Réagir à un acte de cybermalveillance

Mesures de prévention

- **Sensibiliser le personnel à la menace de cybersécurité** (hameçonnage, demande de rançon, fichiers suspects, etc…)
- **Définir et faire connaitre la procédure** d'alerte à l'ensemble des personnels
- **Définir une organisation de crise** en capacité de réagir rapidement en cas d'incident et capable de mettre en œuvre les mesures d'urgence
- En cas de perte de disponibilité des données, **disposer d'un plan de reprise et de continuité du SI**, même sommaire, tenu régulièrement à jour et décrivant comment restaurer les données essentielles
- **Vérifier les engagements contractuels avec vos prestataires** concernant la gestion d'un incident de cybersécurité et la reprise d'activité
- **Etudier le recours à une assurance spécifique** couvrant les pertes potentielles liées à un incident de cybersécurité
- **Améliorer les pratiques** en capitalisant sur les incidents rencontrés

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 votre responsable et votre support informatique** (ou contacter votre prestataire). Rechercher un prestataire de réponse à incident qualifié par l'ANSSI (https://www.ssi.gouv.fr/) ou un prestataire local au travers du portail https://www.cybermalveillance.gouv.fr/
- **Déclarer l'incident sur le portail des signalements** https://signalement.social-sante.gouv.fr ou appeler directement le CERT Santé au **09 72 43 91 25** en cas d'incident majeur (au-delà de 18h et les jours non ouvrés, contacter le CERT-FR (cert-fr.cossi@ssi.gouv.fr , tel : 01 71 75 84 68))

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 permet également parfois de confondre les auteurs. Elle consiste à **décrire l'attaque**, sa réussite ou son échec, les éventuels dommages qui peuvent en résulter ainsi que toutes les autres conséquences (perte de temps pour vérification de l'intégrité des données, pertes d'argent, perte de crédibilité auprès des patients, etc..). Il est donc important de **conserver toutes les traces utiles à l'enquête** (logs, copies écran, …).

Il est recommandé de déposer une plainte pour **atteinte à un traitement automatisé de données** (appellation juridique du piratage) prévu et dont la punition relève des articles 323-1 et suivants du code pénal. Cette plainte peut être recueillie par :

- Le **Service Régional de Police Judiciaire**. Le commissariat de police ou la gendarmerie le plus proche disposent de leurs coordonnées. Une fois en contact avec la S.R.P.J. il faut demander à parler à un « Investigateur en cybercriminalité » autrement dit un I.C.C qui pourra enregistrer la plainte ;
- L'**Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication** par téléphone (01 49 27 49 27) ou par courrier électronique oclctic@interieur.gouv.fr qui orientera la demande (voir coordonnées complètes au lien suivant O.C.L.C.T.I.C.).

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 de contrôle doit être faite **dans les 72 heures à compter de la découverte de l'incident** : la nature de la violation et les catégories et le nombre approximatif de personnes concernées par la violation ; les coordonnées du délégué à la protection des données ou toute autre personne responsable ; les conséquences probables et les mesures de remédiations prises ou envisagées. **En cas de risque élevé pour les personnes physiques**, la notification aux personnes concernées par la violation **doit se faire dans les meilleurs délais**.