FICHE 5 PENDANT UNE CRISE CYBER

DÉFINIR SA STRATÉGIE DE COMMUNICATION DE CRISE CYBER

1 ÉTAT DES LIEUX

Il n'existe pas de stratégie de communication unique en réponse à une crise cyber. La stratégie adaptée dépend notamment des faits, de la situation en matière de communication mais également du contexte au moment de la crise cyber. Au début d'une crise cyber, le communicant doit ainsi réaliser un état des lieux en obtenant les informations essentielles ci-après.

FAITS CONSTATÉS

Demandez un point de situation pour comprendre l'incident, car il existe différents types de cyberattaques. Essayez d'en savoir plus sur les impacts de l'incident sur les métiers et les services/outils. L'objectif est de savoir si l'attaque en elle-même est visible pour vos publics interne et externe (exemple : un rançongiciel ou un déni de service sont très visibles, contrairement à une opération d'espionnage) ou si les impacts de cette attaque sont visibles (exemple : l'impossibilité pour l'entité de payer ses collaborateurs ou de maintenir ses services habituels).

Résumez les premières actions entreprises par votre entité sur l'ensemble des volets : technique, juridique, communication et même organisationnel.

SITUATION EN MATIÈRE DE COMMUNICATION

Faites un point sur la stratégie de communication globale de votre entité pour définir une stratégie de communication de crise cohérente avec l'identité de votre entité, ses objectifs et ses cibles prioritaires.

Dressez un état des lieux des canaux de communication qui restent disponibles malgré la cyberattaque (réseaux sociaux, site web, messagerie interne, etc.) ou avec des contraintes fortes (exemple : canaux accessibles seulement sur des postes déconnectés).

Demandez un point de situation de la perception du sujet en interne, dans les médias et sur les réseaux sociaux reprenant notamment les premières réactions des collaborateurs, des clients, des usagers ou des fournisseurs). Une cyberattaque peut connaître une viralité forte et de nombreux « experts » sur les réseaux sociaux ou journalistes spécialisés peuvent réagir rapidement et publiquement.

Prenez en considération le nombre de demandes presse reçues par votre service de presse et les thématiques abordées.

Demandez à votre délégué à la protection des données (DPO) ou votre service juridique si vous avez des obligations légales qui peuvent obliger votre entité à informer des parties prenantes (par exemple au titre du Règlement général sur la protection des données (RGPD) dans le cas d'un vol de données). Cette information prévue par une disposition légale est à réaliser en sus de la communication publique de crise et peut impacter notamment le timing de communication.

Identifiez si des parties prenantes ont déjà communiqué sur votre incident. Il peut s'agir de la Commission nationale de l'informatique et des libertés (CNIL), de la section J3 Cybercriminalité du Parquet de Paris, d'autorités de régulation ou sectorielle, de vos clients, usagers, partenaires ou prestataires ou dans de très rares cas, de l'ANSSI. Des personnalités politiques peuvent également communiquer sur des crises cyber, allant parfois jusqu'à se déplacer auprès des victimes.

Évaluez la visibilité des attaquants. Certains groupes d'attaquants se distinguent par des stratégies de communication spécifiques, comme la revendication automatique de leurs attaques ou la menace de publication des données exfiltrées. Ces actions peuvent être plus ou moins visibles en fonction du canal de communication privilégié par l'attaquant. Ce dernier peut communiquer sur un site vitrine sur le *dark web*, via une messagerie chiffrée voire même avec un communiqué de presse ou sur les réseaux sociaux. Ayez également à l'esprit que les attaquants peuvent contacter directement des journalistes, des collaborateurs ou différents services de votre entité dont votre service de presse (interne ou externalisé chez un prestataire) par email ou par téléphone, afin d'accroître la pression et forcer une réaction précipitée de la victime.

CONTEXTE

Identifiez d'éventuels points de vigilance liés au contexte dans lequel vous vous inscrivez :

L'actualité de votre entité. Par exemple : une importante campagne de communication qui débute bientôt, la publication prochaine des résultats financiers, des négociations salariales en cours, le lancement à venir d'un produit, voire même le rachat de votre entité.

L'actualité socio-économique et politique entourant votre entité, avec un évènement sectoriel majeur en préparation ou une période électorale en cours ou à venir.

