Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

STRUCTURE DE SANTE - REAGIR À UN ACTE DE CYBERMALVEILLANCE

ORIGINES POSSIBLES

Activation accidentelle d'un lien (hypertexte, chemin d'accès réseau) ou d'un code malveillant véhiculé par un message électronique ou une clé USB, exposition non souhaitée de données internes sur Internet, exploitation d'une vulnérabilité du système par un attaquant, etc…

OBJECTIFS D'UNE ATTAQUE

Les objectifs sont multiples. Il s'agit, en général, pour l'attaquant d'en tirer un profit (paiement d'une rançon en échange du déchiffrement de données, vente des données sur le dark web, chantage, etc.) ou de la notoriété.

RISQUES

- ➔ **PERTE D'INTEGRITE DES DONNEES POUVANT IMPACTER LA PRISE EN CHARGE DES PATIENTS**
- ➔ **PERTE D'IMAGE**
- ➔ **PERTE FINANCIERE**
- ➔ **PERTE DE PRODUCTIVITE**

CONSTAT

- Des postes informatiques, des serveurs ou le site Web ne fonctionnent plus, redémarrent de façon inopinée ou subissent des lenteurs anormales.
- Impossibilité d'accéder aux fichiers (en local ou en réseau)
- Un poste affiche un message indiquant une demande de rançon ou les coordonnées d'un support technique à contacter de toute urgence pour cause de dysfonctionnement grave
- Le site Web est défiguré ou publie en ligne du contenu non identifié
- Un ou plusieurs comptes de messagerie ont été utilisés à l'insu de leur(s) propriétaire(s)

MESURES D'URGENCE

- Ne pas payer de rançon 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 le cas échéant) selon la procédure en vigueur
- en cas de besoin, si vous ne disposez pas de prestataire de confiance, rechercher un prestataire local au travers du portail https://www.cybermalveillance.gouv.fr/ pour une intervention sur site
- Déclarer l'incident sur le portail des signalements https://signalement.social-sante.gouv.fr pour disposer d'un appui du ministère pour mettre en œuvre les mesures d'urgences (structures concernées par le décret n°2016-1214)
- Au-delà de 18h ou lors d'un jour non ouvré et au regard de la criticité de l'incident, en cas de besoin d'une assistance dans les plus brefs délais, informer le FSSI des Ministères sociaux (ssi[@]sg.social.gouv.fr) en parallèle du signalement sur le portail.

S'ORGANISER POUR MIEUX REPONDRE

- 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
- Améliorer les pratiques en capitalisant sur les incidents rencontrés

STRUCTURE DE SANTE - REAGIR À UN ACTE DE CYBERMALVEILLANCE

VIOLATION DE DONNÉES

Lorsqu'un incident porte spécifiquement sur l'intégrité, la confidentialité ou la disponibilité de données de personnes physiques, on parle d'une violation de données à caractère personnel.

OBJECTIF DÉPOT 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, ...).

RESSOURCES

- Portail cyberveille-santé
- Portail cybermalveillance.fr
- Portail cert-fr
- Portail de la CNIL

NOTIFICATION A 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 et au moins reprendre les deux derniers points énoncés ci-dessus.

DÉPOT DE PLAINTE

En cas d'acte de cybermalveillance, 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.).