RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

COLLECTION
GESTION DE CRISE CYBER

ANTICIPER ET GÉRER SA COMMUNICATION DE CRISE CYBER

CAP'COM LE RÉSEAU DE LA COMMUNICATION PUBLIQUE ET TERRITORIALE

COLLECTION
GESTION DE CRISE CYBER

GUIDE

ANTICIPER ET GÉRER SA COMMUNICATION DE CRISE CYBER

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité. Rattachée au secrétaire général de la défense et de la sécurité nationale, elle assure des missions de prévention, d'information, de sensibilisation et de défense. L'ANSSI s'adresse principalement aux opérateurs critiques, du public comme du privé.

SOMMAIRE

ÉDITORIAL

Au fil des années, les attaques informatiques deviennent plus intenses et plus sophistiquées. Toutes les organisations savent aujourd'hui qu'elles risquent, un jour ou l'autre, d'y être confrontées. De plus en plus, elles s'y préparent. Pourtant, lorsque la crise survient, on constate trop souvent que l'action des communicants passe au second plan. C'est une erreur.

Pour une gestion globale de la crise, il est en effet indispensable que la communication travaille main dans la main avec la réponse technique. Prenons le cas, désormais tristement commun, d'une attaque par rançongiciel. Entraînant de profondes conséquences sur le fonctionnement de l'organisation (indisponibilité des outils de travail, compromission de données, etc.), elle est visible immédiatement et peut engendrer une forte médiatisation. Dans une situation qui peut vite devenir anxiogène, intégrer en amont la fonction communication, aussi bien interne qu'externe, est alors plus qu'essentiel pour prendre en compte les réactions médiatiques, politiques et sociétales… et ne pas ajouter une crise à la crise.

Les attaquants eux-mêmes se mettent à la communication en diffusant des communiqués ou en organisant des conférences de presse ! Derrière cette communication se cache en réalité un effet de levier, qui rappelle que les attaques cyber concernent tous les métiers et tous les secteurs.

Ce guide, fruit de l'expérience de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), ne fera pas de vous un expert cyber. L'enjeu est de vous aider à comprendre les spécificités des crises cyber afin de mieux les appréhender au sein de votre stratégie de communication de crise. Avec un maître mot : l'anticipation.

Guillaume Poupard
Directeur général de l'ANSSI

L'océan numérique peut nous porter loin et partout. Il peut aussi se déchaîner : le piratage et bien d'autres attaques cyber font alors perdre les outils qui maintenaient des repères. Dans l'urgence, on cherche à éviter la cacophonie. Les communicants publics sont alors souvent sollicités, autant en externe pour communiquer sur la crise qu'en interne pour acheminer l'information, pour improviser de nouveaux circuits, pour maintenir une écoute.

On oublie peut-être que la communication elle-même est une prise de risque. S'avancer vers l'autre, c'est s'exposer en quittant le confort de la sécurité. Et pourtant le dialogue, dans tous ses aléas, dans toute l'insécurité qui l'entoure, est ce qui permet de maintenir le lien et la compréhension mutuelle, indispensables au fonctionnement de notre société.

Habitués aux enjeux de toute relation, les communicants doivent ainsi être mobilisés au cœur du dispositif dans le cas d'une attaque cyber, où la compréhension inter-équipes est clé. Leur connaissance des usages en temps de crise est un atout et leur expertise y est cruciale : aller au contact – des agents, des citoyens et des élus – reformuler, vulgariser, restituer. En cela, ils doivent-être reconnus, eux-mêmes sensibilisés à la maîtrise du risque, y compris à titre personnel, et ils doivent partager leurs expériences en réseau.

Cette exigence d'exemplarité demande une mise à niveau constante et une attitude humble, comme celle du marin au moment de prendre le large. Confronté à une crise cyber, il faut savoir compter sur la compétence de tous pour construire des solutions efficaces et fédératrices.

Yves Charmont
Délégué général de Cap'Com

PRÉSENTATION

Face à une attaque, la technicité d'une crise cyber peut déstabiliser les plus aguerris des communicants, confrontés à des codes, des enjeux et à un écosystème parfois très éloignés de leur cœur de métier.

Tout en s'attardant sur les spécificités liées au cyber, ce guide tend à démontrer qu'une bonne communication de crise cyber reprend avant tout les réflexes et les outils communs à toute stratégie de communication de crise.

À quoi sert ce guide ?

En se basant sur les situations rencontrées par l'ANSSI depuis sa création en 2009 dans son rôle d'assistance auprès de victimes, ce guide vise à apporter des conseils et des recommandations très opérationnels afin de construire puis de déclencher le volet communication de crise lors d'une attaque informatique.

Si aucune recette magique n'existe en gestion de crise, quelques réflexes et certaines notions essentielles peuvent être intégrés dès aujourd'hui par votre organisation, privée ou publique, afin d'être prêt à faire face à une crise cyber.

Les recommandations de ce guide sont ainsi également adaptées à la gestion de situations qualifiées de « sensibles », qui précèdent souvent une éventuelle crise médiatique.

À qui s'adresse-t-il ?

Ce guide s'adresse à toutes les personnes occupant une fonction de communicant lors de la gestion d'une crise. En fonction de la taille et de l'organisation de l'entité, il peut s'agir d'un professionnel de la communication (DIRCOM, chargé de communication ou agence de communication), mais parfois aussi d'autres profils (cabinet, juriste, décideur), faute de communicants. Selon la situation, l'équipe opérationnelle peut même parfois jouer ce rôle de communicant.

Si ce guide s'adresse en premier lieu aux professionnels de la communication, qui ont un rôle clé à jouer en matière de gestion de crise, il a également pour objectif de donner des outils et des conseils à d'autres métiers, techniques et décisionnels, pouvant intervenir aux côtés des communicants.

Quels sont les prérequis ?

Ce guide vise à apporter un éclairage sur les spécificités d'une communication de crise cyber, telles que perçues par l'ANSSI. Il n'a pas pour objectif de revenir en détails sur la construction d'une stratégie de communication de crise en général. Ce travail doit être idéalement réalisé et testé en amont afin de pouvoir adapter l'organisation et les outils à la singularité d'une crise cyber.

Ce guide propose cependant quelques rappels des fondamentaux de la communication de crise pour familiariser l'ensemble des lecteurs aux notions et aux enjeux clés poursuivis par la fonction communication.

Et d'ailleurs, qu'est-ce qu'une crise cyber ?

Une crise « d'origine cyber » se définit par la déstabilisation immédiate et majeure du fonctionnement courant d'une organisation (arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes, perte d'intégrité majeure, etc.) en raison d'une ou de plusieurs actions malveillantes sur ses services et outils numériques[1] (cyberattaques de type rançongiciel, déni de service - DoS, etc.). C'est donc un évènement à l'impact fort, qui ne saurait être traité par les processus habituels et dans le cadre du fonctionnement normal de l'organisation. Par convention, on parlera par la suite de « crise cyber ».

1. Auxquels sont associés les SI de l'organisation et ceux de ses prestataires.

EN ANTICIPATION

ÉTAPE 1 : initier un dialogue avec les équipes cyber et IT hors période de crise (fiche 1 – p. 12)

ÉTAPE 2 : anticiper les scénarios de crise et les réponses à apporter sur le volet communication (fiche 2 – p. 16)

ÉTAPE 3 : concevoir sa stratégie de communication de réponse à la crise (fiche 3 – p. 20)

ÉTAPE 4 : intégrer la fonction communication dans l'organisation d'une gestion de crise cyber (fiche 4 – p. 24)

ÉTAPE 5 : organiser la communication de crise (fiche 5 – p. 26)

ÉTAPE 6 : créer une boîte à outils dédiée à la gestion d'une crise cyber (fiche 6 – p. 28)

ÉTAPE 7 : former ses équipes à la gestion du volet communication (fiche 7 – p. 30)

Gérer efficacement votre communication de crise, c'est surtout l'anticiper pour permettre rapidité d'action et agilité lorsque la crise survient. En amont de la crise, lorsque les temps sont plus calmes et propices à la réflexion et aux changements, sept étapes sont à adopter et à séquencer selon le rythme propre à votre organisation, en fonction de sa taille et de son fonctionnement. Les fiches pratiques suivantes vous aideront à préparer ces étapes.

ÉTAPE 1

INITIER UN DIALOGUE AVEC LES ÉQUIPES CYBER ET IT HORS PÉRIODE DE CRISE

Lorsque survient une crise cyber, les équipes cyber et IT, dont le responsable de la sécurité des systèmes d'information (RSSI)[2], sont fortement mobilisées aux côtés des acteurs de la gestion de crise.

Faire connaissance dans ces conditions est compliqué. Pourtant, en tant que communicant, vous ne serez pas le seul à « communiquer » : différents fils d'information sortiront de votre organisation à destination des collaborateurs, des prestataires, des partenaires, etc. Pour assurer une cohérence d'ensemble le jour J, il est indispensable de comprendre **les priorités, les enjeux et le langage de chaque métier.**

Pour plus de confort, ce dialogue gagne à être initié en amont d'une crise réelle, en phase de préparation. Si le communicant doit s'adapter aux spécialistes, ces derniers doivent aussi comprendre le contexte global dans lequel s'inscrit la réponse à incident, potentiellement soumis à plusieurs sources de perturbation (pression médiatique y compris via les réseaux sociaux, politique, métiers) en ajoutant un risque de crise médiatique ou sociale à la crise cyber.

2. Le RSSI définit et développe la politique de sécurité de l'information d'une entreprise, d'un établissement public ou encore d'une collectivité territoriale.

Avant toute chose, il faut se poser les questions suivantes : qui est en charge de la sécurité informatique au sein de mon organisation ? Des travaux communs ont-ils déjà eu lieu pour anticiper les risques cyber ? Mon organisation a-t-elle déjà été victime d'une attaque cyber ?

