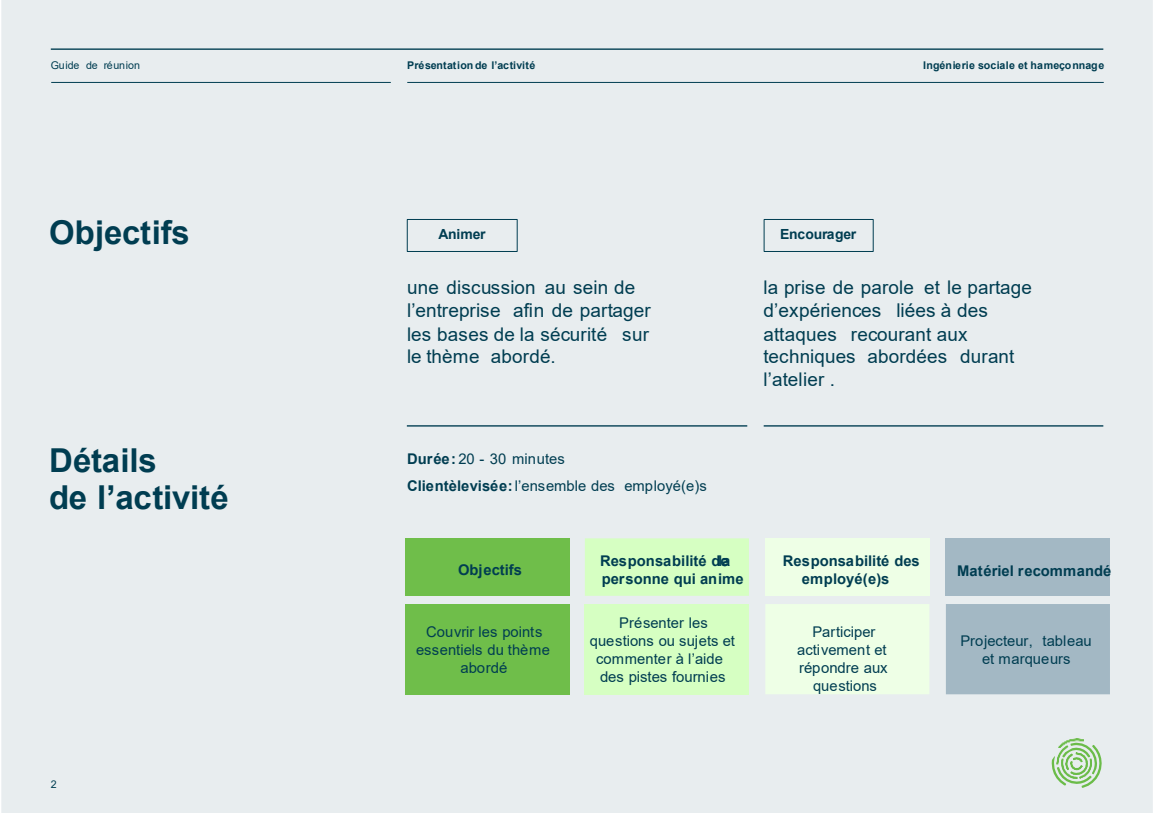
Guide de réunion

Rançongiciels

Présentationde l’activité

cyber eco

Dernière mise à jour : mars 2026



Notes à l'intention de la personne animant l'atelier

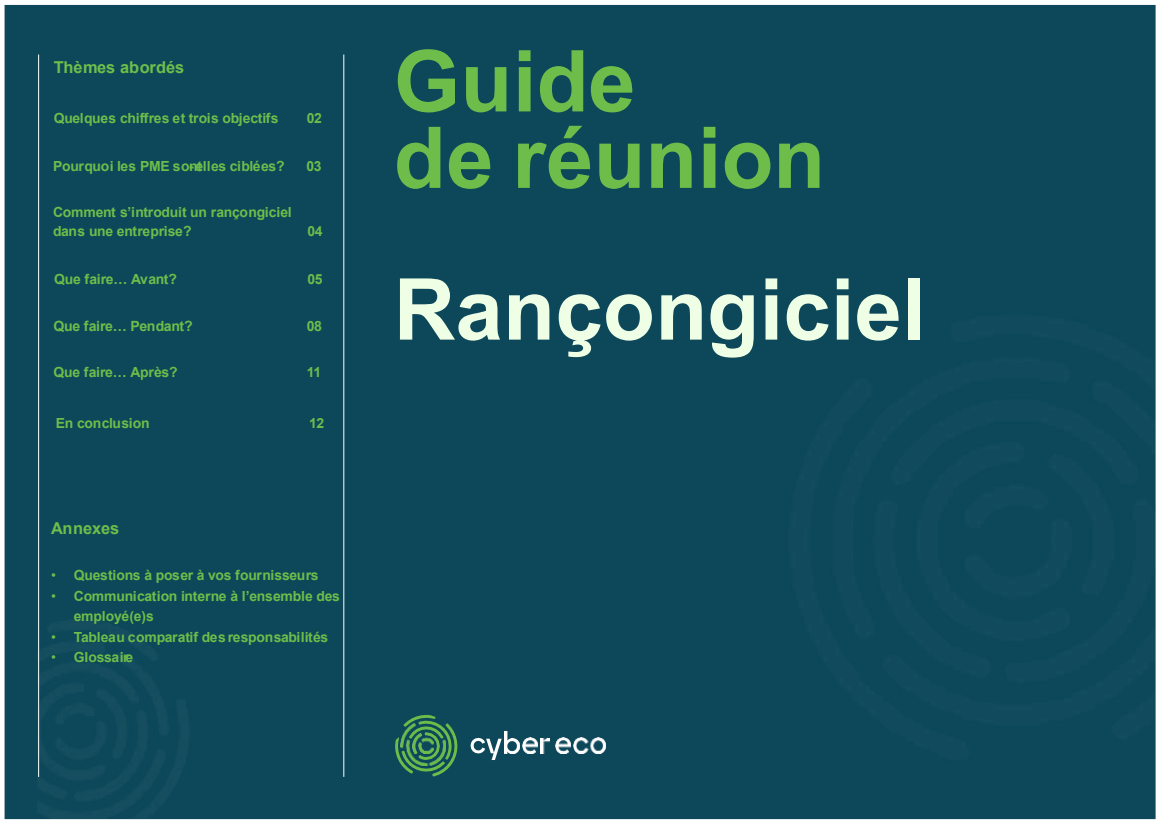
Cette trousse propose des actions simples et immédiates visant à :

- Réduire le temps de réaction advenant un incident
- Clarifier les responsabilités selon que l'on recoure à un fournisseur ou que les serveurs sont installés dans les bureaux de l'entreprise (SaaS vs On-Prem)
- Renforcer la posture de sécurité et la résilience de l'entreprise

Cette trousse s'adresse davantage à la direction de l'entreprise et à ses employé(e)s responsables des services informatiques et/ou de la sécurité.

Nous vous invitons à prendre connaissance des informations ci-dessus avant d'animer l'atelier, et d'utiliser les notes contenues dans les pages suivantes pour compléter l'information transmises à votre équipe à l'aide du **Guide de réunion**.

Bonne présentation!



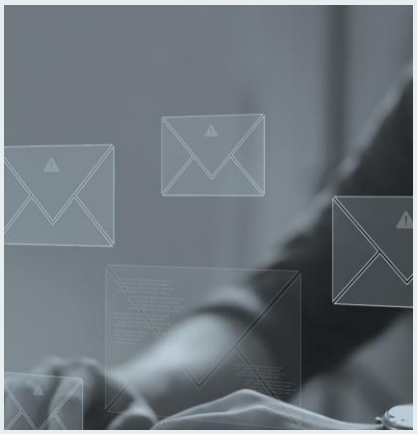
Bonjour et bienvenue à cet atelier, qui devrait durer de 20 à 30 minutes.

