Cigref
RÉUSSIR
LE NUMÉRIQUE

Réagir à une cyberattaque massive

Gérer les conséquences d'une crise d'origine cyber

Février 2023

Cigref

Réagir à une cyberattaque massive

Gérer les conséquences d'une crise d'origine cyber

Février 2023

ÉDITO

Le risque cyber est aujourd'hui considéré comme le risque le plus élevé par la plupart des organisations et entreprises. Le Cigref est fortement mobilisé sur ce sujet et a élaboré une doctrine qui repose sur quatre piliers :

- Le renforcement des capacités de protection des organisations ;
- L'augmentation des moyens de police et justice pour lutter contre la cybercriminalité ;
- L'intensification de la cyberdéfense étatique pour appréhender les criminels jusqu'en dehors du territoire national ;
- L'imposition de normes et d'exigences de sécurité aux fournisseurs de produits numériques.

Le travail d'intelligence collective présenté dans ce rapport a donc pour objectif de contribuer au premier de ces piliers en mettant à disposition des lecteurs des éléments très concrets pour les aider à réagir en situation de crise cyber en effet, les entreprises sont en général dotées de procédures de gestion de crise au regard de leurs activités spécifiques mais une crise cyber n'est pas une crise comme les autres, par sa fulgurance, son impact et sa difficulté d'appréhension et de diagnostic.

Les retours d'expérience de cyberattaques avérées sont toujours très utiles mais peuvent être délicats à partager. Cependant, chacun a conscience qu'une organisation ne peut pas, seule, atteindre le niveau de maturité nécessaire pour faire face à cette adversité. En revanche, la littérature abonde d'ouvrages de fond, de rapports et de référentiels pertinents et de qualité. Ces éléments sont particulièrement utiles pour se préparer. Une bibliographie est disponible en annexe de ce rapport.

Cependant, être prêt n'est pas suffisant, encore faut-il avoir les bons réflexes quand une crise de grande ampleur survient. Le niveau de stress induit, subi par les équipes informatiques, les métiers et la direction générale peut altérer la prise de décisions éclairées et perturber le lancement d'actions décisives et indispensables dans les premiers moments. Le remède peut parfois être pire que le mal. L'objectif de cette étude est de fournir les outils et les méthodes nécessaires pour réagir efficacement à une attaque de grande envergure au fur et à mesure des grandes phases de la crise qui s'installe.

Les thématiques explorées ne sont pas seulement techniques, elles sont également organisationnelles, juridiques, assurantielles et traitent de la communication interne et externe. Les éléments présentés sont issus de l'expérience des membres du Cigref participant aux travaux et représentant des secteurs très divers. De plus, des spécialistes, experts dans leurs domaines ont également contribué aux travaux du groupe de travail.

Ce rapport présente des retours d'expérience, des recommandations, propose un chronogramme, des checklists et plans d'actions ainsi que des indicateurs à destination des DSI, RSSI, Directions des risques et de la communication et plus généralement de tous les membres des cellules de crise des entreprises ou administrations. Le caractère très spécifique du sujet traité nous a amené à décider de conserver l'anonymat des contributions. Que soient remerciés tous les participants qui ont accepté de partager leurs expériences et difficultés en transparence et avec beaucoup d'humilité afin que tous puissent en profiter et renforcer la résilience de leurs organisations.

Le pilote du groupe de travail

SYNTHÈSE

Ce rapport traite de la gestion d'une crise cyber massive, engendrant des conséquences importantes sur l'activité de l'organisation et propose un guide pratique des réponses à apporter face à une cyberattaque. Ces conséquences peuvent être de différentes natures, opérationnelles, financières ou encore réputationnelles.

La gestion de crise cyber est constituée de différentes étapes qu'il convient de bien identifier pour ne pas s'enliser dans la crise. Dans un premier temps, l'organisation doit gérer au mieux les impacts de l'attaque pour éviter une propagation en limitant son périmètre. Puis, elle répare son système d'information avant de le stabiliser. En parallèle, des investigations sont lancées afin d'identifier les raisons de l'attaque et de s'assurer que l'environnement informatique est de nouveau sain. Enfin, il est important de prendre en compte dès le début de la cyberattaque le processus juridique, qui durera bien longtemps après la fin de la crise.

La gestion de crise est menée par deux cellules de crise : la cellule opérationnelle, qui dans le cas d'une crise cyber est essentiellement composée des membres de la DSI, et la cellule décisionnelle qui assure la continuité d'activité de l'organisation. Il convient d'identifier toutes les parties prenantes nécessaires pour gérer les aspects techniques et stratégiques de la crise. Le moment de la mobilisation de la cellule de crise est également clé pour réagir rapidement, ce moment est généralement défini dans les dispositions du PCA (plan de continuité d'activité) et dépend grandement des conséquences sur les directions métiers (soit toutes les directions utilisatrices du SI).

Au-delà des aspects techniques (diagnostic de l'attaque et réparation du SI), la communication est importante pour éviter une crise dans la crise. Il faut pouvoir communiquer en interne en ayant prévu au préalable un système de communication alternatif au SI de l'organisation. Ensuite, il faut communiquer en prenant en compte toutes les parties prenantes au sein de l'organisation, dans l'écosystème et éventuellement vers les médias.

Par ailleurs, une crise cyber entraîne souvent un processus juridique pour lequel la DSI doit se coordonner avec la direction juridique. En cas de fuite de données à caractère personnel, il faut immédiatement notifier la faille à la CNIL. De même, il est important de rapidement prévenir son assurance cyber. Puis, il faut également conserver les preuves de l'attaque afin d'apporter des éléments significatifs à la constitution de sa plainte.

L'appel à des prestataires externes est souvent nécessaire pour renforcer ses équipes et bénéficier d'expertises manquantes en interne. L'ANSSI peut être un allié sur plusieurs fronts lors de la gestion d'une crise cyber.

Plus la crise dure dans le temps, plus les équipes de la DSI seront sur-mobilisées. Il convient de faciliter la vie des équipes en gérant au mieux tous les aspects logistiques sans oublier d'accorder des temps de repos, même aux collaborateurs les plus indispensables et motivés.

Lorsque la crise se termine, le processus juridique doit être suivi avec attention car il peut encore durer plusieurs mois. Enfin, c'est souvent le moment pour la DSI d'améliorer son niveau de sécurité.

REMERCIEMENTS

Nos remerciements vont au pilote du groupe de travail, ainsi qu'à toutes les personnes qui ont participé et contribué à ce groupe de travail. Elles sont au nombre de 54, ayant des fonctions relatives à la sécurité du SI, dans des organisations appartenant à des secteurs très divers :

- Différents domaines de l'industrie (aéronautique, pharmaceutique, automobile…) ;
- Secteur de la banque/assurance ;
- Secteur de l'agroalimentaire ;
- Secteur des bâtiments et travaux publics ;
- Secteur de l'énergie ;
- Secteur des services.

Nous remercions également vivement tous les intervenants experts dans leur domaine qui ont apporté beaucoup de matière à ce travail (ordre alphabétique) :

- Damien Arcuset, Chef du bureau Coordination des analyses, ANSSI
- Hélène Chauveau, *Head of Public Affairs*, AXA
- Christophe Fleury, Responsable d'opérations de cyberdéfense, ANSSI
- Georges Laederich, Consultant senior en gestion et communication de crise, Cabinet Arjuna
- Thibault Richard, Consultant senior en gestion et communication de crise, Cabinet Arjuna
- Maître Corinne Thiérache, Avocat au Barreau de Paris, Associée IP/IT/Privacy du Cabinet Alerion Avocat
- Stéphane Vauterin, Underwriting Manager Professional & Specialty Lines, AXA XL
- Cécile Wendling, Group Head of Security Strategy and Awareness, AXA

Ce document a été construit et rédigé par Aurélie Chotard, Chargée de mission au Cigref.

TABLE DES MATIÈRES

TABLE DES ILLUSTRATIONS

1 INTRODUCTION : LES ENTREPRISES CONFRONTÉES À DES CYBERATTAQUES DE GRANDE AMPLEUR

Après une définition de ce que nous entendons par « cyberattaque de grande ampleur », nous évoquerons brièvement le contexte cyber auquel doivent faire face les entreprises. Cette introduction a pour vocation d'exposer la logique organisationnelle de ce rapport, construit de manière temporelle et pensé comme un véritable guide pratique au service des organisations qui souhaitent se préparer à affronter une crise d'origine cyber.

En plus des retours d'expérience des participants du groupe de travail et de l'intervention d'experts, nous avons parfois innové dans notre méthodologie de travail en nous glissant dans la peau d'une entreprise désirant se préparer à la gestion de crise. Pour ce faire, nous nous sommes notamment inspirés du rapport de l'ANSSI consacré à l'organisation d'un exercice de gestion de crise. Nous avons ainsi réalisé un chronogramme (en annexe) pour identifier les parties prenantes et les actions à réaliser en fonction d'événements successifs, la fiche pratique de l'ANSSI a été d'une grande utilité pour la réalisation de cet atelier pratique.

L'ambition de ce rapport est de se concentrer sur les cyberattaques qui engendrent des conséquences importantes sur l'activité de l'entreprise, voire sur la population dans son ensemble. Nous nous sommes attardés sur le moment qui va de l'avènement de la crise jusqu'à sa résolution, c'est-à-dire la reprise globale de l'activité de l'entreprise. Le sujet traité concerne donc essentiellement des éléments de gestion de crise, et non de prévention ou d'anticipation, bien que nous soyons conscients que l'anticipation est la clé d'une gestion efficace. Cependant, chaque crise est différente et suivre un protocole prédéfini ne suffit pas toujours. L'adaptation est alors nécessaire pour l'appréhender. Ce rapport propose des recommandations et des conseils pratiques pour gérer une crise cyber et faire face aux imprévus.

1.1 QU'EST-CE QU'UNE CYBERATTAQUE DE GRANDE AMPLEUR ?

1.1.1 DÉFINIR UNE CYBERATTAQUE

Selon l'ANSSI, une cyberattaque est une action malveillante destinée à porter atteinte à l'intégrité d'un système d'information. Une cyberattaque représente la concrétisation d'une menace, et nécessite l'exploitation d'une faiblesse dans le SI. Chaque jour, les DSI des grandes organisations sont victimes d'attaques informatiques, mais peu de celles-ci parviennent à leurs fins, si bien que l'on ne parle véritablement de cyberattaque, et non d'incident informatique, que lorsque les dommages créés par les cyberattaquants sur le système d'information ont des conséquences sur l'activité de l'organisation. Il existe aujourd'hui différentes terminologies pour désigner les attaques informatiques qui interviennent à différents niveaux ; voici un glossaire des exemples les plus connus et que nous allons utiliser dans ce rapport :

- Le *ransomware* (ou attaque par rançongiciel) est aujourd'hui l'attaque qui a les conséquences les plus importantes. Elle consiste à infiltrer les serveurs informatiques d'une organisation pour exfiltrer des données puis à les chiffrer (l'exfiltration n'est pas systématique mais est de plus en plus répandue pour augmenter les chances d'obtenir une rançon). Les données de

l'organisation deviennent inaccessibles et les cybercriminels demandent une rançon en échange d'une clé de déchiffrement et de la non divulgation des données.

- Le *malware* (ou virus) désigne tout programme informatique développé pour nuire à l'organisation visée, en altérant un composant technique particulier (*software* ou *hardware*).
- Le *spyware* (ou logiciel espion) est un logiciel dont l'objectif est de collecter des informations pour les transmettre à des tiers. Il répond à un objectif d'espionnage envers une organisation ciblée, soit pour découvrir de nouvelles vulnérabilités dans le SI en vue de commettre une autre attaque par la suite, soit dans une logique de renseignement étatique ou économique. Comme ce logiciel ne modifie pas le fonctionnement du SI, il peut s'écouler longtemps avant qu'il ne soit découvert.
- L'attaque par déni de service distribué (ou DDoS) consiste à surcharger la capacité d'un système numérique pour en altérer la capacité de service, voire à le rendre inutilisable. Il existe aujourd'hui de nombreux moyens de se prémunir contre ce type d'attaque, mais elle reste une attaque répandue affectant davantage les structures les plus modestes.
- Le *phishing* (ou attaque par hameçonnage) consiste pour un cybercriminel à usurper une identité dans l'objectif d'obtenir des informations et/ou d'infiltrer un système informatique. Il s'agit souvent d'une première étape pour ensuite commettre une attaque plus importante.

Il existe encore de nombreuses typologies d'attaques. Le glossaire de l'ANSSI permet d'en avoir les définitions exactes.

1.1.2 LES DIFFÉRENTES CONSÉQUENCES D'UNE CYBERATTAQUE

La notion de cyberattaque « de grande ampleur » ne dépend pas de la typologie de l'attaque mais des conséquences que celle-ci peut avoir sur l'organisme attaqué et sur son écosystème proche ou éloigné. Plus les conséquences sont nombreuses et répandues, plus la cyberattaque rentre dans ce cadre. L'efficacité de l'attaque et la typologie n'ont que peu d'incidences sur ses potentiels impacts. Ces impacts dépendent plutôt de la façon dont l'entreprise aura sécurisé son système d'information en amont et prévu des issues de secours pour faire face aux différentes attaques possibles. Les TPE, les PME et certaines administrations demeurent les structures les plus affectées par des cyberattaques car les moyens cyber mis en place sont souvent insuffisants pour faire face à une cybercriminalité de plus en plus organisée et performante.

Les conséquences d'une cyberattaque peuvent être dramatiques quand elle affecte un Opérateur d'Importance Vitale (OIV)[1] ou un Opérateur de Services Essentiels (OSE)[2], comme les hôpitaux, les transports ou les opérateurs énergétiques. Ces organisations sont alors dans l'obligation d'être aptes à reprendre rapidement leur activité sans en faire peser les répercussions sur la société civile. Le ciblage de ces infrastructures par les cybercriminels est une source de préoccupation majeure. Lors de la crise sanitaire, des hôpitaux ont été largement visés, de même que des communes. Les attaques étaient peu sophistiquées mais les conséquences ont été importantes sur la capacité des hôpitaux à soigner leurs patients et sur celles des communes à répondre aux besoins de leurs administrés.

L'ANSSI, dans son rapport d'activité 2021, mentionnait que 75% de ses interventions étaient liées à des attaques d'espionnage. Mais les attaques qui ont pour finalité l'espionnage n'ont pas ou peu de conséquences directes sur l'activité de l'entreprise et sur son écosystème. Même si elles doivent être

[1] La sécurité des activités d'importance vitale, Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), 18 mars 2016.

