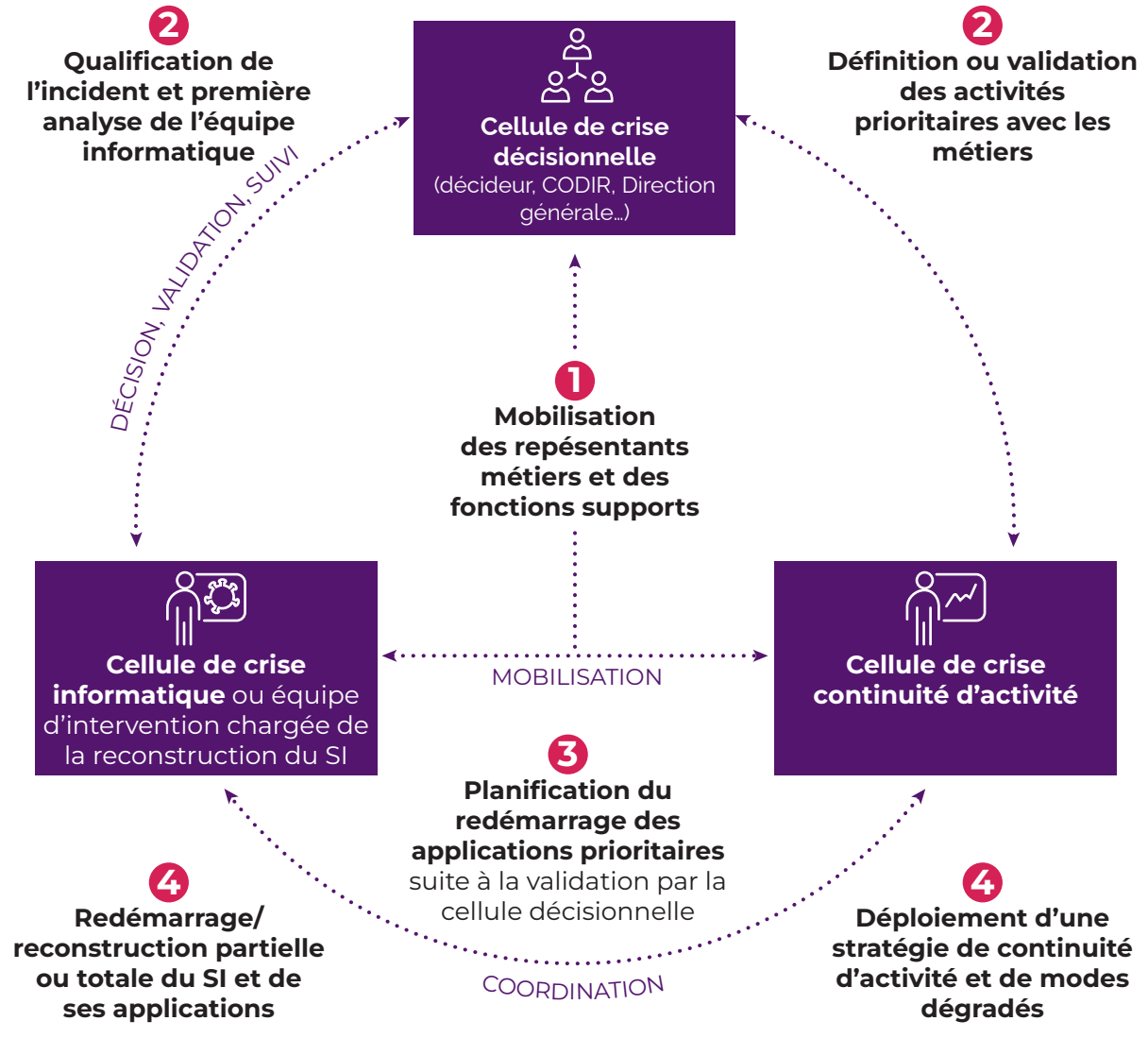


Figure 2 : Schéma de cellules de crise pour une organisation (niveau de maturité élevé)

EXEMPLE D'ORGANISATION DE CRISE (NIVEAU DE MATURITÉ INTERMÉDIAIRE)

D'autres organisations de crise peuvent être privilégiées par l'organisme selon le niveau de maturité. Elles peuvent être formées d'uniquement deux cellules de crise, en fusionnant la cellule continuité d'activité et la cellule dédiée au système d'information. En choisissant cette organisation, il est entendu que les deux objectifs, que sont la continuité d'activité minimale et le redémarrage du système d'information, soient couplés au sein d'une seule cellule, nommée la cellule soutien. Toutefois, cela n'empêche pas l'autonomie des équipes et des experts sur leur sujet de prédilection et le fait que les missions de chacun restent identiques. Il n'est ici question que de modifier l'organisation de la gestion de crise sans pour autant en changer la nature et les étapes.

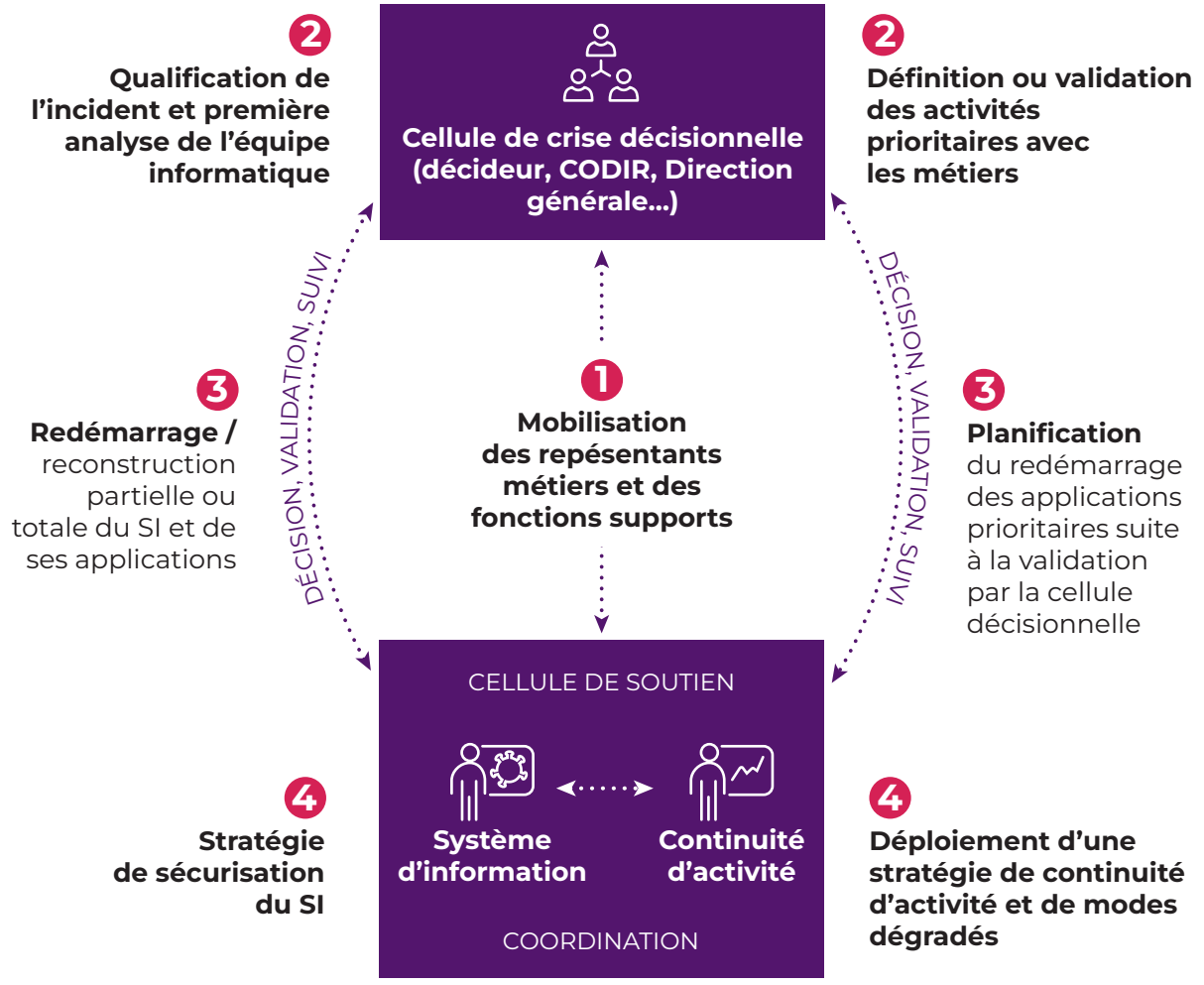


Figure 3 : Schéma d'organisation des cellules de crise pour une organisation (niveau de maturité intermédiaire)

UNE ORGANISATION DE CRISE (MODÈLE DE MATURITÉ DE PREMIER NIVEAU)

Dans ce dernier schéma, une unique cellule est mobilisée et comprend l'ensemble des dimensions de la gestion de la cyberattaque paralysante. L'organisme peut privilégier une organisation telle que celle-ci afin de centraliser les missions et les informations et chapeauter plus activement la gestion de crise. Celle-ci peut également être favorisée pour des raisons logistiques, en fonction de la maturité de la gestion de crise ou bien parce que la taille de l'organisme ne nécessite pas une organisation en plusieurs cellules. Il conviendra de laisser à la charge du décideur ou du CODIR le choix de l'organisation de la / les cellules. Toutefois, il est possible, au cours de la crise, de l'ajuster.

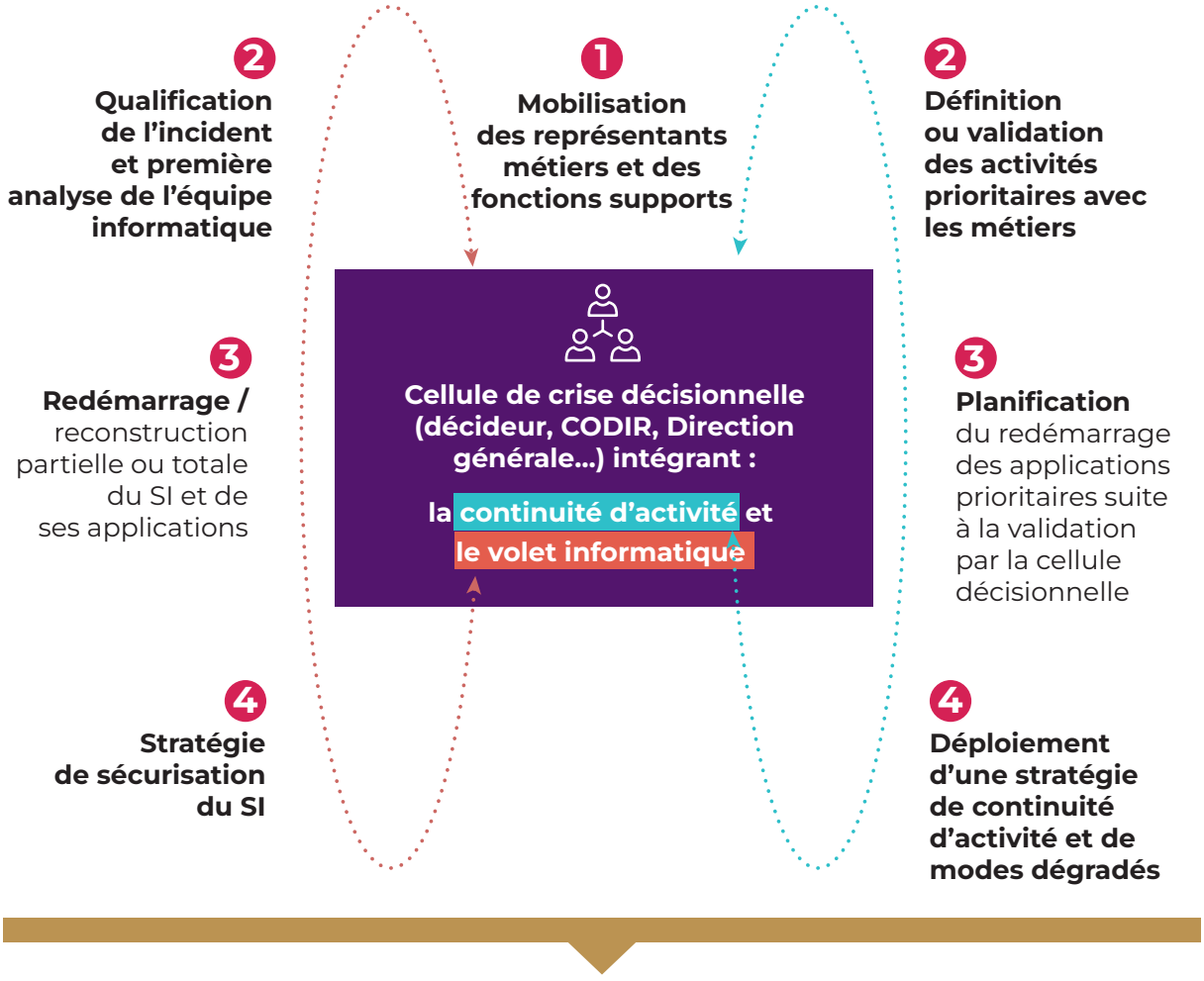


Figure 4 : Schéma d'organisation des cellules de crise (niveau de maturité de premier niveau)

1.3 Stratégie de gestion de crise

Au départ d'une crise, les premières mesures sont primordiales pour assurer la bonne gestion de la crise en elle-même. L'aptitude des décideurs à identifier et définir les différentes étapes et dimensions de la crise est essentielle. La stratégie de gestion de crise fournit donc les lignes directrices de l'organisation de crise et participe à rétablir la confiance au niveau du SI et de l'environnement de l'organisme victime.

Dans le cas d'une cyberattaque paralysante, l'organisme devra structurer son dispositif de réaction et se mobiliser sur deux fronts majeurs avec une stratégie globale et des déclinaisons opérationnelles spécifiques pour :

1. **La reconstruction du SI**
2. **La continuité d'activité Métiers**

En parallèle, les équipes de crise doivent avoir à l'esprit que la crise peut varier d'intensité en fonction de l'évolution de la situation selon différents facteurs ; à cet effet une matrice d'évaluation du niveau d'intensité peut être mise en place. Au-delà des aspects techniques et opérationnels métiers, il faudra s'attacher à couvrir d'autres dimensions clés dans la stratégie de gestion de crise, à savoir notamment :

- Dimension humaine et collectives
- Dimension communication de crise
- Dimension juridique et réglementaire
- Dimension assurantielle

Selon les circonstances, d'autres dimensions pourront également être prises en compte : stratégique et économique, éthique, politique.

AIDE À LA DÉCISION :

Cette stratégie de gestion de crise s'accompagne d'un processus de prise de décision visant à adopter un plan d'actions parmi plusieurs options. L'identification de ces dernières alimente un choix final en fonction des facteurs de pondération (aspects juridiques, techniques, opérationnels, etc.), de la part d'inconnu de la situation et des priorités stratégiques du décideur ou de la structure décisionnelle. Ce même choix va entraîner une action immédiate ou différée visant à minimiser les impacts de la crise. La qualité de l'échange des informations et les considérations temporelles vont impacter ce processus de prise de décision.

Plusieurs difficultés à la prise de décision sont à considérer lors d'une crise. La lucidité, la rationalité et les aptitudes du décideur et de ses équipes vont être mis à rude épreuve. L'énoncé d'objectifs précis aidera à l'établissement d'un processus de prise de décision adéquat. Sans cela, la survie de l'organisme peut être d'autant plus menacée. En

effet, la crise peut s'exacerber et générer des impacts néfastes à long terme. La crise crée un environnement stressant et incertain pouvant faire échouer le processus de décision rationnel influencé par des facteurs humains et culturels par nature faillibles.

En cas de cyberattaque, la visibilité est encore plus réduite et la situation d'autant plus incertaine pour ce type de scénario de crise malveillant, techniquement déstabilisant et mouvant. Qui plus est, la plupart des organismes manquent de recul et d'expérience en la matière. Il est préconisé de réagir très vite lors d'un incident cyber afin d'éviter la propagation de l'attaque dans le système d'information. Une forte pression couplée à l'urgence de décider fait supporter au décideur un stress difficile à gérer. Il est donc conseillé au décideur, en raison de la technicité de la crise, de s'entourer d'un ou plusieurs expert(s) du système d'information (fonctions support) et d'une ou plusieurs personnes dédiées à la continuité d'activité (fonctions métiers) afin de l'épauler dans sa prise de décision et la rendre plus efficiente. Les rôles d'anticipation et de crise sont également à prendre en compte.

1.4 Dimension humaine et collective

Il est fortement conseillé, au-delà d'une étroite collaboration entre les équipes Métiers et SI, de créer une dynamique collective avec les autres parties prenantes et ce de manière continue. Les équipes vont se coordonner entre elles sous l'égide de la cellule décisionnelle de crise.

De plus, et ce malgré la crise, il est important que la dynamique de collaboration soit positive afin que toutes les parties prenantes œuvrent dans le même sens (ce n'est pas le moment de chercher des coupables, mais de maintenir un collectif uni dont le seul but est de surmonter la crise).

GESTION DU STRESS

Une crise provoque de fortes turbulences pouvant entraîner des comportements inhabituels et inadaptés dans le cadre de la gestion d'une crise. Tout au long de la crise, les personnes mobilisées, les clients, les partenaires et le personnel vont être sujets à un stress permanent, généralement intériorisé.

La dimension anxiogène de la crise et ses effets sur les collaborateurs doivent faire l'objet d'une attention particulière. En effet, la crise peut s'installer dans le temps, il faut donc prendre en compte la fatigue des équipes et la possibilité d'avoir une rotation des personnes. Cela implique de pouvoir faire une passation des informations avant chaque relève entre les équipes. Il peut donc être nécessaire, s'il y a beaucoup de salariés impliqués dans la résolution, de nommer une personne chargée de la gestion du planning au sein de la cellule de crise. Mettre en place une logistique de crise prenant en considération les besoins primaires des individus, en fournissant le matériel nécessaire et en organisant le roulement favorisera un climat apaisé. Il s'agit de ne pas provoquer une sur-crise résultant d'une charge mentale trop forte.

Parallèlement, suite aux résultats de l'investigation numérique ou à des problèmes rencontrés durant la gestion de la crise, certains collaborateurs non forcément mobilisés peuvent se sentir fautifs ou frustrés, ayant déjà remarqué la vulnérabilité exploitée par l'agent de menace. Le ou les managers hors cellule doivent être vigilants pour déceler une difficulté chez un collaborateur.

COORDINATION, MISE EN RÉSEAU ET ÉCHANGE D'INFORMATION

La première étape est de définir un canal de communication unique qui servira à la transmission et la diffusion des informations critiques. La transmission de l'information doit être exécutée avec méthode pour ne pas noyer les équipes d'informations. Il est essentiel de synthétiser les éléments diffusés tout en étant clair pour permettre une meilleure compréhension des requêtes et des besoins et ainsi apporter des réponses et des solutions appropriées. Le canal de communication doit, dans la mesure du possible, être indépendant du système d'information actuel qui est compromis et sécurisé. Sur certaines crises, il a pu être observé que l'agent de menace suivait l'ensemble des communications des équipes opérationnelles et pouvait utiliser les canaux de communication pour propager des messages de manipulation et de désinformation afin de mettre l'organisme sous-tension.

En complément du journal de bord (main courante ou minutier), un document de suivi des actions est à déployer pour partager les livrables produits qui sont précisés dans chaque préconisation de la partie 6. Cet outil peut être un document Excel recensant les activités métiers prioritaires, les mesures d'urgence décidées, la stratégie de continuité d'activité socle, les stratégies dérivées et les modes dégradés déployés en fonction. Ce document doit être le plus synthétique possible tout en étant clair et lisible pour chacun. Une dimension IT et une dimension Métiers doivent être implémentées pour permettre aux équipes de comprendre rapidement les missions à exécuter par chacune des équipes.

Le mot d'ordre de cette coordination doit être **la transparence**. Celle-ci se traduit par une clarté de la communication et des points de situation réguliers entre les équipes SI, Métiers et un décideur ou une structure décisionnelle. Pour ce faire, un coordinateur SI et un coordinateur Métiers peuvent être désignés afin de fluidifier la communication et la coordination et notamment de partager les évolutions de la situation et les dernières consignes applicables à destination des collaborateurs.

Pour les points de situation, un document tel qu'une « fiche réflexe » peut être rédigé au préalable ; il comprendra les questions principales à soulever et permettra d'éviter un oubli. Ces points de situation sont à programmer de manière régulière, voire de manière rapprochée en début de crise. Il est ensuite conseillé, en fonction de l'évolution de la crise, d'écourter et de planifier ces points de situation à des échéances plus longues.

DYNAMIQUE COLLECTIVE

Réussir à s'adapter et à se montrer réactif face à des événements imprévisibles est un facteur clé pour minimiser l'impact de la crise. Il est préconisé d'insister sur le besoin de résilience collective des équipes mobilisées. Trois éléments peuvent faciliter l'instauration d'une dynamique collective : la coopération, la flexibilité et l'écoute. La capacité de l'organisation à surmonter le choc, soit sa « résilience » repose sur la résilience des équipes qui est nécessaire à la reprise de l'activité, tant au niveau collectif qu'au niveau individuel. Les coordinateurs SI et Métiers peuvent sensibiliser les équipes en charge de la gestion de la cyberattaque à ces éléments.

Parallèlement à la coordination entre les équipes SI et Métiers, il est fortement préconisé d'entretenir et de consolider l'adhésion de l'organisme à des réseaux d'acteurs (associations, clubs, institutions publiques…).

Les liens entretenus par l'organisme avec les différentes parties prenantes de l'organisation sont également stratégiques. Échanger régulièrement et en toute transparence créera un climat de confiance qui les incitera davantage à apporter leur soutien

à l'organisation. De plus, les partenaires peuvent devenir des alliés dans le cadre de la crise en fournissant, par exemple, du matériel de prêt ou de l'expertise pouvant faire défaut au sein de l'organisme. Ils peuvent également offrir des retours d'expérience pertinents sur la situation.

Cette dynamique collective dépend donc de la capacité de l'organisme et notamment du décideur à engager un processus collaboratif englobant l'ensemble des maillons de l'écosystème organisationnel pour assurer la sauvegarde de l'organisme.

ACTIONS À MENER POUR LES ÉQUIPES DE CRISE

- Déployer une logistique de crise de confort pour les équipes de crise (base vie, repas, utilités...)
- Faciliter la prise en charge financière des coûts exceptionnels liés à la crise : garde familiale, transports, chambres d'hôtels...)
- Mettre à disposition un soutien médico-psychologique dès le début de crise
- Mettre en place du renfort (ressources supplémentaires là où cela est possible et se justifie)
- Organiser une relève des équipes (temps de repos faire souffler les équipes)

BONNES PRATIQUES POUR LA COORDINATION (À PRÉPARER EN AMONT)

- Définir une fiche mission pour le coordinateur SI
- Définir une fiche mission pour le secrétaire de crise
- Définir une fiche mission pour le directeur de crise
- Définir une fiche mission pour l'anticipateur
- Définir une fiche mission pour le coordinateur continuité d'activité
- Dresser une liste des canaux de communication mobilisables en cas de cyber-attaque
- Définir une fiche réflexe pour les points de situation : les questions à poser côté SI et côté continuité d'activité, les besoins de l'équipe SI de la part de l'équipe continuité d'activité et inversement
- Définir une fiche réflexe sur la manière de communiquer / diffuser l'information entre les pôles SI et continuité d'activité
- Modèle de bulletin d'information et de synthèse

BONNES PRATIQUES POUR CRÉER UNE DYNAMIQUE COLLECTIVE (À PRÉPARER EN AMONT)

- Organiser des entraînements à la gestion de crise (exercices de simulation et tests)
- Établir des bonnes pratiques de management (collaboratif et participatif)
- Maintenir le lien avec les grands fournisseurs essentiels et les clients
- Établir la relation avec la communauté des pairs

1.5 Dimension communication de crise

Pour préparer efficacement sa communication de crise en détail, l'organisme pourra se référer au guide de l'ANSSI[1]. L'essentiel est d'anticiper et de mener à bien en amont de la crise les préconisations ci-dessous :

- initier un dialogue avec les équipes cyber et IT hors période de crise ;
- anticiper les scénarios de crise ;
- construire une stratégie de crise en amont pour mieux faire face à la pression et être plus réactif ;
- communiquer auprès des collaborateurs sur l'état de la situation et les consignes à appliquer ;
- identifier les parties prenantes externes possibles (clients, prestataires, partenaires, autorités, interne, médias, etc.) ;
- travailler les argumentaires, les postures de communication et les messages clés, vis-à-vis des menaces de l'organisation et des attaques cyber type ;
- préparer une trame de communication de crise ;
- identifier des porte-parole potentiels afin de les préparer ;
- anticiper les éventuelles questions type ;
- créer une boîte à outils dédiée à la gestion d'une crise d'origine cyber, comprenant une liste des outils de communication disponibles et alternatifs, ainsi qu'un glossaire ;
- former les équipes à la gestion du volet communication.