En l'absence d'équipe(s) en interne, des prestataires de proximité ou des dispositifs comme Cybermalveillance.gouv.fr[3] peuvent donner des clés de compréhension.

Recommandation

Cette acculturation mutuelle peut se réaliser sous différentes formes : ateliers de travail dédiés, définition d'une campagne de sensibilisation interne (et pourquoi pas en octobre pendant le Cybermoi/s !) ou organisation d'exercice(s) de gestion de crise cyber[4].

3. Le dispositif Cybermalveillance.gouv.fr a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, ainsi que de les informer sur les menaces numériques et les moyens de s'en protéger.
4. Pour en savoir plus, consultez le guide de l'ANSSI *Organiser un exercice de gestion de crise cyber.*

FOCUS

UNE CRISE, PLUSIEURS ANGLES DE VUE

Les impacts d'une crise cyber peuvent être visibles immédiatement à la suite de l'arrêt d'un ou de plusieurs services ou de la perturbation des outils bureautiques.

	DU POINT DE VUE DU COMMUNICANT
Les questionnements	Pour les usagers, les collaborateurs ou encore les commentateurs politiques ou médiatiques, les questions sont nombreuses : que s'est-il passé ? Qui est responsable de l'attaque ? Quel est l'impact ? En tant que client ou partenaire, puis-je être victime à mon tour ? Pourquoi nous ? Mais que fait la DSI, le RSSI ? Quel risque d'image pour notre organisation ? Quel impact financier pour notre organisation ? Les questions et le nombre d'interlocuteurs s'accumulent au fil de la crise. Les crises cyber génèrent d'autant plus d'anxiété que le sujet reste relativement récent et peu maîtrisé par le grand public, laissant place à beaucoup de confusion (peur de la propagation d'un virus, attribution rapide à des acteurs étatiques, etc.).
Les actions	Face à cette pression, le communicant doit : ▸ Accompagner les équipes en charge de la gestion de crise en prenant à sa charge certains publics (interne, médias) afin de laisser les équipes opérationnelles gérer les impacts métiers de la crise. Souvent oubliée, la communication interne est aussi fondamentale lors de la gestion d'une crise : il faut informer et rassurer les collaborateurs touchés directement ou indirectement par la crise en cours. ▸ Transmettre des informations fiables, vérifiées et adaptées à la situation sur la base des éléments de compréhension fournis par les équipes cyber et la direction de crise. Or, la compréhension de l'incident et les actions de remédiation prennent du temps, ce qui peut être difficile à expliquer sur plusieurs semaines, voire plusieurs mois. ▸ Préserver la réputation de l'entité : la communication a également comme mission de veiller à l'image de l'entité, souvent dégradée par la crise, et de s'assurer qu'elle ne se dégrade pas davantage par la propagation de rumeurs ou de fausses informations.

Lorsqu'une crise survient, plusieurs acteurs entrent en jeu et proposent une lecture différente de la crise en cours et de son origine potentielle.

DU POINT DE VUE DES ÉQUIPES CYBER ET IT

Les questions s'accumulent vite du côté des équipes cyber et IT : que se passe-t-il exactement ? Comment l'attaque a-t-elle pu franchir les mesures de sécurité en place ? Est-ce que l'attaque peut se propager à différents SI au sein de mon organisation ou à d'autres entités via les interconnexions ?

L'une des caractéristiques des attaques cyber est le temps d'investigation puis de remédiation qui peut être très long. Les analyses techniques ont des délais malheureusement incompressibles. Si les effets d'une attaque sont immédiats, le travail des équipes opérationnelles est fastidieux, d'autant plus qu'elles sont sous pression et avec un effectif souvent restreint.

À noter qu'il existe en général une phase de déni puis une phase de recherche de coupables. Il faut impérativement ne pas tomber dans cette spirale infernale et se concentrer sur les analyses qui permettront de remonter les services critiques. Dans un second temps uniquement, il peut être pertinent de rechercher l'origine de l'attaque.

Cette compréhension de l'incident n'est que le début d'une longue phase de remédiation :

- comprendre la situation : les équipes lancent des investigations pour déterminer les causes et l'étendue de l'attaque ;
- reconstruire de façon maîtrisée les SI endommagés sur des bases saines pour éviter une réplique de l'attaque ;
- revoir en profondeur les mesures de sécurité informatique en place afin de prévenir le succès d'une autre tentative d'attaque.

Certaines organisations peuvent mettre plusieurs mois avant de pouvoir rétablir l'intégralité de leurs services en toute sécurité[5]. Pendant ce temps, la communication doit pouvoir suivre et accompagner les équipes dans cette course de fond.

5. Pour en savoir plus, consultez le guide de l'ANSSI *Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique.*

ÉTAPE 2

ANTICIPER LES SCÉNARIOS DE CRISE ET LES RÉPONSES À APPORTER SUR LE VOLET COMMUNICATION

Chaque organisation est amenée à conduire une analyse des risques menaçant de déstabiliser ses activités[6]. Face à ces risques, des réponses sont apportées, notamment en matière de communication. À l'aide des acteurs impliqués dans la gestion de crise, en particulier des équipes cyber et IT, plusieurs scénarios de crise réalistes peuvent être anticipés afin de réfléchir aux processus de gestion du volet communication de crise.

C'est un exercice d'autant plus intéressant à réaliser pour les crises cyber qu'elles semblent difficiles à aborder, car très techniques. Surtout qu'il existe différents types d'attaques informatiques, et autant de réponses différentes à apporter. On ne traite pas une opération d'espionnage (discrète) de la même façon qu'un rançongiciel ou un déni de service (très visibles). De même, la manière d'aborder une attaque dépendra du contexte. La publication des résultats financiers, des négociations salariales, d'événements majeurs pour le secteur (périodes électorales, lancement d'un produit, etc.) sont des éléments décisifs à prendre en compte. Enfin, on ne traite pas de la même façon une attaque qui a des impacts métiers limités à la seule organisation et une attaque qui se propage vers des clients et/ou des partenaires. Il est impossible de couvrir l'ensemble des scénarios, mais procéder à un travail en amont permet, le jour J, d'avoir un premier référentiel sur lequel s'appuyer.

Recommandation

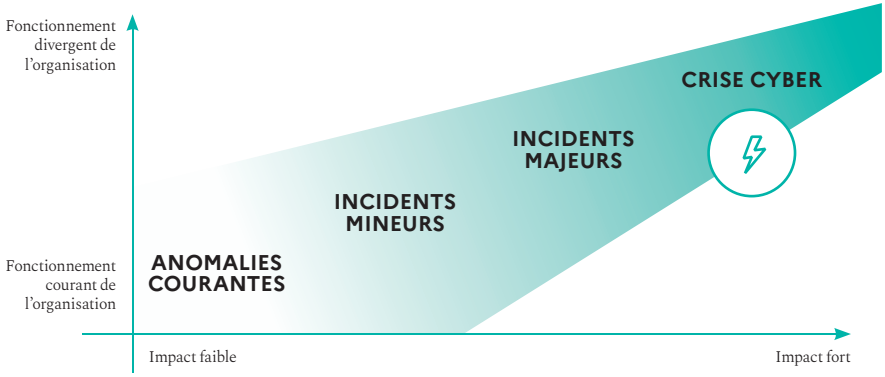
Au-delà des scénarios cyber, vous pouvez lister les événements majeurs et sensibles, ainsi que les problématiques sensibles pour votre organisation et votre secteur d'activité qui pourraient jouer sur vos décisions de communication.

6. Pour en savoir plus, consultez la méthode EBIOS Risk Manager.

LES ÉCHELLES DE GRAVITÉ DANS LE CYBER

On parle de crise cyber lorsqu'une ou plusieurs action(s) malveillante(s) sur le SI génère(nt) une déstabilisation majeure de l'entité, provoquant des impacts multiformes et importants, jusqu'à engendrer parfois des dégâts irréversibles. L'ANSSI distingue plusieurs niveaux de criticité, d'un point de vue technique :

POSITIONNER UNE CRISE CYBER FACE AUX ÉVÈNEMENTS PORTANT ATTEINTE AUX ACTIVITÉS MÉTIERS D'UNE ORGANISATION



À noter cependant qu'en matière de communication de crise, la criticité d'une situation s'apprécie aussi, voire davantage, en termes de pression médiatique, politique, financière, commerciale, interne et sociale subie. Avant une réelle crise cyber, les organisations peuvent être amenées à gérer des situations sensibles en lien avec des problématiques numériques comme, par exemple, la sécurité des données (hébergement, risque de fuite), le choix d'un service ou d'un prestataire potentiellement compromis ou encore une panne informatique « normale ».

ÉTAPE 3

CONCEVOIR SA STRATÉGIE DE COMMUNICATION DE RÉPONSE À LA CRISE CYBER

Une stratégie de communication de crise gagne à se construire à froid. Elle vise avant tout à servir de référentiel et de guide pratique lors de la gestion de la crise qui est marquée par le stress, la pression et la rapidité. On peut identifier plusieurs étapes :

1. Compréhension du **contexte** dans lequel se déroule la crise : cette partie est à adapter à la situation vécue. Les scénarios conçus en amont permettent néanmoins de référencer les questions à se poser le jour J.

2. Définir **les objectifs de communication** (voir l'étape 1 de la partie « En anticipation ») : généralement, il s'agit d'expliquer la situation de façon pédagogique et régulière, de rassurer sur la prise en charge effective de la crise et de préserver l'image et la réputation de l'entité.

3. Identifier **les cibles** de façon exhaustive : ce sont à elles que s'adresseront vos messages, qu'ils soient des acteurs internes (équipes techniques, direction, collaborateurs, actionnaires, prestataires, clients etc.) ou externes (clients, partenaires, autorités, médias, influenceurs, etc.).

