BlackBerry | Cybersecurity

PRÉVENIR LES RANSOMWARES EST POSSIBLE

Une protection efficace contre les ransomwares passe tout d'abord par l'adoption d'une approche Zero Trust et la mise en place d'une stratégie axée sur la prévention. Avec l'apparition des extorsions doubles, triples et quadruples, considérées comme les menaces les plus coûteuses et les plus redoutées, la protection de votre entreprise contre les ransomwares exige d'avoir une posture de défense appropriée, de réduire l'exposition et de neutraliser les auteurs de menaces dès le départ.

Impact des ransomwares

Les ransomwares sont une menace sérieuse pour les entreprises et une forme d'attaque qui a connu une hausse en 2021.

1,8 MILLION $
a été le coût moyen d'une compromission due à un ransomware[1]

21 JOURS
a été la durée moyenne d'immobilisation des entreprises[2]

14 SUR 16
secteurs exploitant des infrastructures critiques ont été ciblés[3]

32 % DU TEMPS
des dirigeants ont quitté leur entreprise après une attaque par ransomware réussie[4]

80 % D'ENTREPRISES
ont été victimes d'une attaque répétée[5]

CHRONOLOGIE DE L'ÉVOLUTION DES RANSOMWARES

1989

Première attaque par ransomware connue

Attaque par ransomware traditionnelle : chiffrement des données → extorsion → clé de déchiffrement fournie en échange du paiement d'une rançon

2017

WannaCry et NotPetya déclenchent une crise de sécurité mondiale

- *WannaCry touche 150 pays*[6]
- *NotPetya crée des dommages s'élevant à environ 10 milliards de dollars*[7]

2019

Première attaque par double extorsion connue

Durant la période d'étude, le nombre d'entreprises dont les données ont été exposées sur un site de fuite de données a augmenté de 935 %[8]

2020

Première attaque par triple extorsion connue

La hausse de 93 % du nombre de ransomwares a été essentiellement le fruit d'attaques par triple extorsion[9]

2021

Première attaque par quadruple extorsion connue

- *Ce type d'attaque est moins fréquent*
- *Le paiement moyen est passé à plus de 312 000 $, soit une hausse de 171 %*[10]

RANSOMWARES : LES TENDANCES

Selon l'étude sur les cybermenaces menée par BlackBerry®, les principaux ransomwares auxquels les entreprises ont été confrontées l'an dernier sont :

REVIL

Vecteurs classiques :
- Attaques par phishing
- Vulnérabilités logicielles connues
- Attaques par force brute sur le protocole RDP

DARKSIDE

- Utilise des tactiques de double extorsion
- Cible les systèmes Windows® et Linux®

CONTI

- Cible les entreprises des secteurs de la fabrication, de la santé et des assurances dans le monde entier
- Hautement personnalisable, ce qui permet de l'utiliser contre une grande variété de cibles

AVADDON

- Première apparition en 2020
- Utilise la double et la triple extorsion

RAGNAR LOCKER

- Présenté par ses auteurs comme un service pour les victimes[11]
- Utilise la double extorsion et héberge un « mur de la honte » répertoriant les victimes

