Guide de réunion

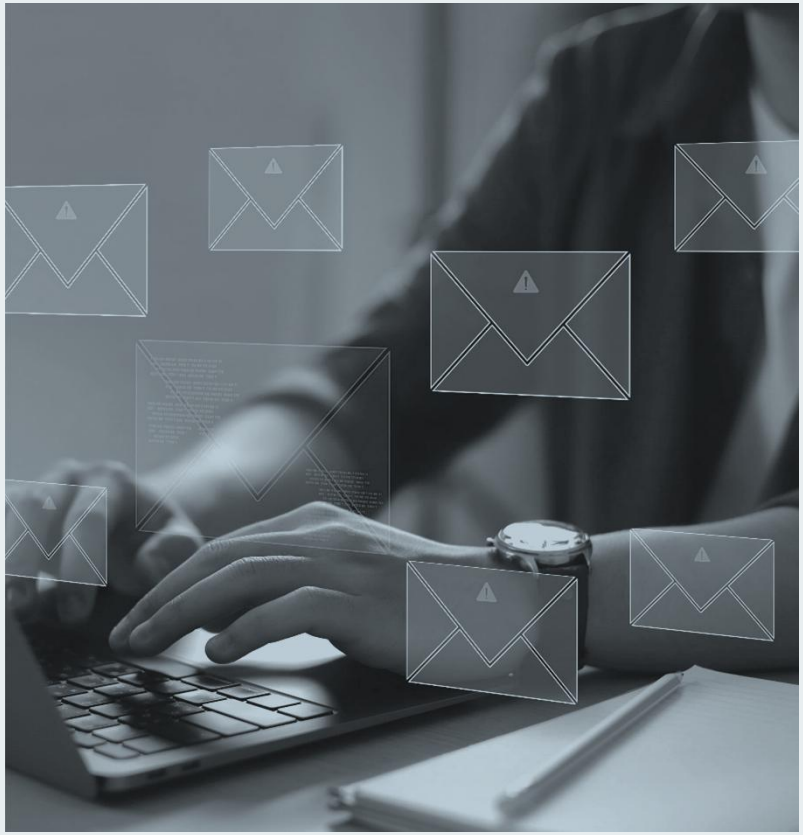
Rançongiciel

Thèmes abordés

Annexes

cyber eco

Quelques chiffres et trois objectifs



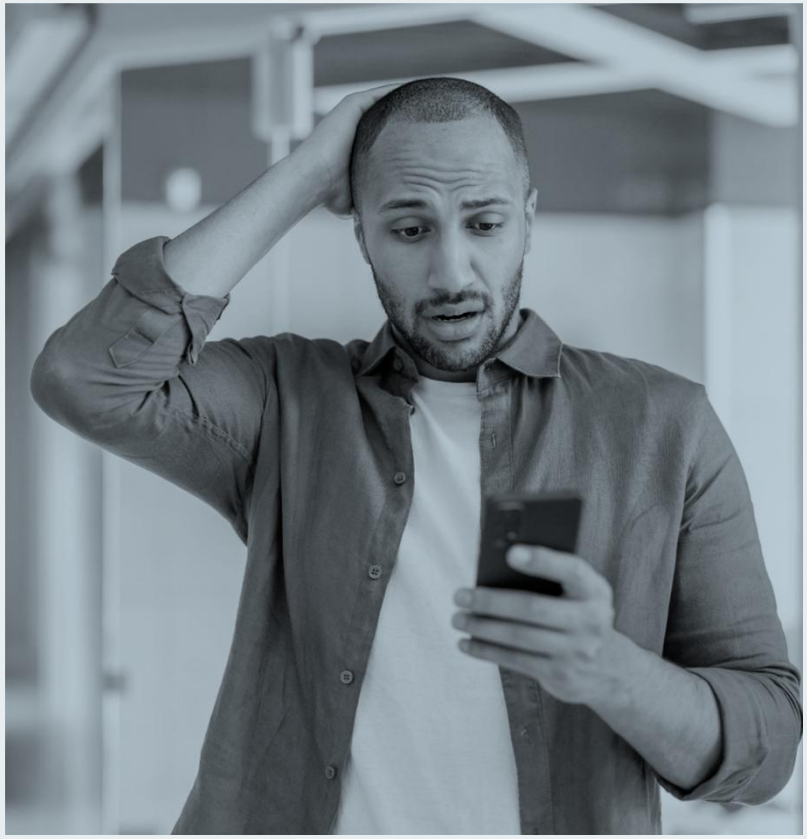
- En 2025, **60 %** des PME victimes d'un rançongiciel **ferment** dans les **6 mois** suivant une **attaque**
- Le **coût moyen** d'une attaque dépasse **200 000 $**

Objectifs de l'atelier : **Prévenir · Répondre · Se relever**

La préparation est notre meilleure défense!