Sentez-vous à l'aise d'intervenir et de poser des questions tout au long de l'atelier.

Aujourd'hui, donc, nous allons parler de **Rançongiciel**.

Commençons par une définition : Qu'est-ce qu'un rançongiciel?
Un rançongiciel est un logiciel malveillant qui prend en otage les données ou le système informatique d'une entreprise et qui exige une rançon pour les libérer.

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!

Page 2 [Lire le contenu de la diapo]

- Aujourd'hui, nous allons regarder les bonnes pratiques à mettre en place pour **prévenir** une attaque par rançongiciel.
- Comme les fraudeurs sont de plus en plus rusés, nous allons aussi regarder les mesures à prendre pour **répondre** à une attaque, advenant qu'un rançongiciel ait infiltré nos systèmes.
- Finalement, nous allons parcourir les mesures à prendre pour se **relever** d'une attaque par rançongiciel.

Bien sûr, on veut éviter à tout prix les étapes « **Répondre** » et « **Se relever** », mais il est préférable de connaître les mesures à prendre, advenant une attaque réelle.

Page 3

Les entreprises comme la nôtre sont des cibles privilégiées d'attaques par rançongiciel parce que, **premièrement**, on a des **ressources limitées** pour se protéger de ces types d'attaques.

Et, **deuxièmement**, parce qu'on dépend de nos **données critiques** pour assurer la continuité de nos activités. Des données critiques, c'est, par exemple :

- les renseignements sur nos clients (noms, courriels, informations de paiement)
- nos propres données financières (factures, états financiers, déclarations fiscales, informations bancaires)
- les données sur nos employé(e)s (numéro d'assurance sociale, dossiers de paie)

Ces **deux facteurs** nous rendent **vulnérables** aux attaques.

Il faut aussi savoir que les fraudeurs peuvent recourir, entre autres, à un « service » en échange duquel la rançon exigée est partagée entre le fraudeur et ce « **service de rançongiciels »** (qu'on voit souvent écrit en anglais : *RaaS – Ransomware-as-a-Service*).

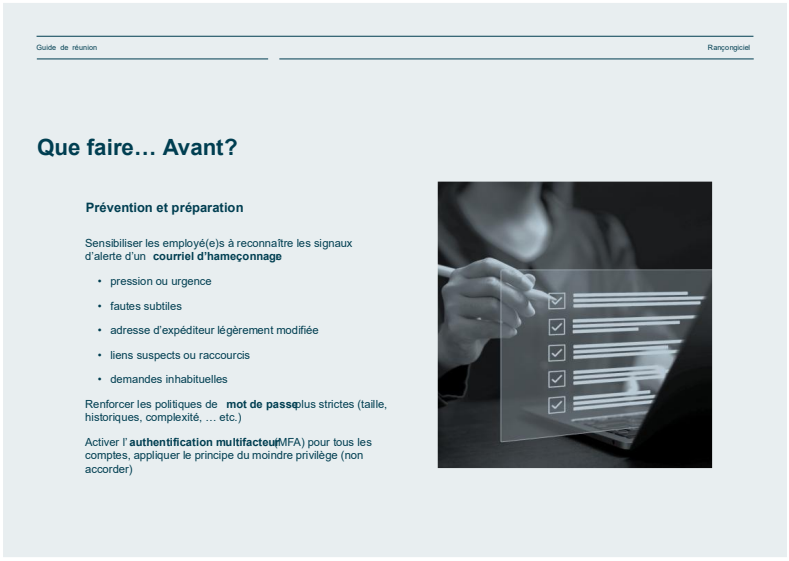
Page 4

Les fraudeurs ont plusieurs moyens d'introduire un rançongiciel dans les systèmes d'une entreprise.