Le rôle de la communication en situation de crise cyber :

- préserver la réputation et l'image de son organisme pendant et en sortie de crise ;
- rassurer rapidement les publics concernés sur le fait qu'un dispositif de crise a été mobilisé et gérer « l'impact émotionnel » de la crise ;
- modérer les impacts de la crise (court terme mais aussi long terme) ;
- montrer la mobilisation de l'organisme pour trouver une solution rapide au problème.

Au sein de la cellule de crise et conjointement avec les experts techniques et la direction, la communication de crise cyber vise à :

- définir la stratégie de communication au regard du contexte (posture pro-active ou réactive ?) :
  - préparer les messages adaptés à chaque cible, ce qui comprend la vulgarisation d'éléments techniques et les décliner en fonction des canaux de communication ;
  - trouver des canaux de communication alternatifs en cas d'indisponibilité des outils de communication ;
- analyser et faire évoluer les postures de communication en fonction de l'évolution de la crise et de sa perception par les publics ;
- assurer la cohérence et la coordination des différents types de communication qui sortent de l'organisme : la communication technique, institutionnelle et politique.

1. *GUIDE ANSSI : 2021 - Collection Gestion de crise* - Anticiper et gérer sa communication de crise cyber.

Quelques recommandations pour une communication de crise efficace :

- être dans la transparence maitrisée, respecter les faits, ne pas mentir ou indiquer les suppositions faites ;
- être accessible, utiliser un vocabulaire simple et pédagogique, éviter le jargon de technicien ;
- être concret, ne pas rassurer sans éléments de fond ;
- éviter d'adopter un ton et un vocabulaire trop anxiogène ;
- garder de la cohérence, ne pas se contredire dans la durée et d'un point d'émission d'information à l'autre ;
- être complet, s'adresser à toutes les cibles, de l'organisation qui sont en droit d'attendre des éléments sur la situation – adresser une attention particulière à l'interne, trop souvent oublié ;
- éviter le « Pas de commentaire » ;
- éviter une attitude négative tout en reconnaissant les problèmes ;
- ne pas se précipiter : respecter et expliquer le temps long des investigations techniques et de la remédiation ; donner de la visibilité sur les actions mises en œuvre sans s'engager sur des dates trop précises ;
- ne pas attendre d'avoir l'exhaustivité des informations et préférer une première communication (même succincte) afin d'éviter qu'un tiers ne communique avant l'organisme ;
- ne pas chercher à désigner un coupable, ne pas faire d'attribution, qui reste une décision particulièrement complexe et politique, qui doit être prise parfois au plus haut niveau de l'État ; faire prévaloir la solidarité ;
- conserver un contact régulier avec les différentes cibles ;
- être réactif, essayer de conserver un objectif de temporalité ;
- en cas de judiciarisation, limiter sa communication pour respecter le secret de l'instruction.

LES BONNES PRATIQUES (PRÉPARER EN AMONT)

- Préparer une trame de communiqué de crise
- Préparer des éléments de langage
- Préparer le Directeur communication en effectuant des exercices de crise
- Connaître les canaux de communication à privilégier durant une crise
- Coordonner les différents fils de parole (des différentes parties prenantes) pour rendre la communication globale de l'organisation cohérente, claire et maîtrisée
- Préparer des formats de communication adéquats en fonction des canaux de communication (posts LinkedIn, tweets, télévision, presse écrite, réseaux sociaux,...)
- Avoir des outils de communication alternatifs à disposition lors d'une cyberattaque
- Tester et évaluer à fréquence régulière les outils de communication alternatifs au cours d'exercices de crise

1.6 Dimension juridique et réglementaire

Le service juridique est un maillon essentiel dans le cadre d'une cyberattaque et lors de la reconstruction après une attaque. Selon le type d'attaque et de données touchées, les actions à mettre en œuvre peuvent différer.

LA GESTION CONTRACTUELLE

Les contrats doivent prévoir plusieurs mécanismes juridiques afin de pouvoir faire face en cas de cyberattaque.

Lors de l'établissement des contrats, que ces derniers soient conclus avec des clients ou des fournisseurs, des clauses spécifiques sur la cybersécurité doivent être définies afin de pouvoir prévoir et protéger les SI et leurs données.

En cas de cyberattaque, les contrats et leurs éventuels engagements de services sont étudiés, afin de pouvoir communiquer au mieux avec les clients ou fournisseurs pouvant être impactés notamment en cas d'arrêt du service.

L'étude des responsabilités est menée du point de vue juridique par le service juridique ou son conseil.

LE DÉPÔT DE PLAINTE

Le dépôt de plainte est préconisé, que l'auteur soit connu ou non. Le plus souvent dans le cas des cyberattaques ce dernier n'est pas identifié mais l'enquête judiciaire ouverte à la suite de la plainte déposée peut permettre son identification.

Le dépôt de plainte peut être fait auprès des forces de l'ordre, en se rendant au service de police ou de gendarmerie le plus proche de l'entreprise (ou du lieu de contestation des faits). Ces derniers redirigeront l'organisme victime vers les services spécifiques de lutte contre la cybercriminalité

Le dépôt peut être fait par le représentant de l'entreprise, muni d'un pouvoir s'il n'est pas le dirigeant et d'un extrait de KBIS si possible. Dans le cas où l'entreprise dispose de ressources dédiées à la cybersécurité, que celles-ci soient internes ou externes, il est important qu'elles soient présentes lors du dépôt de plainte, afin de pouvoir fournir l'ensemble des éléments techniques.

Il sera demandé de fournir les éléments suivants :

- le descriptif précis de l'incident ;
- les coordonnées de l'ensemble des intervenants et prestataires susceptibles de pouvoir communiquer des informations aux enquêteurs ;
- l'ensemble des éléments techniques collectés tels que les traces informatiques (note de rançon, code malveillant…), l'adresse des machines, le type de machines touchées, si le SI est hébergé par un fournisseur externe à l'entreprise ;
- les mails et toutes informations en lien avec la cyberattaque ;
- l'organigramme, la présentation de la société et la liste du personnel.

Il est important de préserver ou de faire préserver toutes les traces de l'attaque (Cf. 2.1), avec notamment une copie de l'état du SI.

Par suite du dépôt de plainte, des investigations peuvent être réalisées, elles peuvent amener les enquêteurs à se déplacer dans les locaux ou solliciter des accès au SI.

LA NOTIFICATION DES AUTORITÉS

Selon la nature de l'activité et le type d'impacts, l'entreprise peut devoir notifier la cyberattaque et ses impacts à des autorités françaises et étrangères.

Cas des données personnelles :

Dans le cas où la cyberattaque impacterait des données personnelles (Règlement Général sur la Protection des Données RGPD en Europe), l'organisme, s'il est responsable de traitement, doit notifier la violation de données à l'autorité de contrôle. Cette notification doit être réalisée dans les 72h suivant la connaissance des faits.

Cette notification doit comporter *a minima* les éléments suivants :

- la nature de la violation ;
- les catégories, nombre de personnes et de fichiers concernés ;
- les conséquences probables de la violation ;
- les mesures de remédiations prises.

L'organisme doit aussi étudier si une communication auprès des personnes concernées doit être faite.

Dans le cas où l'organisme est sous-traitant, il se doit de prévenir dans les plus brefs délais, le ou les responsables de traitement, le plus souvent cette notification et son délai sont prévus contractuellement.

Dans tous les cas, la violation doit être documentée dans le registre afférent.

Cas des cyberattaques concernant un secteur ou une activité soumise à notification :

Certains acteurs selon leur activité (Opérateur d'Importance Vitale ou Opérateur de Services Essentiels...) ou leur secteur (industrie de défense, finances) doivent notifier aux autorités de tutelle les cyberattaques qui les toucheraient. La notification, au-delà des obligations réglementaires, peut permettre de protéger les autres acteurs de la filière en partageant les éléments techniques sur la menace. Les incidents impliquant des informations classifiées doivent également faire l'objet d'une déclaration aux autorités de tutelles. En cas de doute relatif aux obligations de l'organisme, il convient de contacter directement, quand il en existe un, le Centre gouvernemental chargé de la veille, d'alerte et de réponse aux attaques informatiques.

1.7 Dimension assurantielle

L'assurance cyber est un service qui peut fournir plusieurs prestations, généralement financières, en cas de survenance d'un sinistre cyber en échange du paiement d'une prime d'assurance. Pour autant, l'entreprise couverte par un contrat d'assurance cyber doit respecter plusieurs règles et faire preuve de diligence auprès de son assureur pour que le contrat s'applique dans de bonnes conditions.

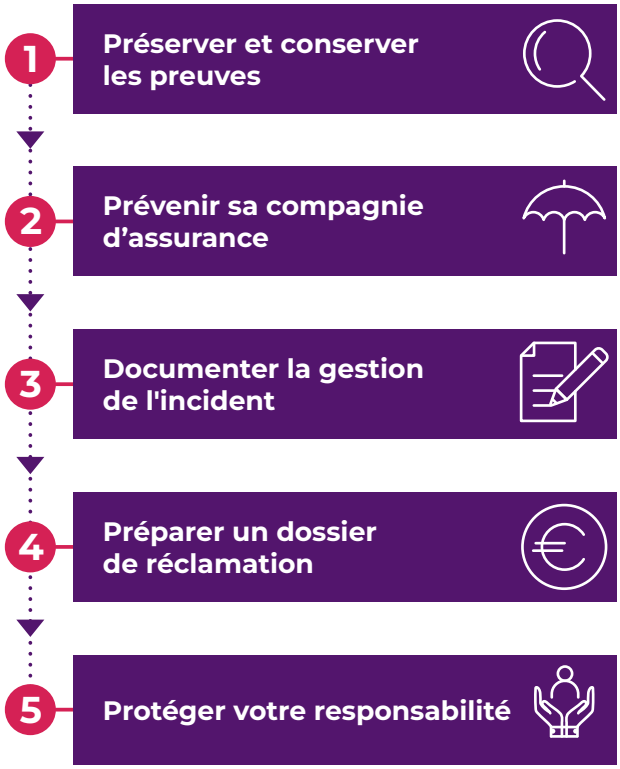


Figure 5 : Cyberassurance : règles à suivre

PRÉSERVER ET CONSERVER LES PREUVES

Elément essentiel de l'activation des garanties du contrat, la preuve qui expose la nature et le mode de survenance de l'incident cyber doit être apportée avec des faits pour rentrer dans une « case de garantie » du contrat. En cas de sinistre, c'est à l'assuré d'apporter la preuve de la nature et de l'étendue de ses dommages pour établir son préjudice. La préservation des preuves joue un rôle capital pour permettre l'indemnisation du sinistre mais également pour repousser les éventuels recours des tiers que l'entreprise pourrait subir en recherche de responsabilité. De même, les preuves seront également utiles aux forces de l'ordre dans le cadre d'un dépôt de plainte.

PRÉVENIR SA COMPAGNIE D'ASSURANCE

Prévenir son assureur (son courtier s'il y en a un) dès la survenance du sinistre, au plus tard dans le délai prévu au contrat, est essentiel pour la bonne gestion du dossier.

Plusieurs assureurs mettent à disposition un service d'assistance à travers un numéro de téléphone communiqué lors de la souscription du contrat. Ce service est inclus au contrat d'assurance mais tous les assureurs ne le proposent pas. Le numéro d'appel est généralement connu du responsable des assurances et doit être partagé avec les cadres d'astreinte (ou responsable sécurité SI). Ce service d'assistance peut fournir des ressources juridiques, techniques (pilotage, investigation numérique, reconstruction) et de communication de crise.

L'assistance n'a pas de caractère obligatoire. Toutefois, il est préférable de l'informer même si l'assuré ne souhaite pas faire appel aux ressources proposées ou les utiliser partiellement. En effet, selon les assureurs, l'appel à la plateforme d'assistance permet de notifier la compagnie d'un incident et en conséquence, elle désignera un gestionnaire pour le suivi du dossier. D'autre part, l'assistance proposée par l'assureur peut être utilisée afin de répondre à des besoins spécifiques (intervention dans un pays à risque ou compenser l'indisponibilité d'une personne clé).

L'assistance repose le plus souvent sur une liste de prestataires mise à disposition par l'assureur. Cependant, lors de la souscription, il est possible de demander à son assureur d'inclure dans la liste, des prestataires de son choix, sous réserve de l'accord de la compagnie.

Si l'entreprise s'appuie sur l'assistance de son assureur, il convient de faire participer le gestionnaire de crise mis à disposition par la compagnie aux réunions techniques et de suivi. De même, le gestionnaire du dossier pourra suivre l'évolution du dossier et proposer des solutions d'assistance complémentaires le cas échéant. L'assureur cyber peut également être force de proposition pour aider l'entreprise à faire face.

DOCUMENTER LA GESTION DE L'INCIDENT

Les preuves doivent être communiquées à votre assureur. Il est recommandé de les sacraliser et de les conserver jusqu'au terme de l'instruction du dossier et notamment :

- les journaux d'évènements ayant servi pour établir le rapport d'investigation numérique ;
- le rapport d'investigation définitif et les rapports d'étape ;
- les notifications aux autorités qu'elles soient européennes ou étrangères ;
- le dépôt de plainte ;
- les éléments de suivi et de chronologie des actions à l'entreprise.

PRÉPARER UN DOSSIER DE RÉCLAMATION

Ces éléments sont à rassembler dès le démarrage de la réponse à incident. Pour fluidifier l'expertise, un chantier peut être mis en place pour réunir les éléments nécessaires à la présentation d'une réclamation qui soit suffisamment documentée. Les actions réalisées par les équipes internes à l'instar des prestataires externes doivent faire l'objet de relevé de temps avec un niveau de détail suffisant pour permettre à l'assureur de comprendre la nature des travaux sur le SI et prendre position. De même, l'ensemble des frais engagés pour atténuer ou maintenir la perte d'activité (communément les frais supplémentaires d'exploitation) doivent être documentés.

Les documents suivants doivent être conservés pour l'expertise :

- les offres reçues, les devis sur l'ensemble des prestations engagées (y compris juridique, communication de crise et mesures pour maintenir la marge de l'entreprise) ;
- les factures reçues ;
- le détail des temps passés y compris pour les collaborateurs mobilisés en interne ;
- les éventuels comptes rendus d'intervention, détail des actions.

PROTÉGER VOTRE RESPONSABILITÉ

Une cyberattaque peut entraîner des conséquences sur vos partenaires en amont et en aval de votre chaine de valeur. De même l'attaque d'un partenaire peut entraîner des conséquences sur votre activité et engager votre responsabilité. Les contrats cyber incluent pour la majorité un volet responsabilité. Si vous êtes victime d'une attaque ou si vous êtes informés que votre SI a pu servir de point rebond ou qu'il est potentiellement suspecté d'avoir un lien avec un incident cyber, il convient de prendre des dispositions pour se protéger dans le cadre du volet cyber de votre contrat.

- conserver les échanges des communications avec les partenaires ;
- si vous êtes obligés d'informer des ayants droit, l'avis du conseil de votre assureur est fortement recommandé avant de communiquer ;
- si vous êtes mis en cause de manière officielle (lettre recommandée avec accusé de réception) par un tiers avec une réclamation chiffrée en dédommagement, communiquez avec votre assureur avant d'envisager une réponse. Toute démarche de règlement en dehors de ce cadre pourrait être considérée comme un geste commercial sans que cela engage votre assureur, donc non indemnisable.

LE RÔLE DES PCA / PRA / PCI ET AUTRES PLANS DE DÉFENSE

Les assureurs sont sensibles à l'ensemble des dispositions et des mécanismes de défense mis en place pour réagir à une cyberattaque. Ces plans sont étudiés par les assureurs avant la souscription et au moment des renouvellements des contrats. Une attention particulière est portée depuis quelques années sur la feuille de route (ou schéma directeur) de la sécurité du SI, les assureurs s'attachant à suivre son évolution tout au long de la vie du contrat. Il en est de même des déclarations sur la réalité technique du SI et des briques de sécurité en place au moment de la souscription car elles sont de nature à influer sur le montant de la prime, les garanties et les montants accordés.

En cas de sinistre, cet aspect sera examiné par l'expert. Ainsi il est recommandé de conserver et de tenir à disposition, si nécessaire, les comptes rendus (CR) de revue du schéma directeur, les indicateurs, les CR de revue opérationnelle et les procès-verbaux (PV) de recette des solutions qui auraient pu être déployées avant l'attaque.

La communication à votre assureur d'un élément de sécurité en phase de souscription peut se traduire par une exclusion dans le contrat. Par exemple, la mise en place de l'authentification multi-facteurs sur les accès distants peut faire l'objet d'une exclusion contractuelle, l'assureur partant du principe que cette fonctionnalité est déployée sur le SI. De manière générale, les déclarations initiales sur la sécurité du SI sont examinées par l'assureur en cas de sinistre et recollées avec les constats effectués par les experts.

Il convient donc d'être vigilant et exhaustif sur les déclarations initiales notamment lors de la souscription du contrat concernant les risques non acceptables et les motifs d'exclusion des garanties.

LE CAS PARTICULIER DE L'ENQUÊTE NUMÉRIQUE

L'activation d'un contrat d'assurance cyber en cas d'attaque impose une vigilance particulière sur deux points de l'investigation numérique.

1. L'investigation numérique doit être menée par un acteur indépendant. En d'autres termes, l'entreprise en charge ne doit pas être un prestataire habituel de la sécurité du SI afin de préserver les voies de recours de la compagnie. En effet, à partir du moment où une compagnie d'assurance prend en charge un sinistre, elle peut par le mécanisme de subrogation, rechercher des responsabilités. Ainsi si l'investigation numérique est confiée, par exemple au prestataire en charge du SOC ou de la supervision des équipements périmétriques, l'assureur (et d'éventuels tiers) peuvent y voir un potentiel conflit d'intérêts et même douter de la véracité des éléments du rapport. L'assureur peut aller jusqu'à solliciter une nouvelle enquête.
2. L'investigation numérique doit porter sur le périmètre touché par la cyberattaque ainsi que les autres équipements au vu de l'enquête et s'appuyer sur des outils éprouvés et si possible automatisés (type agents de collecte). L'assureur peut résilier son contrat en cas de survenance d'un sinistre comme il peut le renouveler. Une vérification intégrale du parc et donc du risque couvert est de nature à le rassurer. Si l'investigation numérique est partielle, une recherche de compromissions sur tout le périmètre *a posteriori* est recommandée pour garantir un maintien des garanties et un renouvellement de la police d'assurance.

LA PERTE D'EXPLOITATION

La perte d'exploitation représente généralement l'impact le plus important dans une cyberattaque de type rançongiciel avec un rapport de 10 à 20 par rapport aux coûts directs (remédiation). L'approche suivie par l'assureur pour évaluer les pertes financières ne se différencie pas de celle pour d'autres types de sinistres (incendie, dégât des eaux, tempête...). En revanche, l'assureur sera vigilant à l'établissement du lien de causalité entre l'indisponibilité du SI et la mise à l'arrêt de l'outil de production en particulier dans les activités de transformation et notamment l'ensemble de l'industrie.

Le fonctionnement en mode dégradé peut comprendre des mesures provisoires (appel à de la sous-traitance, modification de la logistique etc.) pouvant être couvertes par un contrat cyber.

Point de vigilance : les coûts engagés doivent permettre de dégager une marge brute de l'entreprise. Dans le cas contraire, ils ne seront pas pris en charge.

L'activation d'un contrat d'assurance cyber est pertinente s'il apparait rapidement que le coût du sinistre excédera la franchise.

ACTIONS À MENER

- Informer votre assureur
- Préserver les preuves et les échanges avec les tiers
- Faire une copie, conformément à l'état de l'art, du disque pour appuyer la procédure judiciaire. S'assurer que les preuves ne sont pas manipulables et restent intègres tout au long de la procédure
- Tenir une chronologie des actions
- Ne pas hésiter à solliciter l'avis juridique de votre assureur
- S'assurer d'une investigation numérique indépendante
- Documenter tous les frais liés à l'incident
- Maintenir un canal de communication avec l'expert désigné par l'assureur

BONNES PRATIQUES POUR AVOIR RECOURS À L'ASSURANCE (À PRÉPARER EN AMONT)

- Souscrire un contrat d'assurance Cyber (Cf. Annexe A pour plus de détail)
- Documenter l'ensemble des mesures mises en œuvre pour permettre la production en mode dégradé pendant la période de restauration du SI et au fur et à mesure de la réouverture des services spécifiques aux métiers de l'entreprise (comptabilité, ressources humaines, finance, production, vente en ligne...)
- Mettre en place une démarche de prévention des risques cyber et mesures d'hygiène informatique
- Mettre en place des PCA / PRA / PCI
- Réaliser des tests de restauration des sauvegardes, déclenchement PRA
- Réaliser des simulations d'exercices de crise Cyber

PARTIE 2
SPÉCIFICATIONS TECHNIQUES POUR LA RECONSTRUCTION DU SI

La reconstruction du système d'information après une cyberattaque paralysante constitue un défi technique sur plusieurs aspects.

En effet, le système d'information a été compromis par un agent de menace ; si le SI est restauré dans l'état où il l'était juste avant l'attaque, l'agent de menace pourra compromettre de nouveau par la méthode employée la première fois. Par exemple, le SI restauré peut contenir des codes malveillants permettant à l'attaquant de prendre le contrôle une seconde fois des postes et serveurs. La compréhension de l'intrusion à travers l'investigation numérique est un élément indispensable pour permettre de restaurer le SI de façon sûre et de corriger les vulnérabilités exploitées ou facilement exploitables afin d'éviter une nouvelle compromission.

Le travail de reconstruction et de sécurisation est souvent complexe et chronophage. Il a souvent fallu plusieurs années pour bâtir le système, sa reconstruction dans un délai court n'est pas aisée. Lorsque les actions de sécurisation devront être menées, par exemple le changement de l'ensemble des mots de passe / secrets, la cartographie du système d'information sera un élément clef ainsi que la disponibilité d'experts.

Le travail de reconstruction va être une course contre la montre afin de refournir l'accès aux applications et aux données mais aussi de mener les actions de sécurisation nécessaires pour regagner la confiance dans le système d'information. L'ensemble des décisions de la cellule de crise devront se baser sur la compréhension de l'incident et une approche de gestion des risques. Il est nécessaire de trouver un compromis entre le temps nécessaire à la sécurisation du SI et le délai maximum supportable pour l'organisation. La mise en place d'une surveillance du système d'information combinée avec le maintien des actions conservatoires comme l'isolation réseau vis-à-vis d'Internet ou des réseaux tiers peut permettre de maintenir un niveau de risques acceptable et de fournir un accès minimum au système d'information.

