FICHE 6 PENDANT UNE CRISE CYBER

RÉDIGER LES MESSAGES CLÉS

1 INFORMATIONS FACTUELLES ET VÉRIDIQUES

Le sujet cyber est aujourd'hui fortement suivi par une communauté dédiée. Cette communauté cyber est composée d'influenceurs au sens large et de journalistes exigeants, qui aiment comprendre les modes opératoires des attaquants. Elle est très active sur les réseaux sociaux pour alerter sur des incidents, échanger sur des éléments techniques et commenter les revendications d'attaquants et parfois les communications officielles. La communauté cyber garde en mémoire les incidents et peut, même plusieurs mois après, revenir sur la manière dont ils ont été gérés y compris en matière de communication. Toute communication en période de crise est donc observée avec attention.

C'est pourquoi votre communication doit d'abord être **véridique**. Comme pour toute communication de crise, mentir est fortement déconseillé. Vous n'êtes pas obligé de tout dire, à chaque instant et à tout le monde, mais tout ce que vous dites doit être vrai. L'objectif est de faire preuve d'une transparence maîtrisée, par exemple en communiquant des points de situation réguliers. Si vous mentez ou refusez de communiquer, vos parties prenantes en déduiront que vous avez quelque chose à cacher et feront leurs propres suppositions, ce qui peut amplifier la crise médiatique en cours.

Votre communication doit également être **factuelle** : évitez les jugements de valeur. Ne minimisez/exagérez pas volontairement ou involontairement la sophistication de l'attaque subie car la supercherie sera vite découverte. Il est donc nécessaire de se baser sur les évaluations de votre équipe technique.

Enfin, il est conseillé de faire relire et valider vos messages par la cellule de crise stratégique.

FOCUS
LES *FAKES NEWS*

La quantité d'énergie nécessaire pour réfuter des mensonges est supérieure à celle nécessaire pour les produire. Cependant, lors d'une crise cyber, il est impératif de corriger les fausses informations publiées en interne comme en externe par les collaborateurs, internautes, journalistes, bots, etc.

2 TON ET VOCABULAIRES EMPLOYÉS

Lors de l'élaboration de vos messages, portez une attention particulière au vocabulaire et au ton employés. Le ton de votre communication doit être pédagogique, rassurant, et peut bien sûr évoluer avec la crise.

Concernant le vocabulaire à adopter :

- **Évitez les termes trop anxiogènes :** la cyberattaque est déjà génératrice de stress, il n'est donc pas nécessaire d'en rajouter.
- **Adaptez la technicité de vos messages en fonction du public ciblé :** la cybersécurité est par essence technique et connaît des évolutions technologiques rapides. Ainsi, si vous vous adressez à un lectorat non expert, il faudra vulgariser vos messages au maximum et définir les mots les plus complexes lorsque ceux-ci sont indispensables. A contrario, les points de situation transmis notamment à un centre de réponse aux incidents cyber (CSIRT) pourront adopter un vocabulaire technique adapté. Évitez également le jargon employé au sein de votre entité.

Pour vous aider dans la rédaction de vos supports, vous pouvez utiliser le CyberDico de l'ANSSI, gratuit et accessible sur le site Internet de l'Agence. Ce document de référence, liste, par ordre alphabétique, des mots, expressions et sigles du domaine de la cybersécurité. Il présente leur définition en français et en anglais et est mis à jour régulièrement.

FOCUS L'EMPATHIE ET L'HUMOUR

Opposer ou apporter uniquement des arguments factuels à une émotion collective est complexe. Un message d'empathie et d'excuse est indispensable en cas de cyberattaque (surtout si des personnes sont directement touchées, dans le cas d'un vol de données par exemple). De plus, opter pour l'humour afin d'alléger les tensions est déconseillé : la perception de l'incident est très différente en fonction des personnes. L'humour peut être perçu comme le signe d'une gestion légère ou déconnectée de la réalité, en contradiction avec la criticité et le stress vécu par certains acteurs.

