Livre blanc

Prévention des ransomware avec la Veeam Hyper-Availability Platform

À la recherche d'une solution à l'un des principaux problèmes des décideurs IT

Par Christophe Bertrand, analyste principal en protection des données
et Doug Cahill, analyste principal et directeur du groupe de cybersécurité

Août 2018

Ce livre blanc ESG a été commandé par Veeam
et est distribué sous licence ESG.

Table des matières

Synthèse

Les ransomware constituent l'une des principales préoccupations de nombreux dirigeants car leurs entreprises font face aux conséquences potentiellement désastreuses d'une attaque. Les implications commerciales des temps d'arrêt causés par des attaques de type ransomware peuvent être dévastatrices. Elles engendrent le besoin de meilleures pratiques et capacités dans l'ensemble du système informatique, en particulier en termes de protection des données. L'Hyper-Availability Platform de Veeam répond à ces préoccupations grâce à une combinaison de technologies et de solutions permettant de limiter les risques liés aux ransomware et de renforcer une restauration sécurisée.

Introduction

La couverture médiatique abondante en témoigne : les ransomware sont devenus un sujet prioritaire pour de nombreuses entreprises, car les attaques très médiatisées qui les visent ont considérablement augmenté au cours de ces deux dernières années. Selon les recherches d'ESG, près de deux tiers des entreprises interrogées en Amérique du Nord et en Europe de l'Ouest ont subi une attaque par ransomware au cours de l'année écoulée, dont 22 % font part d'attaques hebdomadaires. Ces attaques ont contribué à faire de la cybersécurité un objectif d'investissement IT et les dépenses s'accélèrent.[1]

Les ransomware ne se résument pas à un simple inconvénient technique pour l'IT. Ils représentent une activité criminelle rentable exercée par des acteurs malveillants qui n'hésitent pas à nuire à des institutions publiques et à des entreprises privées. De plus, les attaques par ransomware ne vont pas disparaître de sitôt.

Les recherches d'ESG confirment que les chefs d'entreprise et les leaders technologiques sont très inquiets.[2] Les conséquences pour leurs entreprises peuvent être lourdes, non seulement parce qu'elles affectent la confiance des employés et des consommateurs, mais également parce qu'elles détruisent potentiellement des actifs de données stratégiques qui ne peuvent pas être reconstitués facilement ou de manière économique.

Outre le risque fondamental de perte de données inacceptable pour l'activité, les conséquences directes et indirectes de l'indisponibilité des services et des systèmes peuvent affecter de manière significative une entreprise à court et à long terme.

Les attaques par ransomware s'apparentent à des « sinistres logiques ». En d'autres termes, du point de vue de la restauration, elles ne sont pas si différentes d'altérations de données ou de disques durs défaillants qui deviennent inutilisables. Cependant, la *cause* de ces désastres logiques les distingue clairement et dicte le type d'effort nécessaire pour les prévenir.

Malheureusement, dans la plupart des cas, les risques associés aux données prises en otage et les dommages qu'elles ont subis dissuadent de les utiliser, ou bien elles ne sont pas récupérées,*que la rançon soit payée ou non*.

Pour combattre cette épidémie, de meilleures pratiques et des outils sont nécessaires pour :

- prévenir ou au moins limiter les attaques ;
- protéger les données et les sauvegardes ;
- fiabiliser les restaurations.