[2] Liste des Opérateurs de services essentiels tel que défini dans la Directive NIS : Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

prises au sérieux par les organisations, nous ne les avons pas prises en compte dans le rapport, car les pratiques de gestion de crise qui en découlent ont des spécificités trop importantes. Ce rapport traite donc principalement des attaques de type ransomware.

Les conséquences qui résultent d'une cyberattaque sont de plusieurs natures et peuvent atteindre des proportions critiques pour l'organisation affectée :

1. **Les répercussions sur l'activité de l'organisation** : Une des premières conséquences identifiées concerne l'arrêt partiel ou total d'activité de l'organisme victime. Par exemple, en 2020, suite à une cyberattaque, la compagnie maritime CMA CGM, a dû cesser partiellement son activité pendant 2 semaines en raison des dysfonctionnements importants de son SI.
2. **Les conséquences financières** : Un arrêt d'activité prolongé a des conséquences importantes sur le chiffre d'affaires d'une entreprise. Ainsi, en 2017, le Groupe Saint-Gobain annonçait une perte de 200 millions d'euros à la suite d'une cyberattaque ayant entraîné un arrêt de son activité, complet pendant 4 jours, et partiel pendant 10 jours avant de revenir à la normale. Pour les mêmes raisons, Eurofins en 2019 annonçait des pertes de 70 millions d'euros et Sopra Steria de 50 millions en 2020.
3. **Des conséquences réputationnelles** : Un organisme victime d'une cyberattaque inspire moins confiance à ses clients professionnels ou au grand public, surtout si cette attaque a entraîné une fuite de données importante. Ainsi, l'attaque vécue par l'APHP en 2021 a connu une importante médiatisation critique du fait d'une fuite importante de données concernant les résultats des tests covid de leurs patients. Plus récemment, La Poste Mobile, victime d'un ransomware, a laissé son site hors-ligne pendant une semaine, affectant fortement le service offert à ses clients.

1.1.3 LA CYBERATTAQUE, UNE CRISE SPÉCIFIQUE

Une cyberattaque a des conséquences qui nécessitent la **mise en place d'un dispositif de gestion de crise** par l'organisation qui en est victime. Ce dispositif, même s'il reprend des éléments globaux des principes de gestion de crise, doit être adapté à une crise d'origine numérique pouvant avoir des conséquences multiples et transverses.

En s'appuyant sur le rapport de l'ANSSI, *Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique*, il est possible de dégager les éléments qui font de la crise cyber, une crise spécifique :

- **Une crise en latence** : La crise cyber peut commencer bien avant sa détection. Avant la survenue fulgurante de la crise, l'organisation qui en est victime se trouve déjà en situation de crise, mais elle l'ignore. Cette latence se retrouve également pendant la gestion de la crise, car l'organisation ignore si le cyberattaquant se trouve toujours ou non dans son système d'information. Cette possible persistance du *hacker* dans le cadre d'une crise d'origine cyber peut être particulièrement mal vécue par les gestionnaires de la crise.
- **Une crise multiforme** : Une cyberattaque peut survenir sous différentes formes et à différents endroits de manière coordonnée. Selon la typologie d'infrastructure qu'elle cible, cette action multiforme fait grandir au fur et à mesure l'angoisse de l'organisme visé, voire de la population (si l'organisme a une activité vitale). Par exemple, en Ukraine en 2015, une attaque menée simultanément sur plusieurs opérateurs énergétiques a entraîné une panne électrique de grande ampleur dans le pays. Après s'être introduit dans les systèmes et en avoir pris le contrôle, le *malware* utilisé a rendu les équipements inopérants. En parallèle, une attaque de type DDoS était menée sur les centres d'appel des opérateurs. Cette action multiforme et

simultanée a non seulement empêché les opérateurs de réagir rapidement mais a également augmenté l'angoisse de la population[3]. Ce caractère multiforme oblige l'organisation ciblée à prendre en compte l'ensemble de son écosystème pour évaluer l'importance et les impacts de la crise.

- **Fulgurance de la crise** : Une organisation ciblée par une cyberattaque est immédiatement confrontée à son étendue et à ses effets. Elle est alors dans l'incapacité de mesurer l'impact de la crise et la durée dans laquelle elle s'inscrit. Une crise cyber n'est pas un simple incident informatique auquel il faut remédier. Lors d'une crise cyber, les attaques se succèdent dans le temps.

1.2 UN CONTEXTE PROPICE AUX CYBERATTAQUANTS

L'adoption de nouveaux outils numériques et de nouvelles pratiques entraîne une augmentation des vulnérabilités dans les systèmes d'information. Ainsi, le nombre des cyberattaques a fortement augmenté ces dernières années, impactant l'activité des entreprises et administrations. Ces organisations s'inquiètent de voir les compétences des cybercriminels augmenter plus vite que leurs capacités à se défendre. Alors que les cybercriminels sont de mieux en mieux organisés grâce à une meilleure structuration du *dark web*, certaines entreprises (notamment les PME/TPE) et administrations sont encore mal préparées pour faire face à cette menace grandissante.

Pour répondre à l'augmentation des cyberattaques, l'Union Européenne a proposé une révision de la directive NIS dans l'objectif d'assurer un niveau commun élevé de cybersécurité dans l'Union (la "directive NIS 2"). L'Europe propose également des outils pour aider les États membres à améliorer leur sécurité numérique.

1.2.1 UNE AUGMENTATION EXPONENTIELLE DE LA CYBERMENACE

Selon *Le panorama de la menace informatique* publié par l'ANSSI, 1082 intrusions avérées ont été détectées dans les systèmes d'information en 2021, contre 786 en 2020. Il s'agit donc d'une hausse de 37% en un an.

Cette augmentation exponentielle de la cybermenace est liée à trois phénomènes principaux. Tout d'abord, les groupes de cybercriminels se professionnalisent et se spécialisent dans certaines techniques d'attaques, tel que l'illustre la vente de *Ransomware as a Service (RaaS)*, un abonnement qui comprend tout ce dont une personne malveillante a besoin pour lancer une attaque de ransomware. Un abonnement RaaS typique coûte environ 50 $ et comprend le code du rançongiciel et la clé de déchiffrement. Cette activité commerciale illégale permet de simplifier le développement et l'exécution d'un ransomware, elle s'adresse également aux cybercriminels les moins expérimentés. Par ailleurs, cette vente de code malveillant rend plus difficile l'identification des commanditaires d'une cyberattaque. Le code d'un groupe malveillant peut être utilisé par une multitude de pirates informatiques de différentes nationalités.

D'autre part, cette organisation de la cybercriminalité a été permise par la structuration accrue du *dark web.* Selon une entreprise spécialisée dans la blockchain, les marchés du *dark web* ont généré un

[3] Pour en savoir plus sur cette cyberattaque - Les détails de la cyberattaque qui a mis des centrales ukrainiennes hors service, L'Usine Digitale, 04/03/2016

nouveau record de revenus en 2021, rapportant un total de 2, 1 milliards de dollars en crypto-monnaies. Une part de cette somme, d'environ 300 millions de dollars, a été générée par les boutiques de fraudes, servant d'intermédiaires pour la vente de logins, de cartes de crédit et de kits d'exploitation volés, entre autres.

Enfin, cette augmentation des attaques est également favorisée par un accroissement considérable des vulnérabilités dans les systèmes d'information. La société américaine de cybersécurité Mandiant a ainsi identifié 80 failles « Zero Day » exploitées en 2021, soit plus du double du précédent record qui datait de 2019. Les cyberattaquants cherchent les points d'entrée les plus accessibles. Par conséquent, ils visent la chaîne d'approvisionnement des composants informatiques. Cette méthode permet de propager rapidement l'attaque en ciblant un éditeur de logiciels ou une société de services numériques, et comporte le risque de compromissions en cascade. L'exemple le plus connu à ce jour est une cyberattaque qui a permis d'infiltrer des grandes entreprises privées ainsi que des institutions gouvernementales, notamment aux États-Unis, via le logiciel Orion de la compagnie SolarWinds. Cette attaque a été dévoilée en décembre 2020 par l'agence privée de cybersécurité, FireEye.

1.2.2 UTILISATION DU CYBERESPACE COMME MOYEN DE PRESSION POLITIQUE

La porosité grandissante entre groupes de cybercriminels et acteurs étatiques transforme le cyberespace en un espace de conflits entre États où s'expriment des moyens de pression politique. Quelques exemples récents permettent d'illustrer cet aspect :

- **Augmentation des affaires d'espionnage** : L'augmentation du nombre d'entreprises privées spécialisées dans l'espionnage en ligne est le signe que la pratique s'industrialise, au même titre que les attaques de type ransomware. La société israélienne NSO, à l'origine de l'affaire Pégasus qui a éclaté à l'été 2021, a vendu pendant plusieurs années un logiciel de piratage de smartphones à plusieurs États dont le Maroc, le Mexique ou encore l'Arabie Saoudite, ce qui a permis à ces États d'espionner des dirigeants politiques, des opposants politiques et des journalistes. Ce type d'outils vendus par des sociétés privées sont ensuite utilisés par des groupes de cybercriminels.
- **Militarisation du cyberespace dans le cadre du conflit en Ukraine** : Depuis le début du conflit, la Russie est à l'origine de campagnes de désinformation dans tous les pays qui soutiennent l'Ukraine, et elle lance des cyberattaques vers ses pays limitrophes, notamment les pays baltes, qui bloquent ses opérations. La Lituanie par exemple, est une cible importante, car en appliquant les sanctions de l'UE, le pays bloque l'accès de la Russie à Kaliningrad, empêchant ainsi l'acheminement de certaines marchandises russes. Parallèlement, la Russie subit une vague de cyberattaques en « représailles », principalement en provenance de l'Amérique du Nord et de l'Europe, lancées non seulement par des groupes « d'hacktivistes » qui soutiennent l'Ukraine mais aussi par des acteurs étatiques.

Dans ce contexte, les entreprises sont des cibles de choix que ce soit dans une logique de renseignement économique ou pour déstabiliser l'activité des gouvernements et atteindre la population d'un pays.

1.2.3 UNE PÉNURIE DES TALENTS QUI PÈSE SUR LES ENTREPRISES

Les entreprises connaissent actuellement une situation de pénurie des talents dans le secteur du numérique, et plus encore dans celui de la cybersécurité. Ainsi, 45% des entreprises françaises indiquent qu'elles peinent à recruter dans cette discipline où environ 5000 postes sont actuellement à pourvoir dans l'Hexagone.

Plusieurs raisons peuvent être invoquées selon PwC pour expliquer cette pénurie de talents :

- L'image des métiers de la cybersécurité est en décalage avec la réalité et n'attire que peu de personnes.
- Les cursus de formation dans cette filière sont souvent longs et complexes, et ne recrutent qu'une minorité de candidats.
- La faible mixité dans ces métiers diminue également de moitié les possibilités de recrutement.
- Malgré des salaires attractifs, ces métiers sont peu reconnus et valorisés au sein de la société.

De plus, au-delà du manque d'experts et de spécialistes en cybersécurité dans les entreprises, les principes de base de la cybersécurité ne sont pas connus par l'ensemble des employés. Cette connaissance est pourtant nécessaire pour se prémunir des cyberattaques.

1.3 LES DIFFÉRENTES ÉTAPES DE LA GESTION DE CRISE CYBER

La gestion d'une crise résultant d'une cyberattaque comporte plusieurs étapes intégrant les différents aspects de la gestion de crise classique (remédiation technique, communication, gestion des équipes, mise en place d'un processus juridique…). Nous avons identifié trois temporalités parallèles à prendre en compte pour couvrir l'ensemble du spectre de la gestion de crise d'origine cyber :

1. D'une part, la **gestion des conséquences de la crise** suit une chronologie découpée en quatre grandes phases :
   - Les mesures d'urgence, à prendre dans les premiers temps de la crise (1-3 jours) ;
   - Les mesures de remédiation, pour remettre en route l'activité et revenir à un état d'avant crise. Cette étape consiste à proposer un service dégradé puis à prendre le temps de la réparation. (1-3 semaines) ;
   - La stabilisation de la situation, pour éviter une surenchère des crises et améliorer la sécurité de son SI (plusieurs mois) ;
   - Le retour d'expérience, pour tirer profit de la crise en améliorant son dispositif de gestion de crise par exemple, et éviter qu'une crise similaire se reproduise (plusieurs mois).

2. En parallèle, **les investigations** sont lancées. Dans un premier temps, ces investigations servent à s'assurer que l'environnement informatique de l'organisation affectée est sain pour pouvoir entreprendre sans risque l'étape de remédiation. Ne pas entreprendre ce premier temps d'investigation expose l'organisation à des actions secondaires d'agression de la part des cybercriminels. Il faut s'assurer que l'attaquant n'est plus présent dans le SI ou n'a plus moyen d'accéder au SI pour éviter le sur-accident. Puis, les investigations continuent pour connaître l'origine de la cyberattaque. Ce second temps se déroule à part de la gestion de crise car la connaissance de l'origine d'une crise cyber n'est pas indispensable à sa remédiation. Il est cependant nécessaire et important de mener ces investigations pour combler les potentielles vulnérabilités du SI. Les investigations peuvent prendre plusieurs mois.

3. Enfin, ces investigations permettent également de collecter les preuves nécessaires au **processus juridique**. En parallèle de la gestion de crise, l'organisation doit en effet s'acquitter de ses obligations légales. Ce temps judiciaire est bien plus long que celui de la crise et peut durer des mois, voire des années.

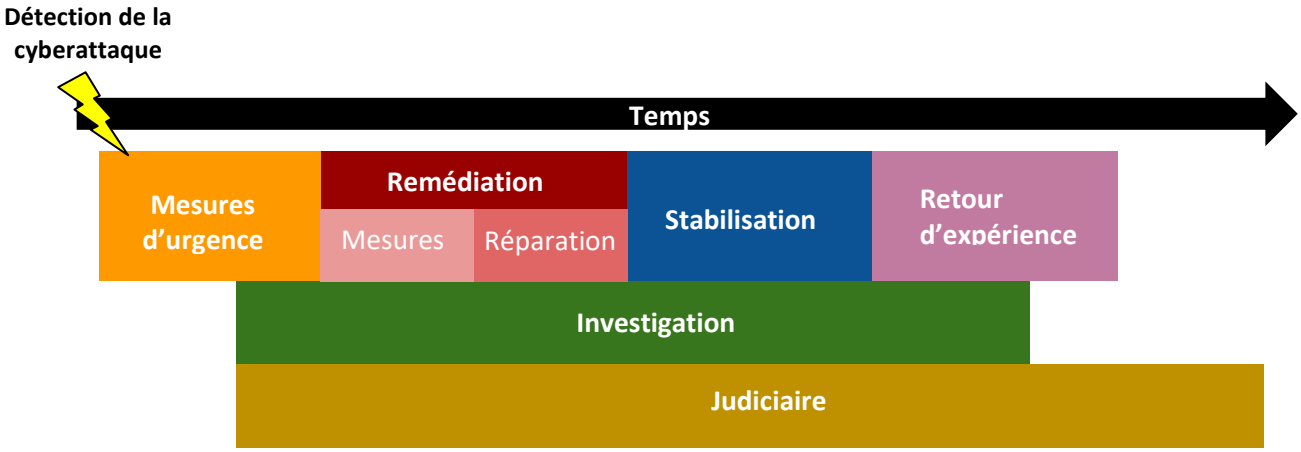

Figure 1 : Étapes de la gestion de crise cyber

Cette chronologie et ce découpage des différents temps de la gestion de crise guide la structure de ce rapport. L'objectif de ces différentes parties est d'apporter des outils opérationnels et des recommandations pour appréhender chacune de ces phases de la manière la plus efficace.

