TechTarget | Custom Media

Évolution du rôle des sauvegardes à l'ère des ransomware

Le rôle des sauvegardes est en train d'évoluer. Face à des attaques qui gagnent en intelligence et en précision, les responsables IT doivent également évoluer avec leur temps. En effet, les cybercriminels étant plus habiles à pénétrer les réseaux, il devient nécessaire de prévoir des sauvegardes plus sophistiquées couvrant une multitude de situations et de types de menace. Nous sommes en train de changer notre manière de travailler, consommer des données, concevoir nos systèmes informatiques professionnels et dépendre de systèmes en ligne plus complexes et cela doit s'accompagner d'une nouvelle façon d'effectuer nos sauvegardes.

Sponsorisé par
Veeam Software

Avril 2018

Examinons d'abord les **conditions de travail dans la plupart des entreprises : elles sont aujourd'hui très différentes de celles de la décennie précédente**. Les collaborateurs sont maintenant disséminés sur l'ensemble de la planète et nombre d'entre eux travaillent depuis leur domicile ou dans de plus petits bureaux distants. Nous faisons presque tous un usage professionnel de notre smartphone sur lequel nous créons des données qui ne résident nulle part ailleurs . Sans compter qu'avec l'allongement de l'amplitude horaire, la stratégie consistant à effectuer les sauvegardes en dehors des heures de bureau devient relativement obsolète. « Avant, votre travail se déroulait à l'endroit où vous passiez la journée. Or, les utilisateurs d'aujourd'hui ont de nouvelles exigences et leurs données doivent être disponibles 24/7, où qu'ils se trouvent », constate Ken Pipkins, gestionnaire de comptes cybersécurité chez Cisco Systems.

Ces tendances font émerger de nouvelles exigences quant à la localisation et la sauvegarde des données. « Vous devez savoir où se trouvent vos données et à quel point elles sont essentielles pour votre activité, et savoir aussi à quelle vitesse elles peuvent être restaurées », souligne Rick Vanover, directeur de la stratégie produit chez Veeam Software. « Cela se traduit par une plus grande dépendance numérique dans les entreprises moyennes, car la visibilité et la résilience des sauvegardes y sont une nécessité. »

Notre **manière de concevoir nos systèmes informatiques a également changé** au cours de la décennie passée. Les anciens outils de sauvegarde n'ont pas été spécifiquement conçus pour les environnements hautement virtualisés d'aujourd'hui. Cela signifie que les sauvegardes ne peuvent pas s'adapter facilement à l'accroissement des exigences d'accessibilité et des volumes de données stockés par les entreprises.

« S'il existe encore de nombreuses applications centrées sur le matériel, la plupart des grandes entreprises utilisent davantage de serveurs virtuels pour mieux tirer parti de leurs investissements matériels », poursuit Ken Pipkins. « La sauvegarde dans les grandes entreprises est devenue un défi, parce que la manière de créer et consommer des données a changé radicalement au cours de la décennie précédente », confirme Ryan Lally, spécialiste en ventes de sécurité chez World Wide Technology.

Pourtant, la virtualisation n'est pas la seule raison du changement de conception de nos systèmes. **Aujourd'hui, la plupart des entreprises ont une empreinte en ligne** et cette présence augmente dans la mesure où davantage de logiciels partent dans le cloud pour y être utilisés à la demande. Cela accroît les exigences de temps de restauration pour remettre rapidement une sauvegarde en ligne. « Nous en sommes arrivés à des sauvegardes imprévisibles, des durées de restauration trop longues, des difficultés à respecter les exigences de conformité et une incapacité à faire évoluer la sauvegarde. Face à l'accroissement de l'accessibilité et des volumes de données stockés par ces entreprises, il faut restructurer vos solutions de sauvegarde », conseille Ken Pipkins.

Notre expansion géographique s'accompagne également d'un potentiel accru pour la cybercriminalité.

