arcserve®

Protéger ce qui n'a pas de prix

VOTRE GUIDE POUR UN AVENIR SANS RANSOMWARE

UNE APPROCHE PROACTIVE POUR RÉPONDRE À LA MENACE DES RANSOMWARE

LIVRE BLANC

LE RANSOMWARE EST DEVENU L'UN DES PLUS GRANDS RISQUES POUR LES ENTREPRISES ET CONSTITUE LA MENACE LA PLUS IMPORTANTE POUR LES SYSTÈMES INFORMATIQUES.

Le ransomware est devenu l'un des plus grands risques pour les entreprises et constitue la menace la plus importante pour les systèmes informatiques. Ce phénomène a atteint des proportions dignes d'une épidémie mondiale, dont les coûts estimés pourraient atteindre 20 milliards de dollars d'ici 2021. [1]

Et pourtant, pour les professionnels de l'IT et les décideurs des entreprises, ces données ne doivent pas nécessairement être catastrophiques. Si les cybercriminels ne montrent aucun signe d'essoufflement, les progrès réalisés en matière de technologies de lutte contre la cybercriminalité et de récupération après sinistre, associés à de bonnes pratiques de gestion informatique, permettent aux organisations de riposter.

Ce rapport explore l'évolution des menaces des ransomware ainsi que les technologies et les pratiques de gestion informatique utilisées pour se défendre, et présente une approche prospective en vue de bâtir un avenir sans ransomware.

CONNAÎTRE L'ENNEMI

Pour suivre le conseil du stratège militaire chinois Sun Tzu, « apprenez à connaître l'ennemi ». En effet, le développement d'une stratégie permettant de sécuriser les systèmes informatiques contre les ransomware nécessite de comprendre de quoi il s'agit. Commençons donc par expliquer ce qu'est un ransomware.

Les données sont les poumons de votre organisation. Elles représentent vos opérations qui circulent entre les différentes unités fonctionnelles. Elles retracent le passé, communiquent l'état actuel de l'entreprise et sous-tendent les décisions. On pourrait même aller jusqu'à dire que sans données, il n'y a pas d'entreprise. Et c'est précisément sur cette idée que le ransomware s'appuie.

Le ransomware est un logiciel malveillant conçu pour empêcher l'accès aux systèmes ou données de votre entreprise, jusqu'à ce qu'une rançon soit payée. Il est capable de stopper net l'élan de votre entreprise, ou, dans le cas d'un logiciel d'extorsion ou logiciel de fuite, il peut aller encore plus loin en menaçant d'exfiltrer et de diffuser vos données.

Les organisations qui stockent d'importantes données sur des ordinateurs ou des réseaux sont exposées, c'est-à-dire la totalité des organisations aujourd'hui. Les gouvernements nationaux et locaux, les autorités policières, les organisations de santé, les banques et sociétés émettrices de cartes de crédit constituent tous des cibles potentielles, sur un secteur du vol d'identité qui alimente le marché avec un montant extorqué aux consommateurs annoncé à 14,7 milliards de dollars en 2018 [2]. Les grandes entreprises ne sont pas les seules à être affectées ; les attaques des ransomware ciblent également les consommateurs et corporations, les petites organisations comme les grandes.

COMMENT FONCTIONNE UN RANSOMWARE ?

Une attaque de ransomware se produit lorsqu'un ordinateur a été infecté par un virus. La plupart des ransomware sont des Cryptolockers qui chiffrent les fichiers sur l'ordinateur affecté en les rendant inaccessibles, jusqu'à ce qu'une rançon soit payée en échange d'une clé permettant de déchiffrer les fichiers. Mais faites attention à ce que vous payez. Encore plus dangereux, le cryptolocker factice chiffre les fichiers et demande une rançon sans donner lieu en échange à l'envoi d'une clé de décryptage opérationnelle. Les victimes de ce genre de ransomware, qui, selon certaines estimations, représentent 50 % des cas, peuvent ne jamais récupérer l'accès à leurs fichiers, même après avoir payé la rançon. Le ransomware sans cryptage place un verrou entre vous et vos données, sans les chiffrer directement.

