

## LISTE DE CONTRÔLE EN CAS DE RANÇONGIELS

### PRÉPARATION EN CAS DE RANÇONGIELS

- Lorsque vous élaborez un plan de prévention et de protection contre les rançongiciels, évaluez périodiquement les éléments suivants :
  - Votre organisation procède-t-elle à des sauvegardes planifiées de manière régulière ?
  - Des périphériques non essentiels sont-ils connectés au réseau de votre organisation ?
  - Votre organisation connaît-elle les risques réglementaires et légaux impliqués par le paiement d'une rançon ?
- Votre organisation met-elle régulièrement à jour ses systèmes logiciels ? Ces mises à jour sont-elles automatisées ?
- Votre organisation dispose-t-elle d'un plan pour traiter les attaques par rançongiciels et les pertes de données ?
- Votre système dispose-t-il d'une politique de cyber-assurance ? Si c'est le cas, dans quelle mesure ce plan couvre-t-il les attaques par rançongiciels ?

### PROTECTION EN TEMPS RÉEL

- Investissez dans des systèmes de protection anti-logiciels malveillants qui s'adaptent à la veille sur les nouvelles menaces en temps réel.
- Évaluez la sécurité de tous les périphériques connectés aux réseaux qui hébergent des informations sensibles ou vitales.
  - Connectez tous les systèmes non essentiels à un réseau distinct.
  - Pensez à sécuriser les configurations de travail à distance. Vérifiez que les outils de sécurité fonctionnent en dehors du réseau pour surveiller l'ensemble du trafic Web.
- Encouragez la formation des employés sur les attaques par hameçonnage et sur la nécessité de protections par mots de passe renforcés.
- Envisagez la mise en œuvre d'une authentification multifactorielle dans l'ensemble de votre organisation, si cela est réalisable.
- Procédez à la mise à jour régulière de tous les logiciels et systèmes.
  - Modifiez les paramètres pour autoriser les mises à jour automatiques, si possible.
- Développez un plan d'intervention en cas d'incident et de gestion de crise afin de savoir comment traiter une attaque par rançongiciel et la perte de données précieuses.
- Préparez un plan de communication externe en cas d'attaque par rançongiciel.

### SAUVEGARDES DE DONNÉES

- Investissez dans des systèmes de sauvegarde sécurisés et régulièrement mis à jour qui protègent vos données.
  - En cas d'utilisation de clés USB ou de disques durs, déconnectez physiquement ces périphériques des ordinateurs en réseau une fois les sauvegardes terminées.
  - En cas d'utilisation d'espace de stockage cloud, équipez les serveurs avec un cryptage de haut niveau et une authentification multifactorielle.
- Créez une copie en lecture seule des écritures comptables pour les pires cas de récupération d'urgence.
- Développez des systèmes qui effectuent une récupération des données et une correction automatiques.
- Élaborez des scénarios pour évaluer la durée de récupération des données critiques et des services de l'entreprise.

## ENVIRONNEMENT RÉGLEMENTAIRE

- Évaluez les directives réglementaires et juridiques pertinentes en cas de rançongiciels dans votre environnement opérationnel.
  - Pensez aux directives nationales spécifiques.
  - Pensez aux directives spécifiques au secteur financier.
  - Pensez aux exigences réglementaires et juridiques internationales.
  - Élaborez un plan pour l'évaluation périodique des directives en constante évolution.
- Évaluez les risques impliqués par le paiement d'une rançon.
- Lien avec l'application des lois.
- Créez des connexions pour le partage rapide des informations dans l'éventualité d'une attaque.
- Évaluez les avantages et les inconvénients des politiques de cyber-assurance pour les rançongiciels.



[CarnegieEndowment.org](https://CarnegieEndowment.org)