4. Identifier **les parties prenantes** : ce sont des acteurs qui pourraient être amenés à communiquer également sur la situation (autorités, clients, prestataires, etc.).

5. Désigner et former de façon continue **le(s) porte-parole(s) représentant(s)** de votre organisation lors d'une crise vis-à-vis des publics externes, notamment les médias.

6. Travailler **les postures de communication** (réactive vs. proactive, ciblée vs. large) ainsi que **les messages** principaux, sous forme d'éléments de langage, à adapter au niveau de criticité de la crise, de l'exposition de l'entité et/ou de la pression médiatique, politique, économique et/ou sociale suscitée.

7. Définir **l'organisation de la communication de crise** et recenser **les outils de communication** à disposition (presse, web, annuaire).

Recommandation

Pour élaborer votre stratégie de communication de crise en cohérence avec l'identité de l'entité, commencez par faire un point sur la stratégie de communication globale de votre organisation.

FOCUS

INTÉGRER LES SCÉNARIOS CYBER À VOTRE STRATÉGIE DE COMMUNICATION DE CRISE

Sur la base des scénarios élaborés avec les équipes cyber et IT, vous pouvez préparer une stratégie de communication de crise en réponse aux situations identifiées en reprenant les mêmes étapes, tout en intégrant les codes et les spécificités du cyber :

1. **Contexte :** anticiper quelques questions, comme de quel incident s'agit-il ? Quels sont les impacts sur les services rendus ? Quelle est l'actualité de mon organisation (publication des résultats, événements majeurs, etc.) ? La partie contexte pourra prendre en compte les réponses aux questions posées à la page 13 (services critiques, etc.).

2. **Objectifs :** vulgariser le vocabulaire technique afin d'apporter une information claire et maîtrisée (les actions de sécurisation, les résultats des premières analyses, etc.).

3. **Publics :** prioriser les communications en fonction de la situation, notamment en cas de risque de propagation.

4. **Parties prenantes** : intégrer les prestataires, souvent mobilisés pour assister à la gestion de la crise. Intégrer les autorités spécialisées (ANSSI, Commission nationale de l'informatique et des libertés CNIL, parquet judiciaire cyber, autorités de régulation) notamment si vous êtes soumis à des obligations réglementaires (OIV, OSE, administrations). wCréer un fichier presse avec les médias, journalistes et influenceurs principaux de l'écosystème cyber, y compris issus de la presse généraliste.

5. **Porte-parole :** former votre/vos porte-parole(s) aux enjeux du cyber.

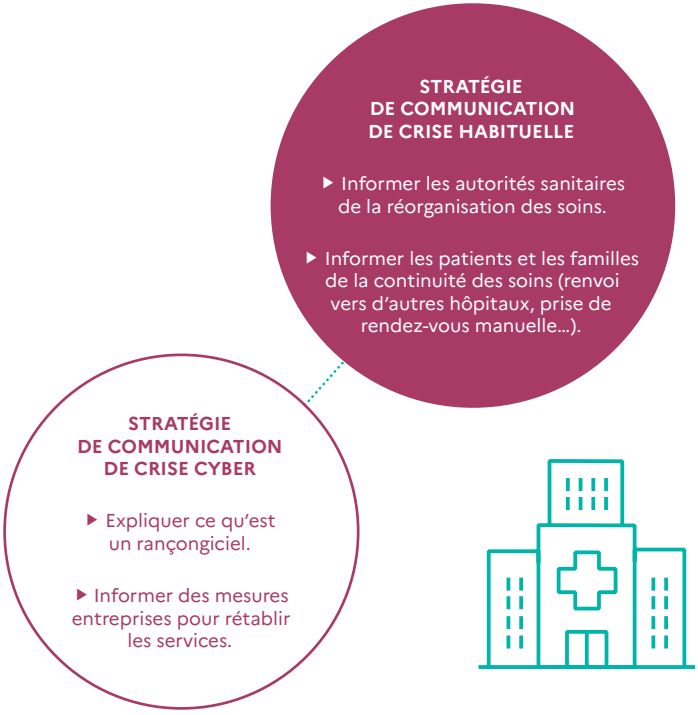
6. **Postures et messages :** se rapprocher des équipes spécialisées pour créer un répertoire de base sur le vocabulaire cyber vulgarisé.

7. **Outils et organisation :** anticiper leur indisponibilité !

Recommandation

La stratégie de communication de crise cyber permet de répondre à une seule facette de la crise, à savoir l'explication des causes, d'origine cyber, de la crise rencontrée. Elle complète de fait d'autres stratégies de réponse s'attachant à la gestion des impacts métiers plus spécifiques à votre domaine d'activité (dysfonctionnement ou fermeture d'un service, rupture de relations commerciales, etc.).

Exemple d'un hôpital, victime d'un rançongiciel qui paralyse son SI bureautique :



ÉTAPE 4

INTÉGRER LA FONCTION COMMUNICATION DANS L'ORGANISATION D'UNE GESTION DE CRISE CYBER

Qu'il s'agisse d'une crise cyber ou non, la communication de crise doit être intégrée dès les premières heures dans le dispositif de gestion de crise global de l'organisation. En tant que communicant, vous avez plusieurs rôles à jouer :

Alerter : vous êtes à l'écoute des tendances ainsi que des réactions sociales et médiatiques sur les sujets d'actualité liés à votre activité. Les premiers signaux d'une crise peuvent venir des médias ou des réseaux sociaux.

Réagir rapidement : lors d'une crise, des messages réfléchis et adaptés aux différents publics, internes et externes, doivent être conçus rapidement, avec l'appui des équipes métiers affectées. Vous êtes déjà familier avec la diversité des publics de votre organisation, qu'ils soient internes ou externes (collaborateurs, dirigeants, actionnaires, membres CA, clients, médias, partenaires, etc.), ainsi que des outils à disposition. Cette expertise est précieuse pour garantir un bon niveau de réactivité.

Analyser et s'adapter : lors de la gestion d'une crise, la communication est vivante et s'adapte aux réactions des publics visés. Cela se traduit par une analyse fine de la perception des publics de la situation et, le cas échéant, des messages transmis par votre organisation.

Cette expertise est partagée avec les autres acteurs de la gestion de crise au sein de plusieurs enceintes dédiées :

- **La cellule stratégique** regroupant la direction et les métiers soutien (juridique, ressources humaines, etc.). On peut y intégrer la communication, les décisions engageant l'image et la réputation d'une organisation étant généralement prises au niveau des décideurs.

- **Les cellules opérationnelles et techniques**, réunissant l'ensemble des métiers impliqués dans la résolution de l'incident sur le temps long. La communication peut s'appuyer sur cette cellule pour obtenir des informations à jour sur la situation opérationnelle.

Retrouvez tous les conseils sur l'organisation de la gestion de crise dans le guide dédié[7].

Une bonne communication de crise ne garantit pas que tout se passera bien, cependant une mauvaise gestion de la communication de crise ne peut qu'aggraver une situation déjà difficile à gérer.

7. Pour en savoir plus, consultez le guide de l'ANSSI *Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique*.

FOCUS

LES ATTAQUES DE DÉSTABILISATION

Une crise cyber peut prendre différentes formes en fonction des motivations des acteurs malveillants. Certaines attaques informatiques, telles que le **DoS** ou la **défiguration** (voir glossaire) de site Internet ont pour objet principal la déstabilisation de l'organisation visée et l'atteinte à sa réputation.

Ces attaques ont des impacts métiers réels, provoquant un dysfonctionnement des services proposés, avec un coût financier parfois non négligeable. Cependant, peu sophistiquées, elles peuvent être détectées et stoppées assez rapidement et elles n'engendrent généralement pas d'impacts à long terme (comme la perte de données ou la destruction du SI).

Elles ont toutefois un **effet symbolique et émotionnel** très important : elles mettent en lumière la vulnérabilité d'un service, voire servent d'étendard pour des hacktivistes aux messages anxiogènes.

Il existe un réel décalage entre **la perception de l'incident**, relayé via les réseaux sociaux et les médias, **et la complexité technique** de l'incident.

Dans ce type de situation, l'expertise « communication » est fondamentale : elle vise à expliquer de façon pédagogique les impacts réels de l'attaque, généralement modérés, afin de rassurer rapidement les publics mobilisés sur la question. En l'absence d'une communication adaptée et mesurée, ces attaques peuvent atteindre leur but final de déstabilisation en provoquant un emballement médiatique et social.

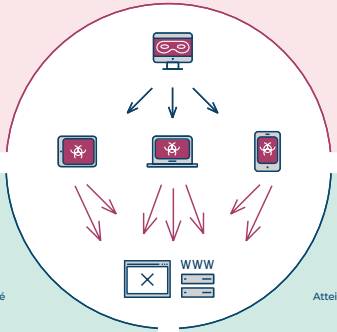
DDOS : ATTAQUE PAR DÉNI DE SERVICE DISTRIBUÉ

L'accès au site que vous consultez est perturbé

QUE SE PASSE-T-IL ?

De nombreuses machines envoient un nombre important de demandes au service et le saturent.

Votre navigation sur le site est fortement ralentie voire impossible.



Impact de l'attaque

Intégrité · Authenticité · Disponibilité · Confidentialité

Motivations principales

Atteinte à l'image · Appât du gain · Nuisance · Revendication · Espionnage

HAMEÇONNAGE

On vous incite à communiquer des informations importantes ? Ne tombez pas dans le piège.

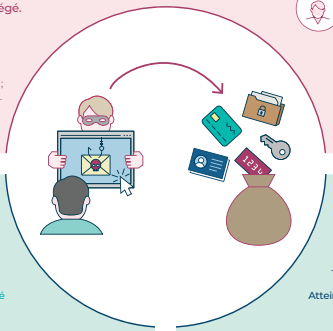
QUE SE PASSE-T-IL ?