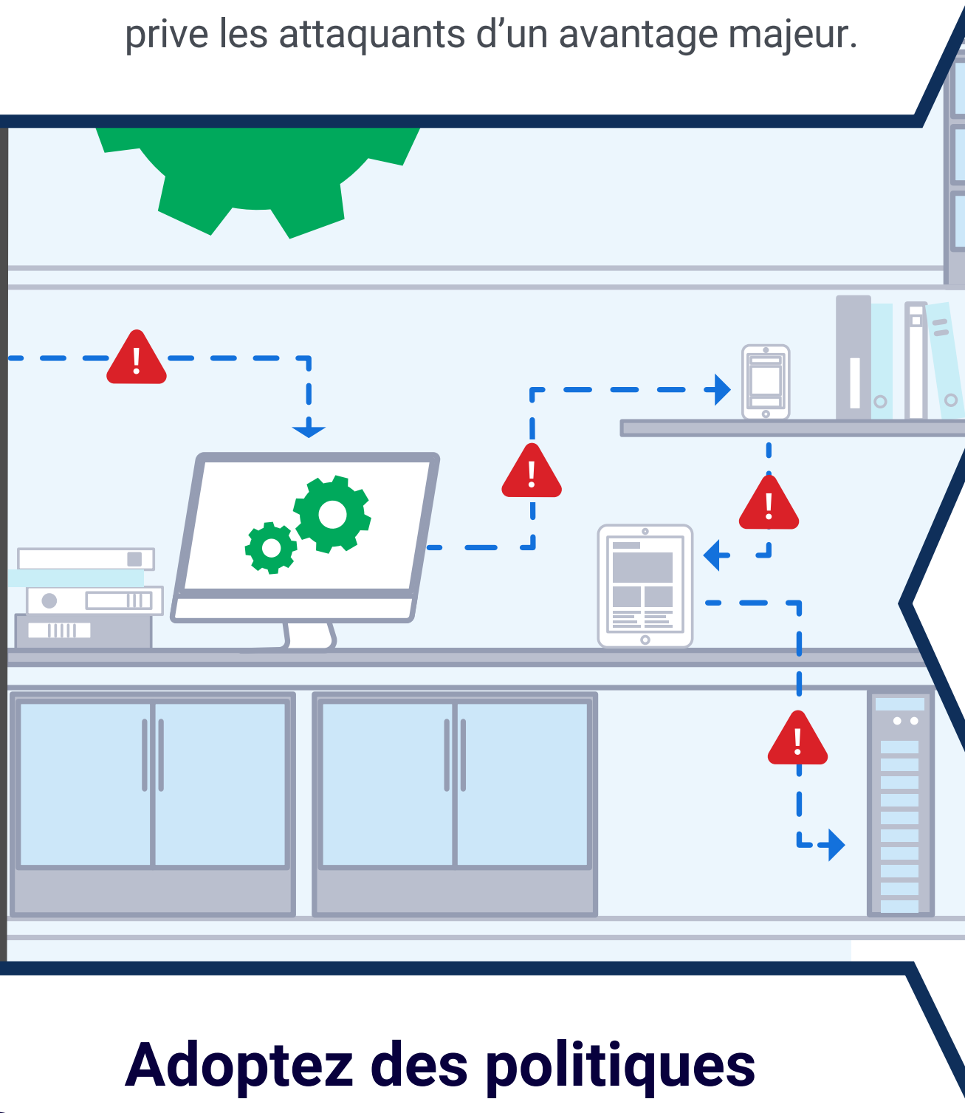
HIVE

- Connu pour utiliser le langage de programmation Go relativement récent
- Utilise la double extorsion

CONSEILS POUR PRÉVENIR LES ATTAQUES PAR RANSOMWARE

1 Maintenez les logiciels à jour

L'exploitation des vulnérabilités connues est au cœur de nombreuses campagnes de ransomwares. Maintenir les appareils à jour prive les attaquants d'un avantage majeur.