Les vecteurs ou points d'entrée les plus fréquents sont les **courriels**, les **accès à distance** compromis ou exposés, et les **vulnérabilités non corrigées**, comme des logiciels qui nécessitent une mise à jour.

Que peuvent faire les employé(e)s?

1. Porter attention à chaque courriel reçu. **Ne cliquer sur aucun lien** et **n'ouvrir aucune pièce jointe** si on a le **moindre doute**.
2. Utiliser un **mot de passe robuste.**



Guide de réunion Rançongiciel

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

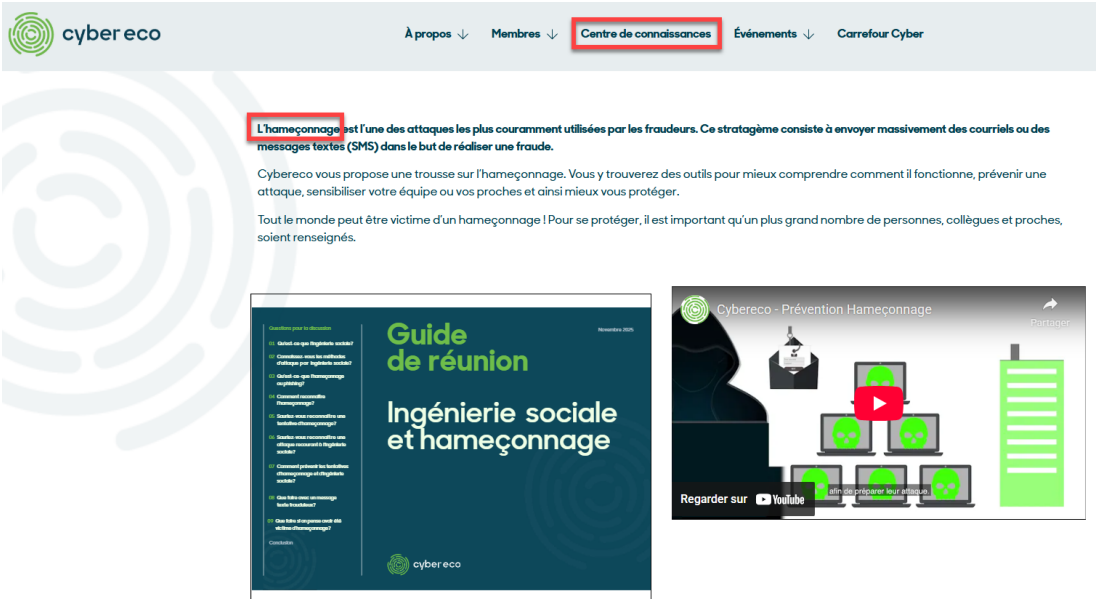
Renforcer les politiques de **mot de passe** plus strictes (taille, historiques, complexité, … etc.)

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

Page 5

UN BON TRUC

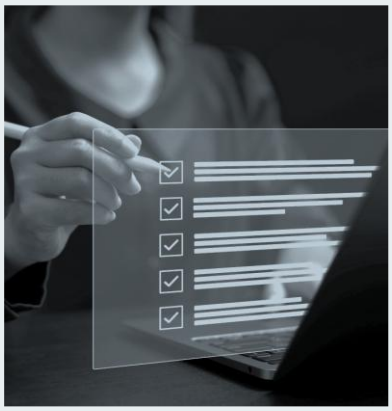
Cybereco propose une [cybertrousse sur l'hameçonnage](). Conviviale et simple à utiliser, c'est un excellent outil pour sensibiliser les employé(e)s.