Le ransomware peut attaquer des fichiers spécifiques, ou le système global via le Master Boot Record (MBR) d'un lecteur ou secteur NTFS de Microsoft, empêchant ainsi le système d'exploitation de démarrer. Le ransomware contourne souvent les systèmes de détection en utilisant un réseau tel que le trafic crypté HTTPS ou Tor. Contrairement à d'autres types de malware qui peuvent fonctionner en tâche de fond, une fois que le ransomware a infiltré l'hôte malchanceux, il se fera connaître en demandant des cryptomonnaies impossibles à retracer pour payer la rançon.

Il peut suffire d'une seule petite action fortuite d'un utilisateur innocent, par exemple cliquer sur un lien malveillant, pour qu'un ordinateur devienne infecté. Typiquement, le ransomware se propage au moyen d'attaques d'hameçonnage, mais les cybercriminels utilisent de nombreuses techniques variées pour infecter les victimes avec leur ransomware. L'infection se produit généralement suite à l'ouverture d'une pièce jointe dans un e-mail ou après avoir cliqué sur un lien frauduleux. Les vecteurs courants utilisés pour répandre les ransomware sont :

E-mails et messages texte incluant des liens vers un logiciel malveillant ou une pièce jointe contenant un logiciel malveillant.

Sites Web dont l'unique objectif est d'attirer l'attention des utilisateurs et les inciter à cliquer sur un lien ou à lancer un téléchargement malveillant.

Malvertising ou publicités malveillantes qui appâtent les utilisateurs avec des liens frauduleux menant à des téléchargements non intentionnels.

Réseaux sociaux qui peuvent sembler connectés à des sources de confiance, mais qui mènent rapidement vers de perfides cybercriminels. À leur insu, les victimes contractent l'infection directement depuis l'application de réseau social, ou bien elles sont invitées à cliquer sur une publicité ou un lien malveillant.

Applications mobiles que les utilisateurs téléchargent intentionnellement sur leur appareil, sans se rendre compte qu'il s'agit d'applications factices conçues pour transférer un virus lors de la prochaine connexion de leur appareil mobile à un ordinateur.

Les hackers sont devenus plus sophistiqués, ciblant les utilisateurs en envoyant des pièces jointes infectées dans un e-mail qui semble provenir d'une personne appartenant à leur liste de contacts. Et si les politiques en matière d'utilisation et la formation contribuent à réduire les comportements à risque des utilisateurs finaux, il est impossible d'éliminer complètement cette vulnérabilité, car les points d'entrée ne sont pas toujours évidents. Le contenu malveillant peut exploiter les vulnérabilités dans le navigateur ou les plug-ins et exécuter un code malveillant à l'insu de l'utilisateur. Une fois établie sur un hôte, une infection peut se propager facilement à d'autres ordinateurs du même réseau.

En plus d'appâter les utilisateurs pour leur faire télécharger sans le savoir un ransomware, les cybercriminels parviennent à accéder aux systèmes via Internet, sans que quiconque ne s'en aperçoive. Grâce à des méthodes brutales et à l'utilisation d'informations d'identification achetées sur l'Internet clandestin, ils accèdent aux ressources et aux données, en exploitant le protocole RDP et les vulnérabilités logicielles.

Un rapport de 2019 a mis en évidence que, pour les entreprises et organisations gouvernementales, les cibles les plus courantes des ransomwaresont les actifs à forte valeur ajoutée tels que les serveurs, l'infrastructure d'application et les outils de collaboration. Si les organisations privilégient, à juste titre, les tendances et les vulnérabilités les plus critiques, elles ne peuvent ignorer pour autant les vulnérabilités plus anciennes ou moins critiques. D'après ce rapport, les vulnérabilités plus anciennes (trois ans ou plus) représentaient plus d'un tiers des attaques, dont plus de la moitié s'en prenaient aux vulnérabilités moins critiques. [3]

LES ATTAQUES DES RANSOMWARE ENTRAÎNENT EN MOYENNE 10 JOURS D'ARRÊT.[4]

Quelles sont les conséquences d'une infection par un ransomware ?