2 FAIRE FACE À LA CRISE : PRENDRE LES PREMIÈRES MESURES DÉCISIVES

Lorsque survient une crise cyber, les premières mesures sont décisives pour le déroulement du reste de la gestion de crise. Dans ces premiers moments, il faut répondre à plusieurs questions :

- Qui fait partie de la cellule de crise ? À quel moment faut-il la mobiliser ?
- Quelles actions entreprendre au niveau de la DSI pour stopper la propagation de l'attaque, s'il n'est pas déjà trop tard ?
- Quelles relations la DSI doit-elle entretenir avec les autres directions de l'entreprise pendant la crise ?
- L'organisation victime de l'attaque dispose-t-elle de toutes les ressources nécessaires en interne pour faire face à la crise ?

Les réponses à ces questions ont normalement été résolues en amont de la crise dans la cadre d'un plan de continuité d'activité et de gestion des crises. Cependant, chaque crise est unique et la capacité d'une organisation à s'adapter aux imprévus est un facteur clé pour savoir les appréhender.

2.1 L'ORGANISATION DE LA CELLULE DE CRISE

Pour gérer une crise cyber, une variété d'équipes dont les actions et les décisions sont à la fois techniques (sécurité du SI, services informatiques, etc.) et stratégiques (continuité d'activité, communication, etc.) doivent se coordonner pour gérer les effets de la crise, tout en rétablissant le bon fonctionnement du système. Au niveau **décisionnel**, il est important d'intégrer la Direction des Systèmes d'Information (DSI) ou le Responsable de la Sécurité des Systèmes d'Information (RSSI) dans un système de gestion de crise régulier pour informer les décideurs sur l'avancement de l'attaque. Ces informations sont nécessaires à l'adaptation et à la coordination des actions correctives. En parallèle, une autre cellule est chargée d'analyser la situation technique et de proposer des actions pour rétablir l'activité. Il s'agit de la **cellule de crise opérationnelle**.

En ce qui concerne l'organisation de la cellule de crise, celle-ci doit être déterminée en amont de la crise. Cela permet de se baser sur des cadres préexistants et de ne pas avoir à tout inventer. Sur ce sujet, l'anticipation est primordiale et doit prendre en compte les différentes manifestations de la crise et donc les différentes manières de s'organiser.

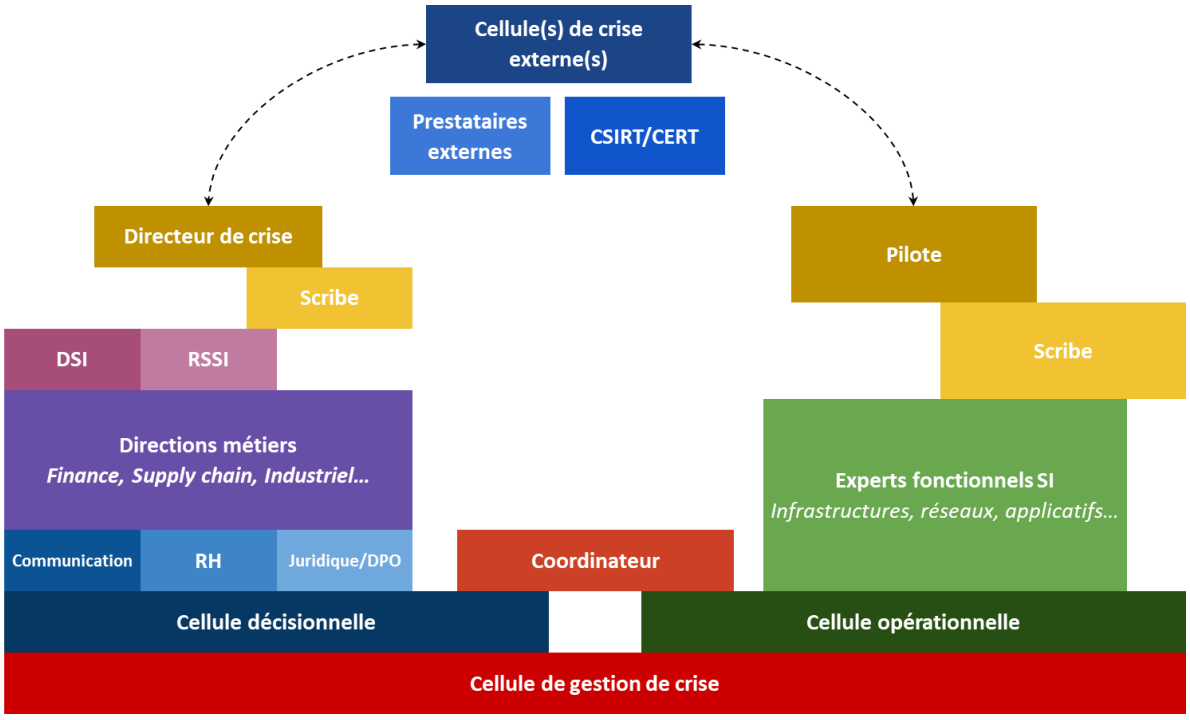

Figure 2 : Organisation de la cellule de crise

2.1.1 LA CELLULE DÉCISIONNELLE, RESPONSABLE DE LA CONTINUITÉ D'ACTIVITÉ DE L'ENTREPRISE

La cellule décisionnelle a pour rôle d'orienter la gestion de crise en prenant les décisions stratégiques. Sa composition est donc importante pour résoudre la crise rapidement et sans trop de dégâts. Si les membres du COMEX forment souvent le cœur de cette cellule, la question de la présence d'autres personnalités peut se poser. La composition de la cellule de crise décisionnelle dépend cependant grandement de la taille et de l'activité de l'organisation.

Dans la cellule décisionnelle, il est primordial d'intégrer **un acteur juridique et un Délégué à la Protection des Données (DPO)**. Selon la typologie d'attaque, le DPO est là en tant qu'auditeur libre ou bien il peut jouer un vrai rôle au sein de la cellule de crise, si la cyberattaque a entraîné une fuite de données à caractère personnel. En fonction du type d'activité de l'entreprise, il est aussi important d'intégrer à la cellule décisionnelle certaines directions métiers, soit parce qu'elles sont indispensables à la continuité de l'activité du groupe en termes contractuel, soit parce qu'elles sont les plus fortement impactées.

Quand plusieurs branches sont touchées par la crise, **plusieurs cellules décisionnelles sont mises en place dans chacune des directions métiers impactées**. La DSI s'inscrit également dans cette organisation. Au niveau de la DSI, deux cellules sont mises en place : une cellule décisionnelle qui regroupe tous les directeurs informatiques et une cellule opérationnelle qui regroupe elle-même plusieurs sous-cellules opérationnelles qui s'activent en fonction des systèmes touchés (industrie, finance…). La difficulté est donc de bien coordonner ces différentes cellules. Ce découpage des tâches est adapté en fonction de la taille de la DSI et de l'organisation.

Selon l'organisation du groupe, le RSSI joue des rôles différents. De manière générale, chaque organisation doit disposer d'un composant stratégique SSI et d'un composant opérationnel SSI, qui peuvent être réunis dans la même personne. **Le RSSI occupe davantage une fonction décisionnelle** car il a la capacité de prendre des décisions importantes pendant la crise, à condition d'en avoir le mandat : couper et isoler des sites, avec des impacts sur les métiers importants. Il faut distinguer les personnes qui font partie de la cellule opérationnelle de celles qui participent aux points d'orientation réguliers de cette cellule. Le RSSI en l'occurrence participe aux points mais ne fait pas véritablement partie de la cellule opérationnelle, et s'il a un pied dans chacune des cellules, il peut également tenir en partie le rôle de coordinateur. Ce cumul de rôles se fait en fonction de la taille de la structure représentée et du positionnement du RSSI dans l'entreprise (à la tête d'une direction indépendante de la DSI, dépendant du DSI…). Le RSSI ne peut cependant pas être le seul à remplir toutes ces fonctions. Il faut prévoir un **roulement au niveau des rôles et des interlocuteurs**, en fonction de la durée de la crise.

Au-delà de la composition de la cellule décisionnelle, une autre problématique relative à une gestion de crise cyber est parfois le **manque de sensibilité à la cybersécurité des collaborateurs dédiés à la gestion de crise**. Les « experts » de la gestion de crise sont en effet plus habitués à gérer d'autres types de crises que la crise cyber. Ils ont parfois des difficultés à matérialiser concrètement les éléments touchés par la cyberattaque et à prendre les bonnes décisions. Dans la cellule décisionnelle, il peut donc être intéressant d'intégrer un « interprète cyber » pour que tout le monde se comprenne entre la cellule décisionnelle et la cellule opérationnelle. Par exemple, une crise cyber nécessite souvent d'isoler les éléments touchés par la cyberattaque, ce qui peut entraîner des problèmes de compréhension sur les conséquences d'une telle action. Il faut donc préalablement expliquer au directeur de crise les impacts et solutions d'une crise cyber. Dans la phase d'investigation, il faut aussi transcrire les données en langage compréhensible pour les métiers.

2.1.2 LA CELLULE OPÉRATIONNELLE IT

Dans le cadre d'une gestion de crise cyber, la cellule qui gère la majeure partie des opérations pour résoudre l'origine de la crise est la cellule opérationnelle issue de la DSI. Son rôle consiste à **préparer les prises de décisions par les dirigeants,** en les éclairant sur la situation et en fournissant un premier

plan d'action. Puis, l'orientation faite au niveau décisionnel aboutit à la définition de la stratégie que la cellule opérationnelle doit poursuivre sur le terrain à travers des plans d'actions.

Pour garantir son efficacité, la cellule de crise opérationnelle travaille de manière indépendante. C'est au **coordinateur** qui a alors un pied dans la cellule opérationnelle et un pied dans la cellule décisionnelle de traduire les décisions et les opérations d'un côté et de l'autre. Quand une crise dure plus de 24h, la fonction de coordinateur est encore plus importante pour traduire ce qui se passe dans chacune des cellules.

2.1.3 QUAND MOBILISER LES CELLULES DE CRISE ?

Du fait de son caractère fulgurant et multiforme, la crise cyber doit être prise en compte par toutes les parties prenantes de l'entreprise le plus rapidement possible. La mobilisation des cellules de crise correspond ainsi à l'une des premières décisions à prendre par le DSI. Nous avons identifié deux éléments principaux qui doivent déterminer la décision :

- **Les dispositions du PCA** (Plan de Continuité d'Activité) : Le PCA prévoit le moment et les modalités de mobilisation de la cellule de crise. Le DSI doit utiliser ce plan pour prendre sa décision, qui peut être graduelle (pré-mobilisation, mobilisation progressive des différents niveaux de la cellule de crise).
- **Les conséquences sur le métier** qui nécessitent de mobiliser la cellule de crise ou de ne pas le faire.

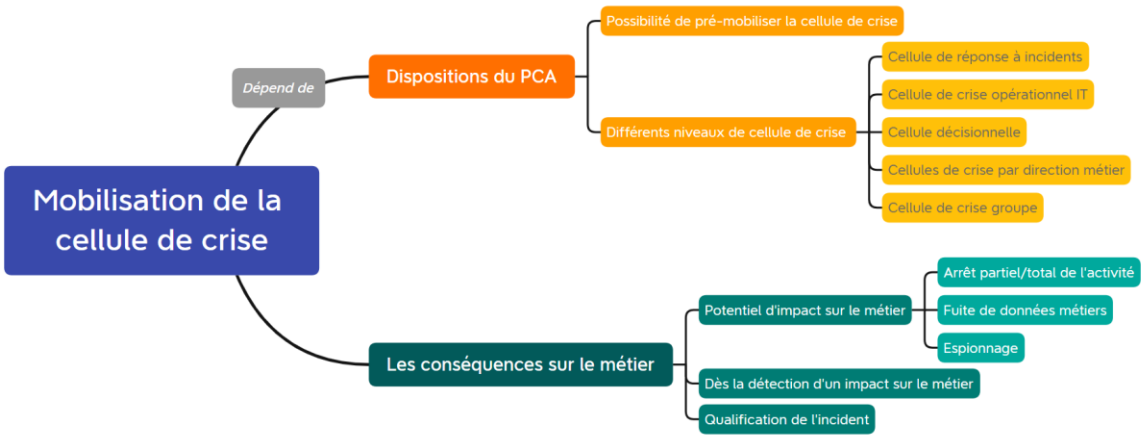

Figure 3 : Arbre à décision n°1 - Mobilisation de la cellule de crise

Au début d'une crise, l'origine de l'incident n'est pas toujours identifiée. Par exemple, un incident de production peut avoir une origine cyber, ou non. Pour faire face à tous types de crise, **l'ensemble de la cellule de crise est mobilisé en début de crise**, les membres qui se révèlent non nécessaires sont ensuite libérés au fur et à mesure par le directeur de crise. La spécificité cyber de la crise interviendrait donc plutôt dans un second temps.

Ensuite, **le déclenchement de la cellule de crise dépend de l'impact sur le métier**. La cellule opérationnelle de crise IT se met parfois en place sans la mobilisation de l'ensemble de la cellule de crise. Dès qu'un impact a lieu sur le métier, la cellule décisionnelle est mobilisée. Lorsqu'une alerte

d'incident est reçue, une pré-qualification de cet incident est effectuée. Si l'incident est réel, une cellule de réponse à incidents est mise en place. Si l'impact de l'incident est visible sur le métier, la cellule de crise est déployée.