3 ÉLÉMENTS DE LANGAGE ADAPTÉS

Pour vous aider à élaborer le contenu de votre communication, vous pouvez utiliser la grille ci-après. Cette dernière présente à la fois :

- **Une structuration selon la méthode FACET** (F pour Faits, A pour Actions, C pour Compassion, E pour Engagement et T pour Transparence) pour rédiger vos communiqués de presse, publications réseaux sociaux ou actualités web.
- **Les questions qui sont habituellement posées en cas de crise cyber.**
- **Des conseils pour écrire vos éléments de langage proactifs ou réactifs.**

FAITS

Potentielles questions posées par vos parties prenantes	Conseils pour écrire vos EDL proactifs
De quel type d'attaque s'agit-il ?	Il est préférable de parler « d'incident de cybersécurité » ou de « cyberattaque » plutôt que de « piratage informatique » pour être moins anxiogène. Dans le cas où l'attaque n'a pas aboutie, vous pouvez indiquer une « tentative d'intrusion sur votre système d'information ». S'il s'agit d'un problème technique et non d'une cyberattaque, il est important de l'indiquer en employant le terme de « panne technique » par exemple.
Quel est le vecteur d'attaque ?	Il existe différents vecteurs d'attaque : « informations d'identification compromises », « logiciels malveillants », « hameçonnage », « DDoS », « exploitation d'une vulnérabilité » ou d'une « vulnérabilité *zero-day* », etc. Les définitions de ces termes sont à retrouver dans le CyberDico de l'ANSSI. En interne comme en externe, limitez au strict minimum le partage des détails techniques sur la manière dont s'est passée l'attaque. Ils ne sont pas utiles pour vos publics et cela risquerait de donner des informations aux attaquants, s'ils sont toujours présents dans votre système d'information (cf. ***Fiche 5***).
Quelles sont les conséquences directes ou indirectes de la cyberattaque ?	Les conséquences peuvent être techniques, organisationnelles ou financières, sur la structure, les services ou les produits de votre entité. Il est également crucial d'indiquer s'il y a eu ou non une latéralisation de l'attaque à des entités partenaires ou clientes.

3 ÉLÉMENTS DE LANGAGE ADAPTÉS (SUITE)

FAITS

Potentielles questions posées par vos parties prenantes	Conseils pour écrire vos EDL proactifs
Est-ce qu'il y a eu une exfiltration de données ?	Dans le cas d'un potentiel vol de données, référez-vous à la ***Fiche 5***.
Quand est-ce que l'incident est arrivé ?	Vous devez indiquer une date plus ou moins approximative du début de l'attaque et/ou de détection de l'incident (exemples : « dans la nuit de vendredi à samedi », « ce matin »). Cet exercice est plus complexe à réaliser dans le cadre d'une attaque de type espionnage ou sabotage, car la compromission a souvent eu lieu plusieurs mois ou années avant d'être détectée. Dans ce cas, vous pouvez uniquement indiquer la date de détection de l'incident.
L'attaque est-elle toujours en cours ?	Si l'attaque est finie, il est possible de répondre à cette question en indiquant qu'« à la suite de nos investigations et de nos actions d'endiguement et de remédiation, nous n'observons plus de trace de l'attaquant dans le système d'information ».

ACTION

Potentielles questions posées par vos parties prenantes	Conseils pour écrire vos EDL proactifs
Quelles sont les actions mises en œuvre ?	**Il est indispensable de mettre en avant :** ▸ Les actions mises en œuvre pour stopper la cyberattaque et rétablir au plus vite les produits ou services affectés (exemple : isolation du réseau, coupure temporaire de certains services, déconnexion des accès clients/tiers pour les protéger, durcissement de certains accès, etc.). ▸ La mise en place d'une cellule de crise. ▸ Les services ou produits affectés ou non par la cyberattaque. ▸ La continuité des activités en mode normal ou dégradé. ▸ Les contacts en cas de question (exemple : adresse email générique ou numéro vert).

3 ÉLÉMENTS DE LANGAGE ADAPTÉS (SUITE)