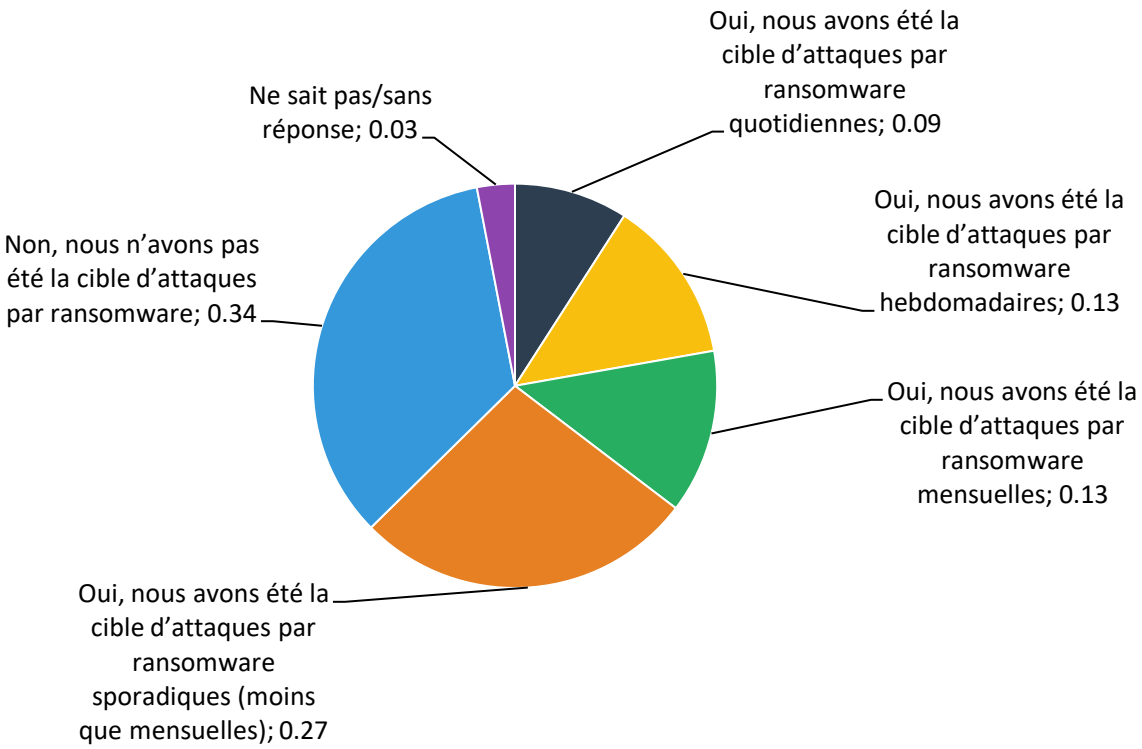
Avec de nombreuses années d'expertise en matière de datacenter et un accent particulier sur la **disponibilité** des données et des systèmes, Veeam offre des capacités étendues pour limiter les conséquences des ransomware.

[1] Source : ESG Master Survey Results, *2018 IT Spending Intentions Survey*, décembre 2017.
[2] ibid.

L'omniprésence des ransomware

La fréquence des attaques par ransomware au cours des 12 derniers mois brosse un sombre tableau de leur omniprésence et montre pourquoi leur élimination et leur atténuation représentent des impératifs stratégiques (voir figure 1).[3]

Figure 1. Fréquence des attaques par ransomware au cours des 12 derniers mois



Source : Enterprise Strategy Group

Les données d'un ancien agent du FBI montrent que les ransomware ont constitué une activité d'un milliard de dollars en 2016.[4] Alors que des résultats plus récents n'ont pas encore été publiés, il est probable que ce nombre déjà stupéfiant aura considérablement augmenté. Notamment, l'étude d'ESG montre que la vente au détail et les télécoms étaient deux fois plus susceptibles d'être victimes *au quotidien* que d'autres secteurs d'activité.[5]