Que faire… Avant (suite)

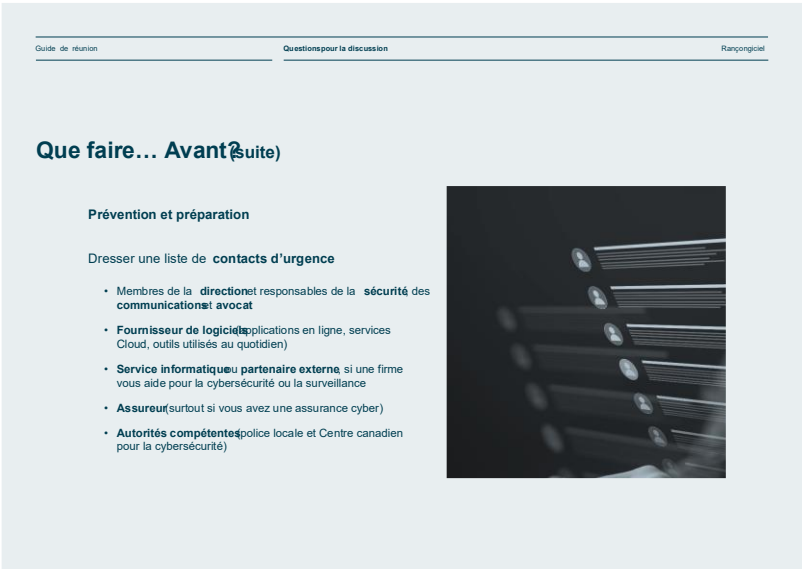
Prévention et préparation

- 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



Page 6 [Lire le contenu de la diapo]

À discuter avec les employé(e)s responsables des services informatiques et/ou de la sécurité.



La liste « **Contacts d'urgence – Cybersécurité** » devrait contenir, pour chaque personne, fournisseur, service ou autre :

- Le nom de l'**organisation**
- Le nom et le titre de la **personne responsable** de votre compte
- Un **numéro de téléphone** en cas d'**urgence**
- L'**adresse courriel** de la personne

Recommandations

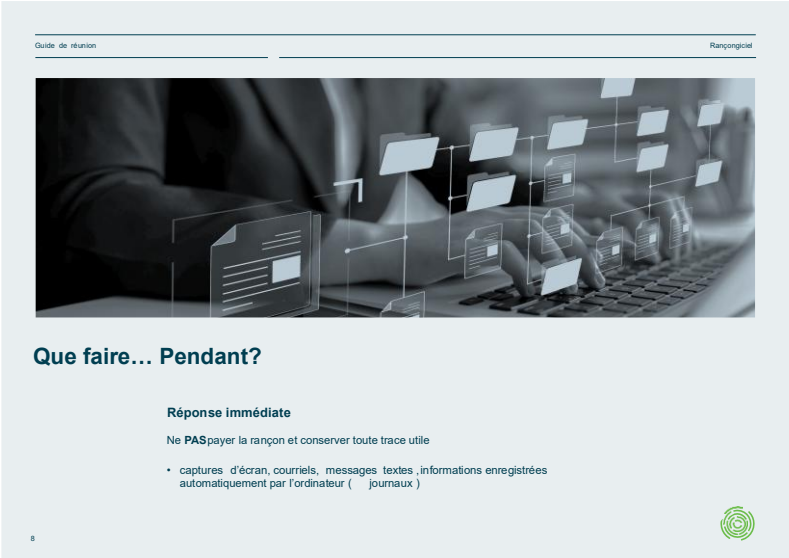
- Procéder à une **mise à jour** de la liste chaque trimestre et ajouter la date de la mise à jour sur le fichier
- Distribuer une **version électronique** ET **papier** aux membres de la direction de votre entreprise et aux employé(e)s responsables des services informatiques et/ou de la sécurité

Page 8

Complément d'information

- Les **sauvegardes immuables** suffisent dans **80 à 90 %** des incidents touchant les PME
- La **copie de secours** (appelée aussi redondance détachée) devient nécessaire si l'entreprise n'a pas de sauvegardes immuables vérifiées et testées, ou si elle veut un niveau de résilience plus élevé