1. Vous recevez un courriel piégé.

Le courriel suspect vous invite à :
- cliquer sur une pièce-jointe ou un lien piégés ;
- communiquer des informations personnelles.

2. L'attaquant se fait passer pour une personne ou un tiers de confiance.

L'attaquant est alors en mesure de :
- prendre le contrôle de votre système ;
- faire usage de vos informations.



Impact de l'attaque

Intégrité · Authenticité · Disponibilité · Confidentialité

Motivations principales

Atteinte à l'image · Appât du gain · Nuisance · Revendication · Espionnage · Sabotage

FICHE 4

ÉTAPE 5

ORGANISER LA COMMUNICATION DE CRISE

En fonction de la taille (équipe communication ou référent unique) et de l'organisation de votre entité (internalisation ou externalisation de la communication), une organisation spécifique de crise de la fonction communication peut être définie en amont avec une répartition des rôles et des missions.

Les principaux postes sont les suivants :

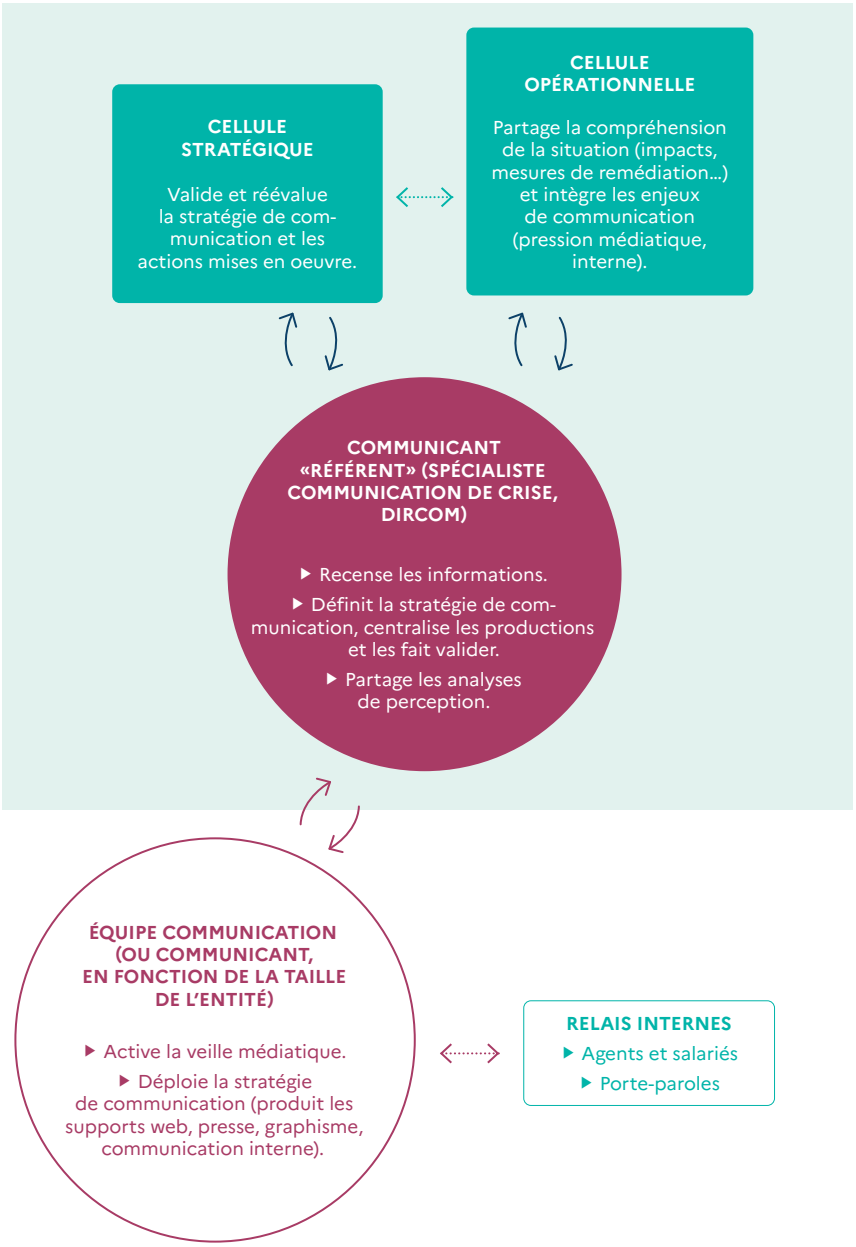
- **Coordination :** un représentant communication participe aux briefs des cellules opérationnelles et stratégiques afin d'intégrer les éléments de perception à l'analyse de risque et de valider les productions internes et externes. Il fait également le lien avec les parties prenantes externes (relais, communicants, etc.).

- **Veille et perception :** une veille médiatique, couvrant la presse et les réseaux sociaux, est mise en place et suivie par une personne dédiée et sert de base pour adapter la posture et les messages tout au long de la gestion de crise.

- **Réaction :** les membres de l'équipe en charge des relations presse, de l'animation des réseaux sociaux, du site web et de la communication interne adaptent et relaient les messages à leurs publics respectifs.

Cette organisation est envisageable si l'équipe communication est composée de plusieurs membres. En cas d'effectif plus restreint, ces rôles restent valables mais doivent être adoptés par un nombre réduit de personnes.

Dispositif de gestion de la communication de crise



ÉTAPE 6

CRÉER UNE BOÎTE À OUTILS DÉDIÉE À LA GESTION D'UNE CRISE CYBER

Pour permettre d'activer très rapidement une communication de crise, il est très utile de constituer une boîte à outils « communication de crise cyber » en amont. Celle-ci contient :

- **La stratégie de communication de crise** (voir l'étape 3 de la partie « En anticipation »).
- Le schéma du **dispositif de gestion de crise** de votre organisation ainsi que celui de l'organisation de la communication (voir les étapes 4 et 5 de la partie « En anticipation »).
- **Les outils de pilotage :** un fichier presse, les codes de connexion aux comptes (réseaux sociaux, applications mobiles, site web, Intranet, etc.), les annuaires des acteurs de la gestion de crise, etc.
- **Un glossaire** ou une forme de catalogue d'éléments de langage sur des sujets sensibles ou de crise. Ce glossaire peut être constitué en amont avec les équipes informatiques.

Cette boîte à outils est ensuite régulièrement mise à jour avec les retours d'expérience, réels ou fictifs (exercice).

Recommandation

Pensez à avoir cette boîte à outils sur une clé USB ou sur un serveur déconnecté en cas d'attaque informatique paralysant vos outils bureautiques. Prévoir également un pool de PC déconnectés du réseau et conserver un exemplaire papier de secours des documents de stratégie de communication de crise.

FOCUS

LA BOÎTE À OUTILS 100 % CYBER

Pour se préparer à faire face à une crise cyber, vous pouvez d'ores et déjà rassembler des supports et des documents utiles à actionner clé en main le jour J. Par exemple, un glossaire « cyber » peut être conçu avec les équipes opérationnelles avec des éléments de langage génériques, à adapter à la situation rencontrée le jour J :

- **Une définition claire et pédagogique des attaques informatiques les plus récurrentes :** DoS, rançongiciel, défiguration. Cette définition gagne à intégrer des réponses sur les impacts de chaque attaque (indisponibilité, possibilité d'exfiltration et de publication de données, perte d'accès à des services, etc.).

- **Une liste des questions à anticiper :** un dépôt de plainte a-t-il été réalisé ? Une déclaration type règlement général sur la protection des données (RGPD) à la CNIL est-elle nécessaire ? Qui est derrière l'attaque ?

Vous pouvez constituer un fichier presse enrichi avec des publications à suivre (presse spécialisée, influenceurs) et des contacts de journalistes spécialisés, y compris issus de la presse généraliste. La communauté cyber est composée de personnes exigeantes, très actives et curieuses qui aiment échanger sur des éléments techniques, débattre sur les réseaux sociaux, commenter des communications officielles.

Recommandation

Pour constituer cette boîte à outils, voici quelques ressources complémentaires au glossaire intégré à la fin du guide :

- **ssi.gouv.fr**
- **Cybermalveillance.gouv.fr**
- **campagnes du Cybermoi/s**

ÉTAPE 7

FORMER SES ÉQUIPES À LA GESTION DU VOLET COMMUNICATION

Les exercices de gestion de crise sont l'occasion de tester la résilience de votre organisation et de vos outils face à une attaque d'ampleur paralysant votre système d'information. Ils permettent notamment de mécaniser certaines actions qui vous permettront de gagner du temps lors d'un incident réel, y compris en matière de communication.

Sur la base des scénarios définis avec les équipes, vous pouvez organiser des entraînements de plusieurs envergures :

- **Un exercice global :** ce type d'exercice vise à tester l'ensemble du dispositif de gestion de crise de votre entité et permet de vérifier la pertinence et l'efficacité des processus d'échanges entre les cellules.

- **Un exercice uniquement dédié à la communication :** quelle que soit votre organisation (une équipe de communicants interne ou un prestataire pour la gestion des relations presse, par exemple), ce type d'exercice vous permet de vérifier la coordination entre les métiers et les personnes et de les familiariser avec l'univers de la cybersécurité.

- **Un exercice avec des participants externes :** cet exercice intègre une dose de complexité supplémentaire en y ajoutant des joueurs externes à l'organisation (autorité sectorielle, clients, etc.).