En raison de l'actualité chargée au sujet d'attaques par des ransomware et du déferlement de statistiques effrayantes, les entreprises ne peuvent plus ignorer la menace et recherchent des solutions efficaces en matière de sécurité et de protection des données. L'effet immédiat d'un ransomware est l'interruption majeure des opérations de l'entreprise tandis que les appareils et systèmes sont arrêtés pour pouvoir procéder à la désinfection. Heureusement, la restauration totale des données est possible avec la mise en place de procédures de sauvegarde planifiée et de stratégies de récupération après sinistre. Les attaques des ransomware entraînent près de 10 jours d'arrêt.[4]

Si le ANSII déconseille de payer les rançons, plus de 2,57 millions de dollars de rançon auraient été payés en 2018[5], aux États-Unis. En moyenne, on estime que le coût moyen pour les entreprises s'élève à 133 000 $ par attaque, pour pouvoir récupérer l'accès à ses propres données. Et malheureusement, il arrive que les victimes payent sans aucune garantie de récupérer leurs fichiers et données. Des études révèlent que les auteurs de ransomware gagnent plus du double du salaire moyen des développeurs qui travaillent sur des projets légitimes [7]. Clairement, ce qui fonctionne pour les assaillants est mauvais pour les organisations et leurs équipes informatiques.

2,57

MILLIONS DE DOLLARS VERSÉS POUR DES RANÇONS[5]

133 000$

EN MOYENNE PAR ATTAQUE[6]

Les entreprises espèrent de tout cœur que leur système de défense contre les ransomware fonctionnera. Mais même si ces systèmes empêchent le pire, ou au moins le limitent, elles doivent tout de même composer avec la perte de données résultant de l'attaque. Les pertes engendrées par une attaque concernent en moyenne 8 % des données [8]. En plus de demander le paiement d'une rançon, les assaillants peuvent extraire des données depuis un ordinateur ou un serveur infecté, exposant ainsi des données sensibles, comme des noms d'utilisateur et mots de passe, des informations sur des paiements et les adresses e-mail de contacts. Les nouveaux ransomware s'attaquent aux fichiers de sauvegarde sur des partages réseau et peuvent même supprimer des copies masquées sur le poste de travail pour empêcher leur restauration. L'attaque et la perte de données qui en résulte sont un double revers pour l'entreprise, et les risques pour sa réputation peuvent avoir un effet dévastateur à long terme et compromettre fortement la crédibilité de la marque.

> *« Les cybercriminels utilisent des tactiques de plus en plus sophistiquées, et, de toute évidence, aucun secteur n'est à l'abri de telles attaques de **ransomware**. En ciblant les systèmes de sauvegarde, les hackers augmentent leurs chances que les organisations touchées payent la rançon, du fait des conséquences dramatiques résultant de la perte de données et de l'arrêt des systèmes, ce qui va bien au-delà des répercussions financières. Lorsque les systèmes et données sont fragilisés, les responsables d'entreprises et directeurs informatiques doivent également tenir compte de l'impact négatif sur la productivité des employés, la confiance des clients, la réputation de la marque et la conformité réglementaire ».*
>
> *- Oussama El-Hilali, Directeur des technologies chez Arcserve*

De quelle manière les professionnels de l'IT protègent-ils leurs organisations contre les ransomware ?

Différentes méthodes sont utilisées pour détecter les ransomware et protéger les systèmes et données de valeur. En voici quelques exemples :

- **Logiciel de protection contre les ransomware** pour identifier des attaques potentielles, en recherchant et en empêchant les intrusions.
- **Pare-feux** pour bloquer les accès non autorisés à un ordinateur ou un réseau.
- **Systèmes de filtrage des fichiers et filtres anti-spam** qui bloquent les sites Web soupçonnés de contenir des malware ou empêchent les pièces jointes indésirables d'entrer dans les boîtes de messagerie des utilisateurs.
- **Logiciel de la stratégie de groupe** qui bloque l'exécution des fichiers depuis des dossiers locaux capables d'infecter le système.
- **Les modules Security Information and Event Management** (SIEM) qui fournissent des informations concernant le trafic réseau afin de détecter des anomalies révélant une violation.
- **Logiciel de sauvegarde** pour protéger les données de l'entreprise en copiant les données depuis les serveurs, bases de données, bureaux, ordinateurs et autres appareils.
- **Surveillance de l'intégrité des fichiers** permettant de vérifier la cohérence entre le fichier actuel et un fichier validé.
- **Logiciel antivirus et anti-programme malveillant** pour empêcher, détecter et supprimer les malware.
- **Solutions Unified Threat Management (UTM)** permettant de réagir à différents types de menace avec un point de défense et une console uniques.