La reconstruction du système d'information est souvent décomposée en plusieurs sous-chantiers qui devront échanger ensemble pour partager les informations notamment la compréhension de l'intrusion.

Un séquencement organisé des actions est le moyen le plus sûr de revenir à une situation normale.

Le diagramme ci-dessous propose un schéma général d'agencement des chantiers à mettre en place sous la supervision de la Cellule de Crise :

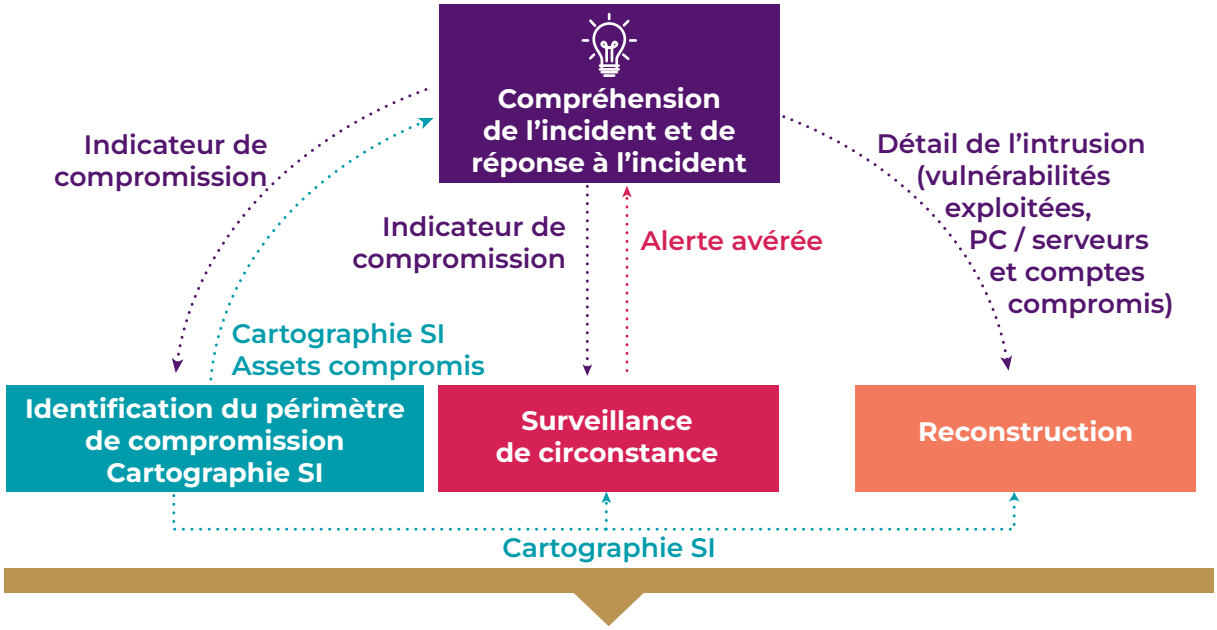


Figure 6 : Articulation des équipes techniques pour la reconstruction du SI

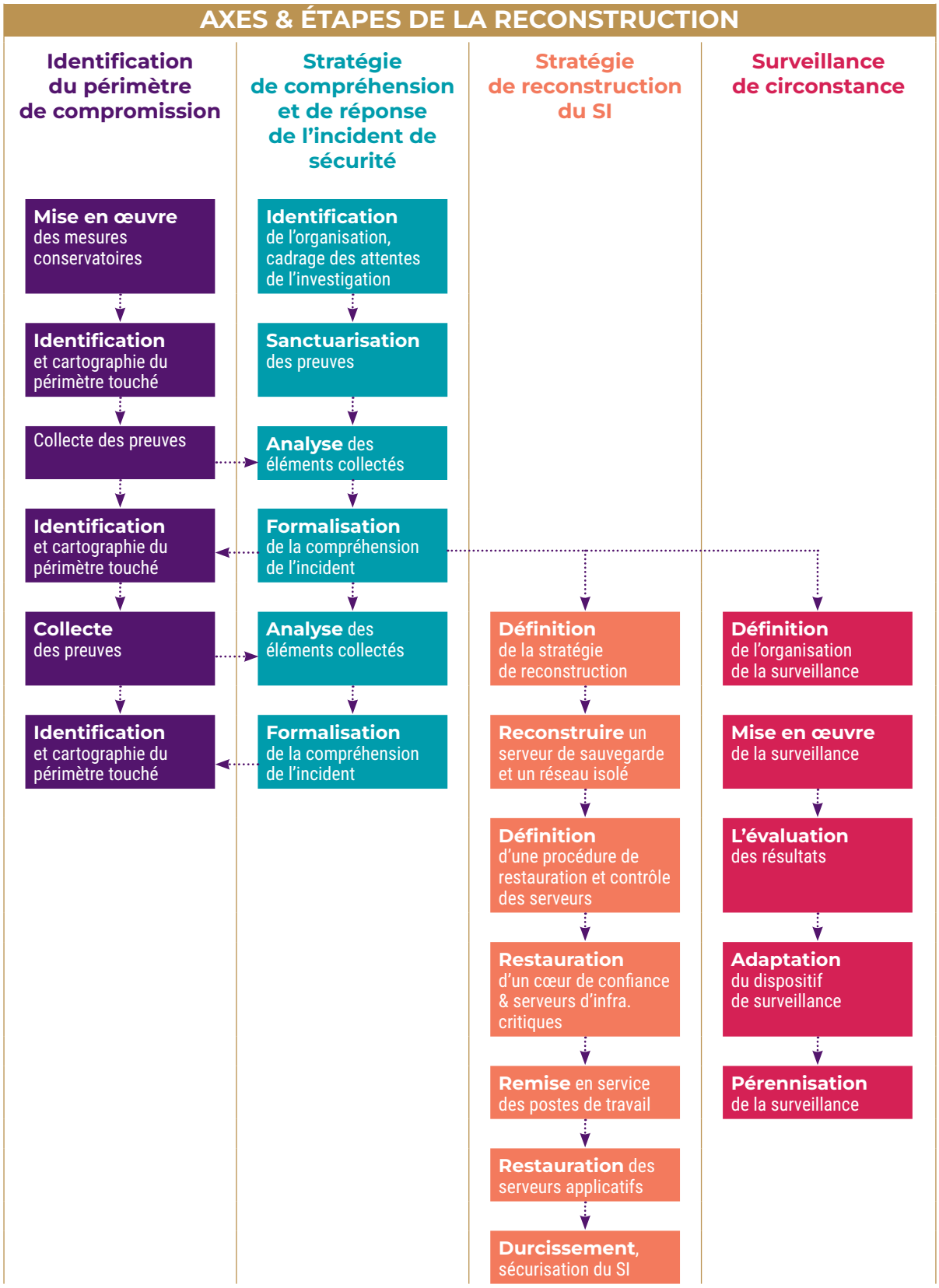


Figure 7 : Répartition des différentes étapes de la reconstruction

Chaque chantier est composé d'étapes dont la teneur sera examinée.

Il est important de comprendre que les travaux sont itératifs : une première identification, sommaire, du périmètre de compromission, alimente la compréhension qui elle-même orientera la nature de la gestion de crise (purement technique, dimension réglementaire, purement curative ou palliative, durée estimée de la phase de reconstruction, suffisance des ressources internes ou recours à l'extérieur, etc.).

L'amélioration itérative de la compréhension influence le travail de préparation de la reconstruction, la conception de la surveillance de circonstance, de préservation de la partie épargnée du SI, etc.

2.1 Stratégie de compréhension et de réponse à incident de sécurité

L'investigation numérique, ou *forensic* en anglais, passe par une analyse technique des systèmes compromis afin d'identifier les modes opératoires de l'agent de menace, les marqueurs de l'attaque (appelés également indicateurs de compromission). Le travail d'investigation permettra également de répondre aux questions de la cellule de crise telles que : quelle est l'origine de l'intrusion ? Quelles sont les vulnérabilités exploitées dans le cadre de l'attaque ? Y a-t-il eu une exfiltration de données ou possibilité d'exfiltration, et le cas échéant, quelles sont les données exportées ou l'ayant possiblement été ?

Les entreprises dotées d'unités capables de procéder aux premières analyses pourront recourir à ces unités. Les autres pourront déclencher l'assistance prévue dans un éventuel contrat d'assurance « cyber » ou recourir directement à des entreprises spécialisées. Dans le premier cas, il est important de noter que, passée la phase des traitements de première urgence, il est recommandé d'impliquer des équipes d'analyse spécialisées (cf. ISO 27042) qui soient en mesure d'émettre des observations en toute indépendance. En effet, si des recherches en responsabilité devaient avoir lieu, les diagnostics menés par les équipes internes, juges et parties, pourraient être contestés par les tiers (entreprises victimes de dommages collatéraux, assureurs).

À l'arrivée de l'équipe d'investigation, plusieurs éléments organisationnels et techniques doivent être partagés pour commencer efficacement le travail (1 par rôle) :

Coté organisationnel, l'identification des contacts et sachants pertinents pour les questions sur l'infrastructure :

- Responsable de la cellule de crise DSI
- Responsable de la sécurité des systèmes d'information (point de contact principal)
- Responsable de production ou des infrastructures ou de l'administrateur système & réseau
- Correspondant juridique sur les aspects Informatique & Liberté (RGPD)

Côté technique : tout élément et preuves pouvant aider à la compréhension initiale :

- Cartographie du SI, schéma de l'architecture du SI ou du réseau ; Une revue / validation de l'architecture peut être nécessaire avec l'administrateur au démarrage de l'incident
- Journaux d'événements archivés et centralisés disponibles
- Journaux anti-virus archivés et centralisés disponibles
- Journaux réseaux archivés et centralisés disponibles
- Une collecte des domaines Active Directory existants

Afin de permettre de mener l'investigation, **il est indispensable de conserver l'ensemble des preuves**, pouvant servir à la fois à l'enquête de police dans le cadre d'un dépôt de plainte mais également pour l'assurance dans le cadre de l'indemnisation.

- ne pas éteindre les machines pour ne pas perdre des informations contenues dans les processus en mémoire ;
- une machine chiffrée peut contenir des éléments de preuve utiles : collecter comme une machine standard ;
- ne pas redémarrer les serveurs mais préférer une approche conservatoire (ex : déconnexion / isolation réseau, etc.).

Parmi les premières demandes des équipes d'investigation, il s'agit de sanctuariser les preuves sur la zone compromise ou zone d'intérêt. Il est nécessaire de collecter les preuves et éléments techniques dans le but de conserver celles-ci dans le cas d'analyses ultérieures (plainte ou recours). Cette phase de collecte doit être itérée pour chaque nouvelle machine identifiée comme compromise. Chaque preuve collectée doit être inscrite dans une main courante pour traçabilité. Cette sanctuarisation doit être faite en doublon, dont l'original devra être stocké dans un endroit sûr pour éviter tout dommage ou altération de celui-ci.

Les informations suivantes sont à collecter sur chaque machine entrant dans la liste de machines à collecter :

- la liste des fichiers présents ;
- les processus en cours d'exécution ;
- les journaux à disposition, les systèmes de détection / supervision (sonde réseau, antivirus / EDR, messagerie, etc.).

De façon optimale il est intéressant de collecter :

- le contenu de la mémoire (RAM) de la machine ;
- les traces réseau (captures réseau ou journaux d'équipements réseau) ;
- ses différents supports de stockage.

Sur la base de ces premiers éléments, les équipes d'investigation vont pouvoir émettre les premiers éléments marquant de l'incident :

- dates, au format universel (UTC) pour éviter tout problème de fuseaux horaires ;
- outils / techniques et artefacts permettant d'identifier l'agent de menace ;
- adresses IP et noms de domaines ;
- comptes compromis utilisés par l'agent de menace ;
- d'autres machines compromises hors du périmètre connu.

Basé sur ces éléments, le périmètre de la crise peut se retrouver augmenté :

- découvertes de nouvelles machines compromises ;
- découvertes de dates antérieures aux dates actuellement connues ;
- découvertes de marqueurs dans les journaux globaux disponibles.

Dans la logique de processus itératif d'investigation décrit précédemment, de nouvelles machines devront être collectées afin de permettre la récupération de nouvelles preuves et marqueurs de l'incident, d'améliorer la compréhension de l'incident, de répondre aux questions de la cellule de crise et ainsi aider à la prise de décision. Ce processus itératif de meilleure compréhension de l'incident doit aider à répondre aux questions métiers, juridique, technique de l'organisation.

La compréhension de l'incident sera formalisée sous forme de rapport d'analyse comprenant les éléments suivants :

- une ligne de temps de l'incident (timeline) ;
- une explication des actions menées par l'agent de menace ;
- les potentielles vulnérabilités exploitées ;
- liste des indicateurs de compromission (adresses IP, noms de domaines, condensats de binaires, règles Yara et Sigma...) déduites des analyses ;
- liste des machines ayant été compromises ;
- liste des machines auxquelles l'agent de menace a eu accès ;
- liste des comptes compromis

La reconstruction débute souvent en parallèle de l'investigation et nécessite de connaître la cause de l'incident, trouvé lors de l'investigation. Cette phase implique donc des échanges quotidiens entre les deux équipes.

Entre autres, les éléments cités précédemment ont pour but d'aider à une reconstruction saine :

- la timeline et la date de compromission initiale, aideront à déterminer l'ancienneté des sauvegardes qu'il faudra restaurer ;
- les indicateurs de compromission permettront de s'assurer de l'intégrité des machines et serveurs recréés ;
- les vulnérabilités exploitées pourront guider sur les actions de sécurisation du SI à mener.

BONNES PRATIQUES

- Mettre en place une centralisation et un archivage des journaux afin de permettre d'identifier les activités réalisées sur le système d'information
- Mettre en place un système de synchronisation de temps sur l'ensemble du système d'information

2.2 Identification du périmètre de compromission

L'identification du périmètre de compromission est un élément indispensable pour identifier l'ampleur et l'intensité de la gestion de crise. L'analyse du périmètre permettra de déterminer l'ampleur de la propagation : zone réseau, une filiale, ou l'ensemble des SI de l'organisation.

En situation de crise, l'identification du périmètre compromis se fera de manière itérative car il est nécessaire de fournir rapidement de l'information à la cellule de crise décisionnelle. L'analyse sera précise et distinguera ce qui est assurément compromis de ce qui l'est potentiellement (par exemple, les traces montrent que tel fichier est sorti ou bien l'on sait que l'agent de menace a pu voir ce fichier sans pour autant être en mesure de certifier qu'il est sorti).

À partir du début des investigations toutes les actions menées doivent être tracées dans un document.

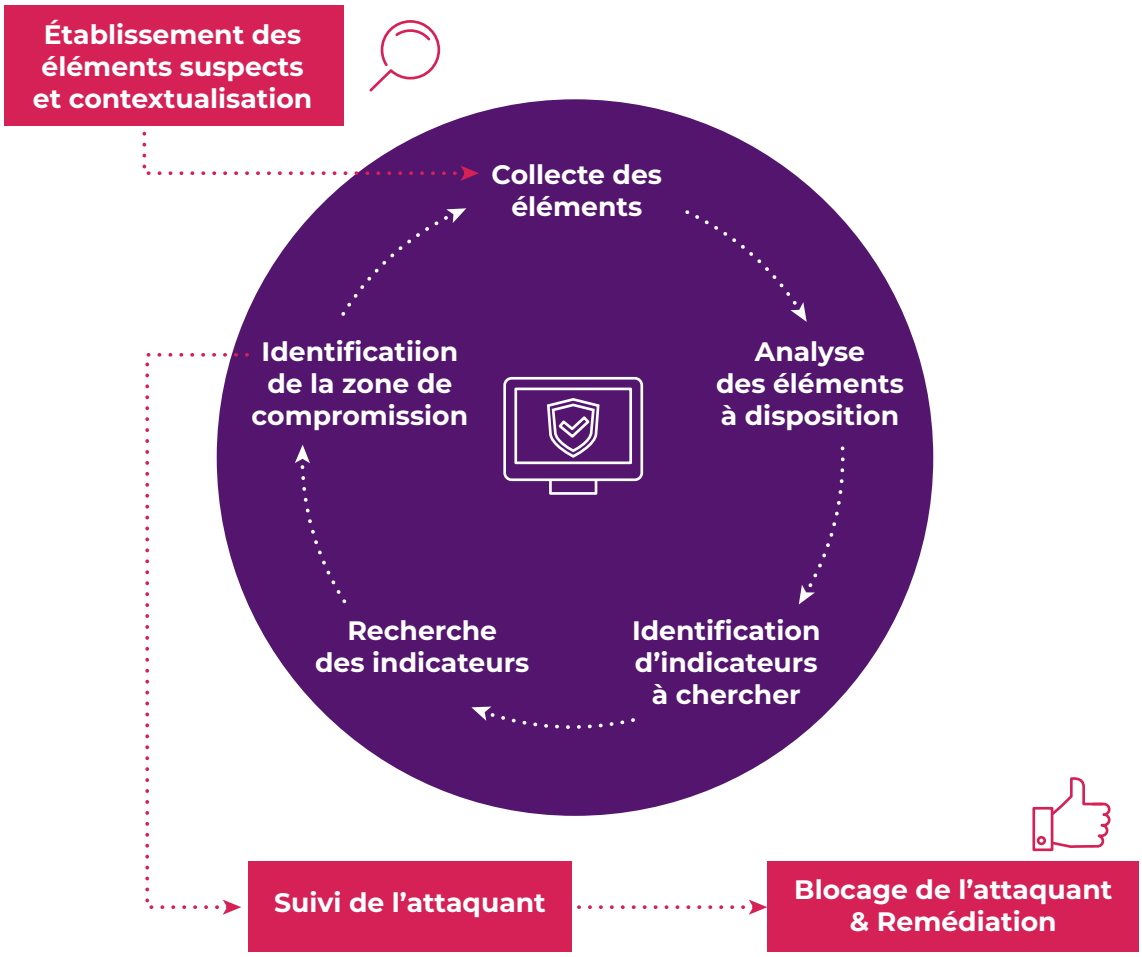


Figure 8 : Démarche itérative de l'investigation numérique

En première approche, lors de la détection de l'incident, il convient de :

- sanctuariser les journaux réseaux et les contrôleurs de domaine Active Directory ;
- caractériser la nature de l'attaque et collecter les éléments visibles (message de rançon, extensions des fichiers chiffrés / groupe d'attaquants) ;
- identifier l'état des systèmes de stockage (NAS / SAN) ainsi que des systèmes de sauvegarde avec la date de dernière sauvegarde ;
- identifier le périmètre compromis observable (systèmes détruits, fonctionnant partiellement, traces identifiées) ;
- identifier les systèmes ayant pu être attaqués car accessibles depuis les machines compromises (au niveau réseau ou via les relations d'approbation entre domaines Active Directory…) ;
- identifier les impacts opérationnels et domaines fonctionnels altérés du SI ;
- collecter les indicateurs de compromission (IOC) respectant un format universel, tel que le formalisme Yara et Sigma, qui facilitera la communication entre experts ;
- rassembler l'ensemble de la documentation permettant la compréhension de l'architecture (schéma d'architecture, inventaire des systèmes, dossier d'architecture, coffre-fort de mot de passe…) et les liens avec des systèmes tiers.

En résumé, il s'agit de décrire aussi précisément que possible ce qu'il s'agit de rechercher et les éléments facilitant le travail de l'équipe d'investigation.

En l'attente de l'obtention de ces détails, et dans l'ignorance du mode opératoire de l'agent de menace, les mesures conservatoires ont été appliquées :

- mise à l'abri des journaux systèmes et réseaux ;
- isolation des réseaux vis à vis des réseaux tiers non compromis et vis-à-vis d'Internet,
- isolation des serveurs ;
- interdiction de la mise sous tension des terminaux éteints au moment de l'attaque.

L'équipe d'investigation numérique demandera aux administrateurs du SI de réaliser plusieurs collectes :

- acquisition de mémoire de processus, de médias de stockage…
- acquisition d'artefacts tel que des journaux, des exécutables, des traces réseaux…

L'analyse sera ensuite réalisée par les experts afin extraire un maximum d'informations et notamment des **indicateurs de compromission**.

Les indicateurs pouvant être recherchés sur un parc sont de différentes natures, ces éléments sont à identifier suivant les capacités de l'organisation et des données à disposition de la victime, par exemple : des condensats, des adresses IP, des noms de domaine, des signatures binaires.

La recherche des indicateurs :

- elle peut être effectuée sur les journaux à disposition ou sur le système d'information en cours de fonctionnement ;
- ces indicateurs doivent être cherchés sur le réseau compromis, mais également sur le réseau reconstruit ;
- ces indicateurs peuvent être partagés pour recherche avec des partenaires afin de les aider à identifier s'ils ont également été victimes de l'attaque.

Identification de la zone de compromission :

- à l'issue de la recherche des indicateurs sur le parc, de nouveaux systèmes compromis peuvent être identifiés. Il faut alors s'assurer que ces nouveaux systèmes compromis ne sont pas en interaction avec d'autres systèmes qui n'ont pas fait l'objet eux-mêmes de vérification ;
- dans le cas où de nouveaux systèmes ont été identifiés, il est fortement recommandé de reprendre une nouvelle itération depuis l'étape « Collecte des éléments ».

Suivi de l'agent de menace :

- dans certains cas, l'agent de menace, ou ses applicatifs sont encore actifs sur le SI ; il peut être alors nécessaire de superviser ses actions, afin :
  - d'identifier des connexions ou des outils encore inconnus des investigations ;
  - de déterminer l'orientation des actions menées ;
- cette activité est réalisable dans certains cas particuliers qui sont à évaluer avec les capacités de la victime et des experts forensiques.

Blocage de l'agent de menace et remédiation :

- déconnexion **totale** des communications avec l'extérieur du SI ;
- remédiation sur toutes les machines simultanément, ou enclencher une bascule vers un système sain construit préalablement.

L'identification du périmètre de compromission sera progressive via le travail itératif de l'investigation numérique. La mise en place d'une cellule de surveillance de ces indicateurs permettra de continuer à identifier les machines compromises et la surveillance de l'agence de menace.

BONNES PRATIQUES

- Disposer d'une cartographie du SI et des réseaux et d'un inventaire des équipements
- Conserver une copie isolée des éléments critiques sur un environnement isolé (SI autonome ou PC isolé ou version papier)

2.3 Stratégie de reconstruction du SI

PRÉREQUIS NÉCESSAIRES POUR LA RECONSTRUCTION :

Afin de démarrer le chantier de reconstruction, il est nécessaire d'avoir certaines informations avant de pouvoir établir la meilleure stratégie de reconstruction :

- avoir une vision claire de l'état des sauvegardes (Cf. 2.2) ou des mécanismes de restauration du stockage avant l'attaque (*exemple : snapshots sur des baies de disque NAS ou SAN*) ;
- identifier la date de la dernière sauvegarde des systèmes et données (pour éviter de restaurer les systèmes et les données dans un état de compromission) – la date des premières activités malveillantes étant à croiser avec les résultats de l'investigation numérique (Cf. 2.1) ;
- repérer les outils (programmes malveillants que l'agent de menace a déposés) et les comptes qu'il a compromis ou crées (Cf. 2.1) ;
- comprendre les vulnérabilités exploitées durant l'attaque ;
- disposer de nouveaux postes de travail / d'administration utilisables pour les administrateurs et qui sont sous surveillance (a minima avoir des postes hors domaine AD ou sous Linux par exemple) ;
- isoler le réseau d'Internet afin de mener les actions dans un environnement que l'agent de menace ne peut plus atteindre.