« Les entreprises ne fournissent pas suffisamment d'efforts en matière de reprise après incident et leurs besoins dépassent les simples sauvegardes », constate Rick Vanover. « Elles sont souvent bien loin d'une expérience de restauration totale et doivent renforcer leurs stratégies pour se protéger plus efficacement contre les menaces actuelles. »

Notre expansion géographique s'accompagne également d'un **potentiel accru pour la cybercriminalité**. Cela change le paysage des menaces, ce qui peut représenter un problème pour les entreprises encore enracinées dans le passé. « À l'époque, personne n'avait encore entendu parler des ransomware. Maintenant, ils font la une tous les jours », constate Ken Pipkins. Et les menaces se multiplient en provenance de l'Internet

des objets et des périphériques connectés aux réseaux de distribution d'énergie ou aux magasins. Il est beaucoup plus difficile de protéger ces zones. »

Certaines entreprises ont cédé et payé la rançon exigée. Cela peut poser problème, car elles n'ont aucune garantie de pouvoir déchiffrer leurs données sur l'ensemble des systèmes affectés ou que leur activité ne sera pas perturbée pendant des jours, voire des mois.

Autre conséquence de ces menaces croissantes : **les sauvegardes doivent s'inscrire dans une stratégie de défense globale et approfondie** portant sur de nombreuses couches de protection différentes. « Vous devez supposer que vous finirez par être victime d'un ransomware ou de tout autre attaque par un logiciel malveillant », conseille Ryan Lally.

Alors que ces circonstances montrent à quel point l'environnement informatique d'aujourd'hui est différent, certaines aspects n'ont pas beaucoup évolué depuis l'apparition des PC. « Une quantité massive de malware proviennent encore du Web et du courrier électronique. Ce sont toujours aujourd'hui les voies les plus faciles pour faire entrer les virus dans les entreprises. », déplore Ryan Lally. « Résultat : les postes de travail constituent encore la plus grande source de menaces. Et avec les tablettes et le cloud, votre sécurité comporte d'énormes points faibles. Les attaquants essaient toujours de trouver des comptes et des mots de passe d'administrateur parce que cela leur donne une flexibilité maximale dans leurs attaques. Nous constatons souvent que de nombreuses entreprises ne savent pas combien elles comptent d'administrateurs ou laissent leurs développeurs avoir un accès complet aux ressources réseau sans réellement en vérifier la nécessité. » Ce constat devrait pourtant être relégué aux années 1980.

Autre conséquence de ces menaces croissantes : les sauvegardes doivent s'inscrire dans une stratégie de défense globale et approfondie portant sur de nombreuses couches de protection différentes.

Selon Ken Pipkins, la sécurité du courrier électronique a été passée de mode pendant un certain temps, mais elle est à nouveau d'actualité. « Nous assistons à une résurgence des attaques par e-mail, en particulier en matière de spear phishing (harponnage) où la messagerie est redevenue un vecteur d'attaque au moyen de sites Web frauduleux incorporés aux messages », explique-t-il.

« Si une partie des attaques de phishing peut être contrée par la formation et la sensibilisation à la sécurité, cela ne suffit pas et les clients ont besoin de mettre en place de solides technologies pour protéger véritablement leurs utilisateurs », poursuit Ryan Lally. De nombreuses grandes entreprises utilisent des technologies telles que DMARC (Domain-based Message Authentication, Reporting and Conformance, authentification des messages par domaine, reporting et conformité) pour tenter de limiter les usurpations d'identité et les rendre plus faciles à détecter. Mais en fin de compte, vous devez durcir la surface d'attaque de votre messagerie. » Il recommande également d'employer l'authentification multifacteur, la connexion unique et l'authentification renforcée pour une meilleure protection contre les logiciels malveillants. « Vous devez comprendre les contextes d'utilisation individuels et les menaces potentielles et prendre également en considération la manière dont les utilisateurs distants accèdent à vos réseaux », conseille-t-il.

Enfin, une autre chose n'a pas beaucoup changé depuis toutes ces années : **la vérification des sauvegardes**. Les entreprises découvrent souvent des lacunes dans leurs sauvegardes seulement après avoir été frappées par des attaques et sont dans l'incapacité de restaurer leurs systèmes ou de récupérer toutes leurs données. « Si vous n'avez pas de bonnes sauvegardes, vous devez avoir honte », conclut Ryan Lally. « Une grande entreprise doit être capable de résister à une attaque par ransomware, mais j'ai vu nombre d'entre elles perdre des millions de dollars de propriété intellectuelle à cause de sauvegardes insuffisantes ou de problèmes d'exploitation après l'attaque. »