Si les méthodes permettant de détecter les ransomware et de protéger les systèmes et données critiques sont importantes et utiles sur le plan individuel, les organisations sont plus fortement exposées. Les techniques utilisées par les assaillants d'aujourd'hui sont plus sophistiquées et ingénieuses. Les stratégies d'attaque combinent souvent plusieurs techniques à la fois, qui ciblent simultanément différentes parties d'un réseau informatique. Les attaques de ransomware utilisent de nouvelles variantes des malware pour contourner les programmes antivirus. Mais alors, quels sont les pièges des stratégies de protection traditionnelles contre les ransomware ?

De nombreux systèmes ont des lacunes quant aux fonctionnalités importantes

Il était plus facile de lutter contre les problèmes liés aux malware lorsque les attaques pouvaient être mises en corrélation avec une technologie antivirus basée sur signature. Au fur et à mesure que les menaces évoluent et incluent des attaques distinctes contre des vulnérabilités courantes, il devient plus difficile d'identifier les menaces en utilisant une technologie basée sur signature.

En outre, de nombreux fournisseurs de protection des données ont pris le train en marche en mettant en avant des « fonctionnalités » en matière de cybersécurité qui, en réalité, permettent uniquement de détecter des anomalies de données, qui peuvent être ou non associées à des ransomware. Et après avoir détecté l'anomalie, elles ne font souvent que fournir une alerte, plutôt que d'essayer de résoudre le problème.

Le recours à différents outils complique la gestion des vulnérabilités croissantes

De nombreuses organisations ont recours à plusieurs outils et fournisseurs pour différentes fonctionnalités de lutte contre les ransomware ; par exemple, elles peuvent utiliser deux fournisseurs pour les pare-feux, un autre pour la protection contre la perte de données (DLP) ou le filtrage Web, un autre pour la récupération après sinistre et des sauvegardes, un autre pour les sauvegardes dans le cloud, pour les centres de données, et encore un autre pour les sauvegardes mobiles.

Le recours à de multiples dispositifs et fournisseurs pour différentes tâches liées à la sécurité rend encore plus difficile de tracer et de prévenir les attaques. Les outils et logiciels doivent être gérés et mis à jour, ce qui n'aide pas à rester au fait des dernières formes de malware lorsque différentes solutions s'accumulent. Le fait de gérer de multiples fournisseurs et solutions augmente les risques, les vulnérabilités et les erreurs. La productivité en pâtit et les coûts grimpent.

Aujourd'hui, vous pouvez transformer les outils existants complexes de lutte contre les ransomware fournis par différents fournisseurs en une solution unique et approfondie de défense intégrant une fonctionnalité complète de sauvegarde et de récupération des données, un réseau neuronal et une protection de point de terminaison contre les malware, les attaques et les ransomware inconnus.