Les étapes de reconstruction du SI sont à adapter au contexte, mais il est possible de dégager les grandes étapes suivantes :

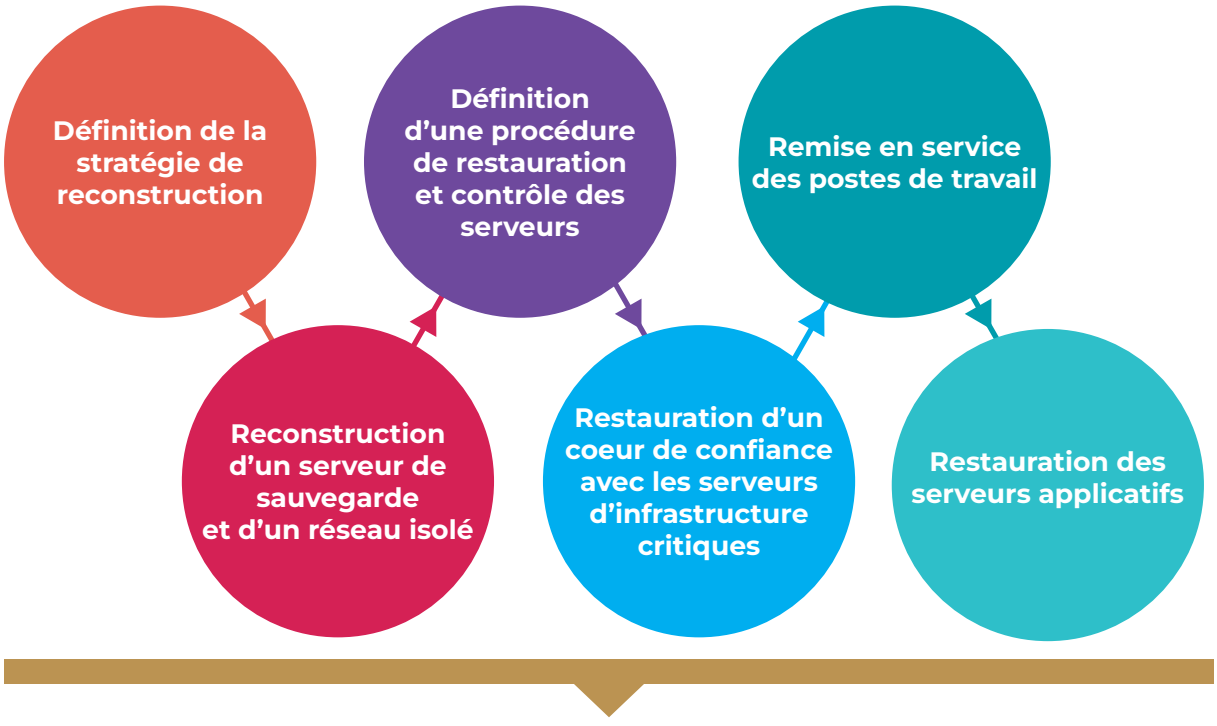


Figure 9 : Grandes étapes de reconstruction du SI

SCÉNARIOS DE RECONSTRUCTION

En fonction de ces éléments, plusieurs scénarios de reconstruction sont possibles. Chaque scénario pouvant présenter des avantages (plus sûr par exemple) mais aussi des inconvénients (délai / charge de reconstruction, perte de données...).

Il est nécessaire d'identifier le scénario le plus adapté au contexte et aux évolutions de l'organisme :

- **Repartir des sauvegardes existantes avant la date de la compromission et d'intrusion.** Les sauvegardes présenteront l'avantage de pas contenir de code malveillant mais le scénario engendre une perte de données si l'intrusion a été réalisée des semaines ou mois avant le blocage de l'attaque. De plus, des actions de sécurisation seront dans tous les cas nécessaires, comme le changement des mots de passe / secrets ainsi que la correction des vulnérabilités exploitées.

- **Repartir de la dernière sauvegarde du système d'information** : cela indique que les systèmes restaurés seront potentiellement compromis et que des portes dérobées auront pu être laissées par l'attaquant. Une procédure de nettoyage et de vérification est alors nécessaire, et présente un risque de code dormant sur les serveurs.

- **Reconstruire le système d'information de zéro.** Ce scénario présente l'avantage de pouvoir repartir sur des bases saines et sécurisées. Mais le temps nécessaire à la reconstruction est important. Cela aura des impacts sur le fonctionnement de l'entreprise et présente un risque de perte définitive des données. Ce scénario est à privilégier quand les sauvegardes ne sont pas récupérables.

À noter que certains laboratoires de récupération de données sur disques peuvent analyser le contenu des disques durs pour essayer de retrouver des données utiles. Ce procédé est notamment déroulé en cas de supports de stockage défectueux (incendie, chute, suppression accidentel). Ce scénario est intéressant si les données ont été supprimées des supports de stockage par l'agent de menace. Mais dans le cas d'un chiffrement des données, il est nécessaire de valider sa pertinence au cas par cas.

Pour retrouver une partie de son patrimoine informationnel, il est nécessaire de prendre contact avec l'ensemble des partenaires, éditeurs, clients ou sous-traitants qui peuvent avoir une partie des données de l'entreprise. Il est également possible de faire l'inventaire des données pouvant être présentes au format papier sur des serveurs distants ou postes de travail non chiffrés.

D'autres scénarios de reconstruction peuvent être également envisagés en fonction des situations :

#

Migration de serveurs vers des services de type SaaS : en effet dans certaines circonstances, l'organisme peut se tourner vers certains partenaires pour retrouver l'accès à certaines applications (Messagerie, ERP…), l'objectif étant de pouvoir continuer à travailler avec la problématique de conduite du changement ainsi que la perte des données / de l'historique.

#

Évolution du système d'information : dans certaines situations comme une fusion-acquisition d'entreprises ou de projets déjà en cours de d'évolution, la reconstruction ne sera pas réalisée à l'identique. L'organisme peut utiliser le contexte de la crise pour migrer ses serveurs ou certains services vers une nouvelle solution, un nouvel hébergeur ou des services informatique de type IaaS. Dans tous les cas, la procédure de migration devait être définie afin de limiter le risque de propagation de l'attaque et intégrer les délais nécessaires à cette migration.

ÉTAPES DE RECONSTRUCTION

Comme pour le scénario de reconstruction, les étapes de reconstruction sont bien évidemment spécifiques à chaque environnement et contexte de la cyberattaque. Dans tous les cas, il est nécessaire de bien définir le séquencement de l'ensemble des actions et les mesures de sécurité à réaliser pour éviter une nouvelle compromission du système d'information :

ÉTAPE 1

Reconstruire / restaurer un serveur de sauvegarde sain et isolé de tout réseau (notamment vis-à-vis d'Internet)

- La mise en place d'un nouveau serveur de sauvegarde permet de limiter le risque que ce dernier soit compromis et ne chiffre pas les sauvegardes. Son isolation du réseau permettra de limiter le risque d'intrusion. Il convient de vérifier l'état réel des sauvegardes et de procéder à des premiers tests de restauration. Il est également nécessaire de désactiver le système de purge / rotation automatique des sauvegardes afin de conserver l'ensemble des sauvegardes disponibles.
- Dans le cas où un serveur est restauré à partir d'une sauvegarde, il est recommandé de conserver le serveur chiffré / compromis en le conservant déconnecté et en l'identifiant pour bien le différencier des autres, afin de conserver les éléments de preuve le plus longtemps possible. Cela peut nécessiter d'avoir un espace de stockage suffisant pour pouvoir restaurer les sauvegardes tout en gardant les machines virtuelles compromises (~ 50 % d'espace disponible) ou de disposer d'accord pour avoir un espace de stockage disponible à la demande. Dans le cas où les données ne seraient pas conservées par manque de place, une purge des anciennes machines virtuelles devra être réalisée par restauration et après la réalisation d'une collecte de preuves.

ÉTAPE 2

Définition d'une procédure de contrôle de l'état de santé des serveurs restaurés « Sanity Check »

Pour s'assurer que les serveurs restaurés sont sains, il est nécessaire de définir une procédure de contrôle de l'état du serveur. Les étapes sont en général les suivantes :

- restauration du serveur dans un environnement isolé ;
- reconfiguration du serveur pour qu'il soit déconnecté du réseau puis démarrage du serveur ;
- contrôle de la présence d'éventuels fichiers malveillants soit via une solution de sécurité (comme une technologie EDR ou un antivirus détectant bien les machines malveillants), soit via un outil de recherche de compromission qui intègre les mécanismes utilisés par l'agent de menace suite à l'investigation numérique ;
- revue des comptes et droits sur le serveur ;
- changement des secrets sur le serveur comme les mots de passe locaux ;
- application des correctifs de sécurité en fonction des résultats de l'investigation sur l'attaque (patchs de sécurité, activation du pare-feu local, désactivation de certains services ou comptes…) ;
- mise en place d'un outil de surveillance et mise en place d'un outil de protection opérationnel et à jour (EDR ou Antivirus) ;
- puis remise sur le réseau de production du serveur (toujours en étant isolé d'Internet).

Dans le cas où des codes malveillants sont présents sur les serveurs lors des vérifications, il est fortement recommandé de réinstaller ces serveurs, afin de s'assurer que l'agent de menace n'aura pas pu laisser de porte dérobée. Il sera alors nécessaire d'installer un nouveau serveur puis de définir une procédure pour migrer le contenu du serveur (données applicatives, configuration) selon les possibilités offertes par l'application hébergée. Dans le cas où la réinstallation n'est pas possible dans l'immédiat, une analyse complémentaire doit être réalisée sur ce serveur ou des mesures de mitigation (isolation réseau, sortie du domaine AD…).

Dans le cas des serveurs physiques, il est recommandé de conserver le serveur en l'état afin de garder la preuve et de préparer un serveur de secours identique y compris les connectiques nécessaires (ex : fibre optique / connectique SAN) et de restaurer les données utiles sur ce nouveau serveur.

Si l'hyperviseur a été compromis, il peut être nécessaire de réaliser un formatage et une réinstallation du système d'exploitation.

ÉTAPE 3

Restauration des serveurs d'infrastructure critiques et contrôle

Pour pouvoir relancer son système d'information, certains services critiques doivent être restaurés en priorité afin de pouvoir démarrer le reste de l'infrastructure. De manière générale, les composants suivants sont parmi les premiers à devoir être relancés :

- serveurs DNS / DHCP ;
- contrôleurs de domaines Active Directory ;
- serveurs d'authentification du SI d'administration (RADIUS / LDAP…) ;
- console d'administration (Antivirus, virtualisation, stockage, firewall…).

Suite à la cyberattaque, l'agent de menace a pu prendre le contrôle des serveurs et des secrets. Le déroulement de la procédure de contrôle de l'état du serveur est nécessaire. Mais pour certains composants, des mesures complémentaires sont nécessaires pour regagner la confiance dans son système d'information.

> ***Focus sur les domaines Active Directory - Directory Services*** *: il s'agit d'un composant clef du système d'information, permettant de prendre la main sur l'ensemble des systèmes Windows membre du domaine. Une analyse du niveau de sécurité du domaine est nécessaire pour évaluer le risque d'élévation de privilèges permettant à un compte utilisateur de passer administrateur domaine.*

De manière générale, les actions de sécurisation suivantes sont nécessaires et doivent être déroulées sur un environnement isolé :

- désactivation des comptes inutilisés / dormants et les comptes utilisés par l'attaquant ;
- durcissement de la politique de mot de passe et des comptes n'étant pas soumis à la politique ;
- changement des mots de passe des comptes du domaine (Utilisateur, Administrateur, comptes de service, les comptes ordinateurs et autres comptes techniques – comme le compte krbtgt) ;
- réduction des droits sur les comptes d'administration (exemple : membre du groupe Domain Admins) et mise en place des bases pour un modèle de délégation des droits en tiers (tiering model) ;
- réinstallation de nouveaux contrôleurs de domaine et application des corrections de sécurité.

La sécurité des environnements Active Directory est un sujet complexe et nécessite du temps pour mettre en place les bonnes pratiques. Il est nécessaire de définir les mesures minimales à mettre en place pour éviter qu'un agent de menace ayant encore un accès à un poste de travail ne puisse reprendre la main sur l'ensemble de l'infrastructure.

ÉTAPE 4

Remise en service des postes de travail

Suite à l'investigation numérique, la cinématique de l'attaque a pu montrer la compromission d'un ou plusieurs postes de travail et la question de la réinstallation de l'ensemble des postes de travail est alors souvent évoquée. Dans le cas où l'agent de menace a lancé le chiffrement des postes de travail, ces derniers sont bien évidemment à réinstaller ou à restaurer, les données étant bien souvent perdues car chiffrées.

Dans le cas où l'agent de menace a uniquement compromis quelques postes de travail, dont la liste peut être considérée comme exhaustive, ces derniers seront à remplacer et une procédure de transfert des données utilisateur est alors à définir afin de s'assurer de ne pas contaminer le nouveau poste de travail. Il est préférable de fournir un nouveau poste de travail ou de remplacer le disque dur afin de conserver les preuves de l'attaque.

Dans le cas où la liste des postes de travail compromis ne peut être identifiée, il est nécessaire de définir une procédure de contrôle de l'ensemble des postes, en prenant les éléments définis pour celle des serveurs, qui peuvent être enrichis par des mises à jour de sécurité / montée de version et d'installation de nouvelles solutions de sécurité permettant de détecter les codes malveillants connus.

ÉTAPE 5

Restauration des serveurs applicatifs

Pour pouvoir reconstruire le système d'information de façon efficace, il est nécessaire d'établir les priorités des métiers (BU prioritaires et applications nécessaires) [Cf. Partie 3] afin d'identifier les serveurs prioritaires à restaurer ou à reconstruire.

Les besoins métiers sont ensuite à convertir en liste de serveurs mais également d'identifier les chaines d'infrastructure associées (frontaux / intergiciels / base de données...) nécessaires au fonctionnement de l'application, ainsi que les dépendances entre les applications (*si l'application B n'est pas présente, l'application A ne fonctionnera pas*). On s'appuiera, pour ce faire, sur les travaux du Plan de Continuité des Activités (PCA), en particulier le volet Plan de Secours Informatique.

La restauration des serveurs doit suivre la procédure de contrôle de l'état de santé du serveur. Une fois les serveurs reconnectés au SI, l'ensemble pourra être mis à disposition du responsable applicatif, des administrateurs métier ou de l'équipe assurant la maintenance de l'application (TMA) afin de valider le bon fonctionnement de l'application ou les flux nécessaires avec l'extérieur (clients, partenaires, système de place, etc.).

Une vérification de la cohérence des données est nécessaire lorsque des serveurs collaborant au sein de la même chaine applicative ont été sauvegardés à des dates différentes. Cette maîtrise des applications, qui n'est pas spécifique au traitement des crises « cyber », doit avoir été documentée et testée au préalable.

Lorsque les métiers confirment le bon fonctionnement des applications et la cohérence des données restaurées, un travail de reconstitution des données perdues est nécessaire (nouvelle saisie, récupération des transactions auprès des tiers, etc.).

Un fichier de suivi doit être constitué afin de suivre l'avancement des restaurations et voir les problèmes rencontrés.

Durant la phase de restauration du système d'information, il est possible de ré-autoriser certains flux maîtrisés avec l'extérieur soit via Internet, soit par des réseaux privés. Ces flux autorisés ne doivent pas représenter de risques pour le partenaire distant mais également de ne pas exposer le système d'information à une nouvelle re-compromission par l'agent de menace. Il s'agit d'approche par liste blanche n'autorisant que certains serveurs ou domaines critiques pour la continuité d'activité.

DURCISSEMENT / SÉCURISATION DU SI

Après la restauration du système d'information en environnement déconnecté d'Internet, il est souvent nécessaire de renforcer le niveau de sécurité avant de pouvoir le reconnecter avec Internet, notamment pour les accès Internet au niveau des postes de travail ou des accès distants. En attendant la sécurisation du SI, il est toutefois nécessaire d'ouvrir des accès Internet de façon restreinte sur la base d'une liste blanche avec uniquement des services de confiance.

Les mesures de durcissement sont spécifiques à chaque environnement, en fonction de son niveau de sécurité actuel et des vulnérabilités exploitées par l'agent de menace.

Plusieurs actions sont souvent à envisager avant la réouverture du système d'information avec l'extérieur :

- réalisation d'une campagne d'application des correctifs de sécurité critiques sur les composants critiques ou exposés à Internet ;
- migration des systèmes d'exploitation obsolètes vers une version supportée par l'éditeur ;
- mise en place d'un mécanisme d'authentification forte pour les accès distants - si cela n'était pas en place ;
- mise en place de postes d'administration et séparé des usages bureautiques et isolé d'Internet et cloisonnement des serveurs d'administration critiques dans un réseau d'administration (*cf. note technique de l'ANSSI sur l'administration sécurisée du SI*) ;
- restriction des flux réseau entrants (ex : VPN, extranet…) depuis des pays de confiance correspondant aux utilisateurs au SI ;
- renforcement de la politique de filtrage pour les accès Internet des utilisateurs ;
- mise en place d'une liste blanche pour les accès Internet sur les serveurs.

La décision de réouverture des interactions avec l'extérieur est à réaliser avec une approche de gestion des risques qui intègre à la fois les mesures de sécurité ayant été mises en œuvre lors de la restauration des systèmes, les mesures complémentaires notamment de mitigation, les capacités de surveillance du SI ainsi que la compréhension de l'attaque à travers l'investigation numérique.

BONNES PRATIQUES

- Définir une stratégie de reconstruction du SI avant l'accident
- Définir des procédures de restauration du SI et un ordre de redémarrage des systèmes en tenant compte des dépendances entre les systèmes
- Définir une politique de sauvegardes comprenant un stockage hors ligne / immuables
- Privilégier un système de sauvegarde ne recourant pas aux technologies les plus sujettes à la cybermenace et ayant son propre réseau et mécanisme d'administration
- Définir une procédure de recette des applications après redémarrage du SI et de disposer de dossier d'architecture permettant de lister les flux nécessaires

2.4 Surveillance de circonstance

La surveillance est une étape importante qui consiste à contrôler l'état de la situation de manière régulière. Elle permet de juger de l'efficacité des mesures conservatoires et des actions de sécurisation entreprises dans le cadre de la reconstruction et de les adapter en cas de résurgence de l'attaque.

La surveillance de circonstance intervient dès la phase de reconstruction du système d'information et notamment lors de la remise en service des postes et des serveurs. La surveillance est à intégrer dans la stratégie de gestion des risques afin de disposer d'un moyen de contrôler la réouverture du SI avec l'extérieur et s'assurer de l'absence d'activités malveillantes.

Les étapes de mise en place d'une surveillance interne ou avec un tiers pourra suivre les étapes suivantes :

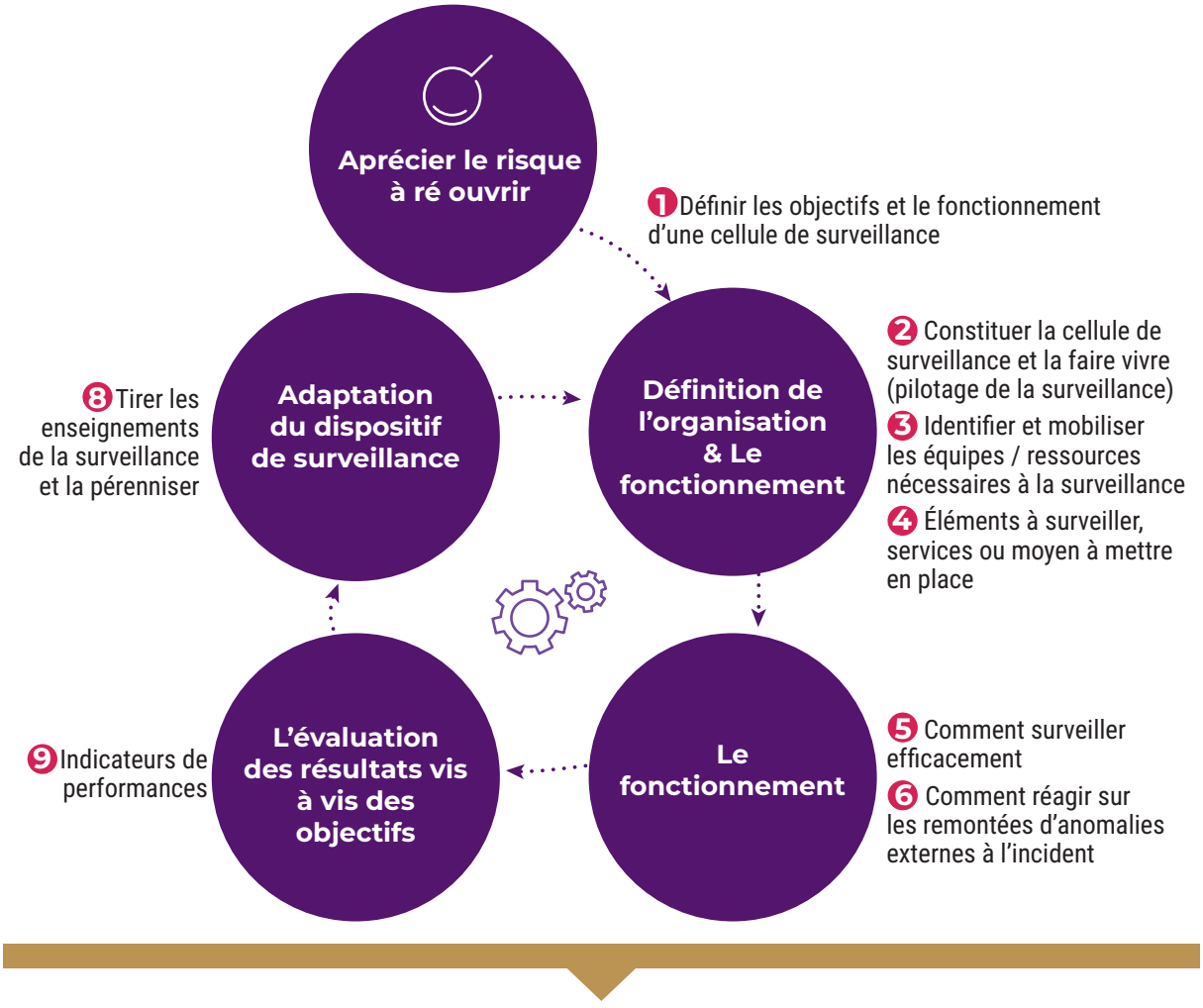


Figure 10 : Processus de surveillance de la reprise d'activité

1 Définir les objectifs et le fonctionnement d'une cellule de surveillance

La première étape est de définir les objectifs de la surveillance de circonstance, il peut s'agir de :

- éviter une aggravation de la situation et / ou une nouvelle attaque ;
- vérifier que l'attaque est bien contenue ;
- être en mesure d'alerter la cellule de crise en temps réel.

2 Constituer la cellule de surveillance et en assurer le pilotage

Les points ci-dessous permettent d'établir la mise en place de la cellule de surveillance et en assurer son bon fonctionnement :

- nommer le responsable de la cellule de surveillance et un relais en cas d'absence ;
- établir le plan de route de la cellule pour réaliser la surveillance avec les compétences nécessaires et manquantes ;
- définir la fréquence de réunion de la cellule de surveillance ;
- identifier les membres de la cellule (restreindre le nombre de participants membres et prévoir des relais terrain) ;
- se faire communiquer les cartographies applicatives et réseau ;
- déterminer les plages horaires (heures ouvrées, astreinte, 24 / 7, etc) ;
- établir une synchronisation avec la cellule de crise, les différents relais sur le terrain, une assistance externe le cas échéant ;
- identifier les points de contrôle et en déduire les moyens techniques à activer ou renforcer ;
- examiner régulièrement l'adaptation des ressources.

