culture
Saguenay–Lac-Saint-Jean

RANSOMWARE

Savoir se protéger des logiciels malveillants et bien réagir en cas d'attaque

QU'EST-CE QU'UN RANSOMWARE ?

Un ransomware (ou rançongiciel) est un logiciel malveillant qui chiffre vos fichiers et réclame une rançon pour les déverrouiller. Sans paiement (et parfois même après), vos données peuvent être perdues ou publiées.

Impacts réels :

- Paralysie totale des systèmes
- Pertes financières majeures
- Atteinte à la réputation
- Violations de données personnelles

COMMENT ÇA ARRIVE ?

- Email de phishing avec pièce jointe piégée (Voire aide-mémoire sur le phishing)
- Lien malveillant dans un courriel ou SMS
- Site web compromis
- Clé USB infectée branchée sur un poste
- Accès RDP non sécurisé (télétravail)
- Logiciel piraté ou mal source
- Attaque via un fournisseur

SIGNAUX D'ALERTE

- Fichiers qui s'ouvrent plus ou ont une extension inconnue.
- Ordinateur anormalement lent ou disque dur très actif
- Message de rançon sur l'écran
- Antivirus désactivé sans raison
- Accès refusé à vos propres fichiers
- Connexions réseau inhabituelles la nuit
- Comptes utilisateurs créés à votre insu

culture
Saguenay–Lac-Saint-Jean

BONNES PRATIQUES DE PROTECTION

✓ SAUVEGARDES	✓ ACCÈS ET SYSTÈMES	✓ VIGILANCE HUMAINE
Plusieurs copies, 2 supports différents, 1 hors site	MFA (authentification multifacteur) partout	Former les employés au phishing régulièrement
Sauvegarde quotidienne automatisée	Mises à jour et correctifs en temps réel	Ne jamais ouvrir une PJ suspecte
Tester la restauration régulièrement	Principe du moindre privilège	Vérifier l'expéditeur avant tout clic
Sauvegardes déconnectées du réseau (air gap)	Segmentation réseau (isoler les systèmes critiques)	Signaler immédiatement tout comportement anormal
Stocker une copie immuable dans le cloud	EDR/antivirus à jour sur tous les postes	Exercices de simulation d'attaque (phishing test)

QUE FAIRE EN CAS D'ATTAQUE ?

Procédure d'urgence

1 ISOLER :
Déconnecter immédiatement le(s) poste(s) du réseau (Wi-Fi, câble, VPN). Ne pas éteindre.
✷ ***Dans la minute !***

2 ALERTER :
Contacter immédiatement le responsable IT/sécurité et la direction. Ne rien tenter seul.
✷ ***Téléphoner ; ne pas envoyer de email !***

3 DOCUMENTER :
Prendre des photos de l'écran (message de rançon). Noter l'heure et les systèmes touchés. ✷ ***Avant de faire quoi que ce soit !***

4 SIGNALER :
Déposer une plainte (police/GRC). Notifier les autorités (si données personnelles touchées).
✷ ***Obligation légale possible***

5 RESTAURER :
Restaurer les sauvegardes saines. Ne jamais payer sans avis expert. Faire une analyse forensique.
✷ ***Depuis une sauvegarde propre***

FAUT-IL PAYER LA RANÇON ?

La réponse est NON dans la grande majorité des cas parce que :

- ✘ Payer ne garantit pas la récupération des données
- ✘ Cela finance et encourage les criminels
- ✘ Vous devenez une cible récurrente connue
- ✘ Des obligations légales peuvent l'interdire

CONTACTS D'URGENCE

- Responsable IT/Sécurité : _____
- Direction / DG : _____
- Service juridique : _____
- Centre canadien pour la cybersécurité : 1-833-CYBER-88 (1-833-292-3788) contact@cyber.gc.ca
- GRC / Police locale : 911

CHIFFRES CLÉS — RANSOMWARE 2025-2026

Toutes les 11 secondes une organisation est victime d'une attaque ransomware dans le monde	Coût moyen 4,9 M$ par incident (incluant récupération, temps d'arrêt, réputation)	Plus de 91% des attaques débutent par un email de phishing	Les organisations avec sauvegardes récupèrent 5× plus vite et paient moins souvent

En cas de doute, NE CLIQUEZ PAS !
→ Signalez immédiatement à votre équipe IT