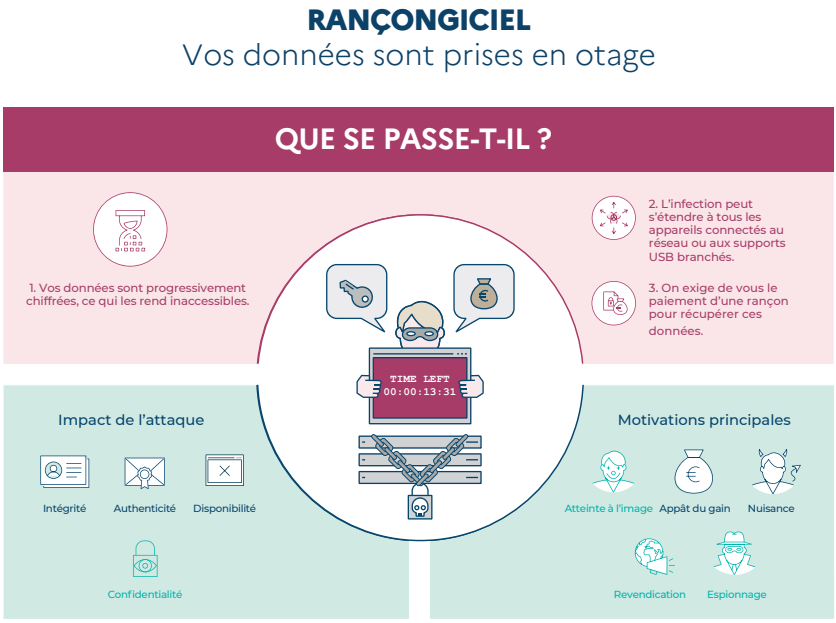
Pour un entraînement réussi, il est intéressant de réaliser, en interne ou via un prestataire, la pression médiatique simulée : faux appels médias, fausses dépêches ou encore faux réseaux sociaux.

Les exercices sont des entraînements efficaces lorsqu'ils s'accompagnent d'une formation en amont et d'un retour d'expérience en aval afin de faire progresser les équipes[8].

8. Pour en savoir plus, consultez le guide de l'ANSSI *Organiser un exercice de gestion de crise cyber.*

FAIRE FACE À UNE ATTAQUE PAR RANÇONGICIEL

Les attaques par rançongiciel[9] (voir glossaire) sont de plus en plus fréquentes et peuvent toucher n'importe quelle entité, quelle que soit son activité, sa nature ou sa taille. En matière de communication de crise, c'est également un entraînement intéressant ; ce type d'attaque est visible, avec des effets immédiats (indisponibilités) et un temps de remédiation parfois très long.



9. Pour en savoir plus, consultez le guide de l'ANSSI *Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ?*

▸ **Le tempo :** l'attaque est généralement visible quasi immédiatement, impliquant une définition rapide de la posture de communication (proactive, réactive) et des messages à porter. Côté technique, la gestion de l'incident engendre un stress et une forte pression sur les équipes techniques et managériales, d'autant que les attaquants privilégient souvent des périodes à effectif réduit (week-end, jour férié, vacances).

À contrario, le temps de remédiation demeure long, avec une estimation souvent incertaine du temps nécessaire pour un retour à la normale. Il est donc impératif de se concentrer sur les éléments critiques.

Recommandation

Pour limiter les pressions, il est nécessaire d'apporter rapidement des réponses aux différents publics, en commençant par la définition du rançongiciel. Il est également essentiel d'être transparent et pédagogique sur les temps d'investigation et de remédiation.

▸ **L'impact émotionnel :** l'attaque est souvent assortie d'un message anxiogène (tête de mort, décompte, menace) qui peut marquer le personnel. Certains groupes cybercriminels n'hésitent pas à développer leur propre communication publique autour de l'attaque pour accentuer la pression sur la victime (menace de divulgation des données par exemple). La demande de rançon génère en elle-même une montée d'angoisse.

Recommandation

La communication interne, institutionnelle mais aussi managériale est fondamentale pour rassurer vos collaborateurs sur la gestion de la crise. Par ailleurs, l'ANSSI recommande de ne pas payer la rançon. Le paiement ne garantit en rien la récupération des données intactes et peut inciter l'auteur (ou d'autres) à perpétrer un peu plus tard une nouvelle attaque sur un « bon payeur ». Le paiement ne permet pas non plus d'éviter les travaux nécessaires à la remise en service du SI et au renforcement de son niveau de sécurité pour prévenir de nouvelles attaques.

▸ **Les outils :** la paralysie possible des outils classiques de communication (fichier presse, accès aux comptes des réseaux sociaux ou au site Internet, mails, etc.) rend difficile la mise en œuvre rapide d'actions de communication, notamment en interne (mail interne, clients, etc.).

Recommandation

En anticipant des modes de communication interne dégradés en amont (listing téléphonique, affichage, etc.), vous gagnerez en rapidité lors de la gestion de la crise interne.

EN RÉACTION

ÉTAPE 1 : intégrer la cellule de gestion de crise (fiche 8 - p.36)

ÉTAPE 2 : réaliser son analyse de risque en matière de communication (fiche 9 - p.40)

ÉTAPE 3 : préparer des éléments de langage adaptés aux publics visés (fiche 10 - p.43)

ÉTAPE 4 : coordonner la communication de votre organisation (fiche 11 - p.46)

ÉTAPE 5 : prendre en charge la communication institutionnelle (fiche 12 - p.48)

ÉTAPE 6 : saisir une opportunité et capitaliser pour sensibiliser davantage en interne et en externe (fiche 13 - p.30)

La crise est là, les cellules de gestion de crise sont actionnées. La fonction communication s'active et vous apportez votre expertise à la gestion de la crise.

Une fois la crise installée, la communication de crise doit s'adapter et intégrer à la réflexion des facteurs situationnels pour de meilleures prises de décision. Là encore, plusieurs étapes se succèdent. Des fiches pratiques détaillent ces étapes dans les pages suivantes.

ÉTAPE 1

INTÉGRER LA CELLULE DE GESTION DE CRISE

Le volet communication et perception de la situation doit être pleinement intégré dans la prise de décision de la direction générale et des équipes techniques. En effet, une pression forte (médias, politique) peut avoir un effet, positif ou négatif, sur les équipes.

En intégrant la ou les cellules de gestion de crise, vous poursuivez un double objectif :

- **Comprendre la situation dans son ensemble :** les éléments techniques et leurs effets sur les métiers et les services/outils de votre organisation.

- **Partager vos éléments de réflexion relevant du domaine d'expertise de la communication :** les réactions internes, médiatiques ou politiques avant ou à la suite de publications effectuées par votre organisation.

L'objectif final du communicant est de préserver la réputation et l'image de son organisation pendant et en sortie de crise.

Recommandation

Afin d'assurer une gestion efficace de la crise, le rôle du communicant, au sein de la cellule stratégique, est de s'assurer que la communication sortante de l'entité respecte au maximum les différents tempos des acteurs (équipes cyber et IT, équipe communication, équipe de direction).

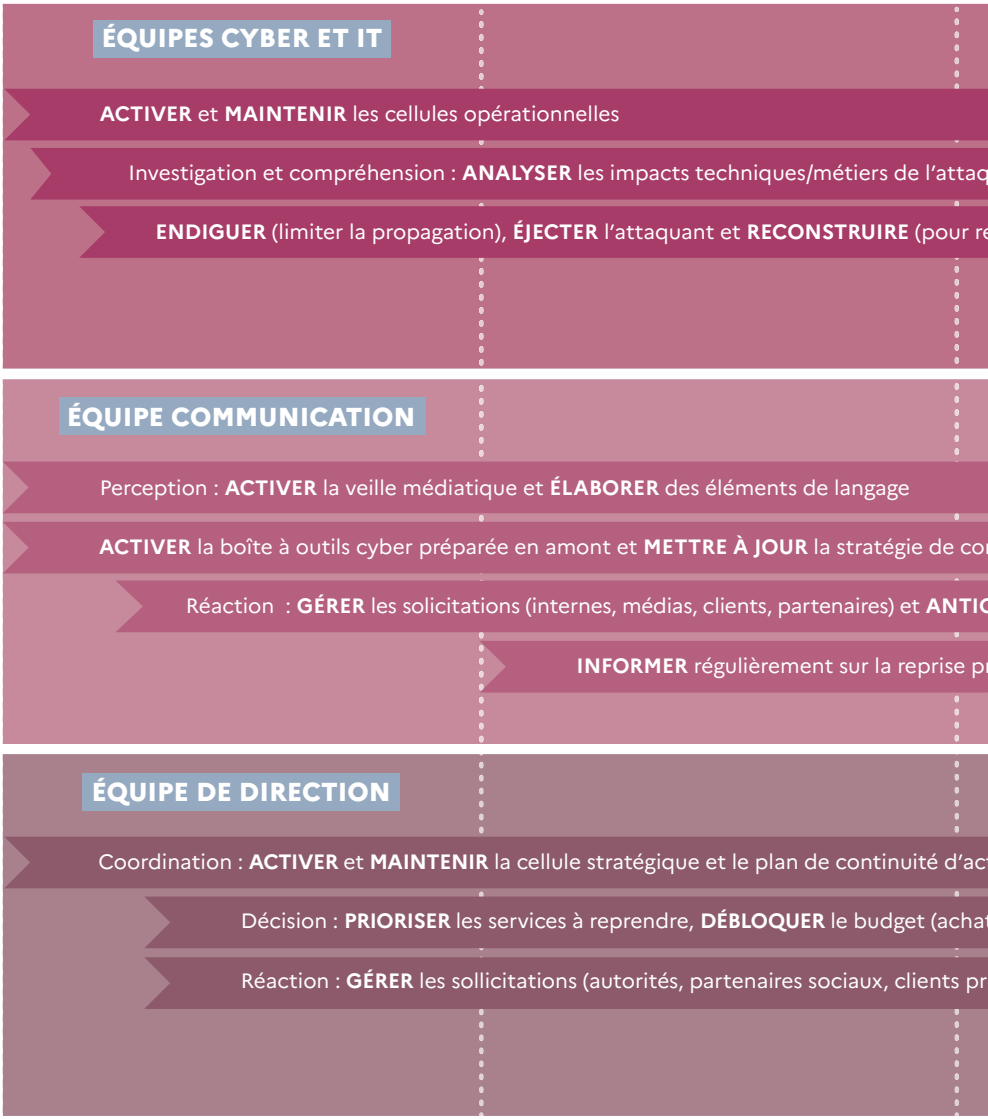
FOCUS

LA FRISE CHRONOLOGIQUE D'UNE ATTAQUE PAR RANÇONGICIEL

La crise peut se lire de différentes manières en fonction du point de vue adopté. Prenons un exemple fictif d'une attaque par rançongiciel et trois angles de vue : le communicant, les équipes cyber et IT et le décideur. Rappel : chaque situation est unique, les étapes et délais indiqués sont à adapter à l'organisation et à la nature de l'attaque.

