MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Groupement de gendarmerie départementale de la Somme

17 janvier 2025

ALERTECYBERGEND80

Ce jour, le directeur d'une **entreprise samarienne** se présente dans la brigade de gendarmerie de son secteur afin de déposer plainte suite à une **cyberattaque** dont son entreprise a été **victime**. L'ensemble des **ordinateurs** de l'entreprise a été compromis par un **logiciel rançonneur** (rançongiciel, ou ransomware en anglais).
Les systèmes sont totalement **inopérants**, son activité est **paralysée.** Un message s'affiche sur chaque écran, réclamant une **rançon** en échange de la restauration des données. Alors même que le montant de la rançon demandée n'a pas encore été spécifié par les cybercriminels, il est d'ores-et-déjà établi que cette attaque entraînera des **pertes financières considérables**.

CONSEILS DE PRÉVENTION

Les rançongiciels constituent une menace de plus en plus importante pour les **entreprises**, les **collectivités** et les **particuliers**. Voici quelques conseils pour vous aider à vous protéger :

- **1. Maintenez vos systèmes à jour** : assurez-vous que vos systèmes d'exploitation et vos logiciels sont à jour avec les derniers patchs de sécurité, pour corriger les vulnérabilités connues ;
- **2. Utilisez un logiciel antivirus fiable** offrant une protection en temps réel contre les menaces émergentes ;
- **3. Soyez vigilant face aux e-mails suspects** : ne cliquez pas sur les liens ou n'ouvrez pas les pièces jointes provenant d'expéditeurs inconnus ou douteux ;
- **4. Sauvegardez régulièrement vos données** : effectuez des sauvegardes régulières de vos données sur un disque dur externe et/ou un stockage cloud sûr. Déconnectez les disques de sauvegarde de votre système lorsqu'ils ne sont pas utilisés pour éviter leur chiffrement ;
- **5. Formez vos employés** : sensibilisez vos employés aux risques liés aux rançongiciels et aux bonnes pratiques de sécurité. Organisez des simulations d'attaques pour évaluer la réactivité de vos collaborateurs ;
- **6. Limitez les privilèges d'accès** : accordez à chaque utilisateur les droits d'accès minimums nécessaires à l'exécution de ses tâches ;
- **7. Sécurisez vos réseaux** : utilisez un pare-feu pour protéger votre réseau des intrusions et un réseau privé virtuel (VPN) pour sécuriser vos connexions (si vous travaillez à distance) ;
- **8. Évitez les réseaux Wi-Fi publics non sécurisés** : évitez d'effectuer des transactions financières ou d'accéder à des informations sensibles sur des réseaux Wi-Fi publics ;
- **9. Mettez en place un plan de récupération après sinistre** : élaborez un plan de récupération après sinistre et testez-le régulièrement pour vérifier son efficacité ;
- **10. Ne payez pas la rançon** : payer la rançon encourage les cybercriminels à poursuivre leurs activités et ne garantit en aucun cas la récupération de vos données.