5. Que faire… Pendant?

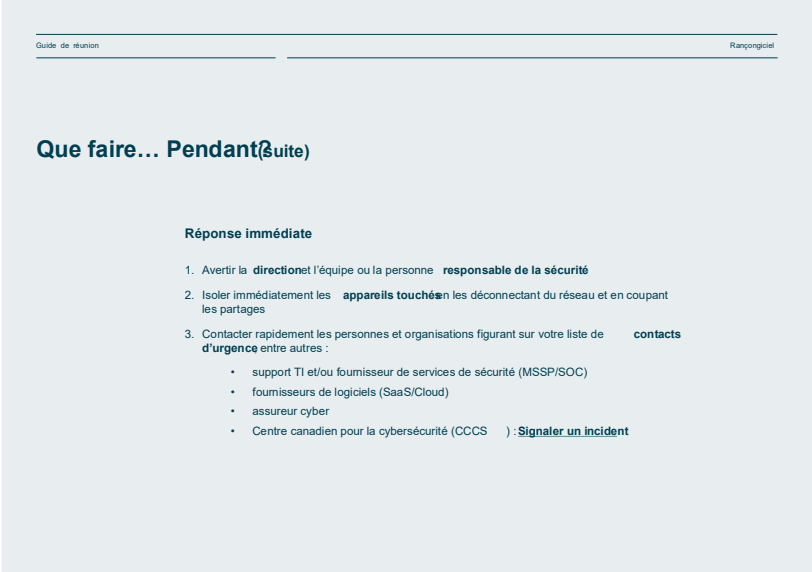


Page 9

Payer une rançon est une erreur, car :

- L'entreprise n'a aucune garantie de récupération de ses données
- Elle s'expose à un risque élevé de récidive
- La rançon ne protège aucunement l'entreprise contre la fuite de ses données
- La posture de sécurité de l'entreprise est affaiblie
- La rançon finance le crime organisé
- L'entreprise s'expose à des risques légaux et réglementaires

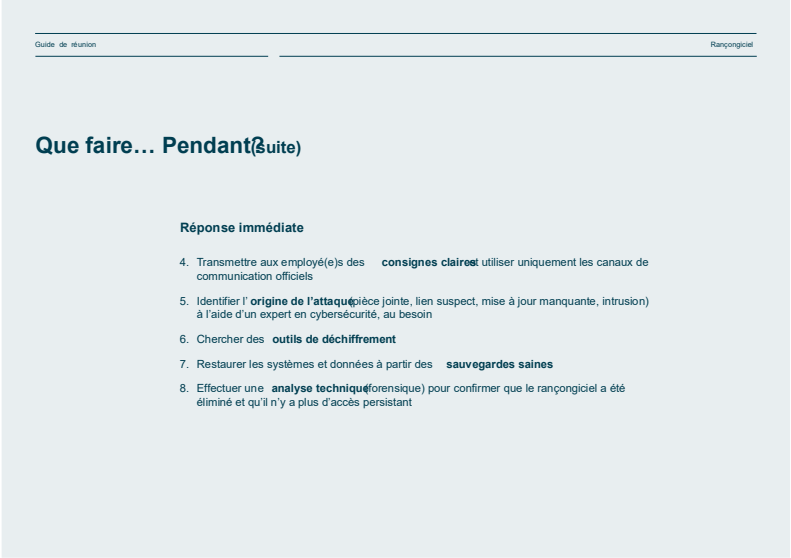
La meilleure défense contre les rançongiciels demeure la **prévention** et la **préparation**, mais **non** le **paiement d'une rançon**.