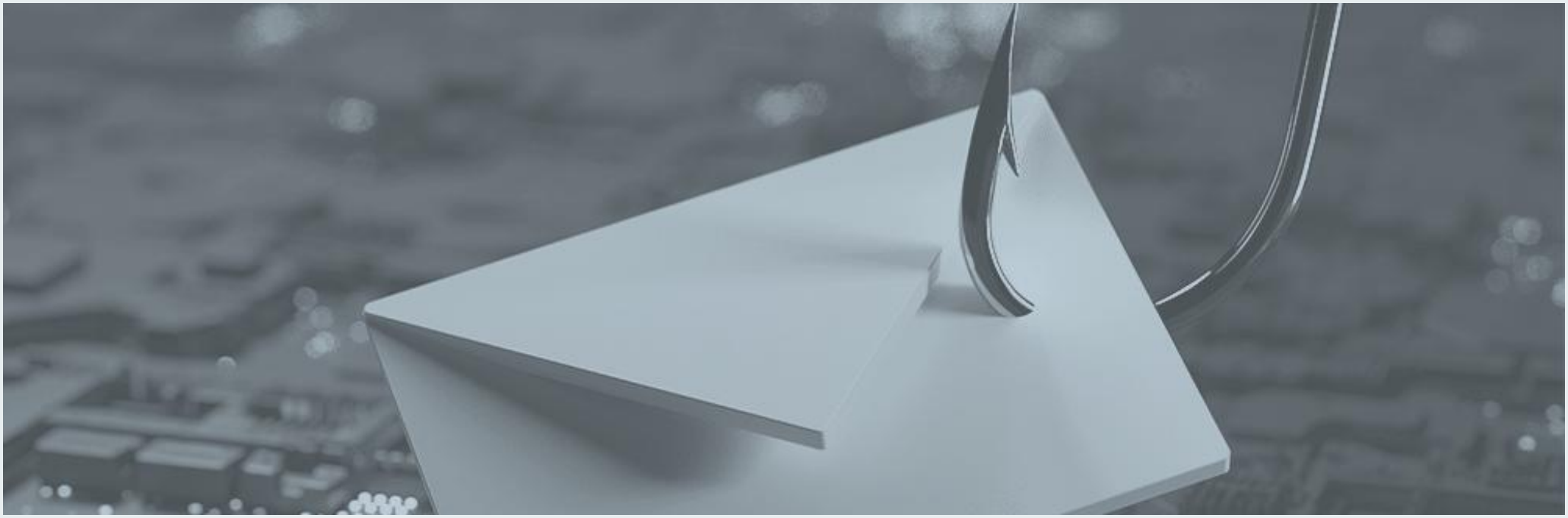
Pourquoi les PME sont-elles ciblées?

- Ressources limitées
- Dépendance aux données critiques (données sans lesquelles l'entreprise ne peut pas fonctionner normalement)



Les attaques par rançongiciel sont facilitées par, notamment, un **modèle criminel répandu** :

- **Rançongiciel en tant que service** (RaaS – Ransomware-as-a-Service)
- Semblable à un abonnement à un service infonuagique… pour activités illégales



Comment s'introduit un rançongiciel dans une entreprise?

Principaux points d'entrée ou vecteurs d'attaque

1. **Courriels frauduleux (hameçonnage)** – quelqu'un clique sur un lien ou une pièce jointe suspecte
2. **Accès à distance mal protégés** – mot de passe faible, authentification multifacteur non activée, RDP/VPN exposés
3. **Logiciels non mis à jour** – failles connues dans les systèmes ou applications

Que faire... Avant?

