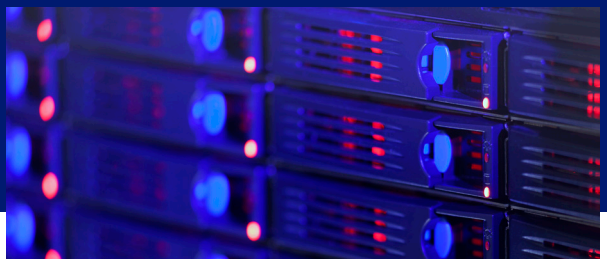
Protection de la sauvegarde : la nouvelle règle du 3-2-1-1



Les attaques par ransomware sont de plus en plus courantes et les entreprises actuelles doivent prendre conscience qu'elles ne sont plus une cible potentielle. Elles sont devenues des cibles certaines et la seule inconnue reste la date à laquelle l'attaque surviendra. D'après un rapport IDC récent de 2021* relatif à une étude menée par des analystes du marché de la technologie, plus de 90 % des entreprises ont été victimes d'un logiciel malveillant ou d'une attaque par ransomware. Et pour plus de 80 % d'entre elles, l'attaque par logiciel malveillant qu'elles ont subie a été fructueuse pour les cybercriminels.

Il faut donc changer d'état d'esprit : se préparer à ces atteintes à la sécurité qui sont inévitables et planifier une méthode permettant de rétablir un fonctionnement normal dans les meilleurs délais. Pour les clients du marché intermédiaire et les grandes entreprises, les attaques par ransomware ont changé la donne. Mais de nouvelles règles et de nouvelles solutions leur permettent de garder une longueur d'avance.

La nouvelle cible : les sauvegardes

Dans son rapport, IDC a identifié les menaces évolutives sur les données de sauvegarde. Les cybercriminels savent qu'en attaquant les données de sauvegarde, ils empêchent l'entreprise d'échapper dans un premier temps à l'attaque en restaurant des données non compromises. Après avoir atteint les données de sauvegarde, ils passent ensuite aux sources de données principales, au rythme et à l'échelle de leur choix.

Les cybercriminels à l'origine des attaques par ransomware exploitent les failles des systèmes de détection pour propager leur logiciel malveillant. Et leurs techniques sont de plus en plus élaborées. On assiste dans le domaine de la cybersécurité à un véritable jeu du chat et de la souris dans lequel certains logiciels de surveillance recherchent des activités d'E/S inhabituellement élevées sur les disques afin de repérer des chiffrements non souhaités de données. Mais les cybercriminels à l'origine des ransomware peuvent réagir en ralentissant le chiffrement. Ils utilisent également une stratégie qui consiste à déclencher une attaque bien après la faille, au-delà de la période des cycles de rétention.

Le rapport mentionne les raisons principales pour lesquelles certaines entreprises ne parviennent pas à protéger leur sauvegarde. Certaines ne préparent pas suffisamment leurs processus et leurs plans de restauration. D'autres s'orientent vers une réponse à partir d'un système de reprise après sinistre. Et d'après l'IDC, les entreprises qui protègent les données de toutes leurs applications ne sont pas nombreuses, ce qui signifie que la majorité d'entre elles restent en partie vulnérables à la perte des données.

Bienvenue dans l'ère de la règle du 3-2-1-1

Les spécialistes de l'informatique sont probablement nombreux à connaître l'ancienne règle du 3-2-1 concernant la protection des données : trois copies de données (une copie principale et deux copies de sauvegarde), deux copies stockées localement dans deux formats distincts (NAS, bande ou lecteur local) et une copie stockée hors site (dans le cloud ou dans un stockage sécurisé). Mais étant donné l'importance de la protection de la sauvegarde, le rapport IDC recommande désormais une nouvelle règle : celle du 3-2-1-1, le 1 supplémentaire faisant référence au stockage immuable.

L'immuabilité est un élément essentiel à l'efficacité d'une protection contre les attaques par ransomware. Elle consiste à convertir les données dans un format non réinscriptible (une seule écriture, plusieurs lectures) qui ne peut pas être altéré. Contrairement au chiffrement des données, elle n'implique pas l'utilisation d'une clé : il n'y a donc aucune possibilité de « lecture » ou d'inversion de cette immuabilité. L'immuabilité est également essentielle lorsqu'elle est associée à d'autres éléments de protection des données (notamment une protection permanente) qui peuvent capturer les données à chaque écriture à des intervalles très proches, mesurés en secondes. Si ces données sont ensuite stockées sous une forme immuable, le client peut avoir un snapshot, c'est-à-dire un « instantané » des données qui ne peut pas être modifié. Si elles disposent de la technologie adéquate et utilisent de bonnes pratiques en matière de restauration et de reprise, les entreprises ont accès à des données intactes quelques minutes à peine après la faille.

