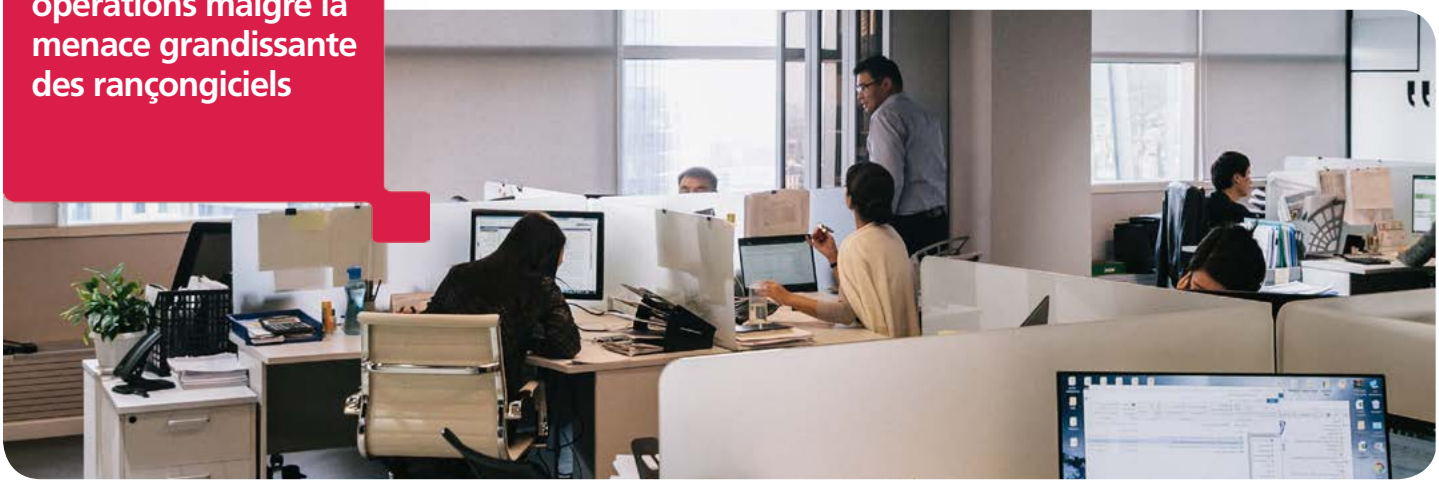
RICOH
imagine. change.

Se concentrer sur la continuité des opérations malgré la menace grandissante des rançongiciels



Protéger les données importantes des employés grâce à une défense contre les rançongiciels de classe mondiale

Les entreprises se préoccupent de plus en plus de la menace grandissante que représentent les cyberattaques. Ces dernières ciblent les données d'identification personnelle des employés, les données des clients, les données financières et d'autres informations commerciales essentielles. Les impacts peuvent être dévastateurs, comme un temps d'arrêt en raison de la fermeture complète des centres de données, de la chaîne d'approvisionnement et des activités de l'entreprise, une perte de réputation auprès des clients et des partenaires et des conséquences financières importantes. Avec le confinement des rançongiciels au sein de leurs protocoles de cybersécurité et de continuité des opérations, les organisations peuvent être assurées que leurs actifs d'informations essentielles et confidentielles sont protégés.

Défis d'affaires

- Menace grandissante des cyberattaques, surtout des rançongiciels
- Augmentation des risques et des vulnérabilités de sécurité associés au télétravail et au milieu de travail numérique, comme les erreurs d'utilisateurs qui cliquent sur des liens dans des courriels menant à des maliciels ou à des sites Web avec du contenu malveillant ou qui utilisent une clé USB contaminée
- Menace grandissante des cyberattaques, surtout des rançongiciels
- Hausse de 200 % des temps d'arrêt par rapport à l'année dernière en raison des atteintes à la sécurité[1]

Résultats d'affaires

- Impact minimal sur l'infrastructure TI et le rendement du réseau
- Possibilité de prévenir d'éventuels verrouillages du système et d'éviter les coûts importants de récupération et de réparation des données
- Conviction d'être en mesure de gérer les atteintes de sécurité probables en se concentrant sur la continuité des affaires
- Capacité à contrer les effets des menaces de sécurité supplémentaires associées au fait d'avoir plus d'employés en télétravail

Problèmes de cybersécurité croissants

La croissance des problèmes de menaces de cybersécurité dans les entreprises a récemment été attribuée à l'augmentation du télétravail et aux initiatives de transformation numérique. Les menaces en ligne ont été six fois plus importantes en 2020 avec une hausse moyenne des paiements de rançons s'élevant à 780 000 $ ou plus pour une grande entreprise[1, 2].

