Fiches réflexes :

POSTE DE TRAVAIL BLOQUÉ PAR UN RANSOMWARE (RANÇONGICIEL)



Situation

Votre ordinateur affiche un message vous informant que vos données sont bloquées ou chiffrées. Une rançon est exigée pour les récupérer.

Objectif

Limiter la propagation de l'attaque, protéger les données, et alerter les bons interlocuteurs rapidement.

Isoler le poste dans l'immédiat :

- Déconnectez immédiatement le réseau (Wi-Fi ou câble Ethernet).
- Si vous n'avez pas d'autre choix, éteignez le poste.

Cela empêche la propagation à d'autres ordinateurs.

Ne pas tenter de corriger seul :

- Ne redémarrez pas le poste.
- Ne cliquez sur rien, ne suivez aucune consigne à l'écran.
- Ne payez jamais la rançon.

Alerter sans délai :

Prévenez immédiatement votre référent cybersécurité ou le service informatique, ainsi que votre responsable hiérarchique.

Transmettez la capture d'écran du message affiché, avec l'heure approximative de l'apparition et ce que vous faisiez juste avant sur la poste de travail.

Ne pas diffuser d'information :

- Ne prévenez pas les collègues vous-même
- Ne communiquez pas en externe

L'équipe responsable organisera la communication officielle

Attendre les consignes :

L'équipe en charge décidera :

- Des analyses à mener
- D'un éventuel déclenchement du plan de gestion de crise
- De la déclaration de l'incident (CERT Santé, CNIL...)

À retenir :

- Un ransomware se propage vite : chaque minute compte
- Votre premier réflexe peut limiter les dégâts
- En cas de doute, mieux vaut prévenir pour rien que tardivement