arcserve®

Ne devenez pas une statistique:

Gardez une longueur d'avance sur les cybercriminels en mettant en œuvre une stratégie globale de protection contre les ransomware

Dans les environnements professionnels permanents et obsédés par les données, les cybermenaces sont au cœur des préoccupations des équipes de sécurité informatique.

Les ransomware en particulier donnent des cheveux blancs aux services informatiques. La fréquence des attaques est en augmentation et les dernières tendances et tactiques deviennent plus ciblées, plus destructrices et plus difficiles à détecter rapidement.

Par exemple, depuis 2019, il y a eu au moins 440 attaques ciblées de ransomware contre des secteurs d'infrastructures essentielles, y compris la santé, les services financiers, le gouvernement et l'éducation. De plus, en 2020, la COVID-19 a donné naissance à une tendance des attaques de hameçonnage et de ransomware sur le thème de la pandémie qui s'établissent chez des employés distraits à la recherche de réponses et de réconfort pendant cette période de grande incertitude.

Les ransomware continuent d'évoluer, de nouvelles tactiques et de nouvelles technologies émergeant régulièrement, telles que :

Double extorsion
Les opérateurs de ransomware non seulement chiffrent vos données, mais ils les publient également sur Internet.

Cryptage à retardement
Les ransomware restent inactifs pendant un certain temps avant de crypter vos données afin d'attendre jusqu'à la fin de vos sauvegardes.

Ciblage des sauvegardes
Certaines souches de ransomware recherchent les fichiers de sauvegarde pour les crypter et faire de la reprise après sinistre un cauchemar.

Comment les environnements informatiques actuels permettent-ils les ransomware?

La nature et la conception des environnements informatiques modernes ont créé un écosystème composé de nombreuses parties mobiles et des systèmes disparates.

Cette déconnexion élargit invariablement la surface d'attaque d'une entreprise et rend la lutte contre les ransomware plus difficile. Certaines des vulnérabilités les plus fréquemment exploitées viennent de quelques sources courantes.

Des niveaux élevés de complexité

Les infrastructures informatiques actuelles sont notoirement complexes. De nombreuses entreprises s'efforcent de prendre en charge et sécuriser leur large gamme de plateformes et d'applications. Les équipes informatiques se retrouvent souvent à jongler entre différents éléments d'infrastructure, notamment :

- Infrastructures sur site et cloud public/privé/hybride
- Informatique et périphériques mobiles
- Solutions telles que Saas (software as a service), PaaS (platform as a service) et Iaas (infrastructure as a service)
- Et bien plus encore

Risque pour les fournisseurs tiers

Lorsque vous vous associez à un tiers, il est essentiel de confirmer que ce dernier prend la cybersécurité autant au sérieux que vous. Tous les points d'accès, réseaux et bases de données partagés deviennent des points faibles pour les opérateurs de ransomware, la diligence et l'évaluation de la sécurité du tiers sont donc primordiales.

Équipes dispersées

La COVID-19 a dispersé une grande partie des équipes. Mais avec peu de temps pour préparer la transition, les entreprises ont dû bricoler une « assez bonne » infrastructure de prise en charge et de sécurité. Souvent, elle n'était justement pas « assez bonne », ce qui a fait des employés à distance des cibles prisées des acteurs malveillants.