La plupart des entreprises ont investi dans plusieurs couches de périmètre et de sécurité des terminaux pour protéger leur infrastructure et leurs actifs d'une éventuelle atteinte à la sécurité. Cependant, les cybercriminels trouvent continuellement de nouvelles méthodes inconnues pour déjouer les solutions de sécurité traditionnelles fondées sur la prévention, ils passent souvent plusieurs semaines, parfois même des mois, à travailler de façon inaperçue à l'intérieur d'un réseau avant de transmettre des données utiles, chiffrant jusqu'à 10 000 fichiers par minute[3].

La hausse du télétravail a augmenté les risques de sécurité, puisque les employés n'utilisent pas toujours le RPV, accèdent aux données de l'entreprise depuis des appareils personnels ou utilisent des clés USB et d'autres périphériques amovibles contaminés pour gérer les fichiers. Comme ils sont seulement à un clic d'une éventuelle attaque de rançongiciel, les dossiers de RH des employés, les données des clients et les informations ainsi que les rapports essentiels de l'entreprise sont alors volés et les appareils et les fichiers sont chiffrés. L'impact pourrait être dévastateur pour l'entreprise : atteinte à la réputation auprès des clients, conséquences financières importantes par la perte d'une estimation de 8 500 $ par heure en raison d'un temps d'arrêt causé par un rançongiciel, les frais juridiques et la rançon payée et interruption des activités de l'entreprise[1].

Lorsque les employés ne sont pas au bureau, ils ont tendance à être moins soucieux des meilleures pratiques en matière de sécurité. Malgré leurs systèmes de sécurité forts, les entreprises reconnaissent qu'il y a un plus grand risque avec plus d'employés en télétravail.

Mise en place d'une « dernière ligne de défense »

Pour aider à se défendre contre les rançongiciels, les entreprises qui ont instauré la solution de confinement des rançongiciels de Ricoh comme dernière ligne de défense reçoivent une alerte instantanément et la solution répond en fermant le terminal attaqué, ce qui inclut les ordinateurs portables. La solution est une application sans agent qui est installée sur un serveur virtuel dans le système informatique central plutôt que sur tous les terminaux et a un impact minimal sur l'infrastructure TI et le rendement. Elle surveille en temps réel les données à l'échelle de l'entreprise. Elle a pour but de détecter une attaque de rançongiciels, habituellement au moyen d'un ordinateur portable ou de bureau, n'importe où dans l'ensemble du réseau même lorsque l'attaque a réussi à contourner les systèmes de sécurité. Elle peut ensuite verrouiller l'emplacement, isoler les fichiers touchés par le chiffrement du maliciel et empêcher le rançongiciel de se propager dans tout le réseau.

Ainsi, l'entreprise peut avoir confiance en sa capacité à gérer les éventuelles atteintes à la sécurité en se concentrant sur la continuité des affaires. Les activités se déroulent sans problème, les systèmes et les applications ne sont pas verrouillés et seulement un petit nombre de fichiers doivent être restaurés et récupérés. Bloquer l'attaque de rançongiciel permettrait également à l'entreprise de préserver sa réputation auprès de ses clients et partenaires sans conséquence financière, comme les frais juridiques, les coûts d'un règlement et le paiement de la rançon ou toutes autres responsabilités financières à long terme.

1. 2021 Ransomware Statistics, Data, & Trends, PurpleSec
2. Cyber-Attacks Up 37% Over Past Month as #COVID19 Bites, InfoSecurity Magazine
3. Ransomware containment: protecting against ransomware attack, Ricoh USA, Inc.

RICOH
imagine. change.
imaginer. changer.