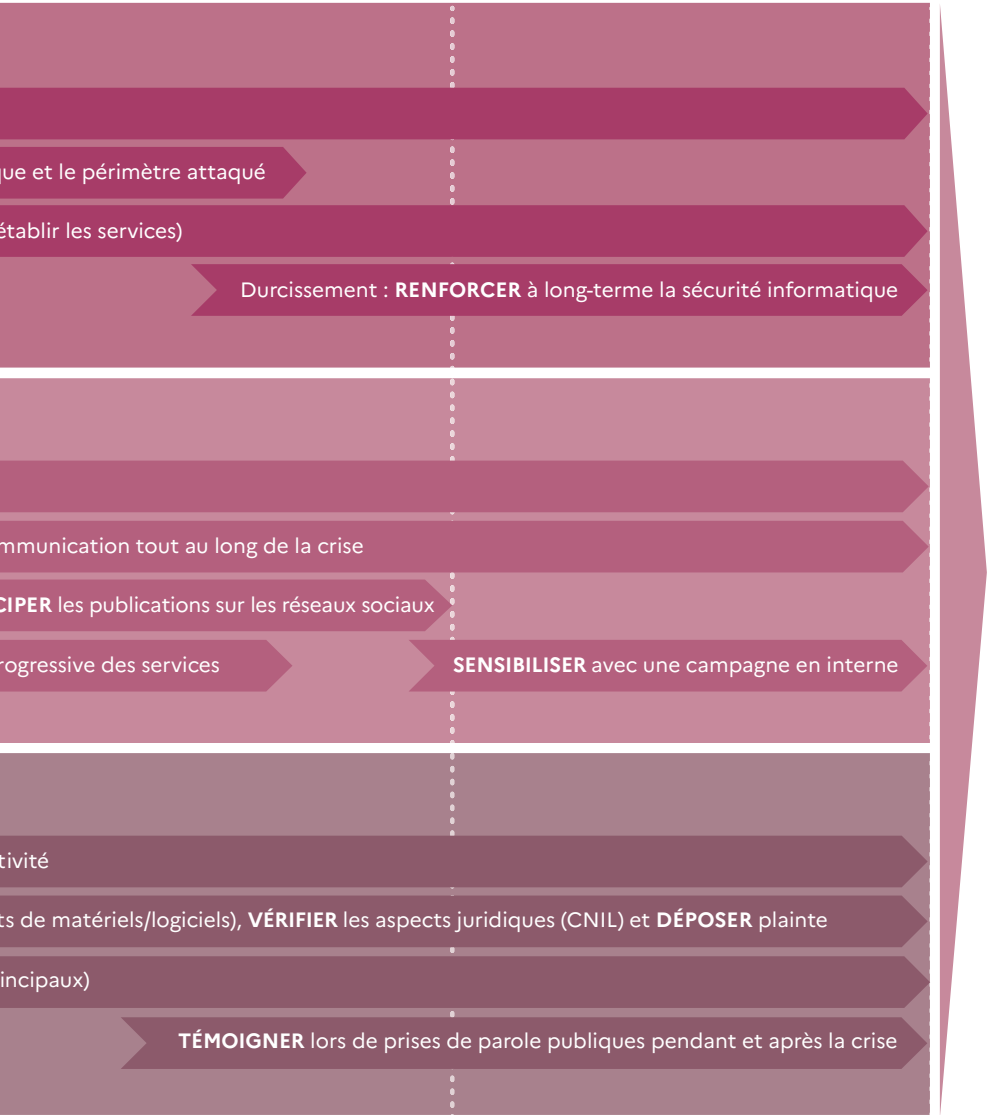
UNE ATTAQUE, TROIS TEMPOS

J-0 : jour de l'attaque



Dans le cadre de ce guide, cette frise est condensée sur quelques mois.
Dans les faits, la gestion d'une crise s'étend sur un temps plus long.

J+4 MOIS


ue et le périmètre attaqué
établir les services)
Durcissement : **RENFORCER** à long-terme la sécurité informatique
mmunication tout au long de la crise
CIPER les publications sur les réseaux sociaux
rogressive des services
SENSIBILISER avec une campagne en interne
tivité
ts de matériels/logiciels), **VÉRIFIER** les aspects juridiques (CNIL) et **DÉPOSER** plainte
incipaux)
TÉMOIGNER lors de prises de parole publiques pendant et après la crise

ÉTAPE 2

RÉALISER SON ANALYSE DE RISQUE EN MATIÈRE DE COMMUNICATION

Il n'existe pas de réponse unique à une crise, d'origine cyber ou non. La réponse adaptée dépend des faits, mais également du contexte au moment de la crise (politique, social, médiatique, économique). La fonction communication a pour mission de réaliser une analyse de risque en termes d'image et de réputation, tant au niveau des publics internes qu'externes à l'entité et aussi bien sur le court que sur le long terme.

Pour réaliser votre analyse de risque communicationnelle, vous pouvez vous appuyer sur la boîte à outils réalisée en amont (voir l'étape 6 de la partie « En anticipation ») à actualiser au regard :

- **Des faits constatés :** que s'est-il passé ? Quels sont les impacts réels ? Quels sont les impacts visibles ? Quels sont les risques et les conséquences à court et à long terme d'une exposition de la crise subie par votre entreprise ?

- **Du contexte :** y a-t-il une actualité cyber ou sectorielle à prendre en compte ? Qui prend la parole ?

- **Des réactions, actuelles ou anticipées :** quelles sont les premières réactions constatées, en interne ou en externe ? Comment réagiront vos équipes, clients, ou fournisseurs si des fuites de données sont constatées ou en apprenant qu'un attaquant a pénétré votre SI ?

Recommandation

Ne pas communiquer est une option ouverte, notamment si une attaque survient lors d'une actualité forte de l'entité (lancement d'un produit, campagne électorale, etc.).

Ce travail est avant tout une analyse coûts/bénéfices qui nécessite, dans chaque cas, une prise de risque à assumer par le décideur sur le court et le moyen terme. Sur la base de cette analyse, le décideur et ses équipes pourront acter une posture de communication (proactive ou réactive) à suivre.

Il s'agit dans ce cas pour l'entité d'accepter le risque d'une fuite d'information sur le sujet, y compris des mois plus tard, et d'assumer les conséquences d'une telle révélation. Des éléments de langage réactifs doivent dans tous les cas être préparés.

FOCUS

UN EXEMPLE D'ATTAQUE INFORMATIQUE DE TYPE ESPIONNAGE

Une attaque cyber n'est pas forcément visible. Le rançongiciel n'est qu'un type d'attaque possible. Nombreuses, discrètes, plus sophistiquées, les attaques à des fins d'espionnage ont des conséquences parfois désastreuses. Par exemple, des attaquants ont pu s'introduire dans les SI, parfois depuis plusieurs années, afin de voler de l'information stratégique d'une entreprise.

Lorsqu'une attaque de ce type est détectée, le volet communication s'aborde différemment, surtout si l'attaque a été détectée par hasard ou très tardivement. L'analyse de risque communicationnelle pose alors les questions suivantes :

- L'attaque risque-t-elle d'être visible ? L'attaquant compte-t-il publier les données collectées ?
- Qui dois-je informer ?
- Faut-il communiquer largement ? En interne ? En externe ?
- Que risque mon organisation en termes de réputation si je dévoile cette attaque ?
- À quel moment faut-il en parler ? L'attaquant est-il toujours actif ?

La réponse à certaines questions prendra du temps. Si le parti pris est de ne pas communiquer, des éléments de réponses doivent être néanmoins préparés et prêts à être diffusés si la posture de communication venait à évoluer.

Recommandation

Pour ce type d'attaque, le volet remédiation est souvent long, l'attaquant disposant généralement des pleins pouvoirs sur le SI. Il faudra prévoir des actions techniques en profondeur pour éjecter l'attaquant et renforcer la sécurité du SI. Et de fait, d'accompagner ces actions d'une communication interne adaptée.

ÉTAPE 3

PRÉPARER DES ÉLÉMENTS DE LANGAGE ADAPTÉS AUX PUBLICS VISÉS

L'analyse de risque effectuée, vous êtes prêts à élaborer et à coordonner les messages à adresser aux différents publics identifiés. Plusieurs paramètres sont à prendre en compte :

▸ **Le niveau et la qualité de l'information à adapter au public ciblé et à réévaluer tout au long de la crise**. Lors de la gestion d'une crise cyber, les analyses techniques prennent du temps et imposent un certain rythme à la communication afin de s'assurer que l'information transmise soit fiable et véridique.

▸ **La technicité de l'information peut également varier en fonction du public.** Si vous vous adressez à des médias généralistes et donc à un lectorat non expert, il faudra simplifier et faire preuve de plus de pédagogie. Bien que simplifiée, là encore l'information transmise doit être fiable et véridique.

▸ **Le rythme de la transmission des informations.** Vous devez occuper l'espace médiatique pour éviter que d'autres acteurs (experts, concurrents) ne s'expriment à votre place. Vous devez donc donner de la visibilité à chaque étape clé, en suivant le « rythme de bataille » défini plus généralement pour la gestion de la crise.