2 POSTURE DE COMMUNICATION

Une fois l'état des lieux réalisé, vous devez définir et proposer à vos dirigeants une posture de communication (proactive ou réactive) à adopter.

POSTURES DE COMMUNICATION

Dans le cas où l'attaque elle-même, les impacts de l'attaque ou les attaquants sont visibles, il est conseillé d'opter pour une posture de

COMMUNICATION PROACTIVE

car l'information est déjà accessible publiquement. L'entité doit donc communiquer rapidement pour expliquer, rassurer et préserver son image et sa réputation.

Dans le cas d'une attaque détectée mais discrète, c'est-à-dire invisible à l'externe (intrusion à des fins de sabotage, espionnage), vous pouvez opter pour une posture de

COMMUNICATION RÉACTIVE

Il s'agit de préparer des communications en amont d'une potentielle médiatisation de l'attaque mais de ne pas prendre la parole proactivement et immédiatement. Il n'est pas rare de voir un incident passer sous les radars médiatiques durant une longue période puis être médiatisé des mois plus tard.

Gardons en tête que le communicant ne fait que proposer une posture de communication qui s'intègre dans une analyse coûts/bénéfices (humains, financiers, juridiques, réputationnels, etc.) globale élaborée avec l'ensemble des parties prenantes de l'entité. Le choix de la posture revient aux dirigeants avec une prise de risques à court et moyen terme assumée.

Cette posture de communication doit être réévaluée tout au long de la gestion de la crise cyber au regard du contexte évolutif de l'incident afin de réorienter les actions de communication en conséquence.

FOCUS
COMMUNIQUER SUR UNE CYBERATTAQUE À DES FINS LUCRATIVES

Un rançongiciel – *ransomware* en anglais – est un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Les rançongiciels figurent au catalogue des outils auxquels ont recours les cybercriminels motivés par l'appât du gain.
Lors d'une attaque par rançongiciel, l'attaquant met l'ordinateur ou le système d'information de la victime hors d'état de fonctionner de manière réversible ou irréversible. En pratique, la plupart des rançongiciels chiffrent par des mécanismes cryptographiques les données de l'ordinateur ou du système, rendant leur consultation ou leur utilisation impossibles. L'attaquant adresse alors un message non chiffré à la victime où il lui propose, contre le paiement d'une rançon, de lui fournir le moyen de déchiffrer ses données.

Ce type d'attaque présente deux caractéristiques propres, différentes d'attaques plus discrètes :

LE TEMPO
visibilité quasi immédiate et systématique de l'attaque

Une attaque par rançongiciel a de très grandes chances d'être rendue publique rapidement, en raison des impacts de la cyberattaque (exemple : impossibilité de rendre un service aux clients ou usagers), d'une fuite d'informations sur la base de captures d'écran de l'entité partagées à l'externe ou de certains groupes cybercriminels qui développent leur propre communication publique autour de l'attaque pour faire davantage pression sur la victime (chantage pour le déchiffrement, la publication d'un échantillon ou la revente des données).

LES OUTILS
paralysie possible des outils classiques de communication

En fonction de la propagation de l'incident, les outils bureautiques peuvent être partiellement ou complètement indisponibles, empêchant l'accès aux outils de travail du communicant (fichier presse, accès aux comptes des réseaux sociaux ou au site Internet, emails, etc.) et la mise en œuvre d'actions de communication rapide (email ou message interne, emails clients/usagers, etc.).

Ces deux caractéristiques obligent le communicant à opter le plus souvent pour une posture de communication proactive dès les premières heures de l'incident pour limiter les impacts de la crise cyber sur l'image et la réputation de l'entité, tant en interne qu'en externe.

FOCUS
COMMUNIQUER SUR UNE ATTAQUE À DES FINS D'ESPIONNAGE

Une attaque cyber n'est pas forcément visible. Discrètes et plus sophistiquées, les attaques à des fins d'espionnage ont des conséquences parfois désastreuses. Des attaquants peuvent s'introduire dans les systèmes d'information, parfois pendant plusieurs années, afin notamment de voler des données stratégiques.

Pour ce type d'attaque, détectée parfois par hasard ou très tardivement, la remédiation est souvent longue, l'attaquant pouvant disposer de droits élevés sur le système d'information. Il faudra alors prévoir des actions techniques en profondeur pour éjecter l'attaquant et renforcer la sécurité du système d'information. Réagir face à une cyberattaque de ce type, c'est également entamer une interaction avec un adversaire : les actions de votre entité et leurs effets peuvent être observés et interprétés par l'attaquant. Sa réaction est variable selon son niveau de compétence, de persistance et d'agressivité.