Cependant, l'alerte d'un incident ne provient pas toujours de l'intérieur de l'organisation, elle peut aussi provenir de l'extérieur (fournisseurs…). Une attaque visant un fournisseur peut avoir des répercussions sur l'organisation. C'est ce que l'on appelle **une attaque par *supply chain*.** Il faut donc être capable de se coordonner avec des cellules de crise externes.

Exemple de l'organisation d'une cellule de crise dans une entreprise du secteur de l'agroalimentaire

Le plan de continuité des activités incluait un aspect *business* et des éléments de remédiation techniques. Trois cellules de crise distinctes mais communiquant entre elles ont été constituées :

- Une cellule de crise au niveau du COMEX pour prendre les décisions stratégiques ;
- Une cellule de crise opérationnelle constituée de la direction de la communication principalement ;
- Une cellule de crise côté DSI pour gérer les aspects techniques.

Le DSI a principalement été mobilisé sur des questions de communication : vers les clients, les partenaires, il a établi une communication quotidienne en interne vers les collaborateurs et géré également la relation avec le COMEX pour qui l'objectif était un redémarrage au plus vite du SI. Le rôle du DSI auprès du COMEX a donc été primordial tous les jours de la crise afin de préserver ses équipes. De son côté, le RSSI a étendu ses fonctions et géré les conséquences de la crise sur les filiales internationales.

Au sein de la cellule de crise DSI, une organisation ad hoc a été construite pour gérer chaque chantier, constituée de trois personnes :

- Une personne applicative ;
- Un collaborateur métier ;
- Une personne technique.

Cette organisation a été maintenue deux à trois semaines après la reprise.

2.2 GÉRER LES PREMIÈRES CONSÉQUENCES SUR LE SYSTÈME D'INFORMATION

Pour prendre les premières mesures opérationnelles adéquates sur le système d'information victime d'une cyberattaque, il est nécessaire de **diagnostiquer l'incident de sécurité informatique.** Il ne s'agit pas ici de découvrir l'origine de l'incident mais d'en identifier les premières conséquences en vue d'y répondre le plus rapidement et efficacement possible.

Afin de diagnostiquer un incident informatique, plusieurs actions peuvent être entreprises par la DSI, comme par exemple :

- Consulter l'EDR (*Endpoint Detection and Response*), un outil de détection avancée de menaces, installé en complément de l'antivirus. Cet outil détecte la menace et agit immédiatement pour l'appréhender ;
- Constater et identifier soi-même la nature de l'incident avec l'aide de collaborateurs de son service ;
- Analyser les logs dans le SIEM (*Security information management system*), un outil qui gère les événements de sécurité du système d'information ;
- Consulter le nombre de tickets d'incidents/alertes remontés soit par le SOC (*Security operations center*), soit par l'équipe en charge d'assurer la sécurité du SI ;
- Contacter l'équipe d'exploitation IT pour réaliser un diagnostic des serveurs ;
- Analyser le volume et les destinataires du trafic depuis/vers Internet.

Ce premier diagnostic repose majoritairement sur **l'utilisation d'outils de supervision et s'appuie sur les travaux des collaborateurs de la DSI.** Le premier objectif est de qualifier le périmètre de l'incident. Dans ce cadre, la journalisation[4] qui permet d'enregistrer tous les mouvements dans un système est un excellent moyen de définir le périmètre affecté par l'attaque mais également de suivre les étapes du diagnostic.

Le périmètre et la nature de l'incident détecté déterminent les premières actions à entreprendre sur le SI. À ce stade, l'objectif est d'arrêter la diffusion de l'incident pour l'empêcher de s'étendre à tous les systèmes informatiques de l'entreprise et de le circonscrire dans son périmètre de départ. C'est ce qu'on appelle les mesures d'endiguement qui ne sont pas des actions pérennes. Ces mesures, si elles ne sont pas effectuées correctement et au bon moment, peuvent avoir un impact sur l'étape de remédiation qui intervient dans un second temps. L'endiguement recouvre un certain nombre de mesures dont voici quelques exemples :

- Isoler les systèmes impactés (serveurs, serveurs de fichiers, postes de travail (ensemble géographique), systèmes les plus vulnérables (a priori sous Windows). Faire cette isolation à partir de la console de l'EDR est le plus pertinent ;
- Faire intervenir une équipe de réponse aux incidents de sécurité ;
- Désactiver la plupart des comptes administrateurs car l'objectif des cyberattaquants est de disposer d'un accès administrateur pour atteindre l'ensemble des systèmes et être en capacité de les modifier ;
- Identifier et sécuriser la dernière sauvegarde saine.

Si le périmètre de la cyberattaque est trop large ou pas clairement identifié, un arrêt complet ou un confinement des systèmes est souvent décidé pour avoir le temps de mener des investigations plus approfondies.

[4] L'enregistrement séquentiel dans un fichier ou une base de données de tous les événements affectant un processus particulier (application, activité d'un réseau informatique…). - Historique (informatique), Wikipédia

2.3 GÉRER LES PREMIÈRES CONSÉQUENCES SUR L'ACTIVITÉ DE L'ORGANISATION : UNE COLLABORATION NÉCESSAIRE POUR LA DSI

Dans le cadre d'une cyberattaque, la DSI est la première direction de l'entreprise à gérer les conséquences de la crise. Cependant, elle ne doit pas négliger les autres aspects de la gestion de crise comme la communication ou la réponse aux obligations légales. Pour traiter tous ces aspects, la DSI doit entrer en collaboration active avec les autres directions de l'entreprise. Une collaboration réussie permet à l'entreprise de mieux répondre aux problèmes rencontrés par un arrêt partiel ou total de l'activité de l'entreprise.

2.3.1 ÊTRE EN LIEN RÉGULIER AVEC LE COMEX

Le COMEX forme le contingent principal de la cellule de crise décisionnelle. Il a donc besoin d'être régulièrement informé des avancées de la crise et des plans d'action entrepris. Pour ce faire, des **points de contact réguliers** sont organisés avec le coordonnateur, le DSI, voire le RSSI pour les tenir informés. Au début de la crise, ces réunions ou points de communication ont lieu très régulièrement, plusieurs fois par jour. Puis, ils s'espacent dans le temps en fonction de la capacité des équipes opérationnelles à résoudre la crise.

Le maintien et la mise à jour d'**un tableau de bord** est le meilleur moyen pour informer les membres du COMEX de l'avancée des plans d'action. Sans rechercher l'exhaustivité, les contributeurs du groupe de travail ont listé les principales informations que le COMEX souhaite obtenir en début, milieu et fin de crise.

Thématiques à traiter	Indicateurs principaux
DONNÉES	Date des dernières sauvegardes saines
	Délai de mise à disposition des dernières sauvegardes
	Estimation de la perte de données (date de restauration possible)
IMPACTS FINANCIERS	Investissements IT nécessaires pour restaurer et améliorer le système d'information (matériels, logiciels…)
	Montant de la franchise de l'assurance cyber
	Chiffre d'affaires non réalisé, du fait de la cyberattaque
	Renforts IT à prévoir (consultants experts)
IMPACTS RÉPUTATIONNELS	Veille médias - Nombre d'annonces ou notifications dans la presse et sur les réseaux sociaux
IMPACTS RH	Nombre de salariés au chômage technique
	Capacité à gérer la paie, du fait de l'arrêt complet ou partiel des systèmes informatiques
IMPACTS SUR LE SI	Volume de PC/Applications/systèmes indisponibles
IMPACTS SUR LES MÉTIERS *(en fonction des secteurs d'activité)*	Nombre d'utilisateurs/clients impactés
	Nombre de processus métiers impactés
	Volume de commandes perdues
	Volume des arrêts de production
NATURE ET PÉRIMÈTRE DE LA CRISE	Ransomware, fuite de données ?
PLAN D'ACTIONS	Pourcentage d'avancement des plans d'action validés
	Nombres de personnes mobilisées dans le plan d'actions
	Pourcentage de serveurs et PC réparés
RELATIONS TUTELAIRES	Suivi des niveaux d'information et alertes, obligatoires ou recommandées

Figure 4 : Tableau de bord à destination du COMEX

2.3.2 PRÉPARER SA COMMUNICATION DE CRISE AVEC LA DIRECTION DE LA COMMUNICATION

La coopération de l'ensemble des parties prenantes est essentielle et joue un rôle crucial pour la communication. Il faut communiquer dans toutes les situations. L'entreprise ne sera jamais blâmée par les partenaires pour avoir été victime d'une cyberattaque mais elle le sera si elle n'a pas communiqué. Même s'il s'avère que l'organisation n'avait pas assez protégé son SI en amont de l'attaque, il est conseillé de ne pas dissimuler d'information. Il faut faire en sorte que tous les points de contacts disposent de toutes les informations nécessaires pour faire face. Il est également essentiel de faire connaître les nouveaux canaux de communication à toutes les équipes de l'entreprise. Ainsi, il est nécessaire de **prévoir en amont ou dès le début de la crise un moyen de communication alternatif au SI de l'entreprise.** Celui-ci permettra de continuer à communiquer si les outils habituels ne sont plus accessibles. Par ailleurs, même s'ils sont accessibles, utiliser un autre moyen plus sûr le temps de s'assurer que les cybercriminels n'y ont pas accès est également recommandé.

La communication de crise est fondamentale mais c'est un exercice très difficile car elle doit être dirigée vers toutes les parties prenantes :

- **Au sein de l'entreprise** : vers les collaborateurs, les métiers, toutes les filiales et vers le COMEX qui doit disposer de tableaux de bord fournissant une visibilité sur l'ensemble de la gestion de crise.
- **Vers l'écosystème** (clients, fournisseurs, partenaires…) : ceux-ci attendent des garanties concernant les données exfiltrées. Il faut donc leur fournir un maximum d'informations sur ce qui est connu.
- **Vers les médias** : Les médias adoptent des postures différentes, certains sont très factuels et d'autres sont très orientés (certains rentrent parfois directement en contact avec les cyberattaquants).

Se coordonner avec la Direction de la Communication

Lors d'une crise d'origine cyber, les capacités techniques et opérationnelles de l'entreprise attaquée peuvent-être fortement mises à mal et toucher ses clients, ses partenaires, ses collaborateurs et plus généralement l'ensemble de ses parties-prenantes.
Restaurer, maintenir ou renforcer leur confiance dans la capacité de l'entreprise à gérer la situation et à préserver leurs intérêts nécessite une analyse et des actions coordonnées.
La direction de la communication est garante de cette stratégie de réponse et elle doit en conséquence être informée rapidement des événements.
Sur la base des enjeux identifiés, son rôle est de définir et de faire valider au plus tôt par la cellule de crise, une stratégie de communication et les messages clés associés destinés à toutes les parties prenantes. Ces éléments validés peuvent être déclinés sur différents formats et transmis aux points de contacts internes susceptibles d'être sollicités. Ces messages seront régulièrement mis à jour tout au long de l'événement.

On distingue quatre familles de parties prenantes :

- Les autorités : selon l'entreprise et les impacts de l'événement, la cellule de crise peut-être en lien avec l'ANSSI, la DRIEETS, l'ANSM, l'ARS, l'AMF, la CNIL, …

- Les interlocuteurs internes : les collaborateurs, les partenaires sociaux, les métiers, les filiales, les actionnaires, le COMEX, …
- Les partenaires professionnels : clients, fournisseurs, prestataires, concurrents, interprofession, assurances, avocats, huissiers, …
- Les interlocuteurs sensibles et les médias : les victimes de l'attaque cyber, les associations, les élus locaux, les influenceurs et leaders d'opinion, les réseaux sociaux, les médias locaux et nationaux, les médias spécialisés, …

Les parties-prenantes constituent autant d'alliés ou de freins potentiels. En fonction de leurs contraintes et de leurs enjeux, une coordination efficace avec elles doit permettre si possible :

- De préserver de bonnes relations
- De faire preuve de transparence
- D'obtenir des informations complémentaires
- De faire relayer ses messages clés

Par temps calme, cartographier l'ensemble des parties prenantes et identifier leurs interlocuteurs internes permet de réagir rapidement.
Exemple : Contacts des RSSI au sein des organisations partenaires (clients, fournisseurs, prestataires…)

Check-list des actions à mener avec la Direction de la Communication

Actions préventives :

- Initier hors période de crise un dialogue entre l'IT et l'équipe communication : Ces échanges sont indispensables pour clarifier auprès des communicants les priorités, les enjeux et les moyens cyber dont dispose l'entreprise.
- Élaborer une stratégie de réponse à la crise cyber : check-list des premières actions, cartographie des parties prenantes, identification des cibles…
- Anticiper les scénarios de crise et pré-rédiger les éléments de communication : communiqués de presse, argumentaires, communication interne, messages à destination des réseaux sociaux, messages clients, messages publiés sur le site Internet et les applications clients…
- Intégrer la fonction communication dans l'organisation de crise cyber ;
- S'entraîner régulièrement et développer des réflexes communs entre l'IT, la communication et les autres membres de la cellule de crise lors d'exercices de simulation.

En situation de crise :

- S'assurer que la fonction communication est alertée et intégrée dans le dispositif de crise ;
- Briefer les communicants sur la situation en cours (éléments techniques et impacts sur les métiers, services et outils) et sur les premières actions initiées ;
- Évaluer avec les communicants les facteurs d'attractivité médiatique du sujet et selon la situation, les risques que l'information sur la cyberattaque soit connue ;
- Contribuer à l'élaboration du plan de communication en identifiant toutes les cibles : internes, clients, médias, autorités, partenaires, … ;

- Contribuer à l'élaboration des messages clés avant leur diffusion vers les parties prenantes identifiées. Détacher si possible un expert Cyber au sein de la cellule communication.
- Lister les questions que pourraient poser des journalistes, et plus particulièrement ceux des médias experts.

Comment préparer ses messages-clés pour la presse ?

Trois familles de messages clés sont à préparer :

- Message factuel : énoncer les faits vérifiés et le plan d'action qui a été mis en œuvre en coordination avec les autorités et les partenaires ;
- Message conceptuel : faire de la pédagogie sur le sujet et plus particulièrement sur les procédures existantes, les dispositifs mis en place, la préparation des équipes ;
- Message d'empathie : prendre en compte les inquiétudes et présenter toutes les mesures mises en œuvre au profit des personnes impactées.

Plusieurs informations doivent être transmises avec pédagogie à la Direction de la Communication pour qu'elle puisse élaborer les messages clés :

- La nature de l'attaque et surtout les impacts sur l'organisation, les services ou les produits de l'entité.
- En cas de fuite de données, les implications pour les clients ou les usagers concernés et les actions qu'ils peuvent mettre en œuvre pour se protéger.
- Les actions mises en œuvre pour rétablir au plus vite les services et les outils de l'organisation.
- Le temps des investigations et de la remédiation.
- Les mesures prises vis-à-vis des autorités le cas échéant :
  - la déclaration auprès de la CNIL, en cas de fuite de données,
  - le dépôt de plainte auprès des services de police ou de gendarmerie spécialisés.