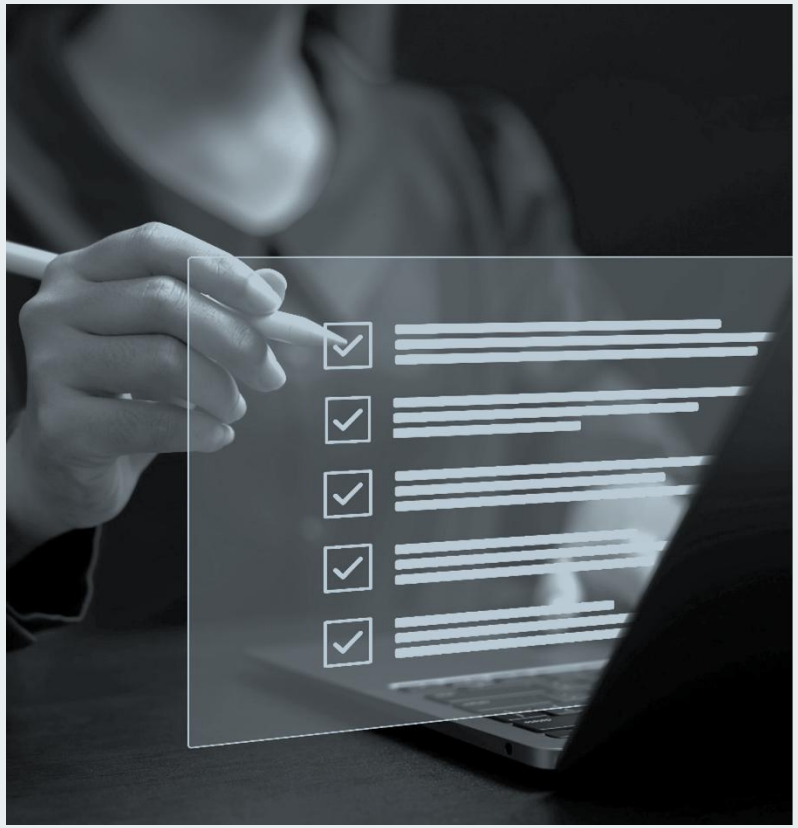
Prévention et préparation

Sensibiliser les employé(e)s à reconnaître les signaux d'alerte d'un **courriel d'hameçonnage** :

- pression ou urgence
- fautes subtiles
- adresse d'expéditeur légèrement modifiée
- liens suspects ou raccourcis
- demandes inhabituelles

Renforcer les politiques de **mot de passe** plus strictes (taille, historiques, complexité, ... etc.)

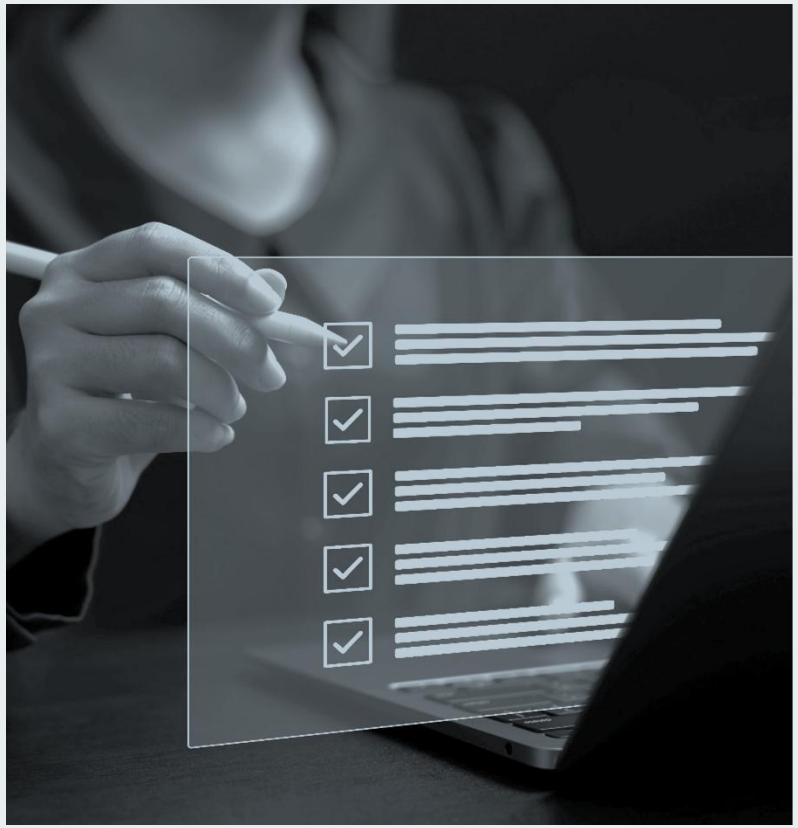
Activer l'**authentification multifacteur** (MFA) pour tous les comptes, appliquer le principe du moindre privilège (non accorder)



Que faire... Avant? (suite)

Prévention et préparation

- S'assurer que le réseau privé virtuel (RPV/VPN) est bien protégé
- Faire une mise à jour des logiciels sur une base régulière
- Corriger les failles connues dans les systèmes ou applications
- Cartographier les données critiques – où sont-elles hébergées? – et nommer des responsables