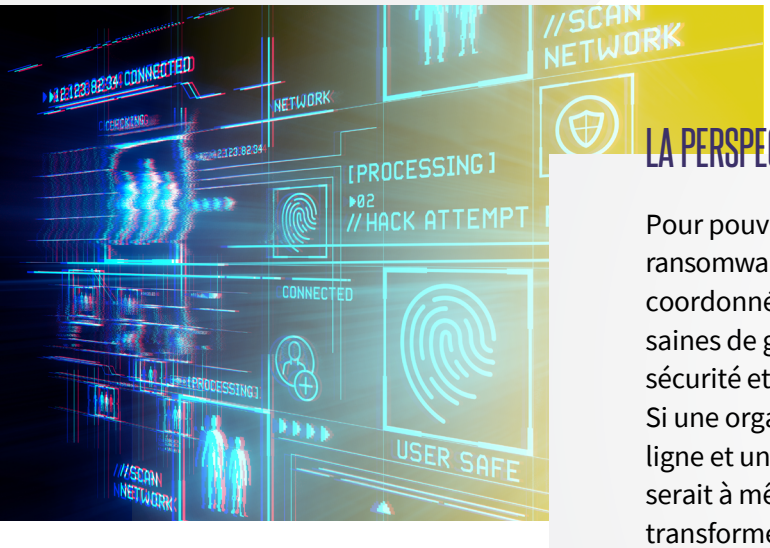
Les professionnels de l'IT doivent également appliquer des pratiques de gestion informatique

Les solutions technologiques sont vitales pour assurer la cybersécurité et la protection contre les ransomware, notamment les pare-feux, systèmes de détection des intrusions et de prévention, et sécurité de la messagerie. Les solutions avancées pour la sécurité et la protection intégrées des données contribuent grandement à protéger l'organisation. De même, des pratiques informatiques saines sont essentielles.

Il est important de reconnaître que les comportements de l'utilisateur final constituent la plus grande menace. Les organisations doivent mettre en œuvre des contrôles de gestion informatique capables de détecter lorsque des employés contournent une politique ou procédure. Les pratiques de gestion doivent inclure un engagement actif des utilisateurs, en expliquant de quelles manières les comportements doivent être ajustés pour garantir la sécurité.

Les professionnels de l'IT doivent également tenir compte de leur portefeuille informatique global afin d'évaluer les risques. Si les systèmes sont la proie des attaques, les agresseurs sont davantage intéressés par les informations critiques qui ne sont pas correctement protégées. Les entreprises doivent hiérarchiser la protection des ressources et utiliser un système de gestion informatique proactif incluant des objectifs de point de récupération afin d'estimer le niveau de perte de données acceptable en cas de défaillance et de consolider les défenses. Ils doivent connaître les ressources dont ils disposent ainsi que la manière dont elles sont configurées, et ils doivent contrôler strictement tout changement.

Un cadre tel que l'ITIL (Information Technology Infrastructure Library) peut aider les organisations à exécuter les pratiques recommandées en termes de gestion informatique. L'ITIL fournit des pratiques en matière de gestion des configurations, gestion des changements et gestion des versions en tant que processus clés que les organisations peuvent maîtriser afin de renforcer la cybersécurité et de mieux lutter contre la menace des ransomware.



LA PERSPECTIVE D'UN AVENIR SANS RANSOMWARE EST-ELLE RÉALISTE ?

Pour pouvoir repousser les attaques variées et diverses des ransomware, il est nécessaire de mettre en place une défense coordonnée associant une technologie adéquate à des pratiques saines de gestion informatique. La solution idéale est un système de sécurité et de protection multicouche de bout en bout.
Si une organisation informatique pouvait déployer une première ligne et une dernière ligne de défense contre les ransomware, elle serait à même d'éliminer la menace des ransomware et de transformer la manière dont elle protège et sécurise les données de l'organisation contre les extorqueurs, hackers et voleurs.

Une étude récente réalisée auprès des professionnels de l'IT a révélé que deux répondants sur trois estiment qu'il est essentiel de trouver des solutions combinant sécurité des données et protection. Pour eux, cela est encore plus important que de trouver des solutions qui incorporent l'intelligence artificielle ou qui permettent d'automatiser la conformité.[10]

STRATÉGIES DE PROTECTION CONTRE LES RANSOMWARE

Nous décrivons ici cinq **stratégies de protection contre les ransomware** qui peuvent aider votre entreprise à aller au-delà des approches de sécurité réactives et à intégrer des technologies anti-ransomware et de prévention des menaces associées à des capacités de récupération après sinistre et de haute disponibilité pour neutraliser les cyberattaques.

1 Gérer activement les accès

Mettre en œuvre les procédures et contrôles adéquats visant à sécuriser les applications et les systèmes contre les utilisateurs non autorisés.