Le sujet cyber est aujourd'hui fortement suivi par les médias de tous horizons, y compris non spécialisés. Toute communication relative au cyber doit être parfaitement mesurée et fondée car elle sera finement analysée par la communauté et les influenceurs compétents.

QUE DIRE ?

Chaque situation étant unique, les messages diffèrent en fonction de la situation et du public ciblée, interne et externe. S'il est difficile de prévoir un message type, plusieurs informations sont attendues :

▸ Expliquer la nature de l'attaque et surtout les impacts sur l'organisation, les services ou les produits de votre entité.

▸ En cas de fuite de données, expliquer de façon pédagogique ce que cela implique pour les clients ou les usagers concernés et les actions qu'ils peuvent mettre en œuvre pour se protéger.

▸ Donner de la visibilité sur les actions mises en œuvre pour rétablir au plus vite les services et les outils de votre organisation. Attention à ne pas donner de date de résolution trop ferme : la complexité des attaques informatiques peut engendrer des délais non prévus.

▸ Faire de la pédagogie sur le temps des investigations et de la remédiation.

▸ Préciser les mesures prises vis-à-vis des autorités le cas échéant :
- en cas de fuite de données, la déclaration auprès de la CNIL ;
- le dépôt de plainte auprès des services de police ou de gendarmerie spécialisés.

Le ton de la communication peut lui aussi évoluer avec la crise : pédagogique, rassurant, authentique, calme. Il faut réussir à doser le discours expert (explication autour de l'incident) avec l'assurance de la mise en œuvre des moyens nécessaires à la résolution de la crise.

À noter que si l'incident est judiciarisé, certains éléments précis ne pourront être dévoilés sans l'accord préalable du service enquêteur compétent. En cas de fuite importante de données personnelles, la CNIL peut également transmettre des recommandations en matière de communication.

Enfin, comme toute crise, le message gagne à adopter un ton empathique, surtout si des personnes sont directement ou indirectement touchées.

Recommandation

Une attention particulière est à apporter sur les choix éditoriaux (vocabulaire, ton employé) : tout en restant transparent, il est plus percutant de rassurer que d'opter pour des termes très anxiogènes. De même, opter pour l'humour afin d'alléger les tensions est un choix fragile : la perception de l'incident est très différente en fonction des personnes. L'humour peut être perçu comme une gestion légère de la crise, en contradiction avec la criticité et le stress vécu par certains acteurs.

ÉTAPE 4

COORDONNER LA COMMUNICATION DE SON ORGANISATION

On peut identifier trois grands types de communication lors de la gestion d'une crise cyber :

- la communication technique, experte, évolutive, factuelle ;
- la communication institutionnelle, maîtrisée et validée par le décideur ;
- la communication politique, portée par les autorités.

La fonction communication n'est donc pas la seule à émettre des informations tout au long de la gestion de crise. D'autres acteurs interviennent et s'adressent à leurs propres publics :

- **les équipes techniques ;**
- **la direction générale ;**
- **les métiers en contact avec des interlocuteurs externes** (services clients, services juridiques, etc.) ;
- **les parties prenantes** identifiées.

Le rôle de la fonction communication est de coordonner les différents fils de parole pour rendre la communication globale de l'organisation cohérente, claire et maîtrisée.

La fonction communication doit avoir une vision exhaustive des outils de communication et des messages transmis, y compris les réseaux sociaux des dirigeants ou des collaborateurs.

FOCUS

QUI COMMUNIQUE AU FINAL ?

Tour d'horizon des fils de communication : objectifs, priorités et enjeux.

La communication

- **Messages :** état de la situation, actions entreprises.
- **Public** : collaborateurs, presse, influenceurs, etc.
- **Mediums :** désignation d'un porte-parole, presse, web, Intranet, etc.

Les équipes techniques

- **Messages :** éléments techniques (marqueurs), point de situation factuel.
- **Publics :** délégué à la protection des données personnelles (DPO), chaîne hiérarchique, homologues (CERT sectoriel, réseaux RSSI), autorités (CNIL/RGDP), prestataire.
- **Medium :** mails, mémos, réunions.

La direction générale

- **Messages :** gestion de la situation et continuité d'activité.
- **Publics :** collaborateurs, autorités, clients, etc.
- **Medium :** mail, presse, téléphone,etc.

Les autres métiers

- **Messages :** gestion de la situation et continuité d'activité ; risque de propagation.
- **Publics :** clients, partenaires, prospects, etc.
- **Medium :** mail, presse, téléphone,etc.

Les autres parties prenantes

- L'ANSSI : partage d'informations techniques, communication institutionnelle en cas d'intervention.

- Les autorités sectorielles, les clients, les partenaires et les prestataires : rassurer sur leur propre situation.

ÉTAPE 5

PRENDRE EN CHARGE LA COMMUNICATION INSTITUTIONNELLE

Le rôle de chacun (entité, parties prenantes) en matière de communication de crise doit être clairement défini et partagé par tous. Pour une meilleure maîtrise du message, il est souvent conseillé de ne pas multiplier les porteurs de la communication institutionnelle officielle. La communication est en charge de gérer certains publics spécifiques, notamment la pression médiatique, interne et sociale. Deux formes de communication en découlent :

La communication interne

▸ **Objectif :** rassurer et expliquer la situation. En cas de fortes perturbations du travail, donner de la visibilité sur les actions menées et les perspectives de retour à la normale.
▸ **Outils :** listing téléphonique / mails, rencontre, Intranet, campagne SMS.
▸ **Vos messages :**
- preuve de pédagogie sur l'attaque et les actions préconisées et/ou mises en place pour sortir efficacement de la crise ;
- transmettre les consignes pratiques aux collaborateurs pour qu'ils puissent travailler et donner de la visibilité sur les étapes à venir jusqu'à la sortie de la crise.

La communication externe

▸ **Objectif :** expliquer tout au long de la crise la situation, les étapes de gestion (compréhension, remédiation).
▸ **Outils :** porte-parole identifié, communiqué de presse, article sur le site Internet, relai sur les réseaux sociaux, éléments de langage évolutifs.
▸ **Vos messages :**
- déterminer le niveau d'information nécessaire à transmettre pour chaque destinataire, en fonction des impacts et du contexte ;
- réévaluer avec l'apport de la veille médiatique et sociale.

FOCUS

LES QUESTIONS TYPES DES JOURNALISTES À ANTICIPER

En cas d'attaque informatique, vous pourrez être sollicité par vos contacts médiatiques classiques (presse sectorielle, généraliste nationale et/ou régionale) mais également par la presse spécialisée en informatique et plus particulièrement en sécurité informatique.

Tour d'horizon des questions types posées par les journalistes spécialisés :

- De quel type d'attaque s'agit-il ? Quel est le mode opératoire ?
- Quelles sont les conséquences directes (techniques, financières) ? Quelles sont les conséquences indirectes ? Propagation ? Latéralisation ?
- Des clients sont-ils victimes ? S'agit-il de clients sensibles ?
- Quand est-ce arrivé ? Combien de temps cela va-t-il durer ? L'attaque est-elle toujours en cours ? À quand un retour à la normale ou à un fonctionnement optimal ?
- Que faîtes-vous aujourd'hui pour réparer le SI ?
- Une plainte a-t-elle été déposée ? Une déclaration RGPD auprès de la CNIL a-t-elle été réalisée ?
- L'ANSSI vous accompagne-t-elle ? Des prestataires ?
- Quelles mesures allez-vous mettre en place à l'avenir ?
- Qui est l'attaquant ? Quelles sont ses motivations ? Avez-vous payé la rançon ?

ÉTAPE 6

SAISIR UNE OPPORTUNITÉ ET CAPITALISER POUR SENSIBILISER EN INTERNE ET EN EXTERNE

Une crise est une opportunité, une fois sous contrôle, pour identifier les axes d'amélioration (processus, boîte à outils) et pour remobiliser les équipes sur les sujets de sécurité numérique.

Pour le volet communication, c'est notamment un point de départ possible d'une campagne de sensibilisation en interne sur les bonnes pratiques informatiques à adopter, chacun à son niveau. Pour trouver de l'inspiration, rendez-vous sur les sites de l'ANSSI et de Cybermalveillance.gouv.fr afin de trouver des ressources et des idées pour mener vos campagnes.

Le partage de votre expérience peut également servir à d'autres acteurs, de votre secteur d'activité par exemple, pour les sensibiliser sur les risques et les mesures plus techniques à mettre en œuvre pour prévenir les attaques informatiques.

N'hésitez pas à partager votre expérience pour montrer comment vous avez relevé ce défi et pour contribuer à renforcer la sécurité en France !

FOCUS

LES RECOMMANDATIONS POUR FAIRE FACE À UN RANÇONGICIEL

À titre d'exemple, l'actualité montre l'augmentation des attaques par rançongiciels à l'encontre de tous types d'organisation. Le Cybermoi/s, organisé tous les ans en octobre, est une belle opportunité pour mener une campagne de sensibilisation en interne.

Les recommandations

- sauvegarder les données ;
- maintenir à jour les logiciels et les systèmes ;
- utiliser et maintenir à jour les logiciels antivirus ;
- cloisonner le SI ;
- limiter les droits des utilisateurs et les autorisations des applications;
- maîtriser les accès Internet ;
- mettre en œuvre une supervision des journaux ;
- évaluer l'opportunité de souscrire à une assurance cyber.