2.3.3 SE COORDONNER AVEC LA DIRECTION JURIDIQUE POUR RÉPONDRE AUX OBLIGATIONS LÉGALES

Lorsque survient une cyberattaque, la Direction Juridique et la Direction de la Conformité accompagnent la DSI et **mettent à sa disposition les outils juridiques** nécessaires pour réagir à la crise et pour l'aider à répondre aux exigences légales :

- Procéder à une notification de faille à la CNIL en cas de fuite de données à caractère personnel si l'incident constitue un risque au regard de la vie privée des personnes concernées (article 33 du RGPD).
- Conserver ou faire conserver les preuves par un professionnel.
- Déposer plainte et suivre la procédure judiciaire.

En l'absence d'experts juridiques au sein des DSI, le rôle de la Direction Juridique lors d'une crise cyber est primordial. Le RSSI peut avoir des compétences juridiques et est alors l'interlocuteur privilégié de cette direction.

Cependant, la Direction Juridique ne maîtrise pas toujours l'ensemble des connaissances en matière de cybersécurité. Il est donc nécessaire de mettre en place un dialogue en amont de la crise pour créer une complémentarité entre les deux directions en désignant des interlocuteurs dédiés, formés et qui se connaissent entre eux.

2.4 FAIRE APPEL À DES PRESTATAIRES EXTERNES

Par définition, la crise est un événement extraordinaire et l'organisation n'y est pas toujours très bien préparée. Sa résolution nécessite donc des moyens qui ne sont pas ceux de la gestion courante et peut conduire à faire intervenir des acteurs dédiés à la gestion de crise.

2.4.1 POURQUOI FAIRE APPEL À DES PRESTATAIRES ?

Trois raisons principales peuvent motiver une organisation pour faire appel à des prestataires externes :

- Elle ne dispose pas de suffisamment de ressources au sein de ses effectifs. L'intervention de prestataires externes permet de **renforcer les équipes internes**.
- Elle a besoin d'une **expertise spécifique** dans un domaine pour lequel elle n'est pas compétente en interne.
- **D'autres acteurs de l'écosystème sont impliqués** et l'utilisation d'un prestataire externe permet de les intégrer dans la résolution de la crise (fournisseurs, éditeurs de logiciels, autorités, partenaires…).
- Les **frais de gestion externes peuvent être remboursés par l'assurance cyber**, ce qui n'est pas le cas du paiement des heures supplémentaires des salariés en interne.

Selon la spécificité de la crise et de l'organisation, d'autres raisons peuvent être invoquées.

Pour accompagner les équipes, certains organismes sont en mesure de venir efficacement aider la DSI lors d'une crise issue d'une cyberattaque :

- Un cabinet juridique spécialisé dans le droit cyber ;
- Un cabinet spécialisé dans la communication de crise cyber ;
- Une entreprise spécialisée dans la gestion de crise ;
- Un organisme spécialisé dans la cybersécurité ;
- L'ANSSI, selon le secteur de l'organisation ;
- Son assurance cyber, qui dispose elle-même de prestataires partenaires pour accompagner ses clients ;
- Un coach pour le DSI afin de l'aider à prendre du recul sur la situation ;
- Une FIR (Force d'intervention rapide) associée à une prestation CSIRT : souscrire ce type de contrat permet de garantir la connaissance des experts du SI, et garantir du présentiel sur site ;
- Le Comité Social Économique (CSE) ou Instances Représentatives du personnel (IRP), pour rassurer face à une crainte légitime de divulgation d'informations personnelles des collaborateurs lors de l'attaque et/ou pour désamorcer tout conflit lié à la charge excessive de travail lors de la crise ou à la non-conformité avec le droit du travail (travail de nuit…) ;

- Un organisme pour gérer la logistique et le soutien aux équipes mobilisées (nourriture, blanchisserie, lieux de repos…).

2.4.2 PRÉVENIR SON ASSURANCE

Si l'organisation victime de la cyberattaque a fait le choix de souscrire une assurance cyber, il est alors nécessaire prévenir l'assureur rapidement dès le début de la crise. Le numéro de l'assurance doit être à disposition du DSI indépendamment de l'accès au système d'information de l'organisation. En effet, lors d'une crise cyber, l'accès aux fichiers informatiques n'est pas garanti.

Une assurance cyber recouvre généralement trois volets :

- **Un volet responsabilité civile** : la police couvre les conséquences pécuniaires, les frais de notification notamment vis-à-vis de la CNIL, les sanctions réglementaires lorsqu'elles sont assurables (ce n'est pas le cas en France mais à l'étranger) ;
- **Un volet dommages** : la police couvre les frais de reconstitution des données, frais de remise en état des systèmes (tels qu'ils étaient avant la cyberattaque, mais ne couvre habituellement pas les frais d'amélioration des systèmes), perte d'exploitation (blocage des systèmes et des activités)[5] ;
- **Un volet assistance** : l'assuré bénéficie d'un service d'assistance 24/7 avec recours à un panel de prestataires et à des experts spécialisés dès la déclaration de sinistres.

Le volet assistance permet à l'organisation de répondre à ses besoins de prestataires extérieurs à des tarifs négociés en amont par l'assurance, avec la garantie d'une intervention rapide.

Quelques notions sur l'assurance cyber

La police d'assurance cyber est un outil particulièrement efficace au service des entreprises lorsque survient une cyberattaque.

Les étapes clés de la gestion d'une cyberattaque peuvent se résumer de la manière suivante :

- Intrusion ;
- Découverte de l'intrusion ;
- Information en priorité de la direction ainsi que du Risk Manager ou du responsable des assurances ;
- Réflexion par la DSI sur la stratégie à adopter (couper/isoler/contrôler) ;
- Signalement des faits à l'assureur Cyber dès que l'on dispose d'une vision globale du problème (normalement dans les 48h suivant la découverte de l'intrusion) ;
- Prise de contact également avec l'ANSSI qui peut apporter une aide selon l'évaluation de la situation ;
- Envoi sur place par l'assureur de son prestataire, conformément à ce que prévoit le volet assistance ;

[5] La perte d'exploitation est calculée sur la marge brute. Un expert est dédié à ce calcul, qui se fait sur la base des factures fournies par l'entreprise et sur les discussions menées entre l'entreprise et l'assurance. Les montants peuvent être très élevés rapidement. Selon le secteur d'activité, le calcul peut être plus ou moins complexe.

- Un premier échange se tient avec le prestataire et la DSI (questions d'ordre général) pour évaluer l'état de la menace ;
- Un second échange plus approfondi se tient avec le prestataire pour définir une stratégie de réponse.

Le prestataire envoyé par l'assureur intervient auprès de l'entreprise dans un rôle de "chef d'orchestre" pour coordonner les actions à mettre en place mais il ne se substitue aucunement aux équipes IT de l'entreprise. Il passe en revue un certain nombre de questions préliminaires afin de déterminer la meilleure stratégie de réponse à apporter. Il s'assure également que toutes les mesures à mettre en œuvre par l'entreprise lors de ce type d'évènement sont bien mises en place. Plus les bonnes décisions seront prises rapidement, meilleure sera la situation pour l'entreprise dans la résolution du sinistre.

L'assureur a à sa disposition, et met à celle de ses clients, un panel de prestataires spécialisés pour intervenir quelle que soit la nature de la menace. Ce panel permet de faire intervenir très rapidement des spécialistes sur la base de tarifs négociés afin d'éviter aux entreprises d'être confrontées à des coûts non maîtrisés du fait de l'urgence de la situation. Il faut noter que, plus une entreprise est sensibilisée et préparée en amont, moins elle est confrontée à des problématiques de pure extorsion. La demande de rançon est intrinsèque à ce type d'activité criminelle, mais les entreprises avec un niveau de prévention suffisamment mature refusent généralement d'en payer le montant du fait notamment de leurs systèmes de back up et de leurs capacités de restauration des systèmes corrompus.

Enfin, des réunions de suivi pour continuer d'optimiser la sécurité informatique de l'entreprise après la résolution de l'incident sont généralement mises en place, mais cela peut se dérouler sans l'assureur.

La fin d'année 2022 a permis des avancées significatives sur la prise en compte du risque cyber par les assureurs suite à l'adoption de deux lois :

L'article 5 de la loi d'orientation et de programmation du ministère de l'intérieur (LOPMI), votée le 14 décembre 2022, **conditionne la couverture assurantielle** des pertes et dommages causés par une cyberattaque, **au dépôt de plainte par la victime dans un délai de 72h**. Cette obligation de porter plainte interroge : elle permet aux pouvoirs publics une remontée d'information quasi certaine afin de lutter contre la cyberdélinquance, mais elle peut également être perçue comme une incitation aux attaques de type ransomware (l'assurance pouvant alors payer la rançon demandée par les hackers).

La loi de finances pour 2023, promulguée le 30 décembre 2022 a prévu un **dispositif de franchise d'impôt pour les provisions de certaines captives de réassurance**. Ce dispositif fiscal favorable a pour objectif de permettre aux entreprises d'améliorer la couverture assurantielle de leurs risques, et notamment cyber.

Enfin, ce nouveau dispositif fiscal renvoie à un arrêté du 13 décembre 2022 qui ajoute dans le Code des assurances deux catégories dédiées aux risques cyber, ce qui pourrait permettre que ces derniers soient mieux pris en compte par les assureurs.

2.4.3 PRENDRE CONTACT AVEC L'ANSSI

L'ANSSI est rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN). Elle est l'autorité chargée d'accompagner et de sécuriser le développement du numérique. Acteur majeur de la cybersécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs régulés. Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

L'ANSSI est composée d'équipes dédiées à la fois à la surveillance de la menace cyber et à la gestion de crise cyber. Il existe des équipes dédiées à la communication de crise et aux différents aspects de la gestion de crise, dont le *forensic*[6]. Il existe également des équipes transverses, chargées de la coordination.

L'ANSSI ne dispose pas de critères fixes pour déterminer son degré d'implication auprès d'une entreprise dans la gestion d'une cyberattaque. Généralement, l'Agence caractérise l'impact sur l'entreprise, sur l'écosystème, sur le champ politique et humain afin de déterminer son action. Ensuite, c'est le rôle du directeur de l'ANSSI de décider s'il envoie des équipes et pour quel mode opératoire : pilotage, accompagnement technique, communication… L'ANSSI couvre en effet de plus en plus de champs et son accompagnement se révèle être un élément rassurant pour les organisations victimes d'attaque.

[6] **L'analyse forensique** (plus fréquemment appelée « ***forensic*** ») consiste à **investiguer un système d'information après une cyberattaque**. Les analystes vont collecter l'ensemble des données brutes (fichiers effacés, disques durs, sauvegardes, journaux des systèmes…), les étudier pour comprendre ce qu'il s'est passé et établir des conclusions. Cette tâche, parfois ardue, permet de produire des preuves nécessaires à une action interne ou au lancement d'une procédure judiciaire par exemple. (Source : Tehtris)

3 QUAND LA CRISE S'INSTALLE DANS LE TEMPS…

Après avoir géré les premières conséquences de la crise cyber, l'organisation victime de la cyberattaque, cherche à maintenir son activité tout en endiguant les effets de l'attaque. Dans un premier temps, la DSI s'active pour limiter les dégâts causés par la cyberattaque sur le système d'information et pour réparer ces dégradations du mieux possible.

Lorsque la crise s'installe dans le temps, tout le fonctionnement normal de l'entreprise doit être repensé. Cette réorganisation est particulièrement contraignante pour les équipes de la DSI, qui doivent gérer une charge de travail supplémentaire, mais aussi pour les équipes métiers, qui doivent travailler de façon dégradée ou sont au chômage technique.

Ce second temps de la gestion de crise correspond aussi au moment où l'organisation doit gérer ses obligations légales et où elle rentre dans un processus réglementaire sur le long terme. Elle doit également communiquer régulièrement ses avancées en interne et en externe. La communication est bien trop souvent oubliée dans les dispositifs de gestion de crise alors qu'elle évite la surenchère des crises (crise réputationnelle dans les médias ou crise salariale, par exemple) et qu'elle facilite le processus de résolution de la crise en informant correctement les différentes parties prenantes.

3.1 LA GESTION TECHNIQUE DES CONSÉQUENCES DE LA CYBERATTAQUE : ENTRE MESURES CONSERVATOIRES ET RÉPARATION DU SI

La DSI est au cœur de la gestion technique des conséquences de la cyberattaque. La gestion technique de la crise répond à deux objectifs principaux qu'il faut bien circonscrire. Le premier objectif est de réparer, voire reconstruire, le système d'information, le second est d'investiguer pour découvrir l'origine de la cyberattaque. Cependant, il est important d'avoir en tête que la connaissance de l'origine de la crise n'est pas nécessaire pour en réparer les conséquences. La majorité des ressources doit donc être positionnée sur la gestion de crise plutôt que sur la recherche de l'origine. Caractériser l'attaquant, connaître son mode opératoire ne sont pas des priorités, même si c'est parfois nécessaire pour reconstruire le SI.

Les décisions prises au cours de la gestion de crise se basent principalement sur des éléments techniques concrets. Depuis quand dure l'attaque ? Est-ce que l'attaque a été détectée dès l'intrusion des cybercriminels dans le système d'information de l'organisation ? Certains détails techniques, comme l'origine géographique de l'attaquant, n'ont au contraire que peu d'importance.

Afin de bien encadrer son processus de gestion de crise, il faut définir des critères de sortie de crise, à la fois techniques et opérationnels. Il faut veiller à ne pas étendre sans limite la partie des investigations pour satisfaire sa curiosité technique.

Retour d'expérience de l'ANSSI sur les étapes clés de la gestion technique d'une crise

Gérer les conséquences d'une cyberattaque sur le système d'information correspond à quatre processus distincts :

- La collecte d'informations,
- La phase d'investigation,
- Les mesures d'endiguement,
- La reconstruction ou « durcissement ».