*IDC Perspective : To Thwart Ransomware, Protect the Backup First by Using Five Key Elements. 2021 IDC. https://cdn.idc.com/getdoc.jsp?containerId=US47666321

Les bonnes pratiques en matière de protection des données intègrent désormais un modèle de type 3-2-1-1 :

Création de 3 copies de vos données (1 copie principale et 2 copies de sauvegarde)

2 copies sont stockées localement sur au moins 2 types de supports de stockage (lecteur local, NAS, bande, etc.)

Stockage de l'une de ces copies hors site (stockage sécurisé, cloud, etc.)

1 copie sur un stockage immuable (sur une appliance OneXafe ou dans le cloud)

Nouvelles solutions

Il n'existe pas de solution miracle aux menaces par ransomware. La meilleure stratégie reste l'approche multimodale. Dans la réalité, la plupart des clients des revendeurs à valeur ajoutée utilisent une combinaison de technologies, de solutions et de fournisseurs. Ces approches en silos peuvent être à l'origine d'insuffisances que les cybercriminels peuvent exploiter.

Mais il y a une bonne nouvelle : il est possible de mêler de nouvelles technologies et de nouvelles solutions en fonction des besoins des clients. Lors de la phase de prévention et de détection des intrusions, les nouvelles solutions utilisent des réseaux basés sur l'apprentissage neuronal pour détecter les menaces, connues et inconnues. Lors de la phase de réponse, certaines solutions utilisent l'analyse comportementale pour bloquer les attaques par ransomware inédites. Lors de la phase de protection et de reprise des données, des solutions telles que l'appliance OneXafe 4400 Series, une nouveauté Arcserve, associent immuabilité et protection permanente des données.

Objectif : la continuité d'activité

Il est difficile de trouver une continuité de solutions couvrant l'intégralité des besoins des clients. La fusion récente d'Arcserve et de StorageCraft a constitué un portefeuille de solutions qui permet aux entreprises de s'orienter clairement vers la continuité d'activité. Qu'il s'agisse de solutions basées sur des appliances et qui associent immuabilité (OneXafe 4400 Series, par exemple) ou détection des intrusions à la technologie du réseau neuronal (Sophos Intercept X Advanced, par exemple), elles sont toutes nécessaires pour contrer les menaces actuelles qui évoluent en permanence.

Une chose est certaine : les menaces que font peser les attaques par ransomware et les logiciels malveillants sur les sauvegardes de données ne vont pas disparaître. En s'intéressant à la continuité d'activité, les revendeurs à valeur ajoutée ont un rôle à jouer auprès des clients en matière de processus, de personnes et de solutions. C'est ce qui fera la différence d'un revendeur à l'autre et ce qui sera également le plus efficace pour le client.

Pour aller plus loin

En savoir plus : arcserve.com/fr ou nous contacter

À propos d'Arcserve

Figurant parmi les 5 principaux fournisseurs de solutions de protection des données à l'échelle mondiale, Arcserve propose la plus large gamme de solutions de pointe pour la gestion, la protection et la récupération de toutes les charges de travail de données, destinées aux PME comme aux grandes entreprises, où qu'elles se trouvent ou quelle que soit leur complexité. Les solutions Arcserve protègent et sécurisent tous les environnements de données grâce à des solutions de pointe, économiques, agiles et largement évolutives, qui éliminent toute la complexité. Elles sont compatibles avec toutes les infrastructures : sur site, dans le cloud (DRaaS, BaaS et d'un cloud à l'autre), hyperconvergées et Edge. Avec son expérience de près de trente ans dans le protocole IP primé et dans la recherche permanente d'innovation, cette entreprise garantit à tous ses partenaires (fournisseurs de services gérés, revendeurs à valeur ajoutée, revendeurs grand compte ou utilisateurs finaux) comme à ses clients qu'ils sont sur la bonne voie : celle des charges de travail et des infrastructures de données de nouvelle génération. Présente dans plus de 150 pays, la société Arcserve est 100 % channel. Elle compte 19 000 partenaires de distribution qui aident à protéger les données stratégiques de 235 000 clients. Pour plus d'informations, consultez le site arcserve.com et suivez @Arcserve sur Twitter.