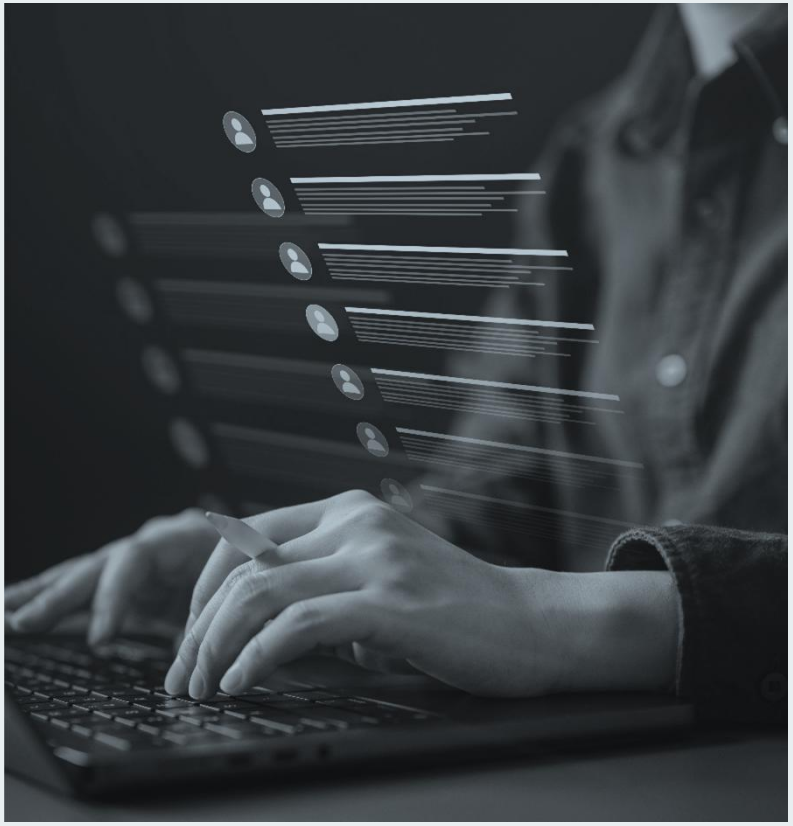


Que faire... Avant? (suite)

Prévention et préparation

Dresser une liste de **contacts d'urgence**

- Membres de la **direction** et responsables de la **sécurité**, des **communications** et **avocat**
- **Fournisseur de logiciels** (applications en ligne, services Cloud, outils utilisés au quotidien)
- **Service informatique** ou **partenaire externe**, si une firme vous aide pour la cybersécurité ou la surveillance
- **Assureur** (surtout si vous avez une assurance cyber)
- **Autorités compétentes** (police locale et Centre canadien pour la cybersécurité)



Que faire... Avant? (suite)

Pour renforcer sa résilience

- Effectuer des **sauvegardes immuables** (verrouillées) et procéder à des tests de restauration chaque trimestre
- Établir un **plan de réponse aux incidents** : rôles, étapes, contacts
- Recourir à une **solution de détection et de réponse** aux menaces (aussi appelée EDR/XDR) pour surveiller les systèmes en continu
- Faire une **copie de secours** isolée du système principal (redondance détachée)

Que faire... Pendant?

Réponse immédiate

Ne **PAS** payer la rançon et conserver toute trace utile

- captures d'écran, courriels, messages textes, informations enregistrées automatiquement par l'ordinateur (journaux)

Que faire... Pendant? (suite)

Réponse immédiate

1. Avertir la **direction** et l'équipe ou la personne **responsable de la sécurité**
2. Isoler immédiatement les **appareils touchés** en les déconnectant du réseau et en coupant les partages
3. Contacter rapidement les personnes et organisations figurant sur votre liste de **contacts d'urgence**, entre autres :
    - support TI et/ou fournisseur de services de sécurité (MSSP/SOC)
    - fournisseurs de logiciels (SaaS/Cloud)
    - assureur cyber
    - Centre canadien pour la cybersécurité (CCCS) : **Signaler un incident**

Que faire... Pendant? (suite)

Réponse immédiate

4. Transmettre aux employé(e)s des **consignes claires** et utiliser uniquement les canaux de communication officiels
5. Identifier l'**origine de l'attaque** (pièce jointe, lien suspect, mise à jour manquante, intrusion) à l'aide d'un expert en cybersécurité, au besoin
6. Chercher des **outils de déchiffrement**
7. Restaurer les systèmes et données à partir des **sauvegardes saines**
8. Effectuer une **analyse technique** (forensique) pour confirmer que le rançongiciel a été éliminé et qu'il n'y a plus d'accès persistant

Que faire… Après?