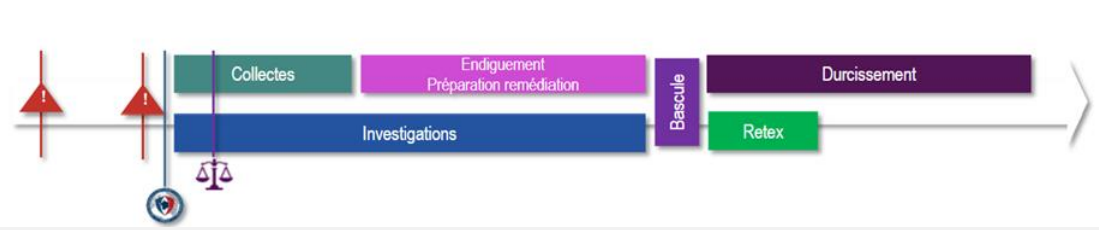

Figure 5 : Exemple de chronologie de la gestion technique de la crise

La collecte d'informations

Lors de l'investigation, les collectes d'informations doivent être ciblées car aucune autre action ne peut être menée en même temps, ce qui est donc très coûteux humainement.
Il existe deux types de collectes :

- Les collectes systèmes, si l'attaque n'est pas trop ancienne : vtx, dd, ORC (ou équivalent), logs AD, logs DNS, logs proxy…
- Les collectes réseaux : logs WAF, pare-feu, configurations…

Ces collectes d'informations doivent être menées de manière discrète car les attaquants sont capables de repérer des petits mouvements. Par ailleurs, les éléments collectés seront utiles pour les forces de l'ordre même si le temps judiciaire est bien différent du temps technique. Il faut donc conserver une copie non analysée des éléments collectés.

La phase d'investigation

La phase d'investigation sert à comprendre l'impact de l'attaque sur le SI, identifier le niveau de privilège de l'attaquant et ses moyens de persistance critique.
Dans une compromission à large échelle, la recherche du « patient 0 », ou de la chaîne de compromission exhaustive, ne doit pas être une priorité. Cette recherche est coûteuse alors qu'elle n'apporte que peu d'éléments pour surmonter la crise.
Actuellement, les cyberattaquants se concentrent sur la recherche d'un moyen d'élever leurs privilèges au sein du SI, notamment par l'accès à un compte administrateur. La reconstruction doit donc se concentrer sur la suppression de ces privilèges aux attaquants. Cependant, les doctrines évoluent rapidement, il faut donc adapter ces techniques d'investigation à l'évolution des techniques utilisées par les cybercriminels.

Les mesures d'endiguement

Les mesures d'endiguement servent à :

- Limiter les conséquences de l'attaque sur le SI ;

- Permettre un fonctionnement dégradé du SI, en isolant une partie du SI ou en désactivant un compte compromis par exemple ;
- Créer un « goulot d'étranglement » pour les cybercriminels.

Ces mesures peuvent avoir un impact sur l'investigation qui est menée en parallèle. Il convient également de veiller à ne pas tomber dans une forme de guérilla face au cyberattaquant. Généralement, ces mesures sont réalisées par les administrateurs des systèmes.

La reconstruction

Avant d'entamer les actions de reconstruction sur le SI, il convient de s'assurer que les moyens de persistance critiques ont été identifiés et que le niveau de sécurité du SI est connu, par rapport à la typologie d'attaque rencontrée.
Ces actions répondent à deux objectifs principaux : reprendre le contrôle du SI et augmenter son niveau de sécurité.
Pour ce faire, la formation et l'accompagnement des administrateurs sont des facteurs clés dans ce processus. Afin de s'assurer que l'incident est bien clos, il est généralement nécessaire de mener une supervision des systèmes. À ce stade, le fait de percevoir encore des tentatives d'intrusion confirme que les systèmes de sécurité mis en place fonctionnent correctement. Il est difficile de définir une liste exhaustive des mesures précises à réaliser lors d'une remédiation car celles-ci dépendent de la typologie de l'attaque et des priorisations données.

Les erreurs à éviter

Lors d'une compromission massive du SI, voici les « choses à ne pas faire » :

- Clarifier insuffisamment les interventions et les besoins auprès des prestataires (répartitions des missions et objectifs) ;
- Se focaliser uniquement sur le point d'entrée ;
- Entamer la remédiation avant la fin (ou le début) des investigations ;
- Confondre remédiation et endiguement (risque de « guérilla ») ;
- Ne pas préserver les journaux ;
- Interagir avec l'infrastructure adverse ;
- Discuter de la réponse à incident sur le réseau compromis : généralement, il faut rester discret ou disposer d'un réseau alternatif ;
- Réparer uniquement les symptômes, et non la cause.

3.2 LA GESTION DES ÉQUIPES PENDANT LA CRISE

Lorsque la crise s'installe sur le long terme, les équipes de la DSI sont mobilisées sur des plages horaires plus importantes pendant une période longue et indéfinie. Pour maintenir la capacité de travail de ses collaborateurs, le DSI se doit de ménager ses équipes. **Cette sur-mobilisation des équipes entraîne également des aménagements logistiques** : ouvrir des locaux à des horaires non conventionnels, prévoir des repas du matin au soir (ouverture du restaurant d'entreprise, le cas échéant). Cet aspect

est rarement pris en compte dans la préparation des dispositifs de crise, il est pourtant majeur pour la réussite de la gestion de crise cyber.

Au-delà des équipes de la DSI, les équipes métiers sont également à prendre en compte, soit parce qu'elles sont au chômage technique, soit car leur charge de travail est alourdie par la nécessité de travailler en mode dégradé. Informer ces équipes de l'avancée de la gestion de crise est également un moyen d'éviter des dissensions internes et de les impliquer dans l'effort collectif. Cette gestion des équipes doit se faire en collaboration avec la Direction des ressources humaines.

D'un point de vue managérial, **la prise en compte du stress et de sa gestion au sein des équipes est primordiale tout au long de la crise**. Pour ce faire, il convient d'identifier les personnes qui ne parviennent pas à gérer leur stress dès le début de la crise pour ne pas les sur-solliciter. De manière générale, tout comportement néfaste à la gestion de crise doit être traité rapidement et efficacement, et cela sans prendre en compte le positionnement hiérarchique.

De manière opérationnelle, voici une liste de conseils pour gérer au mieux ses équipes pendant la crise :

- Protéger les équipes SI pour qu'elles ne soient pas parasitées par des informations ou des sollicitations autres que celles qui leur sont déjà adressées par la personne de la cellule de crise en charge de la coordination ;
- À l'inverse éviter que ces équipes opérationnelles transmettent des informations sans passer par les personnes en charge de ces communications avec la cellule décisionnelle et les métiers ;
- Multiplier les signes de remerciement : par exemple, par l'organisation d'une fête après la crise à laquelle sont conviés les conjoints car ils ont également participé à l'effort collectif ;
- Malgré les nombreuses propositions d'accompagnement externes, il faut privilégier le travail avec les internes qui ont une connaissance plus profonde du SI car le temps ne permet pas d'embarquer de nouvelles personnes ;
- Privilégier une cellule de crise réduite avec les personnes clés uniquement ;
- Séparer les équipes en fonction des objectifs : une équipe pour les travaux de remédiation et de construction et une autre pour les investigations. Pour autant, cette segmentation ne doit pas non plus empêcher les gens de se rencontrer quand cela est nécessaire ;
- Gérer les aspects logistiques : nourriture, ouverture des bâtiments… ;
- Mobiliser le médecin du travail.

A contrario, certaines actions sont à bannir pour gérer aux mieux ses équipes lors de la crise :

- Lors de la résolution de la crise, il faut éviter de rechercher les coupables. Cette recherche se fera une fois la crise terminée, lors du retour d'expérience qui vise à améliorer le dispositif de crise et les processus de cybersécurité. Si la recherche de coupable avait lieu lors de la crise, les équipes pourraient dissimuler des éléments nécessaires à sa résolution. Il faut donc privilégier une transparence totale et accepter le droit à l'erreur.
- Dès que les utilisateurs découvrent des difficultés d'utilisation du SI suite à l'attaque, il ne faut pas leur cacher la situation et mais au contraire leur communiquer les quelques informations déjà disponibles car ils pourraient en rechercher en externe et ainsi, faire fuiter l'information.
- Il ne faut pas restreindre la communication aux simples utilisateurs concernés du groupe mais communiquer vers toutes les branches et filiales pour limiter les risques, en évitant notamment l'utilisation du *shadow* IT lors de la crise.

La gestion des équipes lors de la crise, d'après une entreprise du secteur pharmaceutique

A posteriori, le DSI de cette entreprise du secteur pharmaceutique a fait ressortir des enseignements clés de la gestion des équipes en temps de crise :

- La rapidité du processus de décision est primordiale pour préserver les équipes et redémarrer rapidement. Dans le cas de l'entreprise en question, des décisions majeures (reconstruction de l'AD, déploiement d'un EDR) ont été prises en moins de 24h après la détection de la cyberattaque.
- La mobilisation d'experts a été nécessaire pour soulager les équipes.
- Il faut gérer au mieux les questions obsédantes, par exemple : « est-ce que les hackers sont encore là ? » ou « est-ce que l'on en fait trop ? » ou « est-ce le juste niveau de sécurité ? ».
- Il a fallu réajuster régulièrement la stratégie et l'organisation en fonction de l'évolution de la crise.
- Associer les métiers en continu est un travail fondamental pour maintenir la confiance.
- Favoriser et harmoniser la communication interne et externe : il faut communiquer beaucoup, et aligner les communications externes et internes. Il faut rassurer les partenaires, notamment logistiques et R&D, et prévenir toutes les autorités compétentes.
- La gestion de la fatigue : certaines personnes clés ne veulent pas s'arrêter malgré la fatigue qui s'accumule. Il faut cependant permettre un roulement des équipes, personne ne doit être indispensable.

Communiquer avec ses équipes en temps de crise, d'après une entreprise du secteur de l'agroalimentaire

Lorsque les systèmes informatiques sont inutilisables, les moyens de communication habituels (mail, chat d'entreprise…) le sont également. Cette situation entraîne des difficultés pour communiquer avec ses équipes au début et pendant la crise. Pour faire face à cette difficulté, des comptes Signal ont été créés pour communiquer le nouveau mot de passe de la boîte mail. Sans préparation préalable, il a fallu récupérer la liste des numéros de téléphone de tous les collaborateurs qui ne disposaient pas tous de numéros professionnels.

3.3 LES OBLIGATIONS LÉGALES DES ENTREPRISES EN TEMPS DE CRISE CYBER

Comme nous l'avons vu plus haut dans ce rapport, certaines obligations légales doivent être prises en compte dans les premiers jours de la crise. Le suivi de la procédure judiciaire, à la suite d'un dépôt de plainte, doit cependant être maintenu tout le temps de la crise. La collecte d'informations et les investigations qui sont menées dans le système d'information permettent également d'alimenter le

dossier juridique. Même si les équipes de la DSI doivent garder en tête ces impératifs réglementaires, ils sont remplis en collaboration avec la Direction Juridique et/ou un cabinet juridique spécialisé.

Les obligations légales des entreprises en temps de crise cyber, d'après Maître Corinne Thiérache

Lors d'une crise cyber, une organisation doit s'acquitter de certaines obligations et entamer une procédure juridique à l'encontre des cyber-délinquants :

- **Prévenir l'ANSSI** sans délai de tout incident affectant les réseaux et systèmes d'information en fonction du degré d'impact sur les utilisateurs touchés, de la zone géographique concernée ou encore de la durée de l'incident. L'ANSSI peut décider d'en informer le public.

- **Procéder à une notification de faille à la CNIL** en cas de fuite de données à caractère personnel si l'incident constitue un risque au regard de la vie privée des personnes concernées (article 33 du RGPD).

  Pour cela, il convient de documenter l'incident en précisant :

  - La nature de la violation ;
  - Si possible, les catégories et le nombre approximatif de personnes concernées par la violation ;
  - Les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés (certaines données sont particulièrement sensibles comme les numéros de cartes bancaires. Il faut héberger les données selon leur sensibilité et ne pas mettre toutes les données au même endroit.) ;
  - Les conséquences probables de la violation de données ;
  - Les mesures prises ou envisagées pour éviter qu'un tel incident se reproduise ou pour atténuer ses éventuelles conséquences négatives.

  En cas de risque élevé, il faudra également notifier les personnes concernées (article 34 du RGPD), soit par email, soit par messages d'alerte sur le site (notamment pour la banque).
  Cette notification doit être transmise à la CNIL via un téléservice dédié dans les meilleurs délais et, si possible 72 heures au plus tard après avoir pris connaissance d'une violation présentant un risque pour les droits et libertés des personnes.
  Toutefois, si toutes les informations requises ne peuvent pas être fournies rapidement car des investigations complémentaires sont nécessaires, il est possible de procéder à la notification en deux temps :

  - Une notification initiale dans le délai de 72 heures, ou, si le délai est dépassé, la communication des motifs expliquant le retard ;
  - Une notification complémentaire dès lors que les informations sont disponibles.

  À noter : des entreprises ont été condamnées pour cause de mauvaise notification de faille à un panel de sanctions allant jusqu'à 10M€.

La procédure pourra être clôturée si la CNIL constate que :

- La violation ne porte pas atteinte aux données personnelles ou ne présente pas de risque pour les droits et libertés des personnes ;
- Les personnes concernées ont été correctement informées ;
- Ont été mises en place, préalablement à la violation, des mesures techniques de protection appropriées.

- **Conserver ou faire conserver les preuves par un professionnel**, notamment un exemple de message piégé, les fichiers de journalisation (logs) du pare-feu, des copies physiques des postes ou serveurs touchés (à défaut, conserver leurs disques durs), et quelques fichiers chiffrés qui pourront permettre à l'entreprise de signaler cette attaque aux autorités et qui seront des éléments d'investigation.

- **Déposer plainte**, en parallèle de la résolution technique de l'incident et avant la réinstallation des appareils touchés, de manière à conserver les preuves techniques de l'incident pour pouvoir les fournir aux enquêteurs.

  - Où ? Toute entreprise peut déposer plainte directement au commissariat de police ou à la gendarmerie.
    Si l'entreprise est dotée d'un parc informatique situé dans Paris ou ses trois départements limitrophes (92, 93 et 94), ou lorsque l'acte touche un opérateur d'importance vitale (OIV) ne faisant pas partie d'une Zone à Régime Restrictif (ZRR), il convient de se rapprocher de la Brigade d'enquête sur les fraudes aux technologies de l'information (ex BEFTI) devenue la BL2C (Brigade de lutte contre la criminalité).
    Au Parquet de Paris, une section spécialisée a été créée pour traiter les plaintes pour des faits de cybercriminalité (Section J3).
    Enfin, il est possible de déposer plainte en adressant un courrier au procureur de la République compétent.
    Si l'attaque informatique est d'une particulière gravité, si elle concerne des informations sensibles ou un secteur stratégique, il convient de contacter la DGSI : cyber.dgsi@interieur.gouv.fr

  - Qui ? Le dépôt de plainte doit être réalisé au nom de l'entité. Si l'opération est confiée à un collaborateur, il sera nécessaire de préparer une délégation de pouvoir pour cette personne, signée par un représentant légal de la personne morale afin de permettre le dépôt de plainte.