3 Identifier et mobiliser les équipes / ressources nécessaire à la surveillance

La surveillance d'un système en redémarrage est une activité exceptionnelle qui nécessite des ressources spécifiques à identifier en amont – relais sur le terrain : notamment les administrateurs de solutions techniques. Une répartition des missions devra être proposée au niveau des relais sur le terrain.

Elle peut amener à solliciter des intervenants extérieurs : sociétés spécialisées dans la réponse à incident, l'investigation numérique et potentiellement des autorités régionales ou nationales en matière de cybersécurité.

4 Éléments à surveiller, services ou moyens à mettre en place

Les éléments à surveiller présentés ci-dessous sont à adapter en fonction du contexte :

- journaux des pare-feux, proxies Internet et des concentrateurs VPN (accès distant) : contrôle des flux avec l'extérieur et des tentatives d'accès ;
- sondes réseau (ex : IDS / UEBA) ;
- annuaires et systèmes d'administration : attaques potentielles en cours, surveillance de l'utilisation des comptes de service ou compromis ;
- serveurs : tentatives de connexion en erreur ou à des heures suspectes ;
- postes d'administration : tentatives de connexion en échec avec des comptes à privilège ;

- postes de travail : solution de sécurité (EPP / EDR) ;
- serveurs de messagerie ;
- stockage / sauvegardes : contrôle d'activités suspectes ou contrôle d'intégrité ;
- applications métiers critiques.

Des services supplémentaires externalisables peuvent être mis en place tels que :

- CERT (Computer Emergency Response Team) externe (service managé d'analyse des alertes) ;
- l'assistance d'un prestataire de réponse à incident ;
- des services de détection : EDR, sondes réseau ou autre solution de sécurité dans une logique de déploiement rapide permettant d'avoir une vision sur le SI ;
- la détermination du mode de paramétrage des outils de surveillance (détection ou blocage) ;
- le suivi de la correction des vulnérabilités exploitées ;
- la surveillance du Darkweb pour identifier des fuites de données.

5 Comment surveiller efficacement

Les équipes de surveillance doivent être uniquement dédiées à cette tâche :

- alimenter les équipes sur les techniques / vulnérabilités exploitées par l'agent de menace (Cf. 2.1) ; et s'alimenter de la connaissance de la menace (ex : analyse du groupe d'agent de menaces par une société de cybersécurité indiquant les techniques utilisées) ;
- s'assurer de la mise à jour du tableau de bord de gestion de crise (main courante) de l'évolution de la situation ;
- s'assurer que tous les moyens techniques et RH nécessaires soient alloués.

6 Comment réagir sur des remontées d'anomalie externes à l'incident

La surveillance mise en place à l'occasion de l'attaque, va détecter des événements de sécurité qui ne sont pas liés à l'attaque (mauvais comportement, codes malveillants déjà présents avant l'attaque).

La priorité sera donnée au traitement des incidents liés à l'attaque (correspondance avec les IOCs, de schémas d'attaque, etc.). Seuls ces incidents font l'objet d'une remontée à la cellule de crise. Les autres doivent être consignés et traités pour résolution après la crise.

7 Indicateurs de performance :

- taux de couverture du SI / taux de déploiement des solutions de sécurité ;
- volume d'alertes générées et traitées par l'équipe de surveillance ;
- pourcentage de faux-positif ;
- répartition des alertes, en lien avec l'attaque ou non liés à l'attaque.

8 Tirer les enseignements de la surveillance :

- sur l'organisation à mettre en place pour surveiller ;
- sur les compétences requises ;
- sur le dimensionnement de la cellule de surveillance ;
- sur le type d'outils de surveillance ;
- sur les liens avec les entités externes ou internes.

Les enseignements tirés de cette surveillance, après attaque, vont donner des éléments pour renforcer sa posture avant une nouvelle attaque ou donner les moyens de la prévenir.

L'ensemble des éléments à superviser cités ne pourront être mis en place dans un délai court, ces points de contrôle seront à intégrer dans une feuille de route.

L'organisme étant potentiellement entre deux attaques, il se doit d'entretenir sa démarche de détection permanente.

PARTIE 3
PRÉCONISATIONS POUR LA CONTINUITÉ D'ACTIVITÉ MÉTIERS

Suite à la survenance de la cyberattaque paralysante, une équipe d'intervention ou une cellule de crise a été mise en place dès le début de la crise comme indiqué dans la Partie 1. Parallèlement à la reconstruction du SI (Cf. Partie 2), le maintien de l'activité en mode dégradé va se poser très rapidement. L'objectif principal sera de permettre la survie économique de l'organisme et d'éviter une sur-crise.

La continuité d'activité a minima demande une certaine résilience et capacité d'innovation de la part de l'organisation. Cela peut se synthétiser en la capacité d'être stratège. En effet, il faudra faire preuve de suffisamment d'agilité pour anticiper dès le début de la crise, pour agir de manière non-conventionnelle tout au long de la crise et pour capitaliser sur l'événement suite au retour à la normale.

L'urgence pouvant rendre difficile la prise de décision et l'initiative, il est recommandé de placer à la tête de la cellule de crise métiers en charge de la continuité d'activités, un dirigeant confirmé qui apportera le leadership, l'autorité et la créativité nécessaire. La dimension humaine de la continuité d'activité devra également être omniprésente afin de créer un environnement suffisamment stable malgré l'agitation et les difficultés rencontrées.

Chaque dimension de la crise doit être traitée avec la même importance et la même dévotion afin d'assurer le rétablissement de l'organisme en minimisant autant que cela est possible les impacts directs et indirects.

3.1 Définir les activités métiers prioritaires

À ce stade, les équipes se sont réunies pour s'organiser et faire face à un scénario de crise majeure. La cyberattaque se révélant paralysante, le SI sera indisponible pour une durée prolongée (plusieurs jours, semaines, voire mois). Prendre conscience rapidement de l'ampleur et de la gravité de l'attaque est indispensable pour assurer la survie de l'organisme. Effectivement, même s'il est préparé en amont à gérer une crise (plan de Gestion de Crise, exercices de crise, modes dégradés…), le scénario de la cyberattaque paralysante n'a pas forcément été envisagé mais demande une réponse immédiate.

À présent, une équipe de collaborateurs est mobilisée pour les urgences relatives à la cyberattaque. Une cellule opérationnelle de crise ou une équipe d'intervention dédiée à l'informatique et au redémarrage du SI est formée. Parallèlement la structure s'organise pour assurer la continuité et la reprise d'une activité minimale de ses métiers avec comme première action, la détermination des activités métiers prioritaires.

Pour ce faire, la **Direction générale** nomme une personne faisant autorité, familière des rouages de l'entreprise et de son éco-système et qui pilotera **une organisation de gestion de crise décisionnelle** (comité de direction, cellule de crise formalisée…). Si au sein de l'organisation, il existe déjà une cellule de crise décisionnelle formalisée, elle doit être activée immédiatement, sinon elle doit être créée rapidement.

Ce sera à la cellule de crise décisionnelle de mener cette première action en collaboration avec la cellule de crise métiers en charge de la continuité d'activité. L'objectif est d'avoir une vision globale et de commencer à construire une liste des activités métiers prioritaires en collaboration avec les différents métiers et selon les informations remontées. Si un Bilan d'Impact sur les activités (BIA) a été mené en amont de la crise, la liste des activités prioritaires doit être ajustée ou confortée en fonction de la saisonnalité et des évolutions organisationnelles de la structure. Dès la mise en place et / ou l'activation de la cellule de crise formalisée, l'engagement affirmé et observable de **la Direction générale générera un climat de confiance, de cohésion et une véritable**

dynamique collective. Tout au long de la crise, elle fera également preuve de leadership, en assurant la prise de décision, le suivi et le pilotage de crise.

Le décideur stabilisera, autant que cela est possible la situation, en recentrant l'activité et la prise de décision et en inspirant la confiance auprès de l'équipe et des parties prenantes. Tout l'enjeu est de créer le consensus en termes de décision via une dynamique de travail collaborative où chacun se soutient, se coordonne et communique. En complément, faire preuve de flexibilité et d'adaptabilité sont d'autres qualités requises du décideur en cas de crise. Cela est d'autant plus vrai dans le cas d'une cyberattaque paralysante qui, par nature, soumet l'organisme à de fortes turbulences dans des zones de fortes incertitudes.

La direction des équipes en situation de crise est très différente du management en situation ordinaire. Les modes de décisions et la mise en place de la collaboration sont très spécifiques. Pour mieux s'y préparer il est conseillé de suivre des formations ou d'effectuer des exercices de crise régulièrement. La cellule de crise décisionnelle doit s'être familiarisée avec la gestion de crise en amont afin que les pratiques souhaitables soient appliquées et que les spécificités de la crise cyber soient mieux traitées.

Chaque métier ayant des besoins différents, il va falloir dialoguer et échanger avec chacun afin de déterminer les priorités au sein des métiers. Une réflexion par métier est à mener avec une analyse approfondie pour déterminer les potentiels impacts de l'attaque sur chaque activité prioritaire.

De même, il convient de s'assurer de la présence des ressources nécessaires, qu'il s'agisse des ressources hors SI (humaines, matérielles…) et des ressources du SI (comme développé ci-après).

EXEMPLES

Assurer la paie des salariés est une mesure prioritaire qui demande soit un redémarrage rapide du logiciel de paiement, soit une solution dégradée métier permettant d'assurer un virement des salaires hors logiciel (i.e refaire le virement des salaires des mois précédents auprès du partenaire bancaire, passage temporaire en mode manuel…).

Parallèlement au plan de reconstruction du SI, les métiers travaillent avec leurs correspondants informatiques et dans la mesure du possible pour trouver des solutions alternatives permettant la continuité des activités prioritaires. Ceci implique de disposer de la liste des applications métiers prioritaires, incluant les applications intégrées dans le SI de l'organisme et, le cas échéant, les applications mises en place par les métiers hors SI.

Il est préférable que cette liste soit établie en concertation entre les équipes métiers et les équipes informatiques, afin que chaque partie ait une compréhension suffisante des objectifs et des contraintes de l'autre partie. Dans ce cadre, une véritable coopération, voire une co-responsabilité doit s'établir entre les équipes informatiques et métiers (Cf. Partie 1.4).

ACTIONS À MENER

- S'assurer qu'un décideur en charge du pilotage de crise a été désigné (Autorité et leadership pour prendre des décisions en situation de crise)
- S'assurer qu'un décideur en charge de la mise en œuvre des procédures de continuité d'activité en mode dégradé a été désigné
- Valider la liste des activités prioritaires à maintenir a minima en mode dégradé pendant la crise (hors SI)
- Valider la liste des applications métiers prioritaires à remonter par ordre de priorité lors de la reconstruction du SI

BONNES PRATIQUES (À PRÉPARER EN AMONT)

- Avoir mis en place / avoir testé le plan de gestion de crise
- Avoir réalisé le Bilan d'Impact sur les activités (BIA) de l'organisme (se baser sur la norme ISO 22317 : 2021)
- Avoir réalisé le PCA Global de l'organisme et valider une stratégie PCA (arbitrage Direction générale) en lien avec les risques d'interruption d'activité et les enjeux (se baser sur la norme ISO 22301 : 2019)

3.2 Mettre en œuvre les dispositifs de continuité d'activités prioritaires

À ce stade, les activités métiers prioritaires sont définies / validées et un premier ordonnancement des applications à redémarrer en priorité est enclenché.

À présent, il faut mettre en œuvre les dispositifs de continuité d'activités prioritaires. Le déploiement des outils prioritaires de communication et de continuité d'activités métiers va nécessiter de nombreuses ressources humaines qui seront désignées / choisies en début de crise.

OUTILS DE COMMUNICATION INTERNE ET EXTERNE

En complétement des outils de gestion de crise utilisés par la cellule de crise (Cf. 1.5), l'organisme doit rapidement communiquer aussi bien en interne qu'en externe. La priorité est d'assurer le rétablissement de canaux de communication internes et externes.

Parallèlement, une stratégie de premier niveau est déployée dans laquelle, soit l'organisme active ses outils de communication de secours, soit s'en dote.

Être en capacité de communiquer hors SI vers l'interne, auprès des collaborateurs et vers l'externe auprès des parties prenantes et des clients nécessite une analyse approfondie pour mettre en œuvre des outils de communication alternatifs adaptés et validés, en cohérence avec la stratégie de communication de crise (Cf. 1.5).

La communication de crise auprès des collaborateurs doit être fluide, régulière, simple et précise. Les informations doivent être transmises par un canal de communication unique pour éviter des répétitions ou des non-sens. Il est important de garder à l'esprit que les informations communiquées aux collaborateurs fuiteront potentiellement vers l'extérieur. Prévoir un affichage généralisé dans les locaux (cf. affiches dans les ascenseurs, à tous les étages) de l'organisme pour prévenir de l'attaque et des gestes adéquats minimisera les risques d'amplification de la cyberattaque.

> **Exemples d'outils** : visioconférence, outils des réseaux sociaux, internet, boîte mail externe, O365, messagerie audio et SMS, application mobile de messagerie instantanée, etc.

La communication auprès des parties prenantes externes aura pour objet de dispenser les informations générales à propos des évolutions de la crise et des lignes directrices décidées et suivies pour la continuité d'activité de l'entreprise et vis-à-vis des potentielles personnes directement impactées par la crise. Une réserve est à faire lorsque les entités sont cotées en bourse et / ou soumise à une autorité de tutelle et également lorsque l'affaire est judiciarisée. La confidentialité des informations demeure un élément clé à respecter dans les communications « Droit d'en connaitre ».

> **Exemples d'outils** : site internet institutionnel, site internet de secours, page web de crise, outils des réseaux sociaux, internet, live chat, visioconférence, numéro vert, etc.

Plus particulièrement pour les clients, des outils spécifiques pourront être dédiés. Par exemple, un **numéro vert** pourra être établi pour répondre aux requêtes, aux inquiétudes et aux interrogations.

Quel que soit le ou les choix fait(s) pour communiquer, une gestion centralisée de l'information et de sa transmission est fortement conseillée pour maîtriser la situation de crise. **Toutefois, les crises récentes montrent que généralement les informations fournies portent à interprétation. Il est donc primordial de générer des messages forts, tout en gardant le contrôle. Cela passe par des bulletins réguliers, clairs et peu sujets à l'extrapolation.**

OUTILS DE CONTINUITÉ D'ACTIVITÉS MÉTIERS

La cyberattaque a provoqué de graves dommages et les collaborateurs sont potentiellement dans l'incapacité d'utiliser leurs outils de travail, par exemple leur ERP (Enterprise Resource Planning). L'organisme doit donc ensuite mettre en œuvre ou consolider **une stratégie de mobilisation et de déploiement d'outils alternatifs collaboratifs** (outils de travail, visioconférence, drive sécurisé…) **et de bureautique** (achat / location de pc, d'imprimantes, de scanners…). Les correspondants informatiques vont être d'une grande aide pour cette partie. Leur expertise doit être mobilisée pour trouver des solutions mais surtout pour s'assurer qu'elles sont réalisables et viables.

Les outils alternatifs proposés doivent dans la mesure du possible respecter la **Politique de sécurité des systèmes d'information (PSSI)**. Si une PSSI a été élaborée, celle-ci doit normalement prendre en compte les différents scénarios et prévoir des dérogations entérinées et validées en cas de crise.

Parallèlement, des mesures conservatoires ont été enclenchées pour mettre les systèmes hors-ligne. Les systèmes ne feront l'objet de tests qu'une fois que la situation aura été correctement évaluée par la cellule de crise pour la reconstruction du SI. L'urgence nécessite de rapidement passer cette phase afin de pouvoir avoir une vision du matériel et des logiciels toujours utilisables, des dysfonctionnements et des processus atteints. Ces tests doivent se faire de manière continue pour déterminer les efforts à fournir, les difficultés rencontrées et faciliter la reprise des activités *a minima* en mode dégradé.

Des comptes rendus et des documents synthétiques doivent être produits régulièrement afin d'offrir une vision globale des outils alternatifs utilisés et des outils habituels à nouveau fonctionnels. Leur efficacité et leur pérennité est essentiel, c'est pourquoi un suivi et une évaluation / un contrôle permanents sont préconisés.

ACTIONS À MENER :

- Mettre en œuvre **les outils prioritaires de communication interne et externe**
- Mettre en œuvre **les outils prioritaires de continuité d'activités métiers**
- Valider la **conformité des outils à la PSSI**
- Consigner les dérogations et facilités accordées en vue de favoriser le retour aux conditions optimales de sécurité après la crise
- Tester le matériel et les logiciels informatiques pour savoir s'ils sont utilisables une fois la situation bien évaluée
- Identifier les dysfonctionnements et les processus impactés
- Effectuer des tests de manière continue pour déterminer les difficultés rencontrées et les efforts à fournir
- Effectuer des comptes rendus réguliers afin d'offrir une vision globale des outils alternatifs utilisés
- Évaluer / contrôler en permanence l'efficacité et la pérennité des outils

BONNES PRATIQUES (À PRÉPARER EN AMONT)

- **Pour communiquer rapidement hors SI ou outils habituels :**
  Avoir mis en œuvre préalablement des outils alternatifs (Groupe messagerie instantané, page web pour communication de crise web Domaine de secours...)
- **Pour assurer une continuité des activités métier de premier niveau :**
  Avoir mis en œuvre préalablement des outils alternatifs (Bureautique de secours, mail de secours, drive sécurisé, pc, imprimantes, scanners...) ; avoir fait une copie du système d'applications sur une plateforme alternative ; avoir établi un processus de transfert des sauvegardes de données vers un emplacement accessible depuis la plateforme alternative
- **Pour s'assurer de l'opérationnalité des outils :**
  Les tester régulièrement, faire les mises à jour et en assurer le maintien en conditions opérationnelles (MCO) et en conditions de sécurité (MCS)

- **Pour s'assurer de la maîtrise des outils par les utilisateurs**
  Tester de bout en bout la gestion de crise, idéalement dans le cadre d'exercices de simulation de crise en utilisant les outils alternatifs
- **Élaborer une PSSI**
  Intégrer les dérogations possibles en fonction de différents scénarios. Les faire entériner et valider par la Direction générale ou le Directeur
- **Établir un fichier externe des employés**
  Créer une liste des employés et d'adresses emails permettant de les contacter en l'absence de SI, stocké dans un lieu qui n'est pas soumis aux mêmes mEnaces (informer DPO CNIL) / Être en capacité de reconstituer des listes
- **Établir et maintenir un fichier externe des équipements prioritaires**
  Créer une liste des personnes qui doivent être rééquipées en priorité

3.3 Définir la stratégie de continuité d'activité métiers

À ce stade, les activités prioritaires à réanimer d'urgence, y compris en mode dégradé, ont été définies grâce aux échanges avec les métiers et à un arbitrage effectué par le décideur ou la cellule de crise décisionnelle. Les outils de continuité d'activité métiers et les outils de communication interne et externe ont également été déterminés et déployés.

À présent, il est conseillé au(x) décideur(s) de prendre du recul / de la hauteur par rapport à la situation de crise. Une stratégie de continuité d'activité est à élaborer ou à consolider / ajuster s'il en existe déjà une. Pour cela, il est nécessaire d'avoir une vue d'ensemble, facilitée par les remontées Métiers et la définition des activités prioritaires. De cette base stratégique, vont être déterminées les risques et les ressources prioritaires (humaines, équipements, sites, fournisseurs) qui vont alimenter le plan stratégique global. Il va ensuite se subdiviser en sous-stratégies de continuité d'activité des ressources et des activités. La dimension réglementaire et les engagements contractuels sont à intégrer dans la stratégie globale notamment pour protéger l'entreprise de possibles poursuites et se préparer à un audit en aval. Enfin ces différentes stratégies sont à envisager à court terme, moyen terme et long terme (scénarisation). Tout au long de la crise, elles feront l'objet de réajustement et de réévaluation de leur pertinence et de leur efficience.

LA STRATÉGIE GLOBALE

Pour parvenir à des stratégies opérationnelles et efficientes, il est préférable de développer une stratégie globale afin de déterminer :

- le domaine d'application de la stratégie et des stratégies dérivées ;
- la personne ou les personnes en charge de développer la stratégie socle ;
- les ressources prioritaires (IT, humaines, équipements…) ;
- les coûts et les bénéfices.

Une fois que cette réflexion préliminaire est effectuée, l'organisme a une vue d'ensemble sur les différentes options envisageables (plan d'action). Elle est à présent en capacité de préciser ses objectifs en fonction des différentes activités prioritaires arbitrées et des ressources. Sans stratégie socle et vue globale, il est possible que l'entreprise ne prenne pas la bonne direction et que la déclinaison des stratégies échoue.

DÉCLINAISON STRATÉGIQUE

Les stratégies de continuité découlant de la stratégie globale sont élaborées en fonction de deux facteurs : les ressources et les activités. La liste des ressources disponibles ou mobilisables est à rédiger minutieusement. Certaines stratégies vont être évincées tandis que d'autres vont être privilégiées en fonction de cette liste. Faire preuve d'inventivité, de créativité et d'intelligence collective va faciliter cette démarche.

L'objectif de ces stratégies est de s'assurer que toutes les activités et ressources sélectionnées sont maintenues mais également que le réapprovisionnement, la réparation, le remplacement ou la livraison de ressources alternatives soient effectués afin de répondre à la problématique de continuité d'activité.

Si l'entreprise dispose au préalable de stratégies de continuité d'activité, il est fortement conseillé à l'organisme de s'y référer car celles-ci contiennent les prérequis et les dispositifs alternatifs disponibles et pour la plupart déjà éprouvés. Pour les organismes ne disposant pas de ces outils, les urgences sont déjà en cours de traitement, ne pas se précipiter tout en étant stratège est conseillé. Pour ce faire, les personnes en charge de l'élaboration de ces stratégies doivent avoir conscience qu'ils évoluent dans un environnement particulièrement mouvant. Toutes les dimensions (réglementaire, contractuelle, réputationnelle, financière, commerciale) sont déterminantes pour construire des parades efficaces.

Les interdépendances des activités et des ressources vont notamment être au cœur de la réflexion et du développement des stratégies. Des regroupements vont se former et cela va faciliter la démarche.

En sélectionnant les stratégies les plus pertinentes, les coûts de mise en œuvre et de maintenance vont devoir être évalués. De ce fait, les coûts associés doivent être cohérents avec les objectifs et les capacités financières de l'organisation.

Les partenaires de l'organisation, notamment les fournisseurs et prestataires peuvent fournir une aide précieuse. En ayant forgé en amont des relations durables, le partenaire sera davantage disposé à proposer un soutien conséquent (données clients, équipements, sites, expertise…).

SCÉNARISER À COURT, MOYEN ET LONG TERME

La cyberattaque paralysante est par nature une crise longue et incertaine. C'est pourquoi, scénariser la stratégie à court, moyen et long terme va faciliter la planification, le pilotage et la mise en œuvre des options. Il est fortement conseillé de choisir les options qui couvrent plusieurs scénarios. Si des mesures sont prises dès l'événement déclencheur, au fur et à mesure de la crise, l'organisme va acquérir une plus grande marge de manœuvre pour déployer les stratégies. Effectivement, les ressources et les applications non disponibles ainsi que les activités à l'arrêt vont progressivement être réactivées. La patience et la résilience de l'équipe sont des facteurs clés pour survivre à la crise. Cet échelonnement à court, moyen et long terme, dès le début, va offrir de la visibilité et rassurer les membres de l'organisation. Une prise en compte continue de l'humain et de la nature anxiogène des événements pour les membres de l'organisme

n'est pas à négliger. Un point d'attention capital, sans ressources humaines en capacité de se mobiliser, l'organisme subira une seconde crise. Si une stratégie de continuité d'activité existe déjà, il est important d'avoir suffisamment développé le scénario court terme afin de conserver un temps nécessaire à l'approfondissement des scénarios de moyen et long terme. Ces deux scénarios sont plus compliqués à développer en amont car ils dépendent de la nature et de la gravité de la crise, soit de l'impact.

