Prévention contre les rançongiciels

Vérifiez votre stratégie de réduction des risques. Protégez vos terminaux et vos données de sauvegarde contre les rançongiciels et les cyberattaques associées.

Les rançongiciels existent depuis longtemps. Et ils vont sûrement perdurer aussi longtemps que leurs auteurs verront l'opportunité d'en tirer des gains financiers.

L'Internet Crime Complaint Center du FBI signale 2 084 plaintes pour attaques par rançongiciel au cours du premier semestre 2021, ce qui représente une hausse de 62 % sur l'année[1]. Un rapport Gartner indique que « les rançongiciels peuvent coûter aux sociétés des millions de dollars à court terme, et entraîner potentiellement une perte encore plus grande à long terme, en impactant leur réputation et leur fiabilité »[2].

Les attaques par rançongiciel n'ont pas seulement des conséquences financières. S'y ajoutent aussi les effets provoqués par les tentatives de restauration de toutes les données compromises. D'après une étude Forrester, seulement 25 % des personnes interrogées ont déclaré avoir pu restaurer 75 à 100 % de leurs données après une attaque. Elles sont bien plus nombreuses (39 %) à déclarer avoir réussi à restaurer seulement 50 à 74 % de leurs données[3].

Pourriez-vous gérer votre entreprise avec 50 à 74 % des données dont vous disposiez auparavant ?

Les modèles de rançongiciel changent. Il devrait également en être de même pour votre stratégie de protection des données.

Face aux niveaux de menace élevés et aux coûts importants associés aux rançongiciels, les administrateurs informatiques et de sauvegarde réévaluent avec inquiétude leurs stratégies de protection des données.

Les rançongiciels se présentent sous différentes formes et apparences. Les attaques de type « spray-and-pray » comme le logiciel malveillant CryptoLocker, populaire il y a quelques années, déploient un vaste filet pour atteindre autant de victimes que possible[4]. Leurs modèles ont évolué pour cibler des secteurs spécifiques, par exemple les services publics, les universités et les services de santé[5]. Certaines attaques ressemblent à des attaques par rançongiciel, mais sont en fait destinées à détruire tout simplement les données et les infrastructures[6].

Même les modèles financiers sont en train de changer. L'époque où les pirates demandaient 300 dollars en bitcoins pour déchiffrer les données est révolue. D'après une enquête récente, la moyenne des rançons s'élève à près de 2 millions de dollars[7]. Cette étude rapporte également le paiement de 4,4 millions de dollars autorisé par le PDG de Colonial Pipeline à la suite de l'attaque par rançongiciel de la société[8]. Pire encore, les auteurs de ces attaques adoptent des tactiques en menaçant par exemple de publier les données rançonnées.

Le rôle de la sécurité et de la sauvegarde des terminaux

Lorsque tous les appareils connectés à votre entreprise représentent un vecteur potentiel d'attaque, il devient alors impératif d'assurer la sécurité des terminaux. Cela implique d'identifier et de protéger tous les appareils qui accèdent à votre réseau, où qu'ils soient.

Selon l'organisation Identity Theft Resource Center (ITRC), les 1 291 violations de données qui ont eu lieu au cours des neuf premiers mois de 2021 représentent 17 % de plus que toutes celles de 2020[9]. Comme les violations de données

commencent toujours au niveau des terminaux, le risque pesant sur votre organisation ne cesse de croître à mesure que vous ajoutez des appareils.

En plus de sécuriser vos terminaux, pensez à votre stratégie de sauvegarde. Le stockage d'une copie de vos données sur bande, sur un appareil séparé, voire à un autre emplacement, comme dans le cloud, vous assure de pouvoir la restaurer après une attaque. De nombreuses organisations informatiques répliquent leurs sauvegardes hors site à des fins de reprise d'activité.

Le problème, c'est que vos systèmes de sauvegarde dépendent toujours des serveurs. Ces serveurs dépendent de composants potentiellement vulnérables, par exemple un système d'exploitation et Active Directory, ce qui signifie que vos sauvegardes sont également vulnérables. De plus, les partages réseau étant une cible pour la plupart des rançongiciels, les produits de sauvegarde qui utilisent les partages pour stocker les données présentent davantage de risques.

Pour véritablement protéger votre organisation des rançongiciels, protégez les données de production de vos terminaux ainsi que les données de vos sauvegardes.

Solutions Quest® pour assurer la protection contre les rançongiciels

Les solutions Quest contribuent à empêcher les rançongiciels d'attaquer vos terminaux et sauvegardes.

KACE® de Quest Unified Endpoint Manager

KACE Unified Endpoint Manager automatise l'analyse des vulnérabilités, les correctifs ainsi que les mises à jour de sécurité, non seulement pour les systèmes d'exploitation, mais aussi pour les applications tierces et les mises à niveau sur place. Son système automatisé de gestion unifiée des terminaux (UEM) identifie rapidement les appareils qui présentent des failles CVE (Common Vulnerabilities and Exposures) ou dont les correctifs sont inadéquats avant de les mettre à jour.