La communication doit donc être abordée différemment pour ce type d'attaque car les échanges, qu'ils soient internes ou externes (entre les gestionnaires de la crise, avec les équipes de l'entité ou avec des partenaires, clients/usagers ou prestataires) sont des sources d'information potentielles pour l'attaquant. Il est donc nécessaire de « cacher son jeu » en contrôlant les informations perceptibles par l'attaquant afin de limiter ses possibilités d'adaptation ou de réaction.

Votre posture de communication, généralement réactive, est définie en fonction du niveau de précaution à prendre dans les actions de remédiation pour les protéger de la vue de l'adversaire. Concernant la communication interne, elle doit être mesurée afin de ne pas compromettre les actions de remédiation en cours. Pour la communication externe, il est conseillé de ne pas communiquer en amont de l'éviction définitive de l'attaquant du système d'information mais des messages clés doivent être néanmoins préparés (sans qu'ils soient hébergés dans votre système d'information) et prêts à être diffusés.

Il est recommandé de se référer au guide de l'ANSSI « Cyberattaques et remédiation : préparer la remédiation » pour un développement dédié à ce sujet.

FOCUS
COMMUNIQUER SUR UNE ATTAQUE À DES FINS DE DÉSTABILISATION

Certaines attaques informatiques, telles que le déni de service distribué (DDoS) ou la défiguration de site Internet, ont pour objet principal la déstabilisation de l'entité visée. Un DDoS a pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. L'action peut être malveillante ou être la conséquence d'un mauvais dimensionnement du service. On parle de déni de service distribué lorsque l'attaque fait intervenir un réseau de machines (souvent compromises) afin d'interrompre le ou les services visés. La défiguration est le résultat d'une activité malveillante qui a modifié l'apparence ou le contenu d'un serveur Internet et a donc transgressé l'intégrité des pages en les altérant.

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 système d'information). 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 attaquants aux messages anxiogènes.

Dans ce type d'attaque peu sophistiquée ou lors d'un « faux incident », cela peut générer une crise médiatique plus importante à gérer que la partie technique de l'incident lui-même.
La posture de communication proactive est alors 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.

3 OBJECTIFS DE COMMUNICATION

Une fois l'état des lieux réalisé et la posture choisie, vous pouvez définir vos objectifs de communication. Vous trouverez ci-après les principaux objectifs de communication à atteindre lors d'une crise cyber.

EXPLIQUER ET INFORMER

Faire de la pédagogie sur le type d'attaque auquel l'entité est confrontée et les actions de remédiation qui en découlent afin d'améliorer la compréhension des évènements et le partage de connaissance.

RASSURER

Montrer que votre entité fait le nécessaire pour sortir rapidement de la crise cyber afin de conserver la confiance de ses clients ou de ses usagers mais aussi de l'interne.

PRÉSERVER L'IMAGE ET LA RÉPUTATION DE L'ENTITÉ

Limiter les impacts sur la notoriété de l'entité grâce à une communication transparente (cf. ***Fiche 9***). Il est également nécessaire de s'assurer de la non-propagation de rumeurs ou de fausses informations (cf. ***Fiche 8***).

FAIRE CHANGER LES COMPORTEMENTS

Inciter les collaborateurs à adopter des bonnes pratiques de sécurité numérique dans leurs futurs usages.

4 CIBLES

Lors d'une crise cyber, on retrouve habituellement les cibles de communication suivantes :

→ INTERNES

- **Collaborateurs** (ou uniquement ceux dont les données sont exfiltrées, voire publiées dans le cas d'un vol de données)
- **Managers, CODIR/COMEX, dirigeants**
- **Prestataires travaillant en interne**
- **Filiales ou entités parentes**
- **Instances représentatives du personnel** (comité social et économique, syndicats, représentants du personnel, etc.)
- **Porte-paroles**