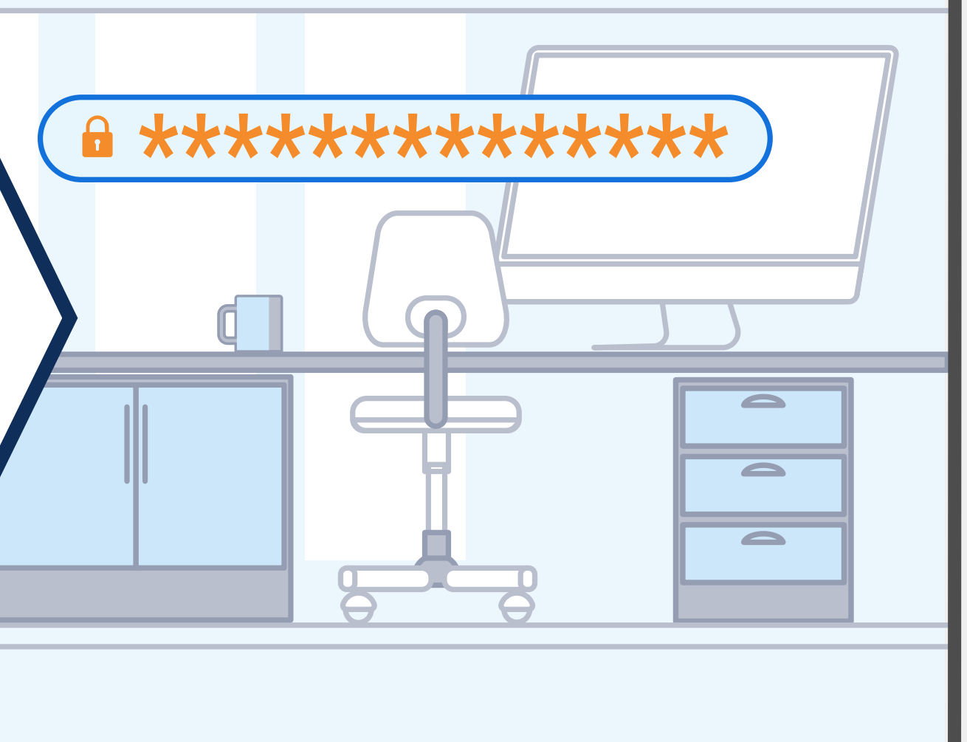


2 Suivez et gérez

Il est important de mettre en place un système de suivi des vulnérabilités au niveau des environnements, des appareils et des services, car la plupart des environnements d'entreprise changent constamment.

3 Adoptez des politiques de mots de passe solides et une authentification multifacteur (MFA)

Les identifiants compromis et partagés constituent une vulnérabilité massive.