Rétablissement et leçons

- **Vérifier** que l'infection est complètement éliminée et que tout est sécurisé
- **Renforcer** la protection : mises à jour, mots de passe robustes, authentification multifacteur
- **Comprendre** ce qui s'est passé et ce qu'on doit améliorer pour éviter que ça se reproduise
- **Informer** les clients ou partenaires si leurs données ont été touchées
- **Revoir** les contrats avec fournisseurs et assureur pour mieux protéger l'entreprise

En conclusion

La préparation est notre meilleure défense!

Références

CCS – Centre canadien pour la cybersécurité :

cyber.gc.ca

Cybertrousses Cybereco

- L'hameçonnage
- La fraude par personnification
- Le mot de passe

Question à poser à vos fournisseurs

1

Quelle est l'étendue de la couverture pour les incidents critiques?

2

Comment sont gérées les sauvegardes (immuables, fréquence)?

3

Est-il possible d'exporter des données en cas de rupture?

4

Offrez-vous du soutien 24 heures sur 24, 7 jours sur 7, et en cas d'escalade de l'incident?

5

Quelles sont vos obligations contractuelles en cas de rançongiciel?

6

Quel est le temps moyen garanti pour la restauration des systèmes et des données?

7

Quelles sont les clauses de responsabilité partagée?

Communication interne à l'ensemble des employé(e)s – Teams ou courriel

Objet : Incident de cybersécurité – Rançongiciel

Bonjour,

Nous faisons face à un incident de cybersécurité par rançongiciel.

Pour nous aider à gérer la situation, les consignes ci-dessous sont de la plus haute importance.

- N'utilisez aucune clé USB
- Ne cliquez sur aucun lien suspect dans vos courriels
- Signalez toute anomalie à [indiquer la personne]

Nous vous tiendrons au courant de l'évolution de la situation.

Merci de votre collaboration!

Tableau comparatif des responsabilités

Modèle	Responsabilités	**Exemple de niveau de service**
Fournisseur de logiciels (Software as a Service – SaaS)	**Partagée** • Le **fournisseur** gère l'infrastructure • L'**entreprise** gère les données, les accès et les sauvegarde	• Soutien 24 h sur 24, 7 jours sur 7 • Restauration selon le contrat de service (SLA) • Temps de réponse variable
Serveurs dans l'entreprise (On-Prem)	**Totale** • Mises à jour servant à corriger les failles de sécurité et à améliorer le fonctionnement des systèmes • Sauvegardes • Documentation de l'infrastructure • Surveillance • Sécurité	• Aucun contrat de service externe • Tout repose sur l'équipe interne, dont la restauration, selon le plan prévu par l'entreprise
Fournisseur d'infrastructure (Infrastructure as a Service – IaaS/Cloud)	**Contractuelle** • Le **fournisseur** gère l'infrastructure et, si un enjeu est trop complexe, il l'envoie à une équipe spécialisée (escalade) • L'**entreprise** gère ses propres logiciels et ses informations (systèmes, données, apps)	• Escalade 24 h sur 24, 7 jours sur 7 • Contrat de service pour incident critique • Restauration rapide de l'infrastructure • Données sous la responsabilité de l'entreprise

Glossaire

Terme ou expression	Définition
Authentification multifacteur	Méthode de sécurité qui met en œuvre des procédés de vérification faisant appel à au moins deux facteurs d'authentification différents pour accéder à un compte, un système ou une application.
Données critiques	Données sans lesquelles l'entreprise ne peut pas fonctionner normalement
EDR **Détection et réponse sur les postes de travail** (Endpoint Detection and Response)	La solution de détection et réponse sur les postes de travail (EDR), surveille et protège les postes individuels : ordinateurs, serveurs, appareils mobiles. Il détecte les comportements suspects, bloque les attaques et fournit des outils d'analyse.
RaaS **Rançongiciel en tant que service** (Ransomware-as-a-Service)	Semblable à un abonnement à un service infonuagique… pour activités illégales
RDP **Protocole de bureau à distance** (Remote Desktop Protocol)	Technologie qui permet d'ouvrir une session à distance sur un ordinateur ou un serveur.

Glossaire

Terme ou expression	Définition
Sauvegarde immuable	Sauvegarde qui ne peut pas être modifiée ou supprimée pendant une période définie.
VPN **Réseau privé virtuel** (Virtual Private Network)	Technologie qui permet de créer une connexion sécurisée entre un appareil et le réseau d'une organisation. Sert à accéder aux ressources internes (fichiers, applications, intranet) de l'externe.
XDR **Détection et réponse étendues** (Extended Detection and Response)	La solution de détection et réponse étendues corrèle les données de plusieurs sources (réseau, courriels, serveurs, cloud, EDR, etc.). Elle offre une vision globale des menaces et automatise plus largement la détection et la réponse.