ACTION

Potentielles questions posées par vos parties prenantes	Conseils pour écrire vos EDL proactifs
Êtes-vous accompagné par l'ANSSI ?	**Le cas échéant, vous pouvez indiquer que :** ▸ Vous avez prévenu l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de la situation. ▸ Vous êtes accompagné par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour traiter votre incident. Cette mention doit faire l'objet d'une validation par l'ANSSI : ***cert-fr@ssi.gouv.fr***.
Êtes-vous accompagné par des prestataires ?	La mention de l'accompagnement de votre entité par des experts en cybersécurité privés (prestataire de réponse à incidents - PRIS) ou par des CSIRT (sectoriel, territorial ou ministériel) est recommandée pour rassurer vos publics.
Est-ce que les collaborateurs, clients ou usagers ont des mesures à prendre ? Peuvent-ils bénéficier de bonnes pratiques ?	**Dans vos différentes communications, vous pouvez transmettre des consignes pratiques à vos collaborateurs, clients ou usagers :** ▸ Demander expressément à ne pas surcharger les lignes téléphoniques du service informatique de votre entité déjà mobilisé sur l'incident. ▸ Donner des consignes techniques ou organisationnelles pour que les collaborateurs puissent continuer à travailler. ▸ Transmettre des bonnes pratiques de cybersécurité, comme le changement des mots de passe, la mise en place de la double authentification ou la forte vigilance sur les emails reçus.
Quelles mesures ont été prises vis-à-vis des autorités ? **En cas de vol de données personnelles, une notification auprès de la CNIL a-t-elle été réalisée ?** **Une plainte auprès des services de police ou de gendarmerie spécialisés a-t-elle été déposée ?**	**Le cas échéant pour montrer votre capacité à gérer correctement votre crise cyber :** ▸ Indiquez dans votre communication que vous avez réalisé une notification initiale et/ou complémentaire auprès de la CNIL et spécifiez, le cas échéant, que les personnes concernées ont été/seront informées individuellement (et spécifier le canal si connu). ▸ Précisez qu'un dépôt de plainte a eu lieu. Cette judiciarisation aura pour conséquence de limiter vos actions de communication car certains éléments précis de l'attaque ne pourront pas être dévoilés sans l'accord préalable du service enquêteur.

3 ÉLÉMENTS DE LANGAGE ADAPTÉS (SUITE)

COMPASSION

Potentielles questions posées par vos parties prenantes	Conseils pour écrire vos EDL proactifs
Est-ce que votre entité a un mot pour les victimes de cet incident ?	Il convient de s'adresser, en faisant preuve de compassion, non seulement aux victimes directes de la crise, mais également à tous ceux qui pourraient se considérer comme telles. La méthode FACET devient CAFET (C pour Compassion en premier et les Faits après les Actions) lorsque la crise fait des victimes physiques (blessés ou décès). Dans ce cas, la compassion à leur égard passe avant toute autre considération.

ENGAGEMENT

Potentielles questions posées par vos parties prenantes	Conseils pour écrire vos EDL proactifs
Quel est le niveau de prise en compte de cet incident au sein de votre entité ?	Il est nécessaire de montrer que votre entité a réagi rapidement et efficacement et est fortement mobilisée pour gérer l'incident, avec notamment la mise en place d'une cellule de crise. Vous pouvez aussi rappeler que la sécurité des systèmes d'information et la protection des données personnelles sont au cœur de vos priorités.
Quelles mesures allez-vous mettre en place à l'avenir ?	Vous pouvez indiquer les actions déjà réalisées en matière de cybersécurité de votre système d'information ces dernières années et les enseignements tirés de cette crise cyber (exemple : la mise en place d'un plan d'action supplémentaire ou le déblocage d'un budget dédié à la cybersécurité).

3 ÉLÉMENTS DE LANGAGE ADAPTÉS (SUITE)

TRANSPARENCE

Potentielles questions posées par vos parties prenantes	Conseils pour écrire vos EDL proactifs
Combien de temps cela va-t-il durer ? **Quelles sont les prochaines étapes à venir jusqu'à la sortie de la crise ?** **À quand un retour à la normale ou à un fonctionnement optimal ?**	Vous devez faire de la pédagogie sur le temps que nécessitent les investigations et la remédiation. Les analyses techniques sont souvent longues, la remédiation peut prendre du temps et des surprises peuvent arriver. Ne vous engagez pas au début de la crise sur une date précise de retour à la normale mais donnez plutôt de la visibilité à chaque étape des investigations ou de la remédiation (cf. ***Fiche 5***). **Les éléments ci-après peuvent être utilisés** : « La durée de l'indisponibilité des produits et services, tout comme le calendrier de retour à la normale ne sont pas encore déterminés. » « Le service est momentanément indisponible. »
Quand partagerez-vous de nouvelles informations ?	Pour répondre à cette question, vous pouvez indiquer que les investigations et la remédiation continuent et que de nouvelles informations seront communiquées dès qu'elles seront disponibles. Par exemple : « Nous continuerons à informer régulièrement nos différentes parties prenantes au fur et à mesure de l'avancée de nos investigations et de la remédiation. ».
Qui contacter en cas de questions ?	En interne comme en externe, il est nécessaire de protéger la cellule de crise et les équipes techniques de nombreuses sollicitations incommodantes avec « un cordon sanitaire » pour leur permettre de se focaliser sur la résolution de l'incident. Vous pouvez par exemple mettre en visibilité un formulaire de contact ou une adresse email générique créée pour l'occasion, mais cela nécessitera de gérer les demandes qui pourront être nombreuses. Il est également possible d'activer un numéro vert pour traiter un grand nombre d'appels. En interne, il est conseillé de cadrer clairement au début de la crise les échanges avec les médias. Demandez aux collaborateurs de renvoyer les demandes presse vers votre service de presse, dans le cas où ils seraient contactés par des journalistes, afin de centraliser la gestion des relations presse.