- Limiter l'accès aux points d'entrée courants des ransomware, tels que les comptes de messagerie personnels et les sites de réseaux sociaux, et utiliser un filtrage Web au niveau de la passerelle et du point de terminaison afin de bloquer les tentatives d'hameçonnage pour les utilisateurs qui sont invités à cliquer sur un lien.
- Utiliser des règles d'authentification et de mot de passe à facteurs multiples et inclure des critères de mot de passe lorsque les utilisateurs communiquent avec des sites Web non classés par le proxy ou le pare-feu.
- Utiliser des serveurs de proxy et des logiciels de blocage des publicités et limiter les autorisations pour installer et exécuter des applications logicielles.
- Contrôler et surveiller les parties tierces qui disposent d'un accès distant au réseau de l'organisation et vos connexions avec les tiers afin de s'assurer qu'ils appliquent les pratiques recommandées en matière de cybersécurité.
- Utiliser une liste blanche d'applications afin d'autoriser uniquement l'exécution de programmes autorisés sur un réseau.

2 Gérer la configuration des systèmes pour l'ensemble des vecteurs d'infection

Déployer des systèmes et procédures de gestion centralisés pour affronter l'éventail complet des menaces des ransomware.

- Évaluer et classer les données sensibles de l'entreprise et mettre en place une séparation physique et logique des serveurs, réseaux et banques de données.
- Veiller à ce que des solutions antivirus et anti-malware soient configurées pour se mettre à jour automatiquement et analyser les messages entrants et sortants afin de détecter un possible hameçonnage, d'empêcher l'usurpation d'adresses électroniques et de filtrer les fichiers exécutables.
- Utiliser un système centralisé de gestion des correctifs permettant de corriger tous les points de terminaison au fur et à mesure que des vulnérabilités sont découvertes, y compris sur les appareils mobiles, systèmes d'exploitation, logiciels et applications, emplacements cloud et l'Internet des objets.
- Déployer des technologies anti-attaque, anti-ransomware et de Deep Learning sans signature, capables de détecter des malware connus et non connus.
- Déployer des technologies intégrées de protection de point de terminaison et de continuité de l'activité afin d'accélérer la prévention des menaces et d'activer la restauration immédiate des données.
- Sécuriser les applications et serveurs Web au moyen de pare-feux d'applications Web.
- Désactiver les scripts des fichiers Microsoft Office envoyés par e-mail et envisager d'utiliser le logiciel Office Viewer pour ouvrir des fichiers Office.

- Contrôler votre réseau afin de rechercher les systèmes qui utilisent le protocole RDP (Remote Desktop Protocol) en fermant les ports inutilisés, au moyen d'une authentification à deux facteurs.
- Détecter et diagnostiquer les comportements, tels que le chiffrement de fichiers de masse, ainsi que les comportements malveillants et de blocage.
- Ajouter une bannière d'avertissement sur les e-mails provenant de sources externes afin de rappeler aux utilisateurs les dangers de cliquer sur des liens et d'ouvrir des pièces jointes.
- Utiliser des systèmes de gestion unifiée des menaces (Unified Threat Management ou UTM) qui combinent un pare-feu, un antivirus de passerelle et des capacités de prévention et de détection des intrusions afin de bloquer l'accès aux adresses IP malveillantes connues.

3 Combiner des solutions de sécurité et de protection des données

Intégrer, tester et tenir à jour une solution complète de cybersécurité et de sauvegarde des données pour une protection de bout en bout.

- Protéger les espaces de sauvegarde contre les malware, les ransomwareet les attaques zero-day.
- Arrêter et supprimer des sauvegardes les menaces telles que les malware et les ransomware
- Conserver les sauvegardes des données sur des dispositifs distincts et utiliser des espaces de stockage hors ligne lorsque ceux-ci peuvent être la cible directe de dispositifs infectés.
- Sauvegarder les machines virtuelles, les espaces de stockage dans le cloud et les systèmes opérationnels en fonction des objectifs de point de récupération, en estimant le niveau de perte de données acceptable en cas de défaillance.
- Utiliser un système permettant de sauvegarder plusieurs itérations des sauvegardes, dans le cas où une copie des sauvegardes inclut des fichiers cryptés ou infectés.
- Intégrer des dispositifs de récupération après sinistre et de disponibilité des applications et tirer profit de l'intelligence artificielle pour assurer une protection de point de terminaison.
- Utiliser l'analyse des vulnérabilités, le chiffrement SSL et d'autres contrôles techniques afin de confirmer que les sauvegardes sont en cours.
- Utiliser la règle 3-2-1 et créer trois copies de vos données, en les stockant sur deux supports différents, dont un hors site.
- Tester régulièrement les sauvegardes afin de s'assurer de l'intégrité des données et de garantir qu'elles sont opérationnelles.
- Tester régulièrement les processus de récupération des données et de récupération après sinistre afin de s'assurer qu'ils sont prêts.

4 Impliquer les utilisateurs dans des formations et communications

Aider les utilisateurs en leur fournissant les formations et pratiques dont ils ont besoin pour se protéger contre les menaces des ransomware.

- Proposer régulièrement des formations et communications de sensibilisation, de sorte que chaque personne au sein de votre organisation comprenne la menace que représente les ransomwareet connaisse les techniques sécuritaires.
- Établir des politiques et procédures de prévention contre les ransomwaredestinées aux utilisateurs finaux.
- Inviter les utilisateurs à ne pas ouvrir les e-mails suspects ou les pièces jointes, ni à cliquer sur les liens douteux, et à faire preuve de prudence lors de l'ouverture de sites Web non connus, ainsi qu'à fermer son navigateur après utilisation.
- Veiller à ce que les employés sachent comment et à qui signaler toute activité suspecte.

5 Tenir à jour et tester un plan de continuité de l'activité et de récupération après sinistre

Établir, tester et tenir à jour les pratiques, procédures et outils technologiques nécessaires pour s'assurer que les applications et les données peuvent être récupérées intégralement en cas de sinistre.

- Mettre en place des plans de contingence et de résolution essentiels pour la récupération et la continuité de l'activité, quelle que soit la source du dysfonctionnement.
- Mener une évaluation des risques qui permette de classer les types de sinistres susceptibles de survenir, et établir des priorités en matière de récupération et de continuité de l'activité.
- Déployer des solutions de récupération après sinistre, de sauvegarde et de haute disponibilité, sur site et hors site.
- Élaborer un plan d'intervention en cas d'incident indiquant les mesures à prendre en présence d'un ransomware, notamment déconnecter le système infecté du réseau afin d'empêcher la propagation de l'infection et déterminer le niveau de sensibilité des données.
- Tester le plan, y compris les dispositifs et systèmes technologiques, afin de s'assurer qu'une protection complète est en place. Signaler toute infection aux autorités concernées.

ÊTES-VOUS PRÊT À LUTTER CONTRE LES RANSOMWARE ?

Téléchargez le guide d'**évaluation de la préparation en matière de ransomware** afin d'estimer vos capacités et d'élaborer une feuille de route pour un avenir sans ransomware.

UNE NOUVELLE TECHNOLOGIE POUR UN AVENIR SANS RANSOMWARE

Depuis des années, les professionnels de l'IT cherchent, en vain, une solution multicouche de sécurité et de protection des données de bout en bout permettant d'offrir aux utilisateurs résilience des systèmes informatiques et prévention des ransomware. La bonne nouvelle est que, désormais, il existe une solution qui fournit exactement cela : une première ligne et une dernière ligne de défense contre la menace des ransomware.

Cette solution combine Arcserve Appliance Series et Sophos Intercept X Advanced for Server afin de proposer une approche multicouche offrant une solution complète de protection et de sécurité des données, le tout au sein d'une plateforme unifiée.

Les utilisateurs bénéficient de l'ensemble des capacités des systèmes indépendants, ce qui supprime la nécessité de recourir à des composants discrets d'une solution complète en offrant une interface centrale pour les outils, l'infrastructure et les processus de sauvegarde. Les dispositifs Arcserve sont les seuls à proposer un stockage Flash accéléré et dédupliqué, un traitement robuste du serveur et une mise en réseau grande vitesse avec des services matériels et cloud à haute redondance.