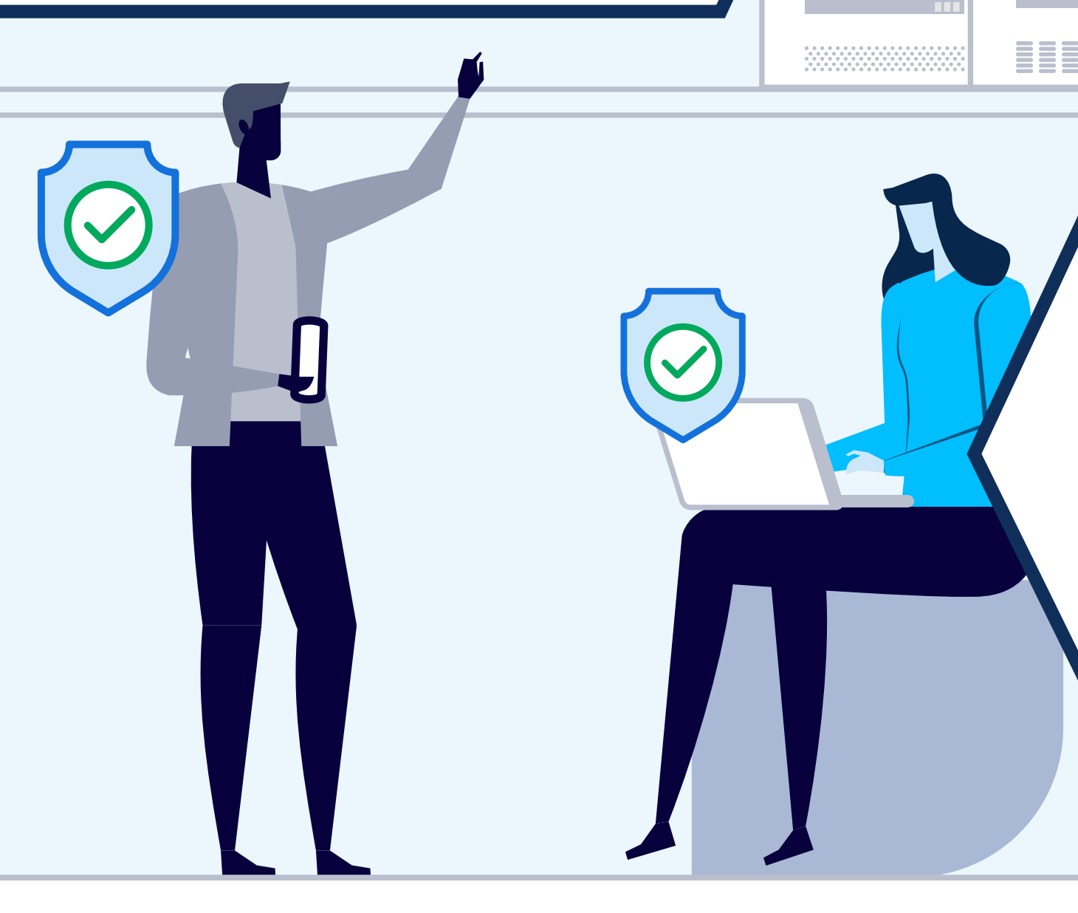


4 Réduisez la surface d'attaque

Suivez le principe du moindre privilège d'accès. Supprimez les appareils et logiciels inutiles. Et dans la mesure du possible, réduisez les connexions et les accès au réseau.[12]

5 Protégez les données

Créez des politiques de récupération (y compris de test des sauvegardes) et de sauvegarde des données solides.



6 Appliquez les bonnes pratiques de sécurité

Formez les salariés, utilisez la MFA, et implémentez des mots de passe forts.

SE PRÉPARER AUX RANSOMWARES

Les entreprises qui veulent franchir un nouveau cap dans la protection contre les ransomwares doivent miser sur l'intelligence artificielle (IA) et des plateformes managées de détection et réponse étendues (XDR). Cylance® Endpoint Security offre une protection renforcée fondée sur l'IA et un framework Zero Trust leur permettant de protéger n'importe quel appareil, où qu'il soit.

Pour plus d'informations sur la prévention et la neutralisation des ransomwares, **consultez notre guide →**

BlackBerry | Cybersecurity

À propos de BlackBerry : BlackBerry (NYSE : BB ; TSX : BB) fournit des logiciels et des services de sécurité intelligents aux entreprises et aux gouvernements du monde entier. La société assure la sécurité de plus de 500 millions de terminaux, dont 215 millions de véhicules actuellement en circulation. Basée à Waterloo (Canada), la société s'appuie sur l'intelligence artificielle et l'apprentissage automatique pour proposer des solutions innovantes dans les domaines de la cybersécurité, de la protection et de la confidentialité des données. BlackBerry est également leader dans les domaines de la gestion de la sécurité des terminaux, du chiffrement et des systèmes embarqués. La vision de BlackBerry est claire : assurer un futur connecté auquel vous pouvez faire confiance.

Pour toute information complémentaire, rendez-vous sur ***BlackBerry.com/fr/fr*** *et suivez* ***@BlackBerry*****.**

---

[1] https://www.itpro.com/security/ransomware/359364/cost-of-ransomware-doubles-in-a-year

[2] https://www.forbes.com/sites/hillennevins/2021/07/26/how-to-survive-a-cybersecurity-attack/

[3] https://www.securityweek.com/ransomware-targeted-14-16-us-critical-infrastructure-sectors-2021

[4] https://www.techrepublic.com/article/the-many-ways-a-ransomware-attack-can-hurt-your-organization

[5] https://www.cbsnews.com/news/ransomware-victims-suffer-repeat-attacks-new-report/

[6] https://dataprot.net/statistics/ransomware-statistics/

[7] https://dataprot.net/statistics/ransomware-statistics/

[8] https://www.rhisac.org/ransomware/ransomware-double-and-triple-extortion/

[9] https://cybernews.com/news/ransomware-surged-93-in-last-6-months-fueled-by-triple-extortion/

[10] https://threatpost.com/ransomware-payments-quadruple-extortion/168622/

[11] https://www.tripwire.com/state-of-security/security-data-protection/ragnar-locker-ransomware-what-you-need-to-know/

[12] https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege