FICHE 7 PENDANT UNE CRISE CYBER

PILOTER SA COMMUNICATION DE CRISE INTERNE

Lors d'une crise cyber, la communication interne est stratégique. Les collaborateurs doivent être informés, rassurés et alignés pour éviter les discours contradictoires, les rumeurs, les fuites d'informations voire la panique.

S'ILS SONT TOUJOURS DISPONIBLES, CONTINUEZ D'UTILISER LES OUTILS DE COMMUNICATION INTERNE « CLASSIQUES » :

- **Réunion d'équipe ou briefing managers** (en présentiel ou en visio)
- **Email interne ou newsletter** (avec un objet clair « Information importante – incident cyber en cours »), qui peut comprendre un message porté par vos dirigeants
- **Intranet**
- **Réseau social d'entreprise**
- **Messagerie interne**
- **Solution d'affichage dynamique sur des écrans**
- **Affichage papier dans les locaux** (salle de pause, cafétéria, etc.)

SI LA CRISE CYBER EMPÊCHE L'ACCÈS À VOS OUTILS « CLASSIQUES », UTILISEZ DES SOLUTIONS ALTERNATIVES POUR MAINTENIR LA COMMUNICATION AVEC VOS COLLABORATEURS :

- **Téléphone et emails personnels**
- **Application de messagerie instantanée temporaire**
- **Groupe fermé sur un réseau social grand public**
- **Brochures avec consignes**
- **Adresse email temporaire** (hors de votre système d'information) **créée sur un service de messagerie gratuit pour les particuliers**
- **Formulaire de contact sur l'intranet**
- **Mode « papier crayon »**
- **Courrier postal**

PRIORITÉ À L'INTERNE

Il est nécessaire de donner la « primeur » de votre communication à votre cible interne (avant la communication externe) car ce sont souvent les premières personnes concernées par les impacts de l'incident. Par exemple, un rançongiciel qui bloque les accès au système d'information se manifeste souvent par l'affichage sur les écrans d'ordinateur d'une demande de rançon, voire d'un décompte. Ce mode opératoire génère très souvent émoi et anxiété au sein des équipes et empêche les collaborateurs de travailler. L'objectif est aussi d'éviter que vos collaborateurs découvrent des informations sur la crise en cours dans les médias ou sur les réseaux sociaux. Tenez également compte de leurs horaires de travail et des éventuels décalages horaires avec vos équipes à l'étranger pour définir le tempo de vos communications internes.

CHANGEMENT DES COMPORTEMENTS

La communication interne est un levier indispensable pour faire changer les comportements en matière de cybersécurité. En cas de cyberattaque, il est fréquent d'adresser des communications internes pour expliquer la mise en place de l'authentification multifacteur (MFA) ou inciter vos collaborateurs à changer leurs mots de passe. L'enjeu est alors d'accompagner le changement sans créer une vague de panique ou de désorganisation en interne.

DISCRÉTION ET CONFIDENTIALITÉ

La porosité entre communication interne et communication externe est plus forte que jamais, ce qui implique de faire attention aux contenus diffusés aux collaborateurs (cf. ***Fiche 5***). Il est très fréquent de voir des communications internes fuiter en externe.
La diffusion ou le rappel de la conduite à tenir de la part des collaborateurs sur les réseaux sociaux ou vis-à-vis des médias est également indispensable.

- **Relations presse :** demandez à vos collaborateurs de ne pas répondre directement aux sollicitations des médias et de les transmettre au service de presse de votre entité ou, à défaut, aux dirigeants. L'objectif est de centraliser les échanges, d'évaluer précisément le niveau de pression médiatique et ainsi de garantir une réponse cohérente et maîtrisée.
- **Réseaux sociaux :** il est recommandé durant la crise de restreindre les prises de parole individuelles sur l'incident en rappelant les risques réputationnels et juridiques (exemples : la clause de confidentialité du contrat de travail ou le devoir de réserve, la discrétion ou le secret professionnel pour les agents de la fonction publique).

PROXIMITÉ

Vous pouvez également utiliser l'ensemble des niveaux hiérarchiques de votre entité (managers, dirigeants, etc.) pour diffuser largement vos messages à destination de vos collaborateurs (cf. ***Fiche 5***). En effet, le manager de proximité demeure le maillon essentiel de la chaîne d'information.

« Une communication de crise maîtrisée implique d'informer rapidement et régulièrement les collaborateurs. Les modalités de communication interne doivent donc être définies à froid. Cela est d'autant plus vrai lorsqu'il s'agit d'anticiper une cyberattaque pouvant provoquer l'indisponibilité de certains outils de communication interne. »

Clémence Picart
Directrice adjointe du dialogue et de la communication de l'Autorité de sûreté nucléaire et de radioprotection

À RETENIR

Informez en priorité vos collaborateurs pour éviter rumeurs et panique. Utilisez des moyens alternatifs si vos canaux « classiques » sont indisponibles. Gardez en tête que vos communications internes risquent de fuiter en externe. Rappelez la conduite à tenir à vos collaborateurs sur les réseaux sociaux ou vis-à-vis des médias. La communication interne vous permettra également d'accompagner les collaborateurs vers de nouvelles pratiques plus sécurisées.