Ajoutez la protection de point de terminaison de Sophos Intercept X Advanced for Server, et vous disposez d'une solution de bout en bout qui inclut un système de détection de malware basé sur signature et sans signature et sans signature, un réseau neuronal/système d'intelligence artificielle avancé (Deep Learning), une solution anti-attaque, ainsi que des technologies anti-ransomware fournissant une protection contre l'éventail le plus varié de menaces du point de terminaison.

Le résultat ? Une solution combinée sans équivalent « tout en un » : cybersécurité du début à la fin, sauvegarde des données, récupération après sinistre et haute disponibilité, le tout combiné en une solution unique couvrant l'ensemble des besoins en termes d'infrastructure.

RÉSUMÉ

Si les ransomware présentaient un risque important pour les entreprises et une vrai menace, l'avenir s'annonce prometteur. Aujourd'hui, les organisations peuvent :

- **déployer des solutions de protection approfondie intégrées** couvrant les domaines comme la sauvegarde avancée, la récupération après sinistre, la haute-disponibilité et la cybersécurité;
- **appliquer des pratiques en matière d'IT** avec des méthodes efficaces d'engagement client, de gestion des données et de récupération après sinistre qui permettent d'obtenir un retour sur investissement ; et
- **fournir une première ligne et une dernière ligne de défense** qui accélèrent la détection des menaces et permettent une restauration immédiate des données sauvegardées.

Alors pourquoi tolérer le statu quo ? Pourquoi consentir à vivre dans un monde ou les cyberextorqueurs, hackers et voleurs utilisent les ransomware pour extraire des gains mal acquis auprès d'entreprises qui cherchent simplement à mener leurs activités ? Défendez-vous ! Gardez vos données en sécurité. Utilisez la technologie actuelle de protection de bout en bout et les pratiques saines de gestion informatique pour s'assurer que, finalement, vous et votre organisation pouvez profiter d'un avenir sans ransomware.

À PROPOS D'ARCSERVE

Arcserve offre des solutions exceptionnelles pour protéger la valeur inestimable des actifs numériques des organisations qui souhaitent mettre en place une solution complète de protection des données à grande échelle. Fondée en 1983, Arcserve est le fournisseur de solutions de continuité de l'activité le plus expérimenté au monde, en proposant des outils permettant de sauvegarder, génération après génération, les infrastructures informatiques grâce à des systèmes et applications disponibles partout, sur site et dans le cloud. Les organisations de plus de 150 pays dans le monde s'appuient sur les technologies intégrées extrêmement efficaces et l'expertise d'Arcserve pour éliminer les risques de perte de données et les temps d'arrêt prolongés, tout en réduisant les coûts et la complexité associés à la sauvegarde et à la restauration des données de plus de 50 %.

À PROPOS DE SOPHOS

Plus de 100 millions d'utilisateurs dans 150 pays ont choisi la solution Sophos comme meilleure protection contre les menaces complexes et la perte de données.
Sophos fournit des solutions de sécurité complètes qui sont faciles à déployer, à gérer et à utiliser, avec un coût de possession total le plus bas du marché. Sophos offre une solution reconnue en matière de chiffrement, sécurité du point de terminaison, Web, messagerie, technologie mobile, serveur et sécurité du réseau qui s'appuie sur SophosLabs, un réseau mondial de services de renseignements sur les menaces.

RESOURCES

1 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

2 https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt

https://www.aarp.org/money/scams-fraud/info-2019/survey-identity-fraud-decline.html

3 https://risksense.com/press_release/risksense-spotlight-report-exposes-top-vulnerabilities-used-in-enterprise-ransomware-attacks/

4 https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

5 https://pdf.ic3.gov/2018_IC3Report.pdf

6 https://www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx

7 https://twitter.com/CarbonBlack_Inc/status/925348051782373382

8 https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

9 Étude Arcserve EMEA, 31 juillet 2019

10 Étude Arcserve EMEA, 31 juillet 2019

Pour en savoir plus sur Arcserve, **visitez le site www.arcserve.com/fr/**