→ EXTERNES

- **Journalistes** (nationaux et régionaux, généralistes ou spécialisés en cybersécurité/tech ou dans le secteur impacté)
- **Influenceurs cyber et du secteur impacté**
- **Prospects**
- **Clients** (cible qui peut être divisée en deux cercles, les clients VIP et le reste des clients)
- **Usagers**
- **Prestataires**
- **Fournisseurs**
- **Actionnaires et membres du Conseil d'Administration**
- **Partenaires** (français, européen et internationaux)
- **Grand public**
- **Personnes dont les données sont exfiltrées, voire publiées** (dans le cas d'un vol de données)
- **ANSSI et le CERT-FR**, notamment si vous êtes soumis à des obligations réglementaires
- **Autorités sectorielles**
- **Autorités politiques ou de tutelles, cabinets ministériels**
- **Homologues techniques** (CSIRT sectoriel, ministériel ou territorial, InterCERT France, CERT-EU)
- **CNIL**
- **Section J3 Cybercriminalité du Parquet de Paris**

Si certaines de vos parties prenantes sont à l'international (collaborateurs, clients, usagers, etc.), gardez à l'esprit l'enjeu de traduction rapide des contenus (a minima en anglais).

Attention, un communicant n'a pas vocation à centraliser la rédaction et l'envoi des communications à l'ensembles des cibles ! Le rôle du communicant est de coordonner les différentes prises de parole pour rendre la communication globale de l'entité cohérente, claire et maîtrisée. Chaque acteur joue donc son rôle, dans le cadre de ses attributions, mais avec une vision collective, partagée et validée.

5 TEMPOS DE COMMUNICATION

Le tempo d'une crise cyber est toujours difficile à expliquer : si l'attaque ou les impacts sont parfois immédiatement visibles, les analyses techniques prennent du temps, tout comme les mesures de remédiation. Cet argument, bien que frustrant, est généralement bien compris des médias spécialisés en cybersécurité mais moins bien par vos autres cibles. Il est nécessaire d'avoir à l'esprit quelques conseils en matière de tempo de communication.

→ DANS LE CAS D'UNE POSTURE DE COMMUNICATION RÉACTIVE :

Questionnez le moment et la pertinence de votre première communication interne et/ou externe, en fonction de l'état des lieux (les faits, la situation en matière de communication et le contexte au moment de la crise cyber).

→ DANS LE CAS D'UNE POSTURE DE COMMUNICATION PROACTIVE :

- **Communiquez rapidement** car dans la société actuelle, les réseaux sociaux et les chaînes d'informations en continu ont fait de l'instantanéité de la diffusion des informations une caractéristique essentielle de la communication de crise. Au début de la crise cyber, vous disposez de très peu d'informations vérifiées. Votre première communication peut alors être courte et se limiter à indiquer que vous avez connaissance de l'incident et que vos équipes sont mobilisées pour le gérer. Dans tous les cas, ne communiquez jamais des informations non vérifiées, elles risquent de se retourner contre vous et de générer un *bad buzz*.
- **Évitez de donner une date de retour à la normale précise au début de l'incident** car des imprévus sont toujours possibles (exemples : l'attaquant revient et lance un rechiffrement, les équipes cyber/informatique sont confrontées à des difficultés techniques lors de la remédiation, etc.). Vous pouvez **informer régulièrement vos différentes parties prenantes** pendant la crise cyber en donnant de la visibilité sur les étapes des investigations et de la remédiation (dès que cette dernière est maîtrisée).
- **Priorisez les communications en fonction de vos cibles** en communiquant notamment auprès de vos collaborateurs et clients/usagers avant de réaliser un communiqué de presse.
- Dans la mesure du possible et sans que cela complexifie la situation pour votre entité, **occupez l'espace médiatique**, pour éviter que d'autres acteurs (experts, influenceurs, prestataires, clients, usagers, concurrents) ne s'expriment à votre place.

FOCUS
COMMUNIQUER SUR UNE EXFILTRATION DE DONNÉES PERSONNELLES

L'exfiltration de données est le vol ou le transfert non autorisé des données depuis un terminal ou un réseau vers une machine extérieure maîtrisée par un acteur malveillant. Une donnée personnelle est une information se rapportant à une personne physique identifiée ou identifiable, qui doit donc pouvoir en conserver la maîtrise. Une personne physique peut être identifiée directement (exemples : nom et prénom) ou indirectement (exemples : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou email, mais aussi par la voix ou l'image).

Une cyberattaque permettant d'exfiltrer des données personnelles est souvent suivie d'un chantage au déchiffrement, de la publication d'un échantillon et de la revente en source ouverte de ces données par l'attaquant.

Ce type d'attaque, par nature visible, a la plupart du temps un impact réputationnel significatif et peut susciter une grande inquiétude de la part de vos clients ou usagers et partenaires. De plus, selon la nature des données concernées, des sollicitations importantes peuvent émaner des médias nationaux ou étrangers et les commentaires sur les réseaux sociaux peuvent être nombreux. Ce type d'attaque nécessite donc une communication de crise adaptée.

FOCUS
COMMUNIQUER SUR UNE EXFILTRATION DE DONNÉES PERSONNELLES (SUITE)

Si un attaquant publie un échantillon de données qu'il désigne comme étant les vôtres, il est nécessaire de communiquer en plusieurs étapes.

1re COMMUNICATION :

Rapidement après la publication des données exfiltrées par l'attaquant, l'ANSSI conseille d'indiquer publiquement que vous avez pris connaissance de ce potentiel incident touchant votre entité. Indiquez qu'une qualification des données est en cours afin de confirmer ou non qu'elles vous appartiennent réellement.

3e COMMUNICATION :

En cas de risque élevé pour les droits et libertés d'une personne physique, l'entité victime doit informer individuellement de le vol de données à caractère personnel les personnes concernées dans les meilleurs délais. Vous trouverez dans l'***article 34*** du Règlement général sur la protection des données (RGPD) les conditions à remplir. Assurez-vous également que les personnes concernées puissent par ailleurs vérifier la légitimité de l'information reçue. L'information aux personnes concernées doit être individuelle par défaut, et sous dérogation peut être remplacée par une communication publique. Pour en savoir plus sur les dérogations prévues, veuillez vous référer à l'article 34 du RGPD.

2e COMMUNICATION :

Si les données exfiltrées n'appartiennent pas à votre entité, un démenti public sera alors nécessaire. Si les données exfiltrées appartiennent réellement à votre entité, confirmez l'exfiltration et la publication de données personnelles en ajoutant également un mot d'excuse vis-à-vis du dommage occasionné aux personnes concernées. Vous devez préciser si les données exfiltrées appartiennent à votre entité ou si ce sont des données de clients stockées par vos soins (dans le cas où vous êtes un sous-traitant). Si c'est le cas, il est important de préciser les mesures prises vis-à-vis des autorités : alerte de l'incident à l'ANSSI, dépôt de plainte auprès des services de police ou de gendarmerie spécialisés, la notification initiale et/ou complémentaire auprès de la CNIL. Pour réaliser une notification, rendez-vous sur ce site ***notifications.cnil.fr/notifications*** et vous pouvez également poser vos questions à ***violations@cnil.fr***. Indiquez également qu'une qualification précise des données est en cours pour déterminer leur nature et qu'un retour vers les personnes concernées par cette exfiltration sera fait, le cas échéant.

« Les crises cyber, par leur interdépendance et leur immédiateté, exigent une communication fondée sur l'objectivité et la pédagogie, structurée autour d'une stratégie pluridimensionnelle impliquant l'ensemble des parties prenantes de l'entreprise. »

Marie-Laure Fraux
Conseillère Communication,
Banque de France

À RETENIR

Il n'existe pas de stratégie de communication unique en réponse à une crise cyber. La stratégie adaptée dépend notamment des faits constatés, de la situation en matière de communication mais également du contexte. Au début d'une crise cyber, le communicant doit proposer à ses dirigeants une posture de communication à adopter : proactive ou réactive. Expliquer, informer, rassurer, préserver l'image et la réputation de l'entité et faire changer les comportements sont les objectifs de communication principaux. Il existe également plusieurs cibles à définir et à adresser aussi bien en interne (collaborateurs, managers, représentants du personnel, etc.) qu'en externe (journalistes, usagers, clients, actionnaires, partenaires, autorités, etc.). Concernant le tempo, le temps de l'analyse et de la remédiation de l'incident n'est pas aligné avec le temps médiatique. En cas de communication réactive, le communicant doit questionner le moment et la pertinence d'une première communication. En cas de communication proactive, le communicant doit communiquer rapidement uniquement des informations vérifiées, ne pas s'engager sur une date de retour à la normale précise, informer régulièrement et occuper l'espace médiatique si cela est possible. Il est également indispensable de prioriser les communications en fonction de vos cibles et notamment en informant en premier lieu vos collaborateurs et vos clients/usagers.