Les éléments suivants sont des sujets que l'ANSSI recommande d'aborder uniquement de manière réactive.

Potentielles questions posées par vos parties prenantes	Conseils pour écrire vos EDL proactifs
Qui est l'attaquant ? Quelles sont ses motivations ?	**Les autorités françaises distinguent l'imputation d'une attaque informatique (à un mode opératoire ou à un groupe d'attaquants) de l'attribution politique à un commanditaire identifié.** ▸ Les attaquants peuvent facilement tenter de se faire passer pour ceux qu'ils ne sont pas en réalisant parfois des fausses revendications, ou en laissant de fausses traces sur leur passage pour brouiller les pistes. L'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. ▸ L'attribution publique d'une attaque informatique est une décision politique, prise au plus haut niveau de l'Etat, qui vise à désigner le groupe d'attaquants ou le commanditaire, généralement un État, comme responsable de cette attaque. C'est pourquoi, même si les médias vont rapidement vous demander qui est derrière la cyberattaque que vous subissez, il est vivement conseillé de ne pas indiquer publiquement d'informations sur les attaquants. Cela vous évitera de vous tromper, de faire la publicité des attaquants ou bien d'ajouter une dimension géopolitique à votre crise, qui sera difficilement maîtrisable.
Avez-vous reçu une demande de rançon et si oui, avez-vous payé la rançon ?	**Si la demande de rançon est déjà publique, vous pouvez la confirmer dans vos messages.** **L'ANSSI recommande de ne jamais payer la rançon.** En effet, le paiement d'une rançon ne garantit pas l'obtention d'un moyen de déchiffrement ou, dans le cas de l'obtention de ce dernier, de reconstituer l'intégralité des fichiers chiffrés. Il ne permettra pas la restitution des données exfiltrées et ne garantit pas la non publication de ces dernières. Enfin, le paiement incite les cybercriminels à poursuivre leurs activités, entretient ce système frauduleux et n'empêchera pas votre entité d'être à nouveau la cible de cybercriminels. **Si vous êtes une entité publique, vous pouvez utiliser les éléments suivants :** « Conformément à la doctrine de l'État français et des administrations publiques, aucun paiement ne sera effectué auprès des cybercriminels. » Si votre entité décide tout de même de payer la rançon, il est obligatoire, dans le cadre du Code des assurances[6], de déposer plainte en amont afin de pouvoir activer les clauses de votre contrat d'assurance. Gardez à l'esprit que même en étant discret, un rétablissement rapide de votre système d'information mettra la puce à l'oreille des spécialistes en cybersécurité. Le paiement de la rançon ne fera pas disparaître la revendication de l'attaquant et l'information du paiement pourra même être relayée par l'attaquant.

6. Code des assurances, Chapitre X : L'assurance des risques de cyberattaques (Article L12-10-1).

EN COMPLÉMENT, GARDEZ À L'ESPRIT QUE :

- **Chaque incident étant unique**, il est indispensable de réaliser des messages adaptés à la situation et aux publics identifiés (cf. ***Fiche 5***).
- **Les messages devront évoluer tout au long de la crise.**
- **La répétition des messages est un principe de base** de la communication et est donc à utiliser sans modération.

« En pleine crise cyber, la réactivité en termes de communication interne comme externe est clef. Il est essentiel d'établir rapidement des éléments de langage clairs, précis et partagés afin de reconnaître et d'expliquer la situation et prévenir ainsi rumeur et emballement médiatique. »

François Lecerf
Directeur Commercial & Marketing,
Groupe LGM

À RETENIR

Utilisez un ton pédagogique et rassurant pour votre communication. Évitez les termes trop anxiogènes et adaptez la technicité de l'information en fonction du public. En utilisant la méthode FACET (F pour Faits, A pour Actions, C pour Compassion, E pour Engagement et T pour Transparence), les informations communiquées doivent être factuelles et véridiques.