FICHE 8 PENDANT UNE CRISE CYBER

PILOTER SA COMMUNICATION DE CRISE EXTERNE

LA VEILLE MÉDIATIQUE

Durant une crise cyber, la veille médiatique est un outil stratégique incontournable pour concevoir et adapter la posture de communication.

En amont de la crise, le veille peut permettre de déceler des signaux faibles, notamment sur les réseaux sociaux, annonciateurs d'un incident technique (publication d'un influenceur, revendication d'un attaquant, etc.). Dans ce cas, le communicant doit alerter les différentes parties prenantes concernées (dirigeants de l'entité, équipe cyber/informatique, etc.).

Au démarrage et pendant la crise cyber, une veille couvrant les médias et les réseaux sociaux, doit être mise en place et suivie si possible par une personne dédiée. Il est également utile de suivre les éventuelles prises de parole politiques et les réactions des collaborateurs en interne (en lien avec le chargé de communication interne). Cette veille permettra de mieux comprendre la réalité médiatique et la pression subie par votre entité, d'orienter votre communication de crise cyber, d'évaluer l'efficacité de celle-ci et d'identifier les questions récurrentes ou critiques fréquentes de vos parties prenantes sur l'incident et sur sa gestion.

Face à la masse d'informations disponibles, réaliser une veille efficace nécessite une démarche méthodique.

1/ IDENTIFIEZ LES INFORMATIONS PERTINENTES SUR VOTRE INCIDENT À VEILLER

Pour suivre la perception de la situation, sélectionnez les bons mots-clés et associez-les à vos outils de veille. Ils doivent être suffisamment larges pour capter un maximum d'informations pertinentes, mais assez précis pour éviter un trop plein de « bruit médiatique ». Pensez à les décliner au pluriel et en différentes langues. Par exemple :

- **Le nom de votre entité**
- **Le nom des produits ou services**
- **Le nom de vos dirigeants**
- **Les termes** « cyberattaque », « incident », « attaque cyber », « attaque informatique », « incident de sécurité », « fuite de données », « vol de données », « vente de données », « publication de données », « piratage », « rançon », « *ransomware* », « *malware* », « faille de sécurité », « DDoS », « déni de service », « hameçonnage », « vulnérabilité », etc.

2/ IDENTIFIEZ LES SOURCES PERTINENTES À VEILLER

Sélectionnez les sources médiatiques que vous souhaitez suivre :

- **Agences de presse**
- **Presse écrite** (titres nationaux, régionaux, internationaux, spécialisés dans votre secteur d'activité, etc.) et leurs déclinaisons (papier, web et comptes sur les réseaux sociaux)
- **Médias en ligne** (sites d'actualités généralistes et thématiques, blogs influents, forums de discussion, etc.)
- **Réseaux sociaux** comprenant des comptes de journalistes, experts, leaders d'opinion et influenceurs
- **Radios et télévisions** (locales, régionales, nationales et internationales)

3/ UTILISEZ DES OUTILS PERTINENTS DE VEILLE

Plusieurs outils et services de veille existent, gratuits ou payants :

- **Des outils d'alerte** vous envoient des notifications directement par email lorsque des contenus récemment publiés (uniquement sur le web) contiennent vos mots-clés.
- **Des outils automatiques** (agrégateurs de contenus ou plateformes de veille professionnelles) vous permettent de tout regrouper au même endroit et travaillent automatiquement en repérant en temps réel les contenus publiés avec vos mots-clés sur l'ensemble des sources.
- **Des agences de communication spécialisées** peuvent également effectuer cette veille pour vous.

4/ ANALYSEZ ET DIFFUSEZ EN INTERNE LES RÉSULTATS DE VOTRE VEILLE

Une fois que vos outils ont repéré des contenus liés à vos mots-clés, analysez-les attentivement en adoptant une vision d'ensemble. Pour faciliter cette démarche, la création de tableaux de bord est recommandée (à l'aide de différents graphiques afin de visualiser rapidement les grandes tendances qui se dégagent). Durant votre crise cyber, votre veille médiatique vous permettra d'analyser :

- **Le volume des publications**, mentions, *likes*, impressions, commentaires, repartages, etc.
- **La tonalité des messages** : positive (soutien, engagement favorable), négative (critique, polémique, mécontentement), neutre (partage d'informations factuel).
- **Les narratifs dominants** (reprise de vos messages clés, rumeurs, accusations, attentes de vos parties prenantes, etc.).
- **La vitesse de propagation des informations.**
- **Les prises de parole sur les réseaux sociaux** (des dirigeants, de vos collaborateurs, des représentants du personnel, etc.).
- **Les sources des messages** (journalistes, influenceurs, personnel politique, etc.) mais également la diffusion par des bots de fausses informations.
- **Le relai et l'engagement suscités par vos actions de communication de crise** (viralité du partage d'un communiqué de presse, engagement de vos publications dédiées à l'incident, etc.).

Les résultats de votre veille peuvent être partagés efficacement en interne via des rapports de veille (qui peuvent aussi être générés automatiquement par les outils), des alertes email, une newsletter, sur l'intranet, etc.

Les *chatbots* d'intelligence artificielle (IA) génératifs, très utilisés sur certains réseaux sociaux, sont devenus des leaders d'opinion et évoquent peut-être déjà votre entité. Lors d'une crise cyber, ils peuvent avancer des informations fausses ou partiellement vraies concernant votre entité, que les utilisateurs peuvent parfois prendre comme véridiques. Il est donc crucial de prendre en compte ces nouvelles sources d'informations dans votre veille médiatique.

LA COMMUNICATION DIGITALE

Les réseaux sociaux et le site web sont des outils incontournables en communication de crise cyber dont il faut faire usage à bon escient.

Suspendez toutes les communications prévues sur vos réseaux sociaux jusqu'à ce que vous ayez défini votre stratégie de communication de crise. N'oubliez pas de supprimer les publications programmées ou sponsorisées sur vos outils de *social media management*. Assurez-vous de la pertinence de votre actualité à la Une sur votre site web au moment de l'incident.

L'information (et la désinformation) circule vite sur les réseaux sociaux, et le public s'attend à des réponses immédiates. Sans précipitation, assurez-vous que **la première publication publiée sur vos réseaux sociaux après le déclenchement de la crise est une réponse pertinente** et qui résonne pour vos cibles externes. La première impression est la plus importante !

Les réseaux sociaux sont des plateformes pour diffuser des informations officielles mais également maintenir le dialogue avec le public. Il est par conséquent **nécessaire de gérer les commentaires ou publications des internautes intelligemment**. Vous pouvez répondre aux critiques légitimes avec des EDL réactifs (à adapter selon votre ligne éditoriale habituelle) ou rediriger vers un canal privé si nécessaire. Il est conseillé de laisser visibles les commentaires négatifs pour éviter une surréaction de leurs auteurs mais déconseillé de répondre aux trolls, particulièrement présents sur certains réseaux sociaux. Leur objectif est de vous discréditer en vous poussant à la faute par tous les moyens, et le plus souvent par la malice et la provocation.

Il est préférable d'**adapter votre message à chaque plateforme en soignant le format des publications** (photo, vidéo, image, texte, etc.). Prenez la précaution de cacher les informations sensibles sur les photos et utilisez des emojis. Il est également nécessaire d'utiliser un hashtag pertinent, souvent le plus utilisé pour qualifier l'évènement en cours. Une attention particulière doit également être portée à la régularité et aux horaires des publications pour être visible par le plus grand nombre. Attention cependant à ne pas trop multiplier les formats afin de conserver une communication d'ensemble cohérente.

Ne laissez pas vos collaborateurs (cf. ***Fiche 7***) **alimenter la crise médiatique par des déclarations spontanées et maladroites sur les réseaux sociaux**. À la place, en utilisant le cas échéant votre programme d'*employee advocacy*, il est recommandé de faire appel aux collaborateurs clés, « vos ambassadeurs », pour qu'ils puissent diffuser des informations prédéterminées et validées via leurs comptes réseaux sociaux. Votre communication sera par conséquent davantage incarnée et amplifiée.

LA COMMUNICATION DIGITALE (SUITE)

Pour partager vos messages, vous pouvez **utiliser l'espace « Actualités » de votre site web**. Si l'incident rend votre site web indisponible, vous pouvez mettre en place un site temporaire le temps de la crise avec les informations essentielles sur votre entité. Si, faute de temps, vous ne pouvez pas l'alimenter, indiquez rapidement dans un bandeau sur votre page d'accueil que les informations concernant la crise cyber en cours sont consultables sur vos comptes réseaux sociaux.

Pour réaliser une communication transparente sur les réseaux sociaux, **montrer les coulisses de la gestion de crise peut être très utile**. Vous pouvez pour cela réaliser des publications (photos, etc.) avec vos collaborateurs « en action » lors de la mise en place de mesures permettant la continuité de service.

Gardez en tête qu'**une publication peut devenir virale et susciter beaucoup de réactions**. Cette diffusion rapide et imprévisible peut être positive, ou au contraire, se transformer en *bad buzz* atteignant ainsi l'image de votre entité ou de vos dirigeants. Le phénomène prend le plus souvent naissance sur les réseaux sociaux avant de se prolonger éventuellement sur d'autres médias.

Vous pouvez également diffuser votre conférence de presse en direct sur les réseaux sociaux pour en maximiser la portée auprès d'une large communauté, pas seulement de journalistes.

Les réseaux sociaux (et notamment LinkedIn) permettent au dirigeant de porter des messages lors d'une crise de manière simultanée et directe (sans le filtre d'intermédiaires), à différentes parties prenantes (collaborateurs, clients, usagers, investisseurs, médias, etc.). **La parole du dirigeant, en son nom, permet d'humaniser le message et de rassurer en montrant que la crise est gérée au plus haut niveau**. Les publications de votre dirigeant peuvent également être repartagées par les comptes réseaux sociaux de votre entité.

LES RELATIONS PRESSE

La manière dont vous interagissez avec les journalistes pendant une crise cyber aura un impact significatif sur la perception de vos cibles (clients/usagers, prestataires, partenaires financiers, autorités, collaborateurs, citoyens, etc.). Vous devez réussir à créer une relation de confiance avec les journalistes, basée sur le respect de leurs contraintes, la transparence et la régularité des informations transmises. Gardez à l'esprit que vous ne pouvez pas contrôler certains paramètres déterminants :

- Chaque journaliste est libre de ses choix éditoriaux (le titre, l'angle, etc.), et il décide avec sa hiérarchie de reprendre ou non les informations transmises.
- La priorité éditoriale peut changer à tout moment en fonction de l'actualité et vous n'avez pas la possibilité de fixer l'heure de publication.

Dans un contexte de défiance médiatique, d'infobésité, de montée en puissance de l'intelligence artificielle, les relations presse peuvent jouer, en fournissant aux journalistes des informations fiables et vérifiées, un rôle de rempart contre la désinformation.

Il est donc crucial de travailler étroitement avec votre équipe en charge des relations presse pour préparer les différents contenus à destination des journalistes :

- **Un communiqué de presse** (voir focus dédié)
- **Une interview** (voir focus dédié)
- **Une conférence de presse** (voir focus dédié)

→ Avant toute chose, si la cyberattaque que vous subissez est visible, mettez en pause toutes les actions presse que vous aviez prévues avant le déclenchement de l'incident. La crise cyber en cours sera le seul sujet d'intérêt des journalistes, il n'est donc pas opportun de communiquer comme si de rien n'était sur d'autres thématiques.

→ En cas d'incident, vous pourrez être sollicité par vos contacts journalistes habituels mais également par la presse spécialisée en informatique et par les journalistes de médias généralistes travaillant au sein des services cybersécurité/tech. L'ANSSI ne communique généralement pas à la place des victimes, c'est pourquoi nous redirigeons automatiquement les demandes presse reçues sur les incidents vers les (potentielles !) victimes.

→ Le rôle de chacun en matière de communication de crise cyber doit clairement être défini, partagé et compris par tous. Pour une meilleure maîtrise du message, il est conseillé de limiter le nombre d'interlocuteurs des médias et de les préparer en amont à l'exercice de la prise de parole médiatique. En période de crise, le dirigeant incarne naturellement le porte-parole privilégié : sa prise de parole souligne l'engagement fort de l'entité et renforce la crédibilité des messages diffusés. Cependant, plusieurs autres porte-paroles peuvent également être identifiés et utilisés de manière graduelle, afin de mobiliser le dirigeant uniquement au plus fort de la crise.

FOCUS
L'IA, UN RECOURS PARFOIS UTILE EN TEMPS DE CRISE

À noter qu'une relecture orthographique de vos contenus avant publication est a minima une action réalisable par une IA générative. Vous pouvez également demander à une IA, à l'aide d'un prompt pertinent, d'écrire vos différents contenus de communication de crise (communiqués de presse, publications réseaux sociaux, etc.). Cependant, ne transmettez aucunes données sensibles ou confidentielles à ce type d'outils et relisez avec un sens critique les contenus proposés. Le Service d'information du Gouvernement (SIG) a élaboré une charte d'usage de l'intelligence artificielle pour les communicants de l'État, en cohérence avec les autres référentiels communs (marque de l'État, charte d'accessibilité, système de design de l'État). Vous trouverez ce document sur le site ***Info.gouv.fr.***

1/ LE COMMUNIQUÉ DE PRESSE

Le communiqué de presse est un outil très utile lors d'une crise cyber lorsqu'il est bien rédigé mais il peut être contre-productif s'il est trop compliqué à comprendre, s'il est trop succinct ou s'il n'est pas envoyé aux bons destinataires.

AVANT DE COMMENCER

Il est nécessaire de réfléchir à l'objectif que vous voulez atteindre avec la diffusion d'un communiqué de presse. Avant de le rédiger, posez-vous les questions suivantes :

- **Pour qui j'écris ?**
  Si vous communiquez sur une crise cyber, vous vous adresserez à la fois à des journalistes spécialisés cybersécurité/tech (et leur lectorat) et à des journalistes généralistes (et leur lectorat).

- **De quoi je parle ?**
  Votre communiqué doit répondre à la règle des 6W :

  Who / Qui ?
  Qui est concerné ?
  Qui est à l'origine ?
  What / Quoi ?
  Quel est l'événement ?
  Que s'est-il passé ?
  When/ Quand ?
  Quand cela s'est-il produit ?
  Quand cela va-t-il se produire ?
  Where / Où ?
  Où cela se passe-t-il ?
  Why / Pourquoi ?
  Pourquoi cela arrive-t-il ?
  Quelles sont les causes ou les motivations ?
  How / Comment ?
  Comment cela s'est-il produit ?
  Comment réagir ?

1/ LE COMMUNIQUÉ DE PRESSE (SUITE)

▸ **Pourquoi j'en parle ?**
Les journalistes reçoivent plusieurs dizaines de communiqués de presse par jour, le vôtre doit être efficace. Gardez en tête que vous n'écrivez pas pour vous, ni pour votre entité, mais pour les journalistes à qui vous vous adressez.

LE CONTENU DE VOTRE COMMUNIQUÉ

Introduction du communiqué :
Mettez votre logo, indiquez le lieu et la date, surtout si vous pouvez être amené à en republier d'autres dans les jours suivants.

Le titre :
C'est la partie la plus importante de votre communiqué de presse :

- Rédigez-le en dernier (une fois le contenu écrit, pour qu'il reflète le reste du communiqué).
- Il doit contenir assez d'informations pour que la personne qui le reçoit comprenne rapidement de quoi il s'agit, sous la forme :
  Sujet > Action > Objet de l'actualité.
- Soyez concis (pas plus de deux lignes). Lorsque votre communiqué de presse sera repris par un média, le titre sera certainement « copié/collé » puis partagé sur les réseaux sociaux.

Le chapô / l'accroche :
Répondez en une ou deux phrases aux 6W énoncés un peu plus haut.Faites au plus simple et au plus concret.

- Ne cherchez pas à ce stade à rentrer dans les détails.

Le corps du communiqué :
Il est recommandé d'adopter la méthode FACET (Faits, Actions, Compassion, Engagement et Transparence) pour rédiger le corps de votre communiqué de presse (cf. ***Fiche 6***).

En complément :

- Vérifiez que votre communiqué répond bien aux 6W.
- Rédigez à la troisième personne, comme un journaliste le ferait dans un article de presse.
- Vous pouvez inclure une citation (de préférence des dirigeants de votre entité) pour incarner un message important.
- Évitez le jargon, car votre communiqué doit être accessible à tous (cf. ***Fiche 6***).

La conclusion :

- Ajoutez des informations complémentaires en quelques mots sur votre entité, ce qu'on appelle plus communément le « à propos » (ou *boilerplate*).
- Indiquez la/les personnes à contacter pour plus d'informations (votre attaché(e) de presse ou votre agence de relations presse).

2/ LA CONFÉRENCE DE PRESSE

Ce format peut être très pertinent, car il permet en une seule prise de parole de transmettre de nombreux messages à un grand nombre de journalistes. La conférence de presse présente également un intérêt pour les journalistes qui auront l'occasion d'échanger avec un ou des porte-paroles lors de la session de questions/réponses.

Cependant, cela reste un exercice périlleux : l'entité doit être en mesure de répondre aux questions, évidemment nombreuses, des journalistes sur la crise cyber ou sur tout autre sujet d'actualité.

Lorsque vous programmez votre conférence de presse, votre première préoccupation doit être de **choisir un moment et un lieu qui s'adaptent à l'emploi du temps des journalistes tout en considérant vos propres contraintes.** Vous devez également dresser une liste des médias à inviter.

Prévoyez de prévenir au plus tôt les journalistes et d'inclure dans l'invitation une brève description de l'objectif de la conférence de presse ainsi que des détails importants tels que la date, l'heure et le lieu. Ayez à l'esprit que votre conférence de presse peut être diffusée en direct sur une chaîne de télévision ou sur le web et que son impact n'en sera que plus important.

Lors d'une crise cyber, l'objectif d'une conférence de presse est généralement de faire un point d'étape sur la situation. Elle se déroule habituellement en 3 parties :

- Une prise de parole descendante, d'un ou plusieurs porte-paroles.
- Une session de questions/réponses avec les journalistes présents.
- Des interviews du porte-parole sous forme de micro-tendu pour les médias audiovisuels à l'issue de la conférence de presse.

Des échanges informels et complémentaires avec certains journalistes peuvent également être organisés dans la foulée.

Attention, la conférence de presse a un caractère exceptionnel. Le format, de moins en moins suivi par les journalistes, car chronophage, ne peut fonctionner que s'il est perçu comme un évènement rare, qui mérite le déplacement.

3/ L'INTERVIEW

L'interview peut être réalisée par écrit, en audio (en studio, par téléphone) ou en vidéo (en plateau, en duplex), enregistrée ou en direct. Dans ce cas, le journaliste attendra de vous :

- Des premières ou nouvelles informations vis-à-vis de votre crise cyber.
- Du concret avec une descriptions des faits (cf. ***Fiche 6***) et des chiffres.
- Un porte-parole qui s'exprime clairement, qui est précis et utilise des formules percutantes.

3/ L'INTERVIEW (SUITE)

À noter qu'il peut être stratégique et efficace de faire une déclaration exclusive à une agence de presse majeure, telles que l'Agence France-Presse (AFP), Associated Press (AP), Reuters ou Bloomberg, selon la nature des activités et les intérêts, français ou étrangers, de votre entité. L'agence, via une dépêche, relaiera ensuite les messages à l'ensemble des médias nationaux et internationaux. Cette méthode présente plusieurs avantages:

- **Contrôle du récit:** en limitant les sources directes, on réduit les risques de distorsion ou de multiplication des interprétations.
- **Gain de temps:** une seule interaction avec une agence évite de multiplier les échanges avec différents journalistes.
- **Couverture médiatique large et homogène**: la dépêche, reprise par les rédactions, assure une diffusion rapide et unifiée de l'information.

« Victime d'une cyberattaque en 2025 atteignant ses bases de données, la ville a immédiatement informé les usagers. Habituée à la gestion de crise par son exposition aux risques industriels, la ville a appliqué les mêmes méthodes, une information précise portant sur les faits et les conséquences connues de l'attaque. »

Romain Boix
Directeur de Cabinet,
Pont de Claix

À RETENIR

En cas de crise cyber, la veille médiatique est indispensable: surveillez les mentions, la tonalité des échanges, et les narratifs dominants pour ajuster votre communication en temps réel. Les réseaux sociaux et le site web sont des canaux stratégiques: suspendez les publications programmées et adaptez vos messages à chaque plateforme. Pour les relations presse, centralisez les demandes via le service de presse et préparez un communiqué de presse en suivant la méthode FACET et la règle des 6W. Attendez-vous à être sollicité par vos contacts médiatiques habituels, mais aussi par des journalistes spécialisés en cybersécurité/tech. L'ANSSI ne se substitue pas aux victimes pour communiquer et redirige systématiquement les demandes presse vers l'entité concernée.