Au sein de ces scénarios sera intégrée une dimension financière, c'est à dire des prévisions de trésorerie et leur mise à jour, une réévaluation des charges fiscales et sociales en fonction des reports de créances possibles et des prévisions d'activité. Une réflexion sur les options de renforcement des fonds propres et ressources financières et sur le BFR (Besoin de fonds de roulement) par des emprunts et des crédits (cf. prêt garanti) est également fortement conseillée.

AJUSTEMENT CONTINU

Une fois que l'ensemble des éléments précédents sont intégrés au sein des stratégies, celles-ci vont être déployées. Tout au long de la crise, elles feront l'objet de réajustement et de réévaluation de leur pertinence au vu de la tournure des événements : aggravation, sur-crise, ampleur des impacts et des conséquences.

Les stratégies doivent évidemment aboutir à une amélioration de la situation. Si les ressources et les activités sélectionnées ne sont pas réactivées progressivement, il faudra changer de posture avec agilité et rapidité.

Livrables à préparer :

- notes / directives internes, planning ;
- plans d'actions des activités à maintenir a minima en mode dégradé pendant la crise (hors SI) en fonction des ressources impactées (*à faire valider par le décideur et les métiers*) ;
- plan de réaffectation et réajustement des ressources disponibles ;
- expression de besoins (réajustée) des applications à remonter par ordre de priorité dans la reconstruction du SI (à faire valider par le décideur et les équipes SI) ;
- plan stratégique, schéma directeur (feuille de route).

BONNES PRATIQUES (À PRÉPARER EN AMONT)

- À partir du BIA, construire une stratégie socle de continuité d'activité (se baser sur la norme ISO 22331)
- En fonction de la stratégie globale sur la continuité d'activité, décliner des stratégies opérationnelles de continuité d'activité (se baser sur les normes ISO 22331 et ISO 22313)

3.4 Déployer les solutions de continuité d'activité métiers

À ce stade, la stratégie globale et les stratégies spécifiques ont été établies. De celles-ci émergent des solutions de continuité d'activité en mode dégradé. Ce sont des plans d'actions élaborés et sélectionnés pour être mis en œuvre dans les jours, les semaines et les mois à venir afin de minimiser l'impact humain et économique de la crise sur l'organisation. Ils doivent être maintenus en conditions opérationnelles (MCO) et en conditions de sécurité (MCS) tout au long de la crise et après la crise pour être activés dès que besoin.

LES MODES DÉGRADÉS

Ces dispositifs doivent faire l'objet d'une étude de faisabilité. Cela consiste à analyser la viabilité et l'efficience de la solution sélectionnée pour le maintien d'une activité spécifique de l'organisation.

La viabilité se mesure en fonction des moyens à disposition de l'organisme. Il est donc essentiel de déterminer les ressources (humaines, financières, IT, équipements, documents, sous-traitants...) nécessaires à la continuité d'activité et de réussir à en mobiliser de nouvelles s'il le faut. En d'autres termes, il faut tout mettre en œuvre pour posséder les outils et les moyens indispensables à la poursuite de l'activité. Cela demande un travail de fond qui se traduit par la production de listes de ressources indispensables à chaque activité métier prioritaire.

Une fois que cela est réalisé, il faut déterminer si l'environnement dans lequel l'organisme évolue rend faisable cette solution. L'environnement concurrentiel, politique, légal et réglementaire doit être analysé afin de ne pas perdre de temps à déployer une solution qui ne peut pas fonctionner dans cet environnement.

Les solutions retenues doivent également répondre aux exigences de maintien des activités prioritaires arbitrées au préalable par un décideur ou par une structure décisionnelle. Ces solutions doivent atteindre des objectifs bien précis, définis en avance. Il est donc important d'évaluer la pertinence des solutions au regard de la satisfaction de ces objectifs.

Enfin ces solutions vont faire l'objet de tests de fonctionnement. L'enjeu est de pouvoir capitaliser sur la crise et donc de créer et déployer des solutions qui sont pérennes sur le long terme. Régulièrement, celles-ci doivent être évaluer et mise à jour pour répondre au calendrier, soit aux objectifs et à l'évolution de ces objectifs en fonction du déroulement de la crise, de son développement dans un sens ou dans un autre.

Parallèlement au déploiement de ces mesures, il est possible de commencer à recenser les dispositifs et les solutions en mode dégradé utilisés pour créer des kits opérationnels mobilisables lors d'une prochaine crise. En possédant une base opérationnelle et en capitalisant sur celle-ci, lors d'une prochaine crise, l'impact pourra être minimisé voire éviter.

PLAN DE REPRISE DE L'ACTIVITÉ

Parallèlement à la gestion de crise et aux dispositifs de continuité d'activité a minima, une dynamique de reprise totale de l'ensemble des activités est engagée et un plan de rattrapage est élaboré. Subissant une cyberattaque paralysante, ce ne sont pas uniquement les activités en tant que telles qui sont touchées mais également les applications. Un redémarrage par vagues prioritaires est enclenché depuis le début de la crise mais au cours de cette étape il va être formalisé sur le long terme.

La première étape est de rassembler, c'est à dire de recréer un esprit d'équipe entre tous les membres de l'organisation, notamment ceux qui n'étaient pas mobilisés pendant la crise. Il est préférable que la vision de l'organisme sur les perspectives de reprise à l'instant T et pour les semaines et mois à venir soit diffusée régulièrement et en toute transparence.

Le plan de reprise totale des activités doit comprendre des objectifs précis en termes de ressources humaines, finances, production, approvisionnement, logistique, commercial, CA, etc. Ce plan intégrera les leçons apprises durant la crise. Un phénomène d'apprentissage et d'amélioration suite à la crise doit permettre de dégager des bonnes pratiques. Il est conseillé au comité de direction ou au chef d'entreprise de mener cette démarche de reprise des activités dans une logique de protection des actifs matériels, immatériels et des emplois. Encore une fois, réinstaurer un climat de confiance et de cohésion sera bénéfique à l'organisation, à son rétablissement et à la redynamisation des activités. Un accompagnement adéquat de la part des managers auprès de leurs équipes, notamment celles qui ne sont pas pleinement en capacité d'exécuter leurs missions est fortement préconisé.

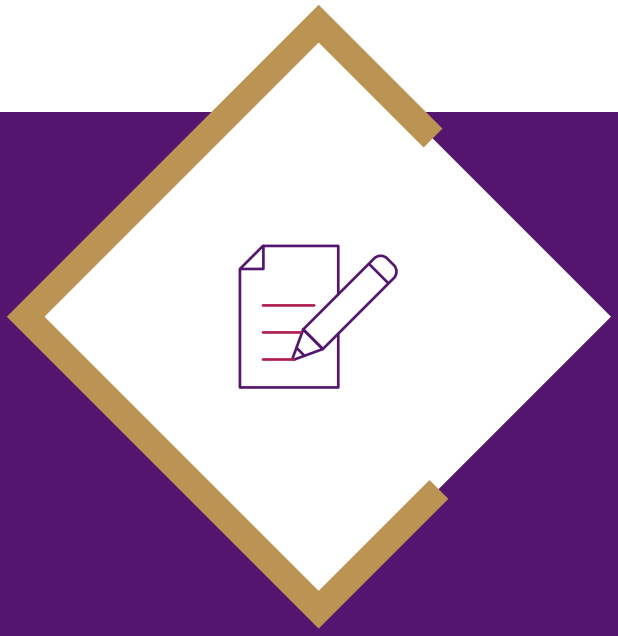
Si la crise a nécessité un usage temporaire mais plein du télétravail, le retour sur site est également à planifier. Une personne ou une équipe chargée de sensibiliser et de diffuser les préconisations en termes de cybersécurité peut être désignée. Ce travail peut s'effectuer en amont ou à partir du retour sur site.

Livrables à préparer :

- créer un document recensant les solutions avec le délai de mise en œuvre, l'efficacité, la faisabilité et la durée de vie ;
- utiliser les outils du BIA pour déterminer les RTO / RPO (liste des applications prioritaires à remonter).

LES BONNES PRATIQUES (À PRÉPARER EN AMONT)

- Disposer de solutions en mode dégradé métiers pour les activités prioritaires (à activer en cas d'indisponibilité prolongée du SI)
- Tester régulièrement et mettre à jour les solutions
- Programmer régulièrement des exercices de simulation de crise (pour entraîner et former les collaborateurs à la continuité d'activité hors SI)



PARTIE 4
SORTIE DE CRISE, RETOUR D'EXPÉRIENCE ET CAPITALISATION APRÈS UNE CYBERATTAQUE

Sortie de crise et bilan

À ce stade, le décideur ou la structure décisionnelle acte la sortie de crise et choisit de démobiliser la ou les cellules de crise une fois qu'il ou elle juge approprié de le faire en fonction des différents curseurs d'analyse. L'annonce de sortie de crise ne suggère pas l'arrêt brutal des actions mises en place. Dans le cas d'une cyberattaque paralysante, même si la crise a été gérée au niveau technique, l'organisme peut se retrouver perturbé durablement dans sa continuité d'activité (reprise de stocks, perte de données, désorganisation).

4.1 Sortie de crise et bilan

À présent, il faut organiser la sortie de crise de l'organisme puis faire un bilan. La crise représente une menace à la survie d'un organisme mais également une opportunité de mieux se structurer et de tirer des enseignements.

La première étape de la sortie de crise est de communiquer auprès des collaborateurs et des parties prenantes. Il est impératif de remercier chacune des personnes qui s'est mobilisée lors de cette crise. En effet, comme rappelé dans le 1.3 (dimension humaine), l'événement et la durée de la crise sont une source de stress importante demandant un engagement / investissement inhabituel qui doit être reconnu et félicité par la direction. Un accompagnement psychologique peut être proposé, le cas échéant.

La seconde étape est la réalisation d'un bilan de crise à chaud. L'objectif est d'offrir l'opportunité à chacun de partager son ressenti, ses impressions sur la crise, en exprimant / développant les difficultés rencontrées et les points positifs de la gestion de crise. Ce bilan immédiat va permettre à l'organisme d'avoir un premier retour et d'en dégager des conclusions. Au cours de ce bilan, il est préconisé de retranscrire les éléments ayant une valeur ajoutée, notamment pour la phase de capitalisation (niveau d'accompagnement, roulement, niveau d'expertise, niveau de cohésion...). Ce n'est qu'une première étape mais elle a toute son importance puisqu'elle est réalisée directement à la sortie de crise. Les événements sont récents et clairs dans l'esprit de chacun. Ce bilan est un premier indicateur de la résilience et de la bonne gouvernance et gestion de l'organisme selon les collaborateurs.

La troisième étape est la structuration des éléments retranscrits, qui pourront servir à réaliser le retour d'expérience dont la démarche est développée en 4.2. En effet, un questionnaire type peut être enrichi par les échanges du premier bilan. Chaque crise est différente et demande un travail de personnalisation et de spécification en fonction.

4.2 Réalisation d'un retour d'expérience

Un retour d'expérience (REX ou RETEX) spécifique doit être organisé à chaud et un second à froid, quelques jours / semaines après la crise. Cela permettra à toutes les parties prenantes de s'exprimer et de définir :

- un dossier de suivi avec une vue d'ensemble de la gestion de la crise ;
- une synthèse globale des bonnes et des mauvaises pratiques ; ce qui a bien marché, qui peut être amélioré, ce qu'il faut éviter ;
- des actions correctives : gestion de la crise et réponse opérationnelle ;
- un plan d'action pour améliorer la gestion de crise ;
- l'amélioration des dispositifs et mesures de sécurité ;
- des mesures préventives (entrainement, exercices...) ;
- une potentielle revue des procédures actuelles ;
- une évaluation de l'impact de la crise sur les aspects financiers, images, humain, réglementaires, opérationnels, etc.

ORGANISER DANS UN DÉLAI MAXIMUM D'UN MOIS UNE RÉUNION RETOUR D'EXPÉRIENCE (REX) AVEC L'ENSEMBLE DES ACTEURS DE LA GESTION DE LA CRISE :

- mener des entretiens individuels peut également être pertinent pour éviter l'effet réducteur de la discussion de groupe ;
- dérouler le REX en respectant la chronologie de la crise et l'enchaînement des évènements, des décisions et des actions ;
- s'appuyer sur le livre de bord ou journal de crise, les points de situation et le bilan de crise ;
- recenser les points forts de l'organisation de crise, les bons réflexes à conserver et à capitaliser ;
- recenser les points faibles et les difficultés rencontrées ;
- lister les actions d'amélioration à réaliser (échéance, responsable) ;
- mettre en place des solutions pour éviter la survenance de l'événement ;
- bâtir le plan d'actions associé.

LE REX COMPREND DES PHASES :

- **Événement et Alerte**
  - Quand et comment a été donnée l'alerte, dans quels délais ?
  - Les modalités d'alerte
  - Le dispositif d'alerte ainsi que les moyens logistiques adaptés
- **Entrée en crise :** Mobilisation et composition
  - Cadrage et évaluation de la gravité de la situation initiale
  - Condition de mobilisation de la cellule de crise
  - Fonctions et missions au sein de la cellule de crise
  - Expertise au sein de la cellule de crise suffisante
- **Logistique**
  - Salle de crise adaptée ?
  - Équipement et moyen de communication adaptés ?
  - Documentations et annuaires à jour ?
  - Mise à disposition d'outils de gestion de crise (fiche missions, etc.)
- **Cadrage de la situation et évaluation des impacts**
  - Évaluation pertinente du potentiel de gravité de la situation au fur et à mesure de son évolution ?
  - Identification exhaustive des parties prenantes impactées par la crise (services, partenaires, etc.) ?
  - Prise en compte des enjeux associés ?
  - Élaboration des orientations stratégiques et tactiques au sein de la Cellule de Crise ?
  - Anticipation systématique des conséquences possibles de la stratégie adoptée ?
  - Validation juridique des décisions prévues et réalisées ?
- **Fonctionnement de la cellule de crise**
  - Fréquence et durée des réunions ?
  - Pratiques utilisées (ordre du jour, compte rendu, suivi des actions, diffusion des comptes rendus) ?

- **Prise de décision**
  - Conception de solutions pertinentes
  - Prise de décisions rapide du passage d'un évènement à l'autre ?
  - Prises de décisions partagées ?
  - Déploiement de mesures de continuité d'activité informatique et métiers ?
- **Relations avec les parties prenantes externes**
  - Performance du dispositif d'information prévu
  - Dispositif de gestion des réclamations
  - Vecteurs d'information utilisés
- **Communication interne et externe**
  - Cohérence des messages
  - Vecteurs d'information utilisés (lettre, annonces)
- **Retour à une activité normale**
  - Délais et modalités de reprise d'activité (tout domaine d'activité)
  - Traitement des restes à faire
  - Travaux de remise en état
  - Assurances
- **Communication post crise**
  - Messages diffusés aux parties prenantes externes (clients, partenaires, etc.)
  - Messages diffusés aux salariés
- **État des lieux de la situation actuelle**
  - Bilan de crise
  - Problèmes non résolus
  - Dispositif de veille et de surveillance de la situation post crise

4.3 Capitalisation : plans d'actions et amélioration continue

PLAN DE RENFORCEMENT DE LA SÉCURITÉ DES SI

L'ensemble des actions de durcissement du système d'information ne peuvent pas être toutes menées dans un délai court, pour des raisons de charge de travail des équipes de production ou de délai d'approvisionnement également. Il est important d'engager une démarche long terme et de définir une feuille de route pour améliorer durablement la sécurité du système d'information ainsi que les capacités de détection.

Plusieurs axes sont à intégrer dans la feuille de route :

- renforcement des capacités humaines et notamment la nomination d'un responsable en charge de la sécurité des systèmes d'information (RSSI) si ce n'est pas déjà le cas ;

- identification des chantiers de sécurité à mener pour renforcer la sécurité du système d'information comme par exemple :

Exemple de chantiers d'amélioration de la sécurité

- mise en place d'un budget dédié à la cybersécurité intégrant notamment les coûts récurrents pour le maintien de la sécurité à la fois sur les processus, les solutions et des moyens de surveillance.

La définition des chantiers peut passer par une évaluation de sécurité externe afin d'identifier les lacunes organisationnelles et techniques. Cela permettra de confronter la vision d'un tiers sur le plan de renforcement de la sécurité.

Afin de mener à bien ce programme de sécurité, il convient de commencer à :

- cadrer les grandes lignes des projets ;
- identifier les prérequis nécessaires ;
- établir une estimation budgétaire ;
- construire un plan projet avec un planning prévisionnel sur une ou plusieurs années.

Cela nécessite également la mise en place de points de contrôle et d'un processus de maintien en condition de sécurité (MCS) pour les systèmes concernés. Cela permettra de garantir dans le temps le niveau de sécurité. De manière générale, il est important d'entamer la mise en place d'un système de management de la sécurité du système d'information (SMSI) permettant de définir une logique d'amélioration continue de la sécurité et de pérenniser les actions entamées.

PLAN DE RÉVISION ET DE MISE À JOUR DU PCA (EN CAS D'INDISPONIBILITÉ PROLONGÉE DU SI)

Au cours de la crise, deux profils d'organismes se dessinent : ceux qui n'avaient pas de Plan de continuité global (PCA) et ceux qui avaient a minima un PCA global, mais sans déclinaison spécifique pour ce type de scénario (mode dégradés métiers hors SI).

L'organisme disposant au préalable d'un PCA va devoir évaluer l'efficacité du PCA lors de la crise cyber et identifier les améliorations possibles. Ces améliorations sont le fruit des retours d'expériences des individus impliqués dans la gestion de crise. Si le PCA est uniquement global, il est préconisé d'introduire un macro-scénario cyber pour répondre aux défis de la continuité d'activité hors SI. L'organisme ne disposant pas d'un PCA, même global, est fortement incité à élaborer un PCA cyber c'est-à-dire, définir les modes dégradés métiers des activités prioritaires hors SI initial.

Au cours de la crise, des modes dégradés auront été déployés dans l'urgence dont certains auront pu se révéler efficaces. À présent que la sortie de crise est actée, il est offert à l'organisme, l'opportunité d'élaborer méthodiquement et de valider durablement des modes dégradés opérationnels pour ce type de crise majeure.

Une cartographie des risques suffisamment exhaustive permettra d'identifier les vulnérabilités et les menaces auxquelles est confronté l'organisme.

Le BIA identifiera les activités prioritaires et les ressources associées pour fonctionner en mode dégradé a minima. Les menaces et les risques associés à ces activités peuvent également être identifiés en menant un BIA.

Les modes dégradés seront élaborés en fonction de la liste des activités prioritaires décidées. La recherche de modes dégradés métiers peut demander un certain temps et nécessiter des échanges réguliers avec les métiers et les équipes IT afin de sélectionner les plus pertinents et durables. Pour évaluer leur faisabilité et leur facilité de mise en œuvre, il est conseillé d'effectuer des tests et des exercices de simulation de crise cyber à intervalles réguliers. De ces exercices émergeront des ajustements qui aboutiront à des modes dégradés suffisamment performants et qui correspondront aux délais de rétablissement décidés en amont.

Pour réduire les risques ou les traiter, plusieurs mesures doivent être envisagées :

- mesures de protection et d'atténuation (réduction de l'impact) ;
- mesures préventives (réduction de la probabilité) ;
- mesures de détection (détection précoce : réduction de l'impact) ;
- mesures correctives (réduction de la probabilité) ;
- mesures de transfert (réduction de l'impact).

L'ensemble de cette démarche doit permettre d'instaurer un système de management de la continuité d'activité performant en cas de cyberattaque. Ce dernier étant voué à évoluer régulièrement via des mesures correctives pour rester résilient et adapté au fonctionnement de l'organisme.

AMÉLIORATION CONTINUE ET CYBER-RÉSILIENCE

Un système de management intégré (SMI) désigne l'intégration des systèmes de management en se référant aux normes ISO. Plus un SMI est mature, plus il inclut de dimensions. La construction d'un SMI doit permettre de rassembler l'ensemble des exigences de chacun des systèmes de management sans diluer les spécificités de chacun. L'objectif premier du SMI est de permettre une amélioration continue de la productivité et de l'efficacité.

Pour satisfaire aux exigences de ce document, il est conseillé de construire un SMI sous la forme d'un système de management de la cyber résilience. En effet, dans le cas d'une cyberattaque paralysante, il est intéressant d'aborder le SMI comme un système combinant la sécurité de l'information (norme ISO 27001) et la continuité d'activité (norme ISO 22301). Architecturer un système plus résilient à la suite de la survenance d'un acte de haute malveillance cyber permettra de construire, pour l'avenir, des capacités utiles et mobilisables lors de l'attaque.

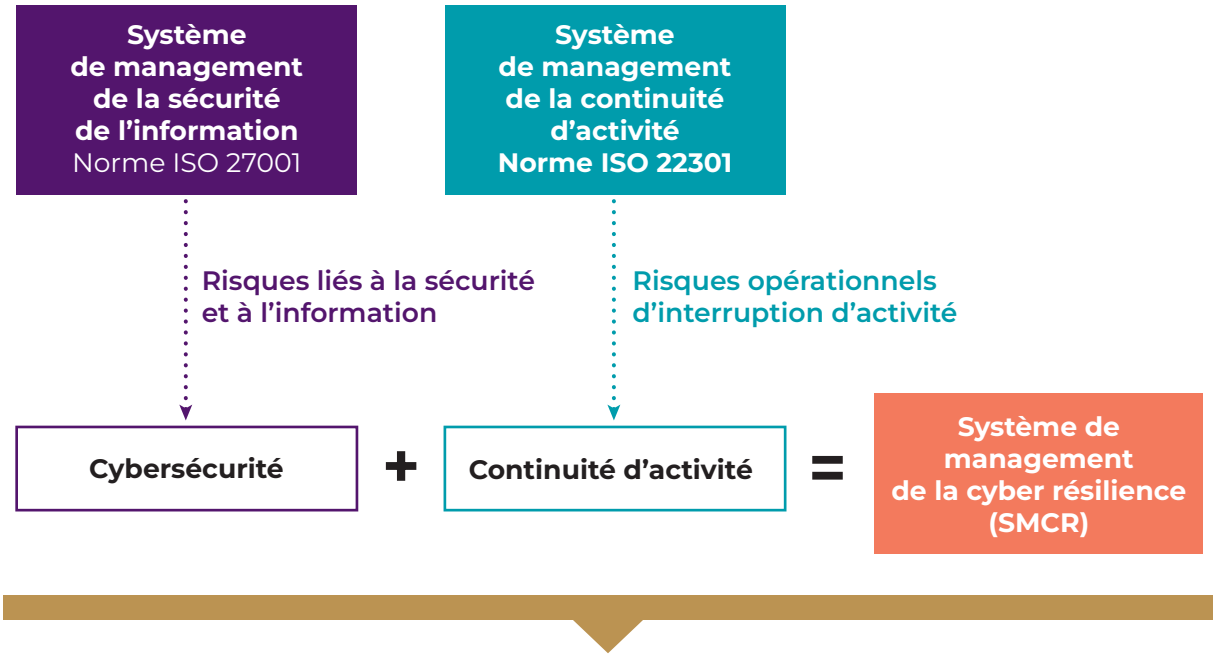


Figure 12 : Schéma d'un Système de Management Intégré ISO 27001/ISO22301 dit « Cyber-résilient »

PARTAGE DES RETEX ENTRE DÉCIDEURS

Enfin, pour capitaliser sur l'événement, il est conseillé de promouvoir une culture du partage des retours d'expérience entre décideurs. Participer à un échange transparent sur les attaques subies par les autres et votre propre organisme permettra de comparer l'efficacité des mesures prises, d'intégrer des idées et de supprimer les actions inefficaces de votre plan de gestion de crise et de continuité d'activité.

