Conseils en cas de cyberattaque

Toutes structures présentes sur Internet, peuvent être la cible des cybercriminels.

Les conséquences d'une attaque informatique peuvent être atténuées, à condition de prendre les bonnes mesures et d'agir vite... car, en matière de cybercriminalité, le temps joue contre nous.

Cette notice explique les premières actions à entreprendre en cas d'attaque par rançongiciel.

PS-SEC/202203.01

COMMENT RÉAGIR EN CAS D'ATTAQUE PAR RANÇONGICIEL

En cas de suspicion d'attaque par rançongiciel, des mesures urgentes doivent être prises :

1. **Isoler votre informatique de l'extérieur :** couper les connexions Internet, l'accès VPN ou tout autre accès distant.
2. **S'assurer que vos sauvegardes sont intègres** et les déconnecter du reste de votre infrastructure. Cela permettra de procéder à la restauration ultérieure des systèmes.
3. **Contacter la Police cantonale (117)** et demander l'entité cybercrime pour annoncer l'incident. Cette entité sera votre point de contact avec les autorités cantonales et vous aidera dans vos démarches (dépôt de plainte et première analyse), et impliquera les experts du Centre opérationnel de sécurité vaudois (SOC) en cas de nécessité.
4. **Une cellule de crise** doit être mise en place le plus rapidement possible avec, au minimum, un responsable de la communication, un responsable informatique et une personne avec des compétences en cybersécurité.
5. **S'appuyer sur un prestataire spécialisé** en *Incident Response,* qui pourra vous aider dans la gestion technique de l'incident en cybersécurité. La collecte de preuves, via les journaux de connexions (logs) de vos équipements, sera une des premières étapes techniques effectuées afin de comprendre l'attaque et son ampleur.
6. **Annoncer l'incident auprès de la Confédération** (NCSC / GovCERT) via le site https://www.report.ncsc.admin.ch/fr/

canton de vaud

Direction générale du numérique et des systèmes d'information (DGNSI)

Prenez en main votre sécurité informatique, utilisez ce QR code et suivez gratuitement une formation en ligne.

Pour les professionnels, rendez-vous sur : www.vd.ch/cybersecurite/