  - Comment ? Dans le cas d'un rançongiciel par exemple, les éléments suivants devront être fournis aux autorités compétentes dans le cadre de la plainte, en fonction du profil de l'entité concernée :
    - Le détail et la chronologie des événements relatant l'incident (la main courante permettant de tracer les actions et les évènements liés à l'incident), notamment la date de la demande de rançon et les faits constatés ;
    - Les emplacements des appareils potentiellement infectés ;
    - Les journaux de sécurité associés à l'incident ;

- L'analyse technique de l'attaque ;
- La collecte d'échantillons de fichiers chiffrés ;
- Les supports ou les machines sur lesquels le rançongiciel s'est exécuté (disque système), d'où l'utilité de bien les préserver quand c'est possible ;
- Les adresses de messagerie électronique et adresses de cryptomonnaie fournies par les cybercriminels ;
- Le texte de demande de rançon ;
- Les coordonnées des témoins de l'incident.

3.4 LA COMMUNICATION EXTERNE, SOUVENT NÉGLIGÉE DANS LA GESTION DE CRISE CYBER

Nous l'avons déjà relevé à plusieurs reprises, la communication est un élément clé d'une gestion de crise réussie. Elle doit avoir lieu en interne et en externe, vers l'écosystème et la presse, selon le type d'organisation. Dans cette partie, nous allons nous attarder sur les fondamentaux d'une communication réussie vers les médias. L'objectif de cette communication est avant tout de maintenir ou de restaurer la confiance. Avant toute prise de parole publique, il est important de définir un objectif clair.

3.4.1 FAIRE LE CHOIX DE COMMUNIQUER VERS LA PRESSE

Choisir de communiquer ou non dans la presse est une première décision à prendre en lien avec la Direction de la Communication. Généralement, il est conseillé de communiquer vers l'extérieur pour éviter qu'une communication parallèle soit faite à l'insu de l'organisation. Cependant, parfois, il peut être opportun de se taire si la crise demeure en interne et qu'il est peu probable qu'elle s'envenime, ou en fonction du contexte.

Pour évaluer la pertinence d'une communication vers les médias, il est important de se poser ces questions préalables :

- **Portée de l'information** : impacts sur la vie quotidienne des citoyens (par exemple, lors d'une violation de données), les enjeux de la crise, l'implication politique potentielle.
- **Visibilité de l'information** : aspect spectaculaire de la quantité de données volées, enjeux réputationnels si le groupe est connu, crise conflictuelle (la question de la sécurisation des données), caractère mystérieux (si on ne sait pas d'où vient l'attaque) ;
- **Charge symbolique de l'information** : capacité à susciter des émotions et des inquiétudes, notamment lorsque les victimes sont innocentes (données très personnelles telles que la santé, la banque, etc.).
- **Opportunités journalistiques** : les cyberattaques sont un sujet médiatique.
- Impacts potentiels d'une communication parallèle, faite à l'insu de l'organisation, et donc non maîtrisée.

L'objectif de cette appréciation est dans un premier temps d'établir si l'entreprise doit communiquer sur la cyberattaque. Le contexte global est également à prendre en compte. Lors d'évènements

nationaux importants, comme des élections présidentielles, le relais de la communication à grande échelle est peu probable.

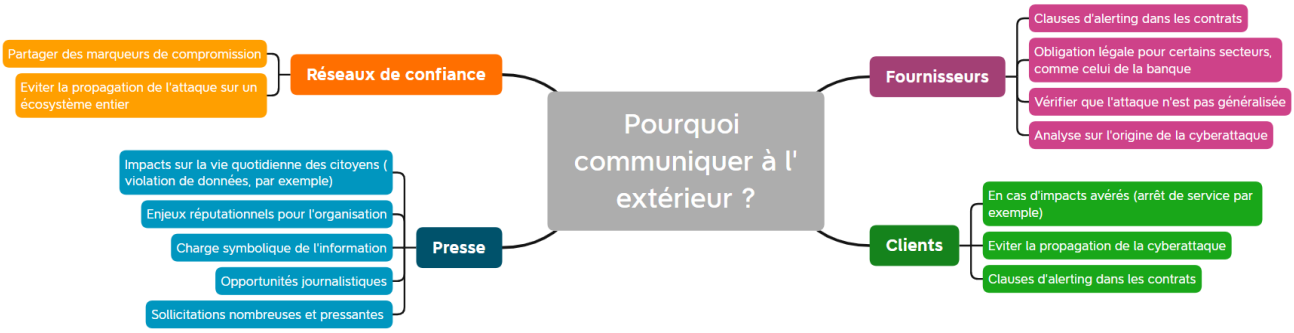

Figure 6 : Arbre de décisions n°2 - Pourquoi communiquer à l'extérieur ?

Par ailleurs, il est important de noter que la décision de la communication vers les médias ne viendra pas toujours de l'entreprise. En effet, l'information circule rapidement et souvent avant même que l'entreprise soit au courant ; elle provient généralement d'un de ces quatre canaux d'information :

- Les agences de presse, comme l'AFP ;
- Les services de l'État ;
- La presse quotidienne régionale et les médias d'investigation locaux ;
- Les réseaux sociaux.

Maintenir une veille informationnelle sur ces quatre canaux est également primordial lors de la crise cyber.

3.4.2 COMMENT COMMUNIQUER AVEC LES MÉDIAS ?

S'il est décidé de communiquer, il faut montrer que l'organisation est dans l'action pour faire face à la crise. Immédiatement après le début de la crise, il faut montrer que des actions ont été engagées pour protéger les données ou les clients. Il faut également être en mesure d'expliquer et de détailler les procédures mises en place : être pédagogue et montrer son professionnalisme. Il s'agit d'un travail de vulgarisation difficile à faire et donc à anticiper. Le vocabulaire doit être adapté pour qu'il soit compréhensible par tout le monde. Puis, il faut témoigner de l'empathie, et si la crise a une répercussion au-delà de son entité, il faut montrer que l'on en a conscience.

Un bon pilotage de la communication repose sur l'identification des parties prenantes, le choix des bons messages et du bon timing. Les quelques questions à se poser sont :

- Quel est le cadre de la crise : nature, impacts, risques, juridiques/assurance… ;
- Qui a le pouvoir sur quoi ? Le Groupe, les autorités compétentes, les partenaires… ;
- Quel est l'état d'avancement des opérations ? la résolution technique, exploitation, lien avec les entités/filiales ;
- Est-ce que je dispose de la globalité des informations ? échanger régulièrement avec les autres parties prenantes pour élaborer la globalité des messages ;

- Quels sont les acteurs : établir une cartographie des acteurs : autorités, partenaires professionnels, collaborateurs internes, interlocuteurs sensibles (médias, associations, victimes et proches, leaders d'opinion…).

Le rôle de la DSI dans cette communication est d'apporter à la Direction de la Communication des éléments concrets sur les conséquences de la crise, sans chercher à minimiser les impacts. Plus que toutes les autres directions, lors d'une crise cyber, la DSI fait de la pédagogie sur les risques et les impacts potentiels.

Il ne faut pas minimiser la crise auprès des médias : ceux-ci ont tendance à révéler et à mettre en évidence les cas où une entité aurait éludé ou cherché à cacher certains éléments. Pour éviter toute dissonance il est important que les éléments de communication soient partagés en interne afin de diffuser un message unique.

En interne comme en externe, on évite de mettre en avant un processus de recherche de responsabilité. Il faut se montrer solidaire avec toutes les parties prenantes de la crise et ne pas pointer du doigt un prestataire ou un collaborateur.

Si la communication donne lieu à une conférence de presse, voire à un passage télévisé, il est absolument nécessaire de bien préparer le porte-parole de l'organisation en travaillant ses messages clés et en réalisant de nombreux entraînements en amont de l'interview. Même si l'organisation est en pleine crise, il ne faut pas négliger cette préparation. Ce porte-parole doit avoir en tête les grandes décisions stratégiques qui ont été prises lors de la crise et échanger avec le DSI pour comprendre le plan d'action mis en place et les impacts qui l'accompagnent.

4 PRÉPARER LA SORTIE DE CRISE

La sortie de crise cyber se constate en fonction de critères définis au début de la crise. Ces critères concernent généralement la fin de ses conséquences sur l'activité de l'entreprise et la réparation totale ou partielle du SI. La sortie de crise peut se poursuivre pendant des mois, voire des années. En effet, une fois les impacts de la cyberattaque réparés, l'objectif est d'améliorer la sécurité du SI. La sortie de crise rime donc souvent avec des investissements importants de cybersécurité pour l'entreprise. Le rôle de la DSI est également d'accompagner la Direction Juridique dans le processus judiciaire qui a été enclenché pendant la crise.

4.1 ACCOMPAGNER LA PROCÉDURE JUDICIAIRE[7]

À la suite de la plainte de l'organisation et grâce aux informations collectées par la DSI, une procédure judiciaire est lancée pour identifier et juger le ou les auteurs de la cyberattaque. Malheureusement, ces procédures sont rarement concluantes.

4.1.1 CYBERATTAQUE : QUE DIT LE CODE PÉNAL ?

La qualification de l'infraction est une première étape de la procédure. En fonction de la typologie de l'attaque et de ses conséquences, plusieurs infractions pénales peuvent être retenues à l'encontre des hackers, en particulier :

- **Extorsion de fonds** : l'article 312-1 du Code pénal stipule : « l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. L'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende ».

En effet, les cyberattaques se caractérisent par une contrainte physique – le blocage de l'ordinateur ou de ses fichiers – obligeant à une remise de fonds non volontaire.

- **L'atteinte à un système de traitement automatisé de données (STAD)**, selon l'article 323-1 du Code pénal :
    - « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 euros d'amende.
    - Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.
    - Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende ».

[7] Cette partie est une synthèse de l'intervention de Maître Corinne Thiérache.

Depuis 2013, la détention ou la cession d'un rançongiciel, sans motif légitime, est passible des mêmes peines (article 323-3-1 du Code pénal).

- Dans le cadre des atteintes aux STAD (systèmes de traitement automatisés de la donnée), la **circonstance aggravante de bande organisée est très souvent retenue** (article 323-4-1 du Code pénal).

En effet, la commission de ces infractions requiert en principe la mise en œuvre de différentes compétences et donc l'intervention de plusieurs personnes pour la conception, l'injection du code malveillant, l'expédition du mail infecté ou encore la collecte de la rançon.

La qualification d'infraction pénale pour les parties prenantes, y compris pour celles qui assistent les victimes, est donc particulièrement importante.

4.1.2 DEMANDER LA RÉPARATION DU PRÉJUDICE

En matière de cyberattaque, l'entreprise victime peut traditionnellement invoquer plusieurs chefs de préjudice (financier, moral et matériel). Le **préjudice financier** peut couvrir, selon les cas :

- Les gains manqués qui affectent l'exploitation de l'entreprise : ils peuvent concerner la privation ou le défaut de trésorerie, la rupture d'approvisionnement, etc. ;
- La perte de chance de réaliser un gain : elle peut notamment être invoquée lorsque l'activité est mise à l'arrêt ou lorsque l'entreprise a perdu un contrat ;
- Le surcoût : il peut être invoqué lors d'un dysfonctionnement de l'entreprise.

La réparation du **préjudice moral** suppose, pour une personne morale, de « démontrer la dégradation concrète de sa réputation ou de son image auprès de ses clients » (Cour d'appel de Versailles, 9ème ch., 30 juin 2021).

Un contrôle strict est effectué sur les justificatifs fournis par la victime. Il est par conséquent indispensable, pour la victime d'une cyberattaque, de réunir les éléments matériels attestant des différents préjudices en lien avec ce type de sinistre.

Toutefois, alors que les entreprises sont souvent lourdement condamnées par les autorités compétentes pour n'avoir pas comblé des failles dans leurs systèmes de sécurité (à titre d'exemple, la société British Airways a été condamnée en juillet 2019 par l'*Information Commissioner's Office* (ICO) à une amende record de 20 millions de livres, du fait d'une enquête menée postérieurement à une cyberattaque massive touchant les données de près de 400 000 personnes, et qui a révélé que la compagnie aérienne n'avait pas suffisamment sécurisé les données de ses clients), **les condamnations des auteurs de cyberattaques sont plus rares et moins significatives** :

- Cour de cassation, Chambre criminelle, 7 novembre 2017, 16-84. 918 : Rejet du pourvoi formé par M. Pierrick Y., contre l'arrêt de la Cour d'appel de Paris, chambre 4-11, en date du 30 juin 2016, qui, pour participation à une entente établie en vue de la préparation d'une entrave au fonctionnement d'un système automatisé de données, l'a condamné à une peine de deux mois d'emprisonnement assortis du sursis avec mise à l'épreuve et s'est prononcé sur les intérêts civils.

Dans cette affaire, le portail Internet de l'Opérateur d'Importance Vitale (O. I. V.) EDF avait fait l'objet en avril 2011 d'une attaque dite par « déni de service distribué », dans le cadre d'une offensive d'envergure menée par l'organisation « Anonymous », et apparaissant sous l'intitulé « Opération

Greenrights » poursuivi du chef de participation à des ententes établies en vue de la préparation d'entraves au bon fonctionnement de STAD.

- TGI Nîmes, 28 juin 2013, n°13/1677 : Condamnation pour accès et maintien frauduleux dans un système de traitement automatisé de données (STAD) d'un étudiant en informatique qui avait conçu et mis à disposition sur Internet le logiciel « TUBEMASTER ++ » permettant l'enregistrement de fichiers diffusés en streaming par le site Deezer au mépris des droits d'auteur. Son outil analysait les flux en provenance de la plate-forme Deezer et récupérait la clé de déchiffrement utilisée par le logiciel d'écoute de ces flux installé sur le poste de l'utilisateur.

Le prévenu a été condamné à une amende de 15 000 €, au paiement à la société Blogmusik de dommages et intérêts s'élevant à 7 285, 02 € ainsi que 5 000 € pour le préjudice moral et à 5 000 € de dommages et intérêts pour chacune des autres parties civiles (SACEM, SDRM, SCPP).

Enfin, même en cas de condamnation, il faudra encore que la décision soit exécutée et que les éventuels dommages et intérêts soient obtenus par la partie victime d'une cyberattaque.

4.2 RECONSTRUIRE LE SYSTÈME D'INFORMATION

Au cœur de la crise, il faut également définir une stratégie de reprise. Il faut donc définir des priorités (si celles-ci n'avaient pas été déterminées avant la crise), certaines s'imposent comme la paie des collaborateurs, le paiement des fournisseurs et la poursuite de l'activité principale. Cette reprise ne doit intervenir qu'au moment où l'on s'est assuré que les systèmes sont de nouveau bien sécurisés.