ANNEXE A

Synthèse des bonnes pratiques

RAPPEL DES BONNES PRATIQUES POUR LA GESTION DE CRISE (À PRÉPARER EN AMONT)

- Établir une grille de qualification des incidents de sécurité et des crises
- Élaborer la composition des cellules de crise : sélection des fonctions métier et support indispensables à l'organisation de crise
- Identifier les personnes intégrant les cellules de crise
- Identifier des salles disponibles et équipées
- Avoir un système d'alerte pour dépêcher les personnes en cellule de crise
- Déterminer les roulements des équipes
- Déployer une logistique de crise de confort pour les équipes de crise (base vie, repas, utilités...)
- Faciliter la prise en charge financière des coûts exceptionnels liés à la crise : garde familiale, transports, chambres d'hôtels...)
- Mettre à disposition un soutien médico-psychologique dès le début de crise
- Mettre en place du renfort (ressources supplémentaires là où cela est possible et se justifie)
- Organiser une relève des équipes (temps de repos, faire souffler les équipes)
- Définir une fiche mission pour le coordinateur SI
- Définir une fiche mission pour le coordinateur CA
- Dresser une liste des canaux de communication mobilisables en cas de cyberattaque
- Définir une fiche réflexe pour les points de situation : les questions à poser côté SI et côté CA, les besoins de l'équipe SI de la part de l'équipe CA et inversement...
- Fiche réflexe sur la manière de communiquer/diffuser l'information entre les pôles SI et CA
- Entrainements à la gestion de crise (exercices de simulation et tests)
- Bonnes pratiques de management (collaboratif et participatif)
- Maintenir le lien avec les grands fournisseurs essentiels
- Établir la relation avec la communauté des pairs
- Préparer une trame de communiqué de crise
- Préparer des éléments de langage
- Préparer le Directeur communication en effectuant des exercices de crise
- Connaître les canaux de communication à privilégier durant une crise
- Préparer des formats de communication adéquats en fonction des canaux de communication (posts LinkedIn, tweets, télévision, presse écrite, réseaux sociaux,...)
- Avoir des outils de communication alternatifs à disposition lors d'une cyberattaque
- Tester et évaluer à fréquence régulière les outils de communication alternatifs au cours d'exercices de crise
- Souscrire un contrat d'assurance Cyber (cf annexe A pour plus de détail)

- Documenter l'ensemble des mesures mise en œuvre pour permettre la production en mode dégradée pendant la période de restauration du SI et au fur et à mesure de la réouverture des services spécifiques aux métiers de l'entreprise (comptabilité, ressources humaines, finance, production, vente en ligne…)
- Démarche de prévention des risques cyber et mesures d'hygiène informatique
- Mettre en place des PCA/PRA/PCI
- Test de restauration des sauvegardes, déclenchement PRA
- Simulation d'exercices de crise Cyber

RAPPEL DES BONNES PRATIQUES POUR LE REDÉMARRAGE DU SYSTÈME D'INFORMATION

- Mettre en place un archivage des journaux et vérifier la chaine de traçabilité / verbosité des équipements afin de permettre d'identifier les activités réalisées sur le système d'information
- Mettre en place un système de synchronisation de temps sur l'ensemble du système d'information
- Disposer d'une cartographie du SI et des réseaux et d'un inventaire des équipements
- Conserver une copie isolée des éléments critiques sur un environnement isolé (SI autonome ou PC isolé ou version papier)
- Avoir une stratégie de reconstruction du SI et une procédure de restauration du SI ainsi que des sauvegardes qui sont hors ligne / immuables pour éviter le risque de se faire compromettre son système de sauvegarde et qui sont testés régulièrement afin de valider l'intégrité et la consistance
- Avoir un ordre / une procédure de démarrage de son système d'information contextualisé à l'environnement
- Définir une procédure de recette des applications après redémarrage du SI et disposer de dossier d'architecture permettant de lister les flux nécessaires

RAPPEL DES BONNES PRATIQUES POUR LA CONTINUITÉ D'ACTIVITÉ MÉTIERS (À PRÉPARER EN AMONT)

- **Avoir mis en place le plan de gestion de crise**
- **Avoir réalisé le Bilan d'Impact sur les activités (BIA) de l'organisme** (se baser sur la norme ISO 22317 : 2021)
- **Avoir réalisé le PCA Global de l'organisme et valider une stratégie PCA (arbitrage Direction générale) en lien avec les risques d'interruption d'activité et les enjeux** (se baser sur la norme ISO 22301 : 2019)
- **Pour communiquer rapidement hors SI ou outils habituels :**
  Avoir mis en œuvre préalablement des outils alternatifs (Groupe messagerie instantané, Site web interne dormant à activer, Domaine de secours…)
- **Pour assurer une continuité des activités métier de premier niveau :**
  Avoir mis en œuvre préalablement des outils alternatifs (Bureautique de secours, mail de secours, drive sécurisé, pc, imprimantes, scanners…) ; avoir fait copie du système d'applications sur une plate-forme alternative ; avoir établi un processus de transfert des sauvegardes de données vers un emplacement accessible depuis la plateforme alternative

- **Pour s'assurer de l'opérationnalité des outils :**
  Les tester régulièrement, faire les mises à jour et en assurer le maintien en conditions opérationnelles (MCO) et en conditions de sécurité (MCS)
- **Pour s'assurer de la maîtrise des outils par les utilisateurs**
  Tester de bout en bout la gestion de crise, idéalement dans le cadre d'exercices de simulation de crise en utilisant les outils alternatifs
- **Élaborer une PSSI**
  Intégrer les dérogations possibles en fonction de différents scénarios. Les faire entériner et valider par la Direction générale ou le Directeur
- **Établir un fichier externe des employés**
  Créer une liste des employés, stockée en lieu sûr dans une autre zone de risque et indépendamment du SI (validation DPO CNIL) / Être en capacité de reconstituer des listes
- **Établir et maintenir un fichier externe des équipements prioritaires**
  Créer une liste des personnes qui doivent être rééquipées en priorité
- **Pour assurer la continuité d'activité des activités prioritaires hors SI**
  - Élaborer le PCA Cyber ou rajouter au PCA existant le scenario d'indisponibilité prolongée hors SI en cas de cyberattaque paralysante
  - Définir les modes dégradés métiers ou autres solutions alternatives pour fonctionner hors SI nominal pendant une période prolongée

ANNEXE B

Fiche souscription cyber assurance

Les assurances cyber qui proposent une assistance à gestion de crise sont présentes sur le marché Français depuis 2015. Une couverture d'assurance cyber permet la prise en charge de nombreux frais consécutifs à plusieurs types d'incidents cyber. Par exemple :

- le vol de données y compris d'information de cartes bancaires ;
- l'atteinte aux données ;
- le cyber-rançonnage ou extorsion (rançongiciel) ;
- le cyber détournement de fonds ;
- l'attaque par déni de service.

Des garanties optionnelles peuvent être souscrites en fonction de l'activité de l'entreprise (par exemple la garantie en cas d'atteinte à l'e-réputation).

Les frais couverts par les contrats cyber sont également ajustables, toutefois les assureurs spécialisés proposent un tronc commun qui se présente comme suit :

- frais d'expertise et d'assistance ;
- frais d'investigation numérique ;
- frais de reconstruction ;
- frais de reconstitution des données ;
- perte d'exploitation (marge brute) limitée le plus souvent à 6 mois max ;
- frais supplémentaires d'exploitation ;
- frais juridiques (couvre généralement le coût des conseils et des démarches auprès des autorités et autres régulateurs) ;
- frais de communication de crise.

Un point d'attention doit être porté sur la garantie en cas de rançongiciel qui est de plus en plus conditionnée et limité. La sinistralité ayant été multipliée par 4 au début des années 2020, les assureurs n'accordent pas systématiquement cette garantie.

En visite de souscription, les assureurs seront naturellement vigilants à la description de la sécurité du SI de l'entreprise mais également aux plans d'actions prévus pour son amélioration continue. En effet, les compagnies ont intégré que la cyber sécurité est un risque à caractère évolutif et elles sont désormais au fait de l'évolution des menaces. Dans leur grande majorité, pour des raisons historiques, les assureurs qui proposent des contrats cyber s'appuient sur l'ensemble des directives du NIST et ses 5 fonctions (Identifier, Protéger, Détecter, Réagir, Récupérer).

En parallèle, de nombreux assureurs, avant la souscription, font appel à des sociétés de notation et d'évaluation de posture de cybersécurité. Il est donc conseillé de connaitre également son risque avant de rencontrer son assureur.

Bien que la protection du SI soit un élément clé pour un assureur, la capacité à détecter, à isoler puis à récupérer sont des points de plus en plus examinés en détail dans la mesure où ils ont un impact direct sur la marge de l'entreprise, étant précisé qu'il s'agit du poste le plus élevé qu'un assureur devra couvrir s'il est appelé en garantie.

Les point ci-dessous sont essentiels en vue de la souscription d'une police d'assurance cyber :

- avoir une PSSI maintenue par le RSSI et validée par la direction de l'entreprise avec au moins les éléments suivants :
  - Une politique de mots de passe conforme aux recommandations de l'ANSSI ;
  - La re-certification régulière (au moins annuelle) des comptes à privilèges ;
  - Une politique d'application des correctifs ;
  - Des procédures de gestion des événements en fonction de leur criticité découlant vers des plans de remédiation ;
  - Une classification des données ;
- maintenir un inventaire à jour de son parc informatique ;
- disposer de solutions d'authentification à facteurs multiples ;
- posséder un système de détection et de prévention d'intrusion sur les terminaux ;
- posséder un système de sauvegardes déconnecté et testé régulièrement ;
- mettre en place une politique de rétention des journaux d'évènements ;
- mener régulièrement des actions de sensibilisations auprès des collaborateurs et faire un exercice de crise au moins une fois par an.

Enfin, les contrats d'assurances cyber disposent d'un volet de Responsabilité Civile qui couvre votre responsabilité en cas de dommages que vous causeriez à un tiers. Par exemple, si votre SI sert de base à un attaquant ou bien, si en cas d'attaque, vous coupiez vos flux de manière prolongée avec vos clients et fournisseurs occasionnant une perte significative…

Le volet RC du contrat cyber (comme celui de votre RC PRO) ne doit pas être ignoré et doit correspondre à la nature de votre activité et du risque. Les dommages aux tiers et les pertes consécutives souvent élevées que vous pourriez causer à la suite d'un incident cyber (dont vous seriez la première victime) ne sont pas à négliger dans la démarche de souscription en vue du transfert de votre risque cyber à une compagnie d'assurance.

ANNEXE C

Guide synthétique pour les petites structures (écosystème français)

Si la plupart des organismes de grande taille (grandes entreprises et collectivités) sont conscientes de la réalité de la cybersécurité, les plus petits (Associations, TPE, PME, ETI[1], petites et moyennes collectivités) qui, bien souvent, ne disposent même pas d'un responsable informatique, le sont moins. Ils ne se sentent pas concernés, le sujet apparaissant comme anxiogène, abstrait, très technique, et – surtout – très coûteux.

Or, ce sont des cibles privilégiées pour les attaquants car insuffisamment préparées et donc plus vulnérables. En effet, les cyberattaques sur de telles entités sont plus faciles et rapides que sur les grandes organisations pour lesquelles les attaquants doivent mobiliser plus de compétences, de technicité, de moyens et de temps. Par conséquent, ceux-ci trouvent dans cette cible spécifique une rentabilité plus grande.

Les statistiques le prouvent : au regard de la répartition des entités victimes d'attaques par rançongiciel dans le cadre des incidents traités par l'ANSSI, force est de constater que les PME/TPE/ETI qui ne représentaient « que » 34 % en 2020 sont devenues majoritaires en 2021 avec 52 % des cas[2].

Les collectivités territoriales sont également des cibles privilégiées des attaques cyber. Or, un cadre réglementaire leur impose de mettre en place différentes mesures destinées à sécuriser leurs systèmes d'information, leurs services numériques, et à protéger les données à caractère personnel de leurs administrés, afin d'éviter la paralysie du fonctionnement du Service Public[3].

1. *Très Petites Entreprises, Petites et Moyennes Entreprises, Entreprises de Taille Intermédiaire*
2. *Source : Panorama de la menace informatique 2021, ANSSI, mars 2022 - https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-002/*
3. *Source : rapport du Sénat* "Les collectivités territoriales face au défi de la cybersécurité", *décembre 2021 - https://www.senat.fr/rap/r21-283/r21-283_mono.html*

COMMENT RENFORCER VOTRE CYBER-RÉSILIENCE

Les constats suite à des incidents ou vis-à-vis de la tendance sectorielle sur la Cyber a conduit les autorités publiques et l'association des PME à éditer le « Guide de la cybersécurité pour les TPE / PME en 13 questions »[4]. Celui-ci présente douze recommandations à destination des non-spécialistes, issues de l'analyse d'attaques réussies et de leurs causes.

ÊTRE ACCOMPAGNÉ ET FINANCÉ

Là aussi, les Régions et les Agences régionales de Développement peuvent proposer aides, conseil et soutien financier pour accompagner les PME dans des démarches d'amélioration continue (conseil, audit, investissements...) autour de la cybersécurité. De son côté, dans le cadre du plan de relance, le Groupe AFNOR permet aux TPE/PME de bénéficier d'un parcours de formation en cybersécurité, 100 % financé par BPI France, dispositif qui se décline en 3 parcours :

1. Faire face à une cyberattaque, points de vigilance et outils pour s'y préparer et réagir ;
2. Comment acculturer et sensibiliser son équipe face à la menace cyber ?
3. Quelles mesures organisationnelles, techniques et juridiques mettre en œuvre pour réduire les vulnérabilités face aux attaques ?

Certaines filières proposent également des opérations d'accompagnement (Aéronautique, Maritime, Clubs ETI...). Côté Collectivités, des parcours de cybersécurité sont proposés dans le cadre du volet cybersécurité de France Relance avec pour objectif de renforcer la sécurité des systèmes d'information des bénéficiaires en proposant un pré-diagnostic et un accompagnement par des prestataires compétents, de la maîtrise d'ouvrage jusqu'à la mise en œuvre.

DISPOSER D'UNE BASE DOCUMENTAIRE

Il existe de nombreux guides et fiches réflexes disponibles sur les sites web des différentes structures mentionnées ci-dessus, en particulier sur le site de l'ANSSI, de Cybermalveillance ou de FranceNum. Citons par exemple :

- « Guide de cybersécurité à destination des dirigeants de TPE, PME et ETI : bonnes pratiques et réflexes à adopter en cas de cyberattaques » (FranceNum) ;
- « La cybersécurité pour les TPE/PME en douze questions » (ANSSI) ;
- le guide de la « sécurité numérique des collectivités territoriales » (ANSSI) ou encore toute une série de fiches réflexes et mémo sur Cybermalveillance.gouv.fr

4. *https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-treize-questions/*

EN CAS DE CYBERATTAQUE : LES ÉTAPES À SUIVRE

Pour réagir face à une cyberattaque, 3 étapes cruciales pour un organisme de petite taille :

SÉCURISER

Les premières démarches à prendre visent à éviter que la situation ne s'aggrave. Il convient donc de ne pas perdre son calme et de prendre quelques mesures simples :

1. **Identifier les éléments touchés et isoler** ceux-ci du réseau informatique. En cas de doute, retirer le câble réseau de ces équipements sans les éteindre afin que le prestataire informatique puisse intervenir. L'objectif est d'arrêter ou de contenir l'incident s'il est toujours en cours.
2. **Contacter les prestataires :** prévenir les prestataires concernés de l'incident et leur demander d'intervenir. Le prestataire informatique pourra assister dans les premières démarches et définir plus précisément le périmètre impacté. Ceci permettra de coordonner les interventions d'autres prestataires sur les systèmes métiers impactés. Si vous avez une cyber-assurance, il est nécessaire de déclarer votre sinistre au plus tôt afin de bénéficier des prestations incluses dans celle-ci. Il est également possible de faire appel à l'assistance aux victimes de cyber malveillance via la plateforme Cybermalveillance.gouv.fr ainsi que par les CERT sectoriels et régionaux.
3. **S'organiser et travailler en équipe :** traiter l'incident sera beaucoup plus facile si deux personnes ou plus travaillent ensemble. Par exemple, une personne peut effectuer des actions tandis que l'autre les documente. Il vous faut donc mobiliser une équipe de réponse à la crise et déclenchez votre Plan de Continuité de l'Activité (PCA), si vous en avez un.
4. **Organiser vos activités :** libérer du temps aux ressources impliquées afin de pouvoir gérer la crise. Rappelons que la reprise peut nécessiter selon les cas quelques heures voire plusieurs semaines.
5. **Confirmer qu'un incident s'est produit avec des éléments de preuve :** effectuer des recherches supplémentaires si nécessaire afin de bien matérialiser l'incident et ses conséquences.

ALERTER

La situation étant stabilisée, il vous faut donner l'alerte rapidement, prendre contact et informer les acteurs concernés :

6. **Contacter les prestataires externes :** prévenir les prestataires concernés de l'incident et leur demander d'intervenir. Le prestataire informatique (si vous en avez un) pourra assister dans les premières démarches et définir plus précisément le périmètre impacté. Ceci permettra de coordonner les interventions d'autres prestataires sur les systèmes métiers impactés. Si vous avez une cyber-assurance, il est nécessaire de déclarer votre sinistre au plus tôt afin de bénéficier des prestations incluses dans celle-ci. Il est également possible de faire appel à des dispositifs d'assistance aux victimes.
7. **Faire les déclarations administratives nécessaires :** dans tous les cas, il est indispensable de déposer une plainte contre X à la gendarmerie afin de vous prémunir contre certaines procédures administratives ultérieures (URSSAF, Impôts...) en lien avec les conséquences de votre incident. D'autre part, une déclaration préalable à la CNIL doit être réalisée dans les 72 heures après la confirmation d'une atteinte aux données à caractère personnel. Celle-ci pourra être complétée dans les 30 jours avec l'aide d'un avocat.

8. **Informer en interne et externe :** penser à informer les collaborateurs de la situation et préciser qu'il y a un besoin de discrétion sur le sujet. La communication externe doit être limitée aux parties prenantes ou à un besoin administratif (CNIL et autres). Il peut être aussi utile d'avertir votre banque et certains de vos partenaires.

REMÉDIER

L'objectif est d'atteindre rapidement une reprise d'activité, même partielle.

9. **Identifier et atténuer toutes les failles qui ont été exploitées :** l'incident peut s'être produit en tirant parti des vulnérabilités des systèmes d'exploitation ou des applications. Il est essentiel d'identifier la source et l'étendue de l'attaque, ces vulnérabilités et de les éliminer ou de les atténuer afin que l'incident ne se reproduise pas.
10. **Essuyer tous les effets de l'incident :** cet effort inclut les infections de logiciels malveillants, les matériels inappropriés (par exemple, les logiciels piratés), les fichiers de chevaux de Troie et toute autre modification apportée aux systèmes par des incidents. Si un système a été entièrement compromis, le reconstruire à partir de zéro ou le restaurer à partir d'une bonne sauvegarde connue.
11. **Vérifier que les opérations ont été rétablies à la normale :** vérifier que les applications et les autres services affectés par l'incident ont été retournés à des opérations normales.
12. **Mettre fin à la gestion de crise :** informer les parties prenantes de la reprise des activités à la normale. Ceci permet de ne pas laisser planer de doute sur la situation et montre que la chaine de vigilance se mette en place.
13. **Capitaliser sur votre Incident :** quelques jours après votre incident, prenez une heure afin d'identifier ce qui a bien fonctionné et ce qui doit être amélioré. Ceci vous permettra de définir un plan d'action (ex. sensibiliser le personnel à l'hameçonnage, contrôler le système de sauvegarde, mettre en place avoir un contrat de maintenance informatique…).

EN CAS DE CYBERATTAQUE : SE FAIRE AIDER

Lors d'une attaque de cybersécurité, les petites structures se trouvent bien souvent démunies et il est difficile pour elles de réagir seules. Heureusement, il existe un ensemble d'organismes publics qui constituent une sorte de « bouclier » pour les aider et les accompagner.

AU NIVEAU NATIONAL (FRANCE)

- **L'Agence nationale de la sécurité des systèmes d'information (ANSSI)** dont le rôle est de faciliter une prise en compte coordonnée, ambitieuse et volontariste des questions de cybersécurité en France. Acteur majeur de la cyber sécurité (c'est un service du Premier ministre, rattaché au Secrétariat général de la défense et de la sécurité nationale – SGDSN), elle apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV) et de services essentiels (OSE). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques ;
- **Cybermalveillance :** la plateforme Cybermalveillance.gouv.fr, portée par un partenariat public-privé autour du GIP ACYMA, est active depuis 2017. Destiné aux particuliers, entreprises et collectivités territoriales, ce dispositif national a pour mission la sensibilisation, la prévention et l'assistance aux victimes d'actes de cybermalveillance. Outre l'ANSSI et les principaux ministères, cette plateforme rassemble de nombreux acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles de type fédération ou syndicat, des assureurs, des opérateurs, des éditeurs de logiciels…
- **Des CERT thématiques ou sectoriels :** certains secteurs d'activités se sont dotés de centres de réponse d'urgence (CERT – Computer Emergency Response Team) dont une des missions centrales est la centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ; il existe par exemple un CERT Maritime, un CERT Santé, un CERT pour la recherche publique (RENATER) ou l'Éducation Nationale (COSSIM), etc.
- **Des plateformes de signalement et de dépôt de plainte :** en complément de Cybermalveillance.gouv.fr, la Police Judiciaire opère différents télé-services comme **Pharos** (Plate-forme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements) pour signaler des contenus publics et comportements en ligne illicites, le site de dépôt de plainte en ligne pour les victimes d'arnaques en ligne **THESEE** ou encore **Infos Escroquerie**, plate-forme téléphonique d'information et de prévention sur les escroqueries sur internet ;
- **Des groupements d'acteurs** qui peuvent vous orienter comme le **CLUSIF** (Club de la sécurité de l'information français), association dont la mission consiste à favoriser les échanges d'idées et de retours d'expérience à travers des groupes de travail, des conférences et publications, et qui rassemble offreurs et utilisateurs, dans tous les secteurs d'activité de l'économie autour de la cybersécurité et de la confiance numérique, **le Cybercercle**, cercle de réflexion, d'expertise et d'échanges sur les questions de confiance et de sécurité numériques, ou encore le **CESIN** (Club des Experts de la Sécurité de l'Information et du Numérique).

AU NIVEAU RÉGIONAL :

- **La plupart des structures régionales d'accompagnement des entreprises** (les agences régionales de développement en particulier) et, à termes, les Campus Cyber territoriaux proposent des annuaires de l'écosystème régional de la cybersécurité. La plateforme nationale Cybermalveillance référence également des prestataires pouvant intervenir en cas de cyberattaques ;
- **Les « CSIRT » régionaux :** impulsé par l'ANSSI et porté par les Régions, le réseau des centres de réponse aux incidents cyber régionaux (CSIRT – Computer Security Incident Response Team), se déploie actuellement au profit des entités implantées sur le territoire régional. Ce sont des centres d'appels (téléphoniques) qui traitent les demandes d'assistance des acteurs de taille intermédiaire, (PME, ETI, collectivités territoriales…) pour leur apporter une aide d'urgence (gestes réflexe) puis les mettre en relation avec des partenaires de proximité (prestataires de réponse à incident, partenaires étatiques, assistance juridique…) ;
- **Les acteurs étatiques :** des correspondants de la Gendarmerie Nationale sont disponibles en région, dans le cadre du Com Cyber Gend (commandement de la gendarmerie dans le cyberespace) qui vise à piloter, conduire et animer le dispositif de la gendarmerie nationale dans la lutte contre les cybermenaces ; la Police Judiciaire dispose, elle, d'une sous-direction de la lutte contre la cybercriminalité, accessible via les commissariats ; on peut aussi mentionner la DGSI, compétente sur les menaces cyber en lien avec l'espionnage et l'ingérence, la prolifération, le terrorisme, les subversions violentes et la protection économique et qui participe aux missions de cyberdéfense ;
- **Des prestataires privés locaux**, certains étant labellisés ou certifiés par CyberMalveillance.gouv.fr (label ExpertCyber) soit par l'ANSSI (voir le référentiel PRIS : Prestataires de Réponse aux Incidents de Sécurité) ;
- **Des associations régionales** composées soit d'antennes régionales des grandes associations nationales comme le CLUSIF (les CLUSIR) ou le CyberCercle, soit d'associations locales dédiées à la cybersécurité ;
- **Un réseau de Campus Cyber régionaux** doit également voir le jour à court terme, en lien avec le Campus national, et dont l'un des piliers d'activité (pilier « Opérations ») vise à développer la capacité des acteurs de l'écosystème à maîtriser le risque numérique et renforcer leur résilience en développant les collaborations entre les acteurs publics et privés, en mettant en relation les structures attaquées et les acteurs qualifiés et référencés de la remédiation.