À partir d'un tableau de bord unique, KACE vous permet de détecter, gérer et sécuriser tous les terminaux qui accèdent à votre réseau, en particulier :

- Les ordinateurs de bureau, ordinateurs portables, serveurs et appareils mobiles Windows
- Les ordinateurs de bureau et ordinateurs portables Mac
- Les machines et serveurs Linux
- Les Chromebooks
- Les appareils mobiles iOS et Android
- Les appareils autres que des ordinateurs, par exemple des imprimantes
- Les appareils IoT (Internet of Things)

Au lieu de rechercher, acheter, apprendre et gérer plusieurs solutions ponctuelles, bénéficiez du système UEM complet dans la console KACE unique. Il centralise votre commande d'inscription, d'effacement et de verrouillage, de découverte, d'inventaire, de gestion des actifs matériels/logiciels et d'exécution de script. De plus, il offre une assistance intégrée pour les tickets de service informatique.

Gérez votre entreprise et non vos services. Avec KACE Unified Endpoint Manager, vous disposez d'une vue d'ensemble complète et centralisée de tous vos terminaux. Vous n'avez donc pas à organiser ensemble des données provenant de différents produits.

Quest NetVault® Plus

Le logiciel de sauvegarde d'entreprise NetVault Plus allie puissance et facilité d'utilisation. Il dispose également d'une protection intégrée contre les rançongiciels. Il associe le logiciel de sauvegarde et de restauration NetVault et la solution de stockage secondaire software-defined Quest QoreStor®.

Sur site et dans le cloud, NetVault Plus renforce votre protection contre les rançongiciels grâce au chiffrement des données de vos sauvegardes. Il fournit un stockage secondaire immuable afin que les données de sauvegarde écrites sur QoreStor ne puissent pas être écrasées, modifiées ou supprimées en dehors des paramètres de conservation que vous définissez.

NetVault Plus renforce la protection contre les rançongiciels en conservant une copie de toutes les données de sauvegarde supprimées dans la corbeille de données QoreStor pendant une durée spécifiée par l'administrateur. Pour une sécurité accrue, sa technologie Secure Connect encapsule les commandes de contrôle et de transfert de données dans une couche TLS 2.0 pour empêcher les attaques sur vos données de sauvegarde.

Pour le stockage de données, NetVault Plus prend en charge les protocoles RDA (Rapid Data Access), qui ne sont pas ouverts, contrairement au protocole Server Message Block (SMB) utilisé pour les partages Windows. Le protocole RDA n'est pas directement accessible par le système d'exploitation, et l'authentification doit se faire en dehors du serveur local ou des constructions contrôlées par le domaine.

Pour finir, NetVault Plus offre un accès robuste basé sur les rôles sans devoir s'intégrer à des services tels qu'Active Directory. Cela apporte un autre degré de séparation de l'environnement de production et empêche l'accès de tout attaquant.

Il est temps de protéger votre organisation contre les rançongiciels

En fin de compte, même l'organisation la mieux préparée ne peut se protéger complètement contre les attaques par rançongiciel. Mais vous pouvez limiter les risques si vous disposez d'une solution qui non seulement protège vos terminaux, mais vous permet aussi de restaurer rapidement et complètement toutes vos données.

Les solutions Quest pour la prévention contre les rançongiciels sont conçues pour vous aider à :

- Limiter les risques d'impact des rançongiciels sur votre entreprise
- Réduire le nombre de composants principaux pouvant être attaqués
- Limiter votre exposition aux techniques de capture des données
- Protéger vos données de sauvegarde contre les rançongiciels

En savoir plus sur KACE Unified Endpoint Manager et NetVault Plus.

1 FBI Internet Crime Complaint Center, « Ransomware Awareness for Holidays and Weekends », septembre 2021. 2 084 plaintes comptabilisées de début janvier au 31 juillet 2021.
2 Gartner, « 6 Ways to Defend Against a Ransomware Attack », novembre 2020.
3 Forrester Research, « Ransomware Recoverability Must Be a Critical Component of Your Business Continuity Plans », octobre 2019.
4 KrebsonSecurity.com, « 2014: The Year Extortion Went Mainstream », juin 2014.
5 CyberWire, « Ransomware: healthcare, utilities, and universities. REvil's old sites are stirring », septembre 2021.
6 The Register, « Ukraine blames Belarus for PC-wiping 'ransomware' that has no recovery method and nukes target boxen », janvier 2022.
7 Ransomware.org, « Ransomware Attacks Ramped Up In 2021 », décembre 2021.
8 CNN, « Colonial Pipeline CEO admits to authorizing $4.4 million ransomware payment », mai 2021.
9 ITRC, « Number of Data Breaches in 2021 Surpasses All of 2020 », octobre 2021.