FICHE RÉFLEXE · GESTION DE CRISE

Cyberattaque : les 10 premiers réflexes

Les premières heures d'une cyberattaque conditionnent l'ampleur des dégâts. Imprimez cette fiche et gardez-la à portée de main, hors de votre système d'information.

01 Isoler sans éteindre

Débranchez le câble réseau et coupez le Wi-Fi des machines touchées. Ne les éteignez pas : leur mémoire contient des traces utiles à l'enquête.

02 Alerter immédiatement

Prévenez votre service informatique, votre RSSI ou votre prestataire, de préférence par téléphone : la messagerie peut être compromise.

03 Ne pas payer la rançon

Le paiement ne garantit ni la récupération des données ni leur non-divulgation. Ne contactez pas les attaquants.

04 Préserver les preuves

N'effacez rien. Notez les heures, les messages affichés, les comportements anormaux. Conservez les journaux.

05 Activer la cellule de crise

Qui décide, qui agit, qui communique ? Utilisez un canal de communication de secours, hors du système d'information.

06 Changer les mots de passe depuis un poste sain

En priorité les comptes d'administration et la messagerie, depuis un équipement que vous savez non compromis.

07 Déclarer

À la CNIL sous 72 h si des données personnelles sont concernées. Si vous êtes soumis à NIS2, alerte précoce à l'autorité sous 24 h. Déposez plainte.

08 Se faire accompagner

Faites appel à un prestataire spécialisé en réponse à incident. Le dispositif public cybermalveillance.gouv.fr oriente vers des professionnels.

09 Prévenir votre assureur

Votre contrat peut prévoir des délais de déclaration et une assistance. Vérifiez-le dès maintenant, pas le jour de l'attaque.

10 Redémarrer proprement

Ne remettez en service qu'après avoir identifié le mode d'intrusion, sur des systèmes reconstruits et à partir de sauvegardes saines.

Fiche indicative : adaptez-la à votre organisation et complétez-la avec vos numéros d'urgence (informatique, direction, prestataire, assureur).