LES BONNES PRATIQUES

Pour un indépendant ou une TPE, une cyberattaque est très rarement une attaque ciblée à l'exception de la fraude au président, la diffamation ou le harcèlement via Internet. Pour le cas le plus fréquent du rançongiciel, l'agent de menace a utilisé une campagne d'hameçonnage pour atteindre l'organisme sans pour autant la connaitre. Ce type d'attaque est souvent complétement automatisée.

La prévention des incidents et attaques informatiques relève souvent de réflexes simples, qui concourent à une protection globale de l'organisme. Le « Guide des bonnes pratiques de l'informatique » développé par l'ANSSI et la CGPME présente douze recommandations à destination des non-spécialistes, issues de l'analyse d'attaques réussies et de leurs causes.

Les bonnes pratiques essentielles, qui doivent être misent en œuvre et contrôlées en amont de l'incident, sont :

- un système de sauvegarde des fichiers de données fréquente sur un support électronique « externe » dédié et / ou via une solution dans le Cloud. Ces solutions ne doivent pas être connectées en permanence de votre système et ne pas réutiliser le même espace de sauvegarde ;
- des systèmes d'exploitation et logiciels supportés par leur éditeur et mis à jour régulièrement ;
- un antivirus supporté par son éditeur et mis à jour régulièrement ;
- les accès logiques doivent être protégés par des mots de passe personnalisés et changés régulièrement ;
- bien connaître et noter les numéros d'appel essentiels, en particulier ceux des CSIRT régionaux ;
- collecter et bien analyser les fiches réflexes et guides à disposition.

Les bonnes pratiques essentielles, qui doivent être misent en œuvre et contrôlées, sont :

- un système de sauvegarde des fichiers de données fréquente sur un support électronique « externe » dédié et / ou via une solution dans le Cloud. Ces solutions ne doivent pas être connectées en permanence de votre système et ne pas réutiliser le même espace de sauvegarde ;
- des systèmes d'exploitation et logiciels supportés par leur éditeur et mis à jour régulièrement ;
- un antivirus supporté par son éditeur et mis à jour régulièrement ;
- les accès logiques doivent être protégés par des mots de passe personnalisés et changés régulièrement.

ANNEXE D

Fiche de déclenchement d'un Plan de Continuité Informatique (PCI)

Au sein de la cellule de crise décisionnelle et une fois le point de situation initial effectué, plusieurs actions vont être menées. La liste ci-après doit permettre de décider le déclenchement ou non d'un PCI.

Prérequis :

- le PCI existe, il est conçu en cohérence avec les besoins de continuité d'activité de l'organisme ;
- le PCI est vérifié opérationnel grâce à des tests effectués régulièrement ;
- le PCI est connu des parties prenantes de la fonction informatique et des correspondants métiers.

Actions préliminaires au déclenchement :

- évaluer les opérations en cours et à venir (projets en cours,...) ;
- identifier les priorités des actions ;
- mobiliser des experts, si nécessaire, suivant la situation ;
- se rapprocher de l'assureur pour le remboursement d'éventuels dégâts.

Si l'analyse de la situation montre qu'elle nécessite de déclencher le PCI (impact sur la continuité informatique), le pilote de la cellule de crise doit décider du déclenchement du PCI directement ou après validation par la Direction.

Une fois le PCI déclenché :

- coordonner la mise en œuvre des solutions de continuité informatiques suivant le type d'événement ;
- se rapprocher de l'assureur pour le remboursement d'éventuels dégâts et la prise en charge des mesures de continuité informatique ;
- évaluer les impacts métiers et suivre les modes dégradés mis en œuvre en conséquence ;
- évaluer les besoins puis coordonner le déploiement des moyens informatiques.

Traiter le volet INFRASTRUCTURES, notamment :

- se coordonner et échanger pour valider les places disponibles sur d'autres sites pour les fonctions pouvant être relocalisées ou les activités transférées en télétravail ;
- mettre en conditions opérationnelles les éventuels sites de repli internes et/ou externes.

Traiter le volet OPERATIONNEL / METIER, notamment :

- suivre la mise en œuvre des modes dégradés (solutions de contournement) ;
- si cela n'est pas suffisant, ordonner aux métiers impactés d'activer les modes dégradés ;
- proposer de moduler des solutions pré-identifiées si nécessaire.

Les experts mobilisables sollicités doivent :

- gérer les phases de diagnostic des problèmes ;
- faire régulièrement des rapports sur la situation, sa gravité et son évolution ;
- contribuer à assurer la continuité informatique le cas échéant.

Traiter le volet RH :

- gérer la communication interne ;
- gérer les collaborateurs qui vont travailler en mode dégradé, sur un autre site, en travail à distance,...

Jusqu'à la résolution de la crise :

- se synchroniser, au travers des membres de la cellule, avec les relais sur le terrain et les équipes opérationnelles ;
- faire appliquer les choix effectués (directement ou après validation par la Direction si ceux-ci sont structurants) ;
- effectuer un point de situation régulier, notamment sur les personnels, les locaux, les matériels et le SI ;
- coordonner la poursuite des mesures de continuité informatique.

Bibliographie

NF ISO 31000 : 2018 – Management du risque.

NF ISO 22300 : 2021 – Sécurité et résilience — Vocabulaire.

NF ISO 22301 : 2019 – Sécurité et résilience – Systèmes de management de la continuité d'activité SMCA – Exigences.

ISO 22313 : 2020 – Sécurité et résilience – Systèmes de management de la continuité d'activité SMCA – Lignes directrices pour l'utilisation de l'ISO 22301.

ISO/TS 22317 : 2021 – Sécurité et résilience – Systèmes de management de la continuité d'activité SMCA – Lignes directrices pour le Bilan d'Impact sur l'activité (BIA).

ISO/TS 22331 : 2018 – Sécurité et résilience – Systèmes de management de la continuité d'activité SMCA - Lignes directrices relatives à la stratégie de continuité d'activité.

ISO/TS 22330 : 2018 – Sécurité et résilience – Systèmes de management de la continuité d'activité SMCA - Lignes directrices concernant les aspects humains de la continuité d'activité.

ISO/TS 22318 : 2021 – Sécurité et résilience – Systèmes de management de la continuité d'activité SMCA - Lignes directrices pour le management de la continuité de la chaîne d'approvisionnement.

ISO/IEC 27000 : 2020 – Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire

ISO/IEC 27001 :2013 – Management de la sécurité de l'information.

ISO/IEC 27002 : 2022 – Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information.

NF ISO/IEC 27005 : 2018 – Gestion des risques liés à la sécurité de l'information.

NF ISO/IEC 27031 : 2011 – Préparation des TIC pour la continuité d'activité.

ISO/IEC 27035-1 : 2016 – Gestion des incidents de sécurité de l'information - Partie 1 : Principes de la gestion des incidents.

ISO/IEC 27035-2 : 2016 - Gestion des incidents de sécurité de l'information - Partie 2 : Lignes directrices pour planifier et préparer une réponse aux incidents.

ISO/IEC 27041 : 2015 – Préconisations concernant la garantie d'aptitude à l'emploi et d'adéquation des méthodes d'investigation sur incident

ISO/IEC 27042 : 2015 – Lignes directrices pour l'analyse et l'interprétation des preuves numériques.

ISO/IEC 27043 : 2015 – Principes et processus d'investigation sur incident

ISO/IEC 27102 : 2019 – Lignes directrices pour la cyber-assurance

NF EN TS 17091 : 2018 – Gestion de crise – Recommandations pour le développement d'une capacité stratégique.

GUIDES SGDSN : 2013 – Guide pour réaliser un Plan de Continuité d'Activité.

GUIDE ANSSI : 2020 – Collection Gestion de crise - Organiser un exercice de gestion de crise cyber - co-production avec le CCA.

GUIDE ANSSI : 2021 – Collection Gestion de crise - Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique avec le CDSE.

GUIDE ANSSI : 2021 – Collection Gestion de crise - Anticiper et gérer sa communication de crise cyber avec Cap'Com.

FD Z 90-004 : 2022 – Fascicule de documentation publié par AFNOR - Continuité d'activité et résilience des organismes en cas d'indisponibilité prolongée du SI, particulièrement à la suite d'une cyberattaque - Guide sur l'état des bonnes pratiques et recommandations.

Lexique

Les termes en italique sont définis dans le lexique.

Activité prioritaire : Activité à laquelle une urgence est donnée afin d'éviter des impacts inacceptables pour l'activité de l'***organisme*** pendant une ***perturbation***. *[SOURCE : ISO 22300 :2021, 3.1.186]*

Agent de menace : Une personne ou un groupe de personnes, qui agit ou qui a la capacité d'agir, pouvant engendrer ou soutenir une menace.

Bilan d'impact sur l'activité (BIA) : Processus d'analyse de l'impact dans le temps d'une ***perturbation*** sur l'***organisme***. *[SOURCE : ISO 22300 :2021, 3.1.24]*

Cellule de crise – équipe de gestion de crise : Groupe d'individus qui a pour fonction d'orienter l'élaboration et l'exécution du plan de réponse et de continuité opérationnelle, de déclarer la présence d'une ***perturbation*** opérationnelle ou d'une situation de crise / d'urgence et de définir l'orientation à prendre lors du processus de rétablissement, aussi bien avant qu'après un ***incident*** perturbateur.

Note 1 à l'article : L'équipe de gestion de crise peut comprendre aussi bien des individus issus de l'***organisme*** que des intervenants d'urgence et des premiers intervenants, et des parties intéressées. Personne ou groupe de personnes dont la fonction consiste à gérer la crise pour le compte de l'organisme

Crise : Situation instable impliquant un changement brutal ou substantiel imminent qui requiert une attention une action urgentes visant à protéger la vie, les actifs, les biens ou l'environnement. *[SOURCE : NF EN ISO 22300:2021 – Terminologie - 3.1.60]*

Crise « d'origine cyber » : Déstabilisation immédiate et majeure du fonctionnement courant d'un organisme (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.). *[SOURCE : GUIDE ANSSI : 2021 - Crise d'origine cyber - Introduction]*

Cyberattaque « paralysante » : Crise d'origine cyber, caractérisé par un acte malveillant envers un ***système d'information*** qui va le rendre indisponible pour une durée prolongée (plusieurs jours, voire plusieurs semaines ou mois) et allant jusqu'à la paralysie de son activité. Une cyberattaque paralysante peut émaner de personnes isolées, d'un groupe de « pirates » ou de vastes organismes ayant divers objectifs dont géopolitiques.

Cyber-résilience : Aptitude d'un organisme (3.29) à absorber notamment les cyberattaques mais aussi à se préparer, à résister à des ***événements perturbateurs*** issus du cyberespace, et à s'adapter à des environnements numériques changeants. L'objectif est de reprendre, rétablir et restaurer les activités informatiques, tout en assurant une continuité d'activité métiers a minima en mode dégradé. Il s'agit de limiter les impacts, faciliter le retour vers un fonctionnement normal. L'organisme développe également sa capacité d'adaptabilité et d'innovation en tirant tous les enseignements pour améliorer sa ***résilience***.

Note : la définition de cyber-résilience se veut plus large afin d'intégrer de nouvelles dimensions et de satisfaire les nouveaux défis des environnements numériques, notamment la possibilité de poursuivre son activité sans techniques de communication numériques.

Cyber : Préfixe servant à former de très nombreux mots relatifs à l'utilisation du réseau Internet [SOURCE : Larousse]

Cybersécurité : État recherché pour un système d'information (3.30) lui permettant de résister à des événements issus du cyberespace susceptibles de com-

promettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. *[SOURCE : ANSSI : 2022 – Glossaire - https://www.ssi.gouv.fr/entreprise/glossaire/c/]*

Événement perturbateur : Occurrence ou changement, anticipé ou non, qui interrompt les activités, les opérations ou les fonctions planifiées. *[SOURCE : ISO 22300 :2021, 3.1.76]*

Forensique / analyse d'investigation : Méthode scientifique permettant d'authentifier des biens matériels en confirmant un élément authentifiant ou un attribut intrinsèque, via l'utilisation d'un appareillage spécialisé par un expert qualifié ayant des connaissances particulières. *[SOURCE : ISO 22300 :2021, 3.2.20]*

Gestion de crise : Processus de management holistique qui identifie les impacts potentiels qui représentent une menace pour un ***organisme***, et qui fournit un cadre pour construire la ***résilience***, avec une capacité de réponse efficace préservant les intérêts des parties intéressées essentielles de l'organisme, la réputation, la marque et les activités créatrices de valeur de l'organisme. *[SOURCE: ISO 22300:2021, 3.1.61]*

Note 1 à l'article : La gestion de crise implique également la gestion de la préparation, des mesures d'atténuation et de la continuité ou du rétablissement en cas d'***incident***, ainsi que la gestion du programme global par le biais de formations, de répétitions et de revues afin de veiller à ce que les plans relatifs à la préparation, à la réponse et à la continuité soient en vigueur et à jour.

Gestion des urgences : Approche globale de prévention des situations d'urgence et de gestion de celles qui se produisent. *[SOURCE : ISO 22300 :2021, 3.1.88]*

Note 1 à l'article : Généralement, la gestion des urgences utilise une approche management du risque pour la prévention, la préparation, la réponse et le rétablissement avant, pendant et après la survenue d'***événements*** et / ou de ***perturbations*** potentiellement déstabilisants.

Incident : Événement qui peut être, ou conduire à, une ***perturbation***, une perte, une situation d'urgence ou une crise [SOURCE : ISO 22300 :2021, 3.1.122]

Indicateurs de compromission : Élément technique issu de l'investigation numérique qui indique qu'un équipement ou un réseau a été compromis par un agent de menace.

Objectif de délai de rétablissement – en anglais Recovery time objective (RTO) : Durée après un incident pendant laquelle un produit et service ou une activité sont repris, ou des ressources sont rétablies. *[SOURCE : NF EN ISO 22300 :2021 – Terminologie – 3.1.203]*

Organisme : Personne ou groupe de personnes ayant un rôle avec les responsabilités, l'autorité et les relations lui permettant d'atteindre ses objectifs. *[SOURCE : NF EN ISO 22300:2021 – Terminologie - 3.1.165]*

Note 1 à l'article : Le concept d'organisme englobe sans s'y limiter, les travailleurs indépendants, les compagnies, les sociétés, les firmes, les entreprises, les administrations, les partenariats, les organisations caritatives ou les institutions, ou bien une partie ou une combinaison des entités précédentes, à responsabilité limitée ou ayant un autre statut, de droit public ou privé.

Note 2 à l'article : Il s'agit de l'un des termes communs et définitions de base de la structure-cadre des normes de systèmes de management de l'ISO.

PCA Cyber : Plan de Continuité d'Activité Métier en cas d'indisponibilité prolongée du ***SI*** à la suite d'une ***cyberattaque paralysante***. Ensemble des procédures et modes dégradés qui permettent à l'***organisme*** d'assurer a minima la continuité de ses ***activités prioritaires*** sans tout ou partie du SI initial à travers la planification de solutions métiers dégradées ou alternatives. *[SOURCE : AFNOR FD Z 90-004]*

PCA Global : Plan de Continuité d'Activité de l'***Organisme***. Il doit être vu comme le socle qui pourra être complété par des PCA opérationnels dédiés dit ***PCA Métiers et Supports***. *[SOURCE : AFNOR FD Z 90-004]*

Scénarios retenus du PCA Global :

- Indisponibilité des personnels ;
- Inaccessibilité et indisponibilité des sites ;
- Indisponibilité de l'outil de production ;
- Indisponibilité ou panne majeure du SI (cf. ***PCI***) ;
- Défaillance de prestataires / fournisseurs critiques.

PCA Métiers : Plan de Continuité d'Activité dédié à une direction, un service ou une entité liée aux processus « métiers » c'est à dire ceux qui contribuent directement à la réalisation des produits ou services conformément à la mission ou la finalité de l'organisme. *[SOURCE : AFNOR FD Z 90-004]*

PCA Supports : Plan de Continuité d'Activité dédié à une direction, un service ou une entité liée aux processus « supports » de l'organisme c.-à-d. ceux qui contribuent au bon déroulement des autres processus en leur apportant les ressources nécessaires (Humaines, financières, technique logistique, informatique). *[SOURCE : AFNOR FD Z 90-004]*

PCI - Plan de Continuité Informatique : Plan de Continuité d'Activité de la Direction des ***Systèmes d'Information*** ou du service informatique, constitué de l'ensemble des dispositifs / procédures visant à assurer, selon divers scénarios de crises (cf. ci-dessous), y compris face à des chocs extrêmes, le maintien des prestations essentielles de la DSI (Direction Système Information) dont la continuité du SI, le cas échéant de façon temporaire selon un mode dégradé, puis la reprise planifiée des activités [SOURCE: AFNOR FD Z 90-004]

Scénarios retenus :

- Indisponibilité des personnels de la DSI ;
- Inaccessibilité et indisponibilité des sites de la DSI ;
- Défaillance de prestataires stratégiques de la DSI (sociétés de service, sous-traitants, ...) ;
- Indisponibilité ou panne majeure du SI (voir ***PRA SI***).

Perturbation : ***Incident***, anticipé ou non, qui entraîne un écart négatif non planifié par rapport à la livraison ou la fourniture attendue de produits et services selon les objectifs d'un ***organisme***. *[SOURCE : ISO 22300 :2021, 3.1.75]*

Plan de continuité d'activité : Information documentée qui guide un ***organisme*** pour répondre à une ***perturbation*** et reprendre, rétablir et restaurer la livraison ou la fourniture de produits et services en cohérence avec ses objectifs de continuité d'activité. *[SOURCE : AFNOR FD Z 90-004]*

Point de récupération des données – en anglais en anglais : Recovery Point Objective (RPO) : Point à partir duquel les informations utilisées par une activité doivent être restaurées afin de permettre un fonctionnement en reprise. *[SOURCE : NF EN ISO 22300 :2021 – Terminologie – 3.1.202]*

Note 1 à l'article : Il peut également être désigné en tant que « perte maximale de données ».

PRA SI - Plan de Reprise d'Activité du Système d'Information : Plan de Continuité d'Activité Support qui couvre le secours des moyens informatiques, ensemble des procédures et dispositifs pour la reprise des capacités du ***SI*** lorsqu'une ***perturbation*** se produit. [SOURCE : AFNOR FD Z 90-004]

Scénarios retenus du PRA SI :

- Destruction ou arrêt des salles informatiques ;
- Interruption du système d'information et des applications utilisées par les directions ;
- Interruption de tous les services téléphoniques ;
- Défaillance de fournisseurs stratégiques (constructeurs, équipementiers, éditeurs, opérateurs, hébergeurs...).

Remédiation : Restaurer les systèmes dans leur état initial en éjectant l'attaquant du système et améliorer la sécurité pour éviter une attaque similaire par l'application de mesures d'assainissement. *[SOURCE : GUIDE ANSSI : 2020 - Collection Gestion de crise - Organiser un exercice de gestion de crise cyber – page 15]*

Réponse aux incidents : Actions menées pour interrompre les causes d'un danger imminent et / ou pour atténuer les conséquences d'événements potentiellement déstabilisants ou de ***perturbations*** et se rétablir à une situation normale [SOURCE : ISO 22300 :2021, 3.1.126]

Note 1 à l'article : La réponse aux incidents fait partie intégrante du processus de ***gestion des urgences***.

Résilience : Caractéristique mécanique définissant la résistance aux chocs d'un matériau.

Psychologie : Aptitude d'un individu à se construire et à vivre de manière satisfaisante en dépit de circonstances traumatiques.

Écologie : Capacité d'un écosystème, d'un biotope ou d'un groupe d'individus (population, espèce) à se rétablir après une perturbation extérieure (incendie, tempête, défrichement, etc.).

[SOURCE: Dictionnaire Larousse]

Résilience informatique : Capacité d'un système à continuer à fonctionner, même en cas de panne. *[SOURCE: Dictionnaire Larousse]*

Note : La résilience informatique ou résilience des systèmes d'information consiste dans la capacité d'une entreprise ou d'une organisation à assurer la continuité de son système d'information.

Le terme de résilience numérique peut aussi être employé dans une approche globale du numérique et s'entendre à l'échelle de l'organisme mais également de son écosystème dans une logique d'entreprise étendue. Il s'agit d'assurer la résilience du numérique face aux menaces informatiques à travers la gestion de crise, la communication de crise, la gestion des tiers, la cyberdéfense et la reconstruction des systèmes d'information.

Résilience organisationnelle : Aptitude d'un ***organisme*** à absorber et s'adapter dans un environnement changeant. *[SOURCE: ISO 22300:2021, 3.1.206]*

Retour d'expérience (RETEX) : Temps collectif (tour de table) et / ou individuel (entretien) au cours duquel l'ensemble des participants s'exprime sur son expérience durant l'exercice ou durant la crise. *[SOURCE : GUIDE ANSSI : 2020 - Organiser un exercice de gestion de crise cyber - Glossaire]*

Système d'Information : Ensemble des ressources (matérielles ou logicielles) et dispositifs d'une organisation permettant de collecter, de stocker et d'échanger les informations nécessaires à son fonctionnement. *[SOURCE : GUIDE ANSSI : 2021 - Crise d'origine cyber - Glossaire]*

Système de gestion des incidents : Système définissant les rôles et responsabilités du personnel et les procédures de fonctionnement à utiliser dans le cadre de la gestion des incidents. *[SOURCE : ISO 22300 :2021, 3.1.124]*

Système de Management de la Continuité d'Activité (SMCA) : Partie du système de management global qui établit, met en œuvre, exploite, surveille, passe en revue, maintient et améliore la continuité d'activité.

Note 1 à l'article : Le système de management inclut la structure organisationnelle, les politiques, les activités de planification, les responsabilités, les procédures, les processus et les ressources. *[SOURCE : ISO 22300 :2021, 3.1.21]*

Système de Management de la Cyber-Résilience (SMCR) : Système de management intégré reposant sur les ***systèmes de management de la continuité d'activité*** et de la ***sécurité de l'information***. Il s'appuie sur les normes ISO 22301 et ISO 27001.

Système de Management de la Sécurité de l'Information (SMSI) : Partie du système de management global qui établit, met en œuvre, exploite, surveille, passe en revue, maintient et améliore la sécurité de l'information.

Système de Management Intégré (SMI) : Ensemble des systèmes de mangement de la qualité, de la santé et sécurité au travail et de l'environnement. Il repose sur les normes ISO 9001, 14001 et OHSAS 18001. Il n'est pas exclu qu'il intègre d'autres systèmes de management (SMSI, SMCA).

Communication groupe AFNOR – S2211044 – 10/2022 – Conception graphique : GAYA.

POUR EN SAVOIR PLUS

norminfo@afnor.org