Une fois que la reprise est effectuée, la DSI a pour objectif d'améliorer le SI de manière durable en termes de cybersécurité. Les projets mis en place peuvent être les suivants :

- Élévation du niveau de sécurité de l'Active Directory et limitation des comptes à privilèges (travaux qui peuvent être menés en collaboration avec l'ANSSI) ;
- Refonte des pratiques d'administration et utilisation de technologies d'authentification multifacteurs ;
- Déploiement de la technologie EDR sur tous les serveurs et PC. Si certains vieux systèmes ne supportent pas l'EDR, il faut néanmoins les protéger par d'autres solutions ;
- Cloisonnement des infrastructures centrales et locales ;
- Maîtrise des flux ;
- Nettoyage des réseaux mondiaux et restauration des serveurs.

5 LES BONNES PRATIQUES DE LA GESTION DE CRISE CYBER

Sur le plan technique **:**

- Définir des critères de sortie de crise.
- Ne pas s'attarder sur les investigations afin d'assouvir sa curiosité technique mais chercher à se prémunir d'une récidive de l'attaque.
- Ne pas chercher le responsable en interne de la cyberattaque pendant la crise, cette recherche a lieu pendant le retour d'expérience.
- Dans un premier temps, endiguer l'attaque, puis y remédier. Il ne faut pas confondre les deux temps.
- Percevoir la crise comme une opportunité pour augmenter le niveau de sécurité du SI.

Sur la gestion des équipes :

- Ne pas sous-estimer la fatigue des collaborateurs engagés dans la gestion de crise.
- Gérer le stress des équipes et agir rapidement et efficacement en cas de comportement qui entrave la gestion de crise.
- Organiser un système de roulement des équipes pour que personne ne soit absolument indispensable.
- Faciliter la vie des collaborateurs en gérant les aspects logistiques (ouverture des locaux 24h/24, ouverture du restaurant d'entreprise du matin au soir…)
- Prendre rapidement les décisions pour faciliter le travail des équipes opérationnelles.
- Faire preuve d'une certaine souplesse : ne pas hésiter à changer de stratégie si celle entreprise ne fonctionne pas.
- Impliquer les équipes métiers dans les processus et communiquer un maximum d'informations en interne.
- Préserver les équipes techniques des communications des cellules de crise, pour qu'elles ne risquent pas de les parasiter.
- Faire appel à des prestataires pour soulager les équipes et apporter de l'expertise.

Sur la communication de crise :

- Disposer d'un système de communication alternatif au réseau principal.
- Communiquer en interne, primordial pour éviter toute fuite d'informations en externe.
- Communiquer vers l'écosystème (fournisseurs, clients…) dès que les conséquences de la crise sont connues.
- La communication vers les médias est à envisager, mais elle doit répondre à un objectif précis et doit faire l'objet d'une préparation minutieuse.

Sur le plan juridique

- S'acquitter de ses obligations légales dès que la crise est connue : prévenir l'ANSSI, notifier la CNIL, porter plainte.
- Collecter et conserver les preuves nécessaires à la procédure judiciaire.
- S'acquitter de ses obligations contractuelles de prévenance lors d'une suspicion d'agression ou d'agression avérée.

6 CONCLUSION

Les entreprises et administrations publiques sont de plus en plus confrontées à des cyberattaques. Les conséquences sont multiples, sur l'activité de l'entreprise et sur ses collaborateurs, mais elles sont aussi financières et réputationnelles. Une cyberattaque de grande ampleur n'est pas caractérisée par le mode opératoire utilisé mais par les impacts qu'elle peut avoir sur l'organisme attaqué et sur tout son écosystème.

Les premiers temps de la crise sont primordiaux pour limiter la propagation de la cyberattaque car c'est le moment où l'organisation interne se met en place et où les premières orientations stratégiques sont prises. Même s'il s'agit d'une crise d'origine informatique, la DSI n'est pas la seule direction impliquée dans le processus de gestion de crise. Elle se doit de collaborer avec les autres directions et de leur relayer un maximum d'informations. Mettre en place une communication transversale dès le début de la crise est essentiel pour réussir sa gestion de crise.

Le fort de la crise peut durer quelques jours comme quelques semaines. Bien que le cœur des opérations soit à la DSI, il ne faut pas négliger les directions métiers. Quand la crise dure, les équipes sont sous tension et se fatiguent rapidement. Gérer les équipes en intégrant tous les aspects logistiques essentiels évite une surenchère à la crise cyber. De la même manière, une crise qui s'allonge augmente les chances d'une médiatisation du sujet. Mettre en place une communication de crise précise peut éviter une crise réputationnelle.

La sortie de crise cyber peut durer des mois, voire des années. Quand la crise est passée, il est temps de renforcer la sécurité du système d'information et d'accompagner le processus juridique.

Gérer une crise cyber ne s'improvise pas, anticipation et préparation sont nécessaires pour y parvenir avec succès, mais les organisations ne sont jamais suffisamment préparées. La cyberattaque peut se produire au mauvais moment, avoir des conséquences imprévues, et lorsqu'elle advient, il n'est plus temps d'organiser des exercices de crise ou de revoir ses plans de continuité d'activité. Se mettre en situation de réaction de crise, tel que nous l'avons fait dans le groupe de travail, prend alors tout son sens.

La multiplication du nombre d'organismes victimes de cyberattaque a au moins permis de libérer la parole. Ces témoignages d'organisations permettent de faire émerger des pratiques et conseils opérationnels à diffuser largement pour augmenter le niveau global de cybersécurité.

7 ANNEXES

7.1 RÉALISATION D'UN CHRONOGRAMME

Dans le cadre de ce groupe de travail, nous avons réalisé un atelier qui s'apparente à un exercice de gestion de crise. Lors de cet exercice, les participants ont été placés dans le contexte d'une grande entreprise devant faire face à une attaque de type *ransomware* et ont été amenés à réagir face à l'évolution de la situation. Nous nous sommes concentrés sur les premiers instants de la crise. Vous trouverez le résultat de cet exercice dans le tableau ci-dessous, que vous pouvez adapter à votre organisation afin simuler une gestion de crise. Si vous souhaitez organiser un exercice de gestion de crise, vous pouvez vous appuyer sur la fiche pratique de l'ANSSI.

Horaire	Évènement	Actions/Décisions	Acteurs impliqués
17H00	Ordinateurs inutilisables par certains collaborateurs.	1. Qualifier l'incident 2. Isoler tous les postes de travail du département concerné grâce à l'EDR	1. Pré-mobilisation de la cellule de crise 2. Direction de gestion des risques 3. Direction de gestion de crise 4. Plusieurs acteurs de la DSI : ● le centre d'assistance informatique ● l'équipe de la sécurité opérationnelle ● le responsable de production ● le responsable réseau ● le responsable Windows et poste de travail
17H15	Attaque par ransomware : chiffrement des données et demande de rançon.	1. Isoler tous les systèmes et couper les moyens de propagation 2. Déclenchement de la cellule de crise cyber 3. Investiguer sur le périmètre touché	1. Autorités compétentes des pays concernés 2. La cyberassurance (selon contrat) 3. Les membres de la cellule de crise (cf. composition plus haut)
17H45	Propagation du virus dans tous les départements du groupe.	1. Communiquer ces informations aux fournisseurs et clients 2. Isolation complète des systèmes 3. Arrêter et isoler les sauvegardes 4. Déposer plainte	1. Déploiement de la cellule de crise groupe, si ce n'est pas déjà le cas
17H50	Annonce de la cyberattaque sur un réseau social.		1. Direction de la communication
18H00	Demande de visibilité de la part du COMEX et des métiers.	1. Publication d'un tableau de bord synthétique mise à jour régulièrement communiqué à tous les membres de la cellule de crise 2. Points réguliers au sein de la cellule de crise	CELLULE DE CRISE
18H12	Le comex réalise qu'une opération critique est à réaliser dans 2 jours. (ex : paiement des salaires)	1. Activer le plan de continuité d'activité 2. Proposer une solution de fonctionnement en mode dégradé	
18H30	Attaque revendiquée par un groupe de cybercriminels et données publiées sur le *darkweb*.	1. Analyse du type de données volées	

Figure 7 : Chronogramme synthétique réalisé à l'occasion d'un atelier sur la gestion de crise

7.2 PETIT MEMO DES OUTILS PROPOSÉS PAR LES PARTICIPANTS

7.2.1 QUE FAIRE DÈS L'AVÈNEMENT DE LA CRISE ?

Voici une check-list de choses à faire ou à penser lorsqu'une cyberattaque a été détectée :

- Identifier le périmètre de la crise et stopper la propagation le plus rapidement possible ;
- Déployer un outil de communication alternatif au SI ;
- Selon le périmètre de la crise, communiquer le plus largement possible les éléments dont vous disposez (à minima en interne, puis aux fournisseurs et aux clients, et éventuellement à la presse) ;
- Déployer les cellules de crise décisionnelle et opérationnelle ;
- Activer le plan de continuité d'activité ;
- Proposer un premier plan d'action et un tableau de bord synthétique pour décrire la situation initiale, à l'actualiser en fonction des avancées ;
- Prévenir son cyberassureur ;
- Prévenir l'ANSSI ;
- Préparer l'organisation de la crise (points réguliers) et gérer les aspects logistiques (hébergement, nourriture, ouverture des locaux pour les équipes).

7.2.2 ANTICIPATION : QUE FAIRE EN AMONT D'UNE CRISE CYBER ?

Bien que l'anticipation ne soit pas le cœur de la réflexion de ce rapport, nous avons quand même établi une liste des « choses à faire » absolument, en amont d'une crise cyber (l'ordre ne correspond pas à un degré d'importance) :

- Disposer d'un annuaire des coordonnées des autorités compétentes selon les pays d'implantation de l'organisation (ANSSI, CNIL, FBI…), du cyberassureur, de ses prestataires externes… ;
- S'assurer d'avoir accès au PCA métier ;
- Avoir un moyen de communication alternatif au SI ;
- Disposer d'un annuaire des membres de la cellule de crise ;
- Organiser des formations à la gestion de crise ;
- Prévoir l'organisation de la cellule de crise et identifier plusieurs personnes pour chaque poste ;
- Sensibiliser les collaborateurs à la cybersécurité ;
- Prévoir un format de reporting (tableau de bord, « météo »…) ;
- Disposer de *backups offline* sur des « SI indépendants », y compris dans les contrats des offres souscrites en SaaS ;
- Disposer des éléments clés de la constitution du SI : schémas d'architecture, cartographie des flux, plan d'adressage réseaux, inventaire des actifs (propriétaire, sensibilité, métier concerné…) ;
- Identifier une liste de prestataires en capacité d'intervenir en *forensics* ;
- Rédiger et afficher une fiche réflexe des premières actions à entreprendre ;
- Prévision des aspects logistiques (taxis, nourriture, hôtels, accès aux sites en 24/7…) ;

- Tous les documents et listes doivent être imprimés et accessibles, même en cas d'indisponibilités du SI.

7.3 BIBLIOGRAPHIE : QUELLES RESSOURCES POUR AMÉLIORER SON DISPOSITIF DE CRISE ?

Les principaux guides publiés par l'ANSSI sur la gestion de crise cyber :

- TOP 10 des vulnérabilités 2021.
- Panorama de la menace informatique 2021.
- Campagne d'attaque du mode opératoire APT31 : description, contre-mesures et code.
- État de la menace rançongiciels à l'encontre des entreprises et institutions.
- Points de contrôle Active Directory.
- Recommandations de sécurité pour l'architecture d'un système de journalisation.
- Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory.
- Panorama des métiers de la cybersécurité.
- Organiser un exercice de crise cyber.
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique.
- Anticiper et gérer sa communication de crise cyber.

Sur la gestion de crise cyber :

- Les fondamentaux de la gestion de crise cyber, Laurane Raimondo, Ellipses, 2022.
- Plan de continuité des activités et gestion de crise, Cécile Weber, Afnor, 2021.
- Cyber-crise, bonnes pratiques dans la gestion de crises de cybersécurité, CCN-CERT, 2020.
- Fuite de données : gestion de crise, mode d'emploi, Guillaume Tissiers, CEIS, 2018.
- Common practices of EU-level crisis management and applicability to the cyber crises, ENISA, 2016.

Sur la cyberassurance et les aspects juridiques :

- Etude LUCY : LUmière sur la CYberassurance d'AMRAE, Mai 2021 .
- Rapport sur l'assurabilité des risques cyber, Haut Comité Juridique de la Place Financière de Paris, 28 janvier 2022.
- Règlement général sur la protection des données, 27 avril 2016.
- Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, version révisée et adoptée le 6 février 2018.
- Notification d'incidents de sécurité aux autorités de régulation : comment s'organiser et à qui s'adresser ? CNIL, 18 mai 2020.
- Rapport d'information fait au nom de la délégation aux entreprises relatif à la cybersécurité des entreprises, Sébastien Meurant et Rémi Cardon, Sénat, 10 juin 2021.
- Le droit pénal à l'épreuve des cyberattaques, Le clubs des juristes, Avril 2021.
- La Cyber-assurance, Valéria Faure-Muntian, Assemblée Nationale, 2021.
- Code de la cybersécurité, Dalloz, 2022.

Cigref
RÉUSSIR
LE NUMÉRIQUE

Au service de la croissance économique et de la compétitivité de nos membres, grandes entreprises et administrations publiques françaises, utilisatrices de solutions et services numériques, par la réussite du numérique

Le Cigref est un réseau de grandes entreprises et administrations publiques françaises qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un acteur fédérateur de la société numérique. Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative.

Pour réussir sa mission, le Cigref s'appuie sur trois métiers, qui font sa singularité.

Appartenance
Le Cigref incarne une parole collective des grandes entreprises et administrations françaises autour du numérique. Ses membres partagent leurs expériences de l'utilisation des technologies au sein de groupes de travail afin de faire émerger les meilleures pratiques.

Intelligence
Le Cigref participe aux réflexions collectives sur les enjeux économiques et sociétaux des technologies de l'information. Fondé il y a près de 50 ans, étant l'une des plus anciennes associations numériques en France, il tire sa légitimité à la fois de son histoire et de sa maîtrise des sujets techniques, socle de compétences de savoir-faire, fondements du numérique.

Influence
Le Cigref fait connaître et respecter les intérêts légitimes de ses entreprises membres. Instance indépendante d'échange et de production entre praticiens et acteurs, Il est une référence reconnue par tout son écosystème.

www.cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr