# FICHE 1 AVANT UNE CRISE CYBER

# INITIER UN DIALOGUE INTERNE ET ANTICIPER DES SCÉNARIOS

Lorsque survient une crise cyber, l'équipe cyber/informatique, dont le responsable de la sécurité des systèmes d'information (RSSI) et le délégué à la protection des données (DPO), et l'équipe communication sont fortement mobilisées. Faire connaissance dans ces conditions est compliqué.

Pour assurer une communication de crise cyber pertinente, il est donc indispensable d'initier un dialogue entre les équipes cyber/informatique et communication en amont. L'objectif est de mieux se connaître et de comprendre les priorités, les enjeux et le vocabulaire de chaque métier. Le responsable informatique est capable de rendre compte en temps réel de la situation technique et de ses possibles évolutions. Le communicant dispose, lui, d'une connaissance fine des cibles (interne et externe) de l'entité ainsi que des moyens de communication disponibles. Cette acculturation mutuelle peut se réaliser sous différentes formes :

- **Ateliers de travail dédiés.**
- **Campagnes de sensibilisation interne,** à l'occasion par exemple du Cybermois, organisé chaque année en octobre pour sensibiliser les publics européens à la cybersécurité et leur permettre d'adopter les bons réflexes.
- **Exercices de gestion de crise cyber**[1]**.**

Chaque entité doit également conduire une analyse des risques[2] menaçant de déstabiliser ses activités. Les acteurs impliqués dans la gestion de crise et l'équipe cyber/informatique doivent anticiper plusieurs scénarios de crise cyber réalistes (DDoS, rançongiciel, défiguration, etc.). Il est alors recommandé de préparer des stratégies de communication de crise (cf. ***Fiche 5***) en réponse aux différents scénarios identifiés qui peuvent ensuite être testées dans le cadre d'un exercice. Sans être exhaustif, l'anticipation de ces stratégies de communication permet, le jour J, d'avoir une première base sur laquelle s'appuyer pour avancer efficacement et gagner du temps.

1. Pour en savoir plus, consultez le guide de l'ANSSI « ***Organiser un exercice de gestion de crise cyber*** ».
2. Pour en savoir plus, consultez la méthode EBIOS Risk Manager.

## FOCUS
## LES RESSOURCES DE CYBERMALVEILLANCE.GOUV.FR

En l'absence d'une équipe cyber/informatique en interne, des prestataires ou des dispositifs comme Cybermalveillance.gouv.fr[3] peuvent donner des clés de compréhension de la cybersécurité.

**À RETENIR**

En amont d'une crise cyber, il est indispensable que les équipes communication et cyber/informatique se rencontrent afin d'avoir une meilleure compréhension mutuelle des priorités, des enjeux et du vocabulaire de chacun. Sur la base des scénarios de crise cyber probables (DDoS, rançongiciel, défiguration, etc.), il est recommandé de préparer différentes stratégies de communication.

> « L'acculturation régulière des équipes communication aux différentes formes de menaces cyber est indispensable pour faciliter la coordination lors d'une crise. »

Laurent Baude
**Responsable de la communication sensible et de crise, Groupe RATP**

3. La plateforme ***Cybermalveillance.gouv.fr***, lancée en 2017, est un dispositif national de sensibilisation, de prévention et d'assistance aux victimes d'actes de cybermalveillance pour les particuliers, entreprises et collectivités territoriales.