Journal du gestionnaire des incidents

Date : 2025–05-05	**Entrée** : 1
Description	Rapport d'incident de cybersécurité impliquant un rançongiciel ayant causé une interruption majeure des services dans une petite clinique américaine spécialisée en soins primaires.
Outil(s) utilisé(s)	Aucun
QQQOP	• **Qui :** Un groupe organisé de pirates informatiques, connu pour cibler les secteurs de la santé et des transports. • **Quoi :** Un incident de sécurité impliquant un rancongiciel • **Où :** Dans une petite entreprise du secteur de la sante, située aux États-Unis • **Quand :** Mardi matin, vers 9 heures. • **Pourquoi :** l'incident a ete cause par un groupe de hackers malveillant qui ont reussi a acceder aux systemes de l'entreprise par le biais d'une attaque **rançongiciel** (attaque par hameçonnage). Ensuite, ils ont deploye leur rancongiciel au sein des systemes de l'entreprise et chiffre des fichiers critiques. Le groupe exige une forte rançon en échange de la clé de déchiffrement, suggérant une motivation financière claire.
Autres remarques	**1. Prévention** : L'entreprise pourrait réduire les risques futurs en : • Formant ses employés à reconnaître les tentatives d'hameçonnage. • Mettant en place un filtre de messagerie performant. • Effectuant des sauvegardes régulières et hors ligne. • Mettant à jour les systèmes et logiciels régulièrement. **2. Payer la rançon ?** : Le paiement n'est **pas recommandé** par les autorités compétentes (ex. FBI, ANSSI), car : • Il n'y a aucune garantie de récupération des données. • Cela alimente le modèle économique des cybercriminels. • Des alternatives existent via des spécialistes en récupération ou grâce à des sauvegardes (si disponibles).