Réagir à un acte de cyber-malveillance

Qu'est-ce qu'un acte de cyber-malveillance ?

Un acte cyber malveillant est une cyber attaque visant le système informatique **d'une entreprise** ou **d'une solution**. Plusieurs situations peuvent en découler comme un chiffrement via un rançongiciel, une extraction de données ou un déni de service.

1 Mesures d'urgence :

En cas de demande de rançon, **ne pas la payer, ni prendre contact avec un tiers suggéré** ;

Déconnecter les machines du réseau (ne pas les éteindre) ;

Alerter les responsables ou contacter les prestataires :

- Rechercher un **prestataire de réponse à incident qualifié par l'ANSSI** (https://www.ssi.gouv.fr/) ;
- Rechercher un **prestataire local au travers du portail cyber malveillance** (https://www.cybermalveillance.gouv.fr/)
- **Pour les structures de santé**, contacter le **CERT-Santé** au 09 72 43 91 25 ou signaler l'incident ici : https://signalement.socialsante.gouv.fr

Ressources mises à disposition :

- Réaction à un acte malveillant (PDF);
- En cas d'incident de l'ANSSI (Site web).

2 Dépôt de plainte :

La plainte déposée a pour but de **protéger l'établissement** dans le cas où les infrastructures corrompues aient été utilisées à mener des attaques sur des tiers. Elle consiste à **décrire l'attaque**, sa réussite ou son échec, les éventuels dommages qui peuvent en résulter ainsi que toutes les autres conséquences. Il est donc important de **conserver toutes les traces utiles à l'enquête** (logs, copies écran, etc.).

3 Notification à la CNIL :

Lorsque l'incident implique **des données à caractère personnel présentant un risque pour les droits et libertés des personnes**, il faut notifier les informations demandées à la CNIL au lien suivant https://notifications.cnil.fr/notifications/index.

La notification à l'autorité doit être faite **dans les 72 heures à compter de la découverte de l'incident.**

4 Réagir efficacement suppose de se préparer en amont :

- **Sensibilisation du personnel** à la menace de cybersécurité ;
- Définition d'une **organisation de crise** en capacité de réagir ;
- Disposition d'un **plan de reprise et de continuité du SI** ;
- Recours à **une assurance spécifique** couvrant les pertes potentielles ;
- Amélioration **des pratiques en capitalisant sur les incidents rencontrés.**