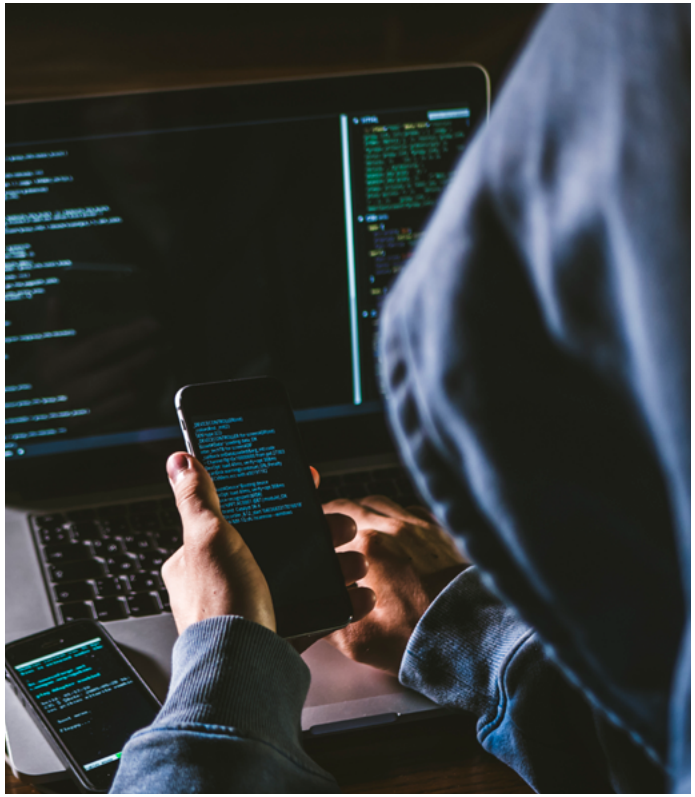
Correctifs et mises à jour manqués

Les correctifs et mises à jour de sécurité sont chronophages et fastidieux. Ce sont également deux des meilleurs moyens d'empêcher les ransomware. Des études montrent qu'une faille de sécurité sur trois pourrait être évitée si les correctifs étaient à jour. En réalité, le flux de correctifs publiés est infini, et de nombreuses équipes informatiques sont trop occupées pour suivre le rythme.

Anciens systèmes

Les anciens systèmes et logiciels sont une invitation ouverte pour les opérateurs de ransomware. Les anciens systèmes ne s'intègrent pas bien aux solutions de cybersécurité plus récentes, ce qui signifie qu'ils ne sont pas correctement protégés..

La COVID-19 a dispersé une grande partie des équipes. Mais avec peu de temps pour préparer la transition, les entreprises ont dû bricoler une « assez bonne » infrastructure de prise en charge et de sécurité.



Accumulation des coûts directs et indirects des ransomware

L'impact d'une attaque réussie de ransomware variera considérablement d'une entreprise à une autre, selon le secteur, le niveau de risque et la gravité de l'attaque. Cependant, toutes les entreprises doivent avoir en tête une vérité universelle: Les dommages des ransomware vont bien au-delà de la première attaque.

Les impacts les plus évidents et les plus immédiats des ransomware sont nombreux, notamment:

- Temps d'arrêt et perte de productivité en raison du cryptage des données
- Perte de revenus en conséquence de ces temps d'arrêt
- Risque de perte de données si les sauvegardes sont incomplètes ou non sécurisées
- Coûts directs des efforts de nettoyage et des paiements des rançons — si vous décidez de suivre cette voie, ce que nous déconseillons

Cependant, il existe plusieurs impacts à long terme moins tangibles, mais tout aussi préjudiciables, à connaître. Par exemple, il est difficile de quantifier le préjudice subi par la réputation de votre entreprise. Les brèches de sécurité nuisent à la confiance que les clients et les actionnaires ont dans votre entreprise, il se peut donc qu'il y ait une baisse du nombre de nouveaux clients, que des clients actuels passent se tournent soudain vers un nouveau fournisseur de solutions ou que vous perdiez en compétitivité sur le marché.

Selon votre secteur et la gravité de la brèche, votre entreprise peut également se retrouver à subir des répercussions en matière de conformité et de réglementation ou empêtrée dans des litiges et des procédures d'indemnisation qui entraînent des amendes et des sanctions importantes.

Les brèches de sécurité nuisent à la confiance que les clients et les actionnaires ont dans votre entreprise, il se peut donc qu'il y ait une baisse du nombre de nouveaux clients, que des clients actuels passent se tournent soudain vers un nouveau fournisseur de solutions ou que vous perdiez en compétitivité sur le marché.

Adoption d'une approche globale de la protection contre les ransomware

Face à une nouvelle série de menaces de ransomware, de nombreuses entreprises pensent que leurs anciennes stratégies de sécurité et de réduction des menaces ne suffisent plus. Les équipes de sécurité informatique adoptent donc à la place des solutions globales et proactives pour lutter contre les ransomware.

Adopter une approche globale de la protection contre les ransomware est comparable à ajouter un champ de force autour de votre entreprise. Il s'agit d'intégrer une stratégie de sécurité complète qui bloque l'accès et minimise les préjudices à votre infrastructure informatique en prenant des mesures à la fois offensives et défensives.

Une protection totale contre les ransomware implique une combinaison des éléments suivants :

- **Outils et technologies de cybersécurité**
- **Fonctions de reprise orchestrée**
- **Plans à mettre en œuvre pour gérer les employés, les règles et les processus**

Outils et technologies de cybersécurité

La protection des infrastructures multi-générationnelles et des données essentielles est un objectif primordial pour les équipes de sécurité informatique. Dans le cadre d'une stratégie globale de protection contre les ransomware, la cybersécurité englobe la protection des terminaux et les pare-feux, la gestion des identités et des accès, ainsi que la prévention des pertes de données.

Pour relever les défis actuels que présentent les ransomware, votre solution de cybersécurité doit comprendre des technologies de détection et de prévention, notamment :

- Détection des logiciels malveillants basée sur signature et sans signature
- Réseau neuronal deep learning
- Technologie de lutte contre les attaques, telle que Sophos Intercept X Advanced

Fonctions de reprise orchestrée

Dans un monde idéal, on empêcherait 100 % des ransomware, 100 % du temps. En réalité, il est fort probable que votre entreprise sera touchée à un moment donné. Une reprise rapide après une crise dépend de votre niveau de préparation et de vos capacités d'orchestration, ce qui doit être abordé dans votre stratégie de protection globale.

Les entreprises très résilientes disposent d'un plan de reprise après sinistre testé et prêt à l'usage bien avant d'en avoir besoin. Une des principales composantes d'un solide plan de reprise après sinistre est une sauvegarde sécurisée, complète et à jour ; mais cela ne suffit pas.

Votre plan de reprise doit absolument comprendre une sauvegarde sur le cloud, mais vous devez également inclure une protection contre de nouvelles souches de ransomware qui ciblent les fichiers de sauvegarde. La stratégie de sauvegarde traditionnelle 3-2-1 n'est plus suffisante. Pour garantir des capacités de reprise totale, il faut maintenant inclure des sauvegardes Air Gap, ce qui en fait un plan de sauvegarde 3-2-1-1.

Comme de plus en plus d'entreprises accompagnent les employés à distance à l'aide de solutions basées sur le cloud telles que Microsoft Office 365, il est crucial de mettre en place un plan visant à protéger vos applications SaaS contre la perte de données. De nombreuses solutions SaaS utilisent un modèle de responsabilités partagées, ce qui signifie que si vous ne sauvegardez pas vos données, vous vous exposez à des difficultés.

Mesures pour les employés, les règles et les processus

Les êtres humains sont en général le maillon le plus faible de tout effort de protection contre les ransomware. Et si vous pouviez faire de tous vos employés une extension du service informatique, pour qu'ils deviennent la première ligne de défense de votre entreprise ?

L'éducation est la première étape pour réduire l'erreur humaine. Voici certains des domaines clés sur lesquels se pencher :

- Exercices de reprise après sinistre des données
- Formation à la cybersécurité, pour que les employés connaissent les menaces à surveiller
- Formation de sensibilisation à la sécurité pour leur apprendre quoi faire (et ne pas faire) pour prévenir les brèches de sécurité et les infections par des logiciels malveillants

D'autres moyens de réduire l'aspect relatif à l'erreur humaine des menaces que présentent les ransomware sont de mettre en œuvre des politiques d'accès sécurisé, telles que l'authentification multi-facteurs, et une diligence raisonnable, notamment des vérifications des antécédents des employés, des évaluations des risques de tiers et une bonne sécurité physique traditionnelle.

> **Les êtres humains sont en général le maillon le plus faible de tout effort de protection contre les ransomware.**

Bénéficier d'un avenir sans ransomware avec le bon partenaire

Lorsque vous êtes prêt à mettre en œuvre une stratégie globale de protection contre les ransomware, il est important de vous associer à un fournisseur de solutions qui dispose d'une certaine expertise en matière de prévention des ransomware.

Même au-delà de l'expérience, vous avez besoin de quelqu'un qui partage les valeurs de votre entreprise et comprend votre activité.

Lorsque vous parlez la même langue qu'un partenaire et que vous partagez les mêmes objectifs, il est beaucoup plus facile de travailler en équipe pour réaliser vos objectifs commerciaux. Le bon fournisseur de solutions peut vous aider à mettre en œuvre une stratégie globale de protection contre les ransomware en vous aidant à déterminer les composantes clés d'un plan de sécurité des données et des systèmes très solide.

Lorsque vous parlez la même langue qu'un partenaire et que vous partagez les mêmes objectifs, il est beaucoup plus facile de travailler en équipe pour réaliser vos objectifs commerciaux.

Intégration et sécurité

L'intégration de la cybersécurité et la protection des données est le seul moyen de se protéger entièrement contre les ransomware. Lorsque votre stratégie de protection contre les ransomware comprend les forces combinées de solutions telles que Sophos Intercept X, Nutanix HCI et Arcserve Unified Data Protection vous pouvez:

- Réduire la complexité des infrastructures
- Améliorer les accords de service (SLA)
- Intégrer sans difficulté la protection informatique et des données sur site, sur le cloud, sur l'infrastructure hyperconvergée (HCI) et sur les workloads SaaS.

Sauvegarde et reprise

On n'insistera jamais assez sur l'importance d'une sauvegarde sécurisée, testée et à jour pour une reprise réussie après une attaque de ransomware ou une autre perturbation imprévue. Le bon partenaire peut aider votre entreprise à trouver des solutions adaptées de sauvegarde et de reprise qui répondent à vos besoins actuels en matière de stockage et de protection des données — et ceci évoluera selon les besoins pour adapter votre stratégie de sécurité..

Protection des données par abonnement

Il est important de trouver un partenaire qui met les objectifs de votre organisation au cœur de chaque transaction. Ceci est particulièrement vrai lorsqu'il s'agit de budgétiser une solution de protection contre les ransomware.

Lorsque vous vous associez à un fournisseur de solutions qui offre des licences universelles, vous pouvez être sûr que toutes vos données sont protégées et que vous savez exactement ce que vous payez. Il n'y a pas de coûts cachés, et vous payez uniquement pour ce qu'il vous faut, vous pouvez donc faire évoluer votre forfait selon vos besoins.

Défendre, évoluer et s'adapter

Les ransomware et autres cyberattaques ne vont pas disparaître, notre seule option est donc d'apprendre à défendre nos systèmes, nos applications et nos données.

Ces menaces évoluent et s'adaptent en permanence, ce qui signifie que nous devons également faire évoluer et adapter nos stratégies de sécurité.

La sécurité totale des données commence par une approche gérée pour protéger les infrastructures informatiques et les données de sauvegarde contre les cyberattaques, mais cela ne s'arrête pas là.

Le chemin vers un avenir sans ransomware doit intégrer des technologies de cybersécurité, une sauvegarde et une reprise orchestrées, ainsi que des règles complètes, des processus et des formations pour gérer le côté humain de la prévention contre les ransomware. Les équipes de sécurité informatique doivent gérer les menaces de ransomware de façon proactive et continue grâce à une stratégie de protection globale qui évolue avec le paysage des menaces.

Le chemin vers un avenir sans ransomware doit intégrer des technologies de cybersécurité, une sauvegarde et une reprise orchestrées, ainsi que des règles complètes, des processus et des formations pour gérer le côté humain de la prévention contre les ransomware.

arcserve®

Pour savoir comment Arcserve peut vous aider à garder une longueur d'avance sur les cybercriminels, contactez-nous ci-dessous.

EN SAVIOR PLUS