Page 10

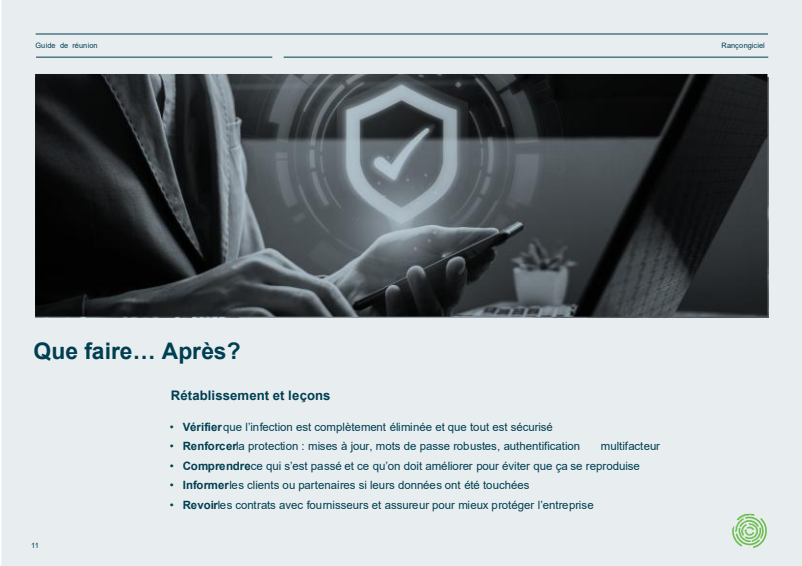
Signaler un incident au Centre canadien pour la cybersécurité permet au Centre :

- d'analyser l'incident à un niveau national
- de détecter des campagnes plus larges
- de partager de l'information pour protéger d'autres organisations



Page 11

Avant d’envoyer des consignes aux employé(e)s, on doit valider que les outils habituels (Teams, courriel, téléphone) fonctionnent normalement. Au moindre doute, il faut appeler directement les collègues ou le fournisseur TI pour confirmer que les communications n’ont pas été touchées.



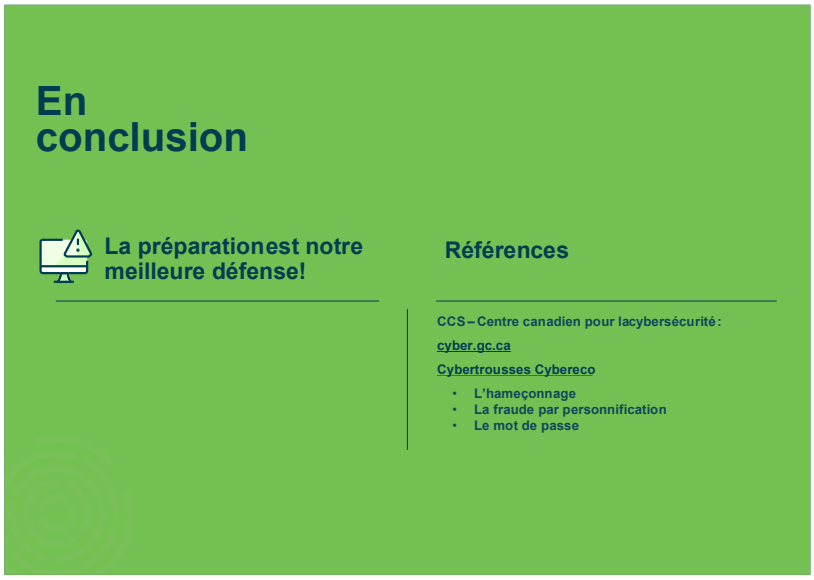
Page 12

IMPORTANT

Le **délai de rétablissement** après une attaque par rançongiciel peut prendre un certain temps, en fonction des mesures préventives mises en place au préalable.

Bien que cela soit normal et fasse partie du processus de sécurisation, une préparation adéquate permet de réduire considérablement ce délai.

Plus l'organisation est préparée, mieux et plus rapidement elle pourra se remettre d'une attaque.



Page 13

En plus de cette trousse sur le rançongiciel, Cybereco propose trois autres trousses pour aider les petites entreprises à sensibiliser leurs équipe sur :

- l'hameçonnage
- la fraude par personnification
- les mots de passe

Merci d'avoir participé à l'atelier!

Annexes

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 cyber sécurité – 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.