Ressources existantes

- Le guide de l'ANSSI, réalisé en partenariat avec la direction des affaires criminelles et des grâces (DACG) du ministère de la Justice ; *Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ?*
- Les bandes dessinées interactives du Cybermoi/s, édition 2020.
- Fiches pratiques du dispositif Cybermalveillance.gouv.fr

CHECK-LIST

- ☐ **Préparer** dès maintenant votre boîte à outils de communication de crise pour faire face à une attaque informatique.
- ☐ **Contacter** les équipes cyber et IT et les métiers mobilisés par la gestion de crise en général, pour concevoir des scénarios de crise et des contenus génériques, ainsi que démarrer les processus d'échange.
- ☐ **Intégrer** la communication au bon niveau au sein du dispositif global de gestion de crise de votre entité pour accompagner les équipes et répondre aux sollicitations internes et externes lors de la crise.
- ☐ **S'intéresser** à l'écosystème de la cybersécurité : les médias, les influenceurs, les actualités, le vocabulaire.
- ☐ **S'entraîner** et tester l'ensemble du dispositif, en intégrant un volet de pression médiatique simulée pour la partie communication.
- ☐ **Se rapprocher** de votre RSSI pour sensibiliser vos collaborateurs aux risques cyber et aux bonnes pratiques à adopter afin d'éviter une crise cyber.

GLOSSAIRE

CYBERSÉCURITÉ : permet de résister à des événements issus du cyber-espace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

LES TYPES D'ATTAQUES

DÉFIGURATION D'UN SITE INTERNET : altération par un pirate de l'apparence d'un site Internet, en modifiant le contenu des pages, faisant figurer souvent des slogans ou des images sans lien avec l'objet du site attaqué.

DÉNI DE SERVICE (DOS) OU DÉNI DE SERVICE DISTRIBUÉ (DDOS) : attaques visant à rendre indisponible un service sur Internet par l'envoi de multiples requêtes jusqu'à le saturer provoquant une panne ou une forte dégradation du service.

ESPIONNAGE : type d'attaque consistant pour un attaquant à prendre pied discrètement dans le SI de la victime pour en exfiltrer de l'information stratégique pour l'entreprise. Une telle attaque, souvent sophistiquée, peut durer plusieurs années avant d'être détectée.

HAMEÇONNAGE *(PHISHING)* : technique frauduleuse destinée à tromper l'internaute en se faisant passer pour un tiers de confiance (faux SMS, mail, etc.) pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires. Ce type d'attaque peut être utilisé tant pour une attaque d'espionnage que pour une attaque de type rançongiciel.

RANÇONGICIEL *(RANSOMWARE) :* type d'attaque consistant pour un pirate à faire exécuter un logiciel malveillant sur le SI de la victime, pour chiffrer l'ensemble de ses données, y compris les sauvegardes et lui demander une rançon en échange du mot de passe de déchiffrement. De plus, il n'est pas rare que le pirate menace de divulguer des données préalablement exfiltrées afin d'augmenter l'incitation à payer la rançon.

LE VOCABULAIRE OPÉRATIONNEL

ATTRIBUTION D'UNE ATTAQUE INFORMATIQUE : décision de l'autorité politique, prise

au plus haut niveau, qui vise à désigner le commanditaire, généralement un État, comme responsable de cette attaque.

CODE MALVEILLANT *(MALWARE)* : programme développé dans le but de nuire à un SI. Remarque : les virus ou les vers sont deux types de codes malveillants connus.

IMPUTATION D'UNE ATTAQUE INFORMATIQUE : se concentre sur la caractérisation technique des outils, des techniques et des tactiques de l'attaquant afin de déterminer ses intérêts et ses méthodes de travail, de le relier à des cyberattaques connues et enfin, d'identifier un groupe d'attaquants ou un commanditaire. Ce travail technique, auquel un niveau de certitude variable est accordé, sert ensuite de base de décision pour une éventuelle attribution.

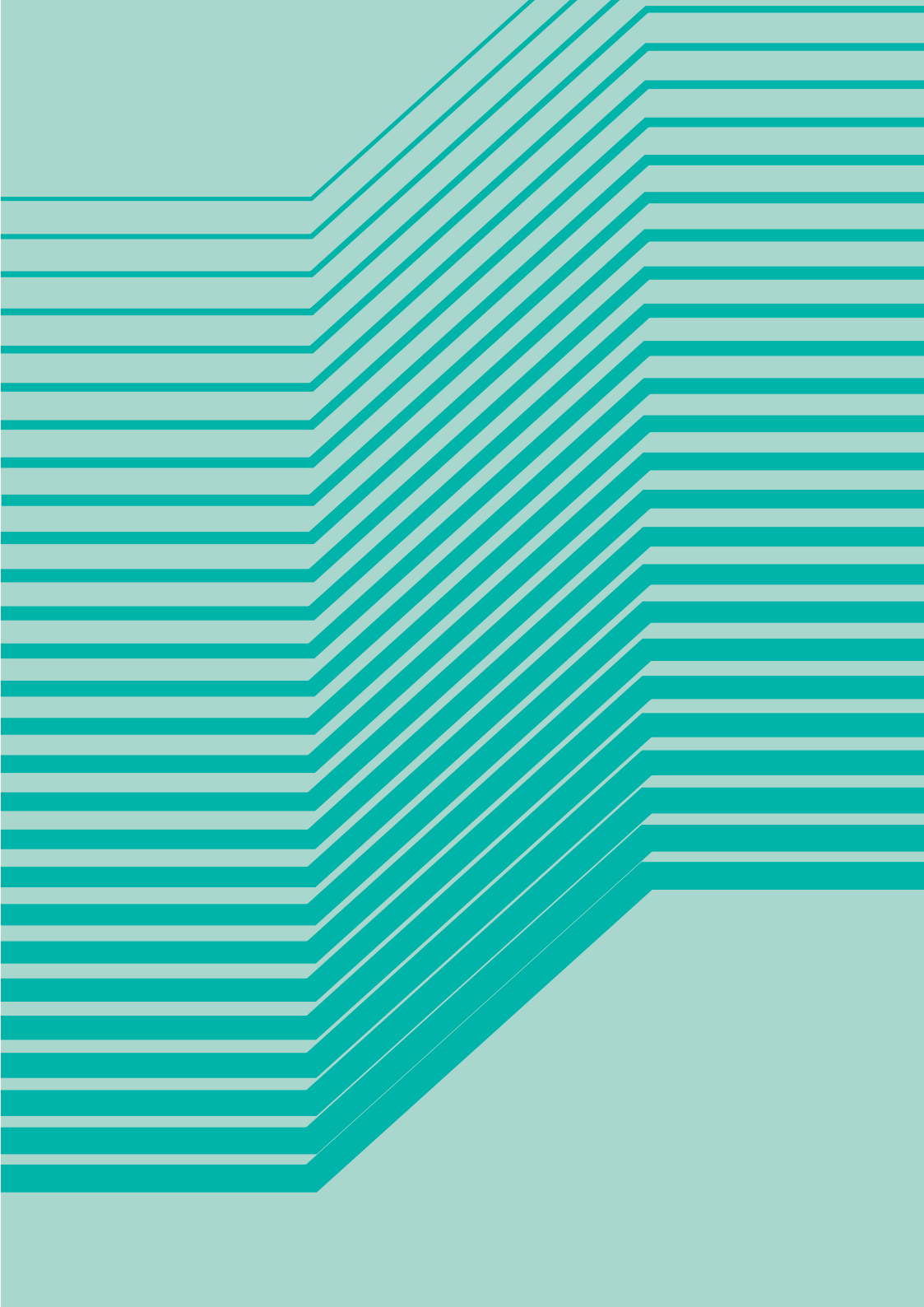
MARQUEUR TECHNIQUE OU INDICATEUR DE COMPROMISSION (IOC) : information technique, telle que l'adresse IP d'un serveur malveillant ou le nom d'un site Internet piégé, permettant de détecter et de caractériser une attaque. Le partage de ces éléments de connaissance permet notamment d'empêcher des compromissions futures. En revanche, de telles informations ne doivent parfois pas être communiquées si l'attaque a été judiciarisée.

MODE OPÉRATOIRE D'UN ATTAQUANT (MOA) OU D'UN GROUPE D'ATTAQUANTS : équivaut à la signature de l'attaquant, sa façon d'opérer pour cibler et attaquer ses victimes.

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) : encadre le traitement des données personnelles sur le territoire de l'Union européenne. La CNIL est notamment en charge de traiter les plaintes et de développer de nouveaux outils de conformité pour garantir à tous la protection des données personnelles.

VECTEUR D'ATTAQUE : moyen d'accès utilisé par un acteur malveillant pour exploiter les failles de sécurité et accéder à un serveur ou un équipement (pièces jointes, pages Internet, vulnérabilités non corrigées).

VULNÉRABILITÉ : faille de sécurité pouvant affecter un logiciel, un SI ou encore un composant matériel. Elle peut servir de porte d'entrée pour des acteurs malveillants s'ils parviennent à l'exploiter. Les vulnérabilités sont généralement corrigées lors des mises à jour ou par des correctifs publiés par les éditeurs.



COLLECTION
GESTION DE CRISE CYBER

« Lorsqu'une crise cyber survient, l'action des communicants passe trop souvent au second plan. C'est une erreur. Pour une gestion globale de la crise, il est indispensable que la communication travaille main dans la main avec la réponse technique. »

Guillaume Poupard, directeur général de l'ANSSI

Face à une attaque, la technicité d'une crise cyber peut déstabiliser les plus aguerris des communicants, confrontés à des codes parfois très éloignés de leur cœur de métier.

Réalisé en partenariat avec Cap'Com et fruit d'une riche expérience en communication de crise cyber, ce guide vous accompagnera dans la conception et le déploiement de vos stratégies de communication lors d'une attaque informatique.

Version 1.0 – Décembre 2021 - **ANSSI-PA-091**
Licence ouverte/Open Licence (Etalab — V1)
ISBN : 978-2-11-167110-2 (papier)
ISBN : 978-2-11-167111-9 (numérique)
Dépôt légal : décembre 2021

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