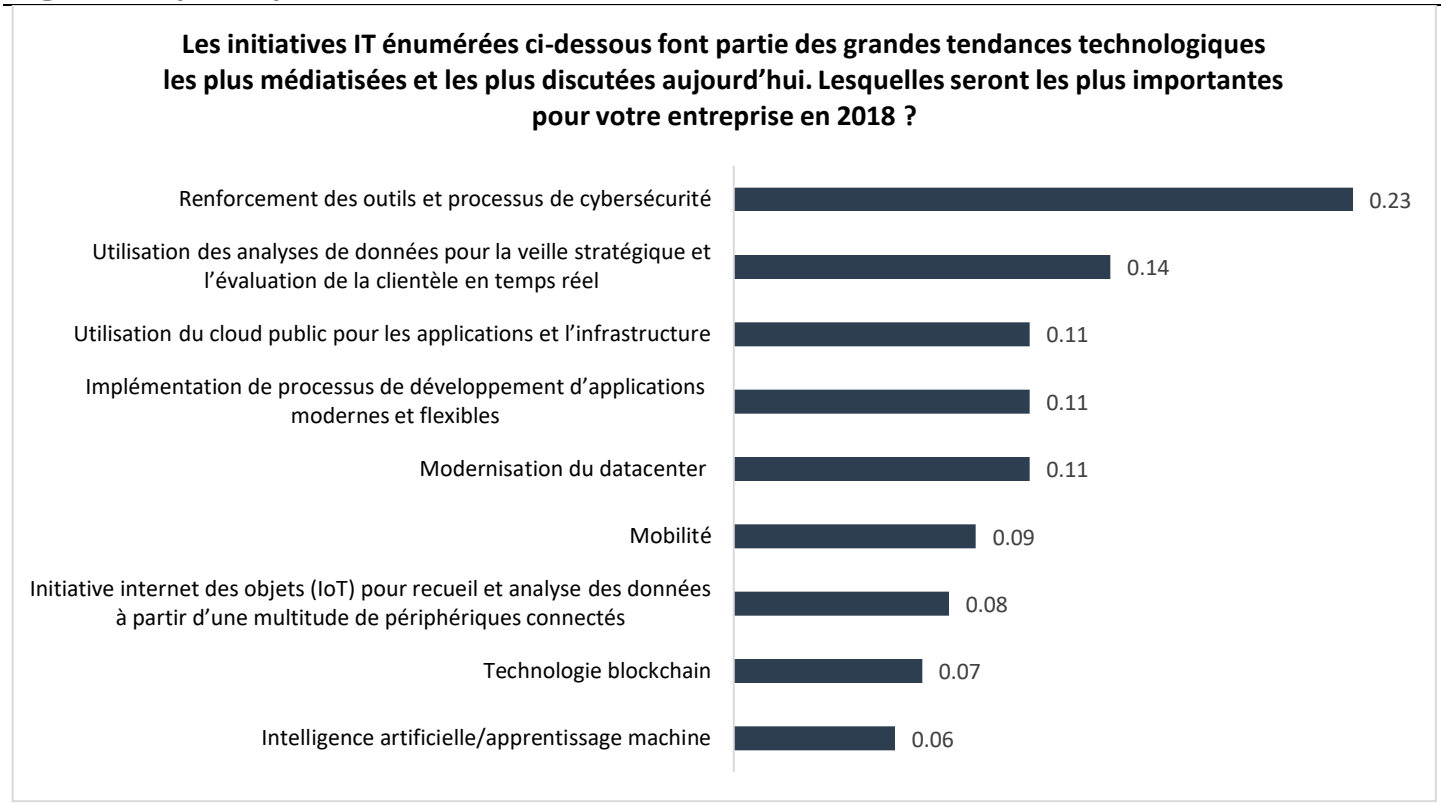
Les attaques par ransomware sont en constante évolution et tirent parti de tactiques, techniques et procédures sophistiquées. La liste s'allonge et change continuellement, ce qui complique la défense pour les entreprises. Les attaques se produisent également sur plusieurs fronts, le courrier électronique étant un vecteur d'intrusion courant. Les coupables comptent sur la complicité involontaire des utilisateurs finaux et exploitent la vulnérabilité humaine avec des pièces jointes et des liens. Le téléchargement à la volée est aussi fréquemment mis à profit.

[3] ibid.
[4] https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise
[5] Source : Brief ESG, *Ransomware: A Priority for 2018*, janvier 2018.

Les cybercriminels ont optimisé leurs processus de demande de rançon afin d'en faire de véritables transactions. On peut les considérer comme une forme perverse de service à la clientèle qui « aide » les victimes à accélérer le paiement de leur rançon. Certaines variantes apparues il y a quelques années, comme Jigsaw, incluent même une fonctionnalité de chat. De plus, divers datastores sont ciblés, allant des données non structurées de postes de travail aux enregistrements structurés de bases de données situées dans le cloud. Les datastores de sauvegarde sont également visés.

De toute évidence, les ransomware ne sont pas qu'un simple problème technologique. La cybersécurité est devenue une priorité pour les entreprises. L'étude ESG montre que le renforcement des outils et des processus de cybersécurité est la principale initiative IT en 2018 (voir figure 2). Cela n'est pas surprenant si l'on considère que 62 % des entreprises interrogées ont subi une attaque par ransomware en 2017. Notamment, 45 % des responsables IT interrogés déclarent que leur entreprise dépensera davantage en solutions de protection des données.[6]

Figure 2. La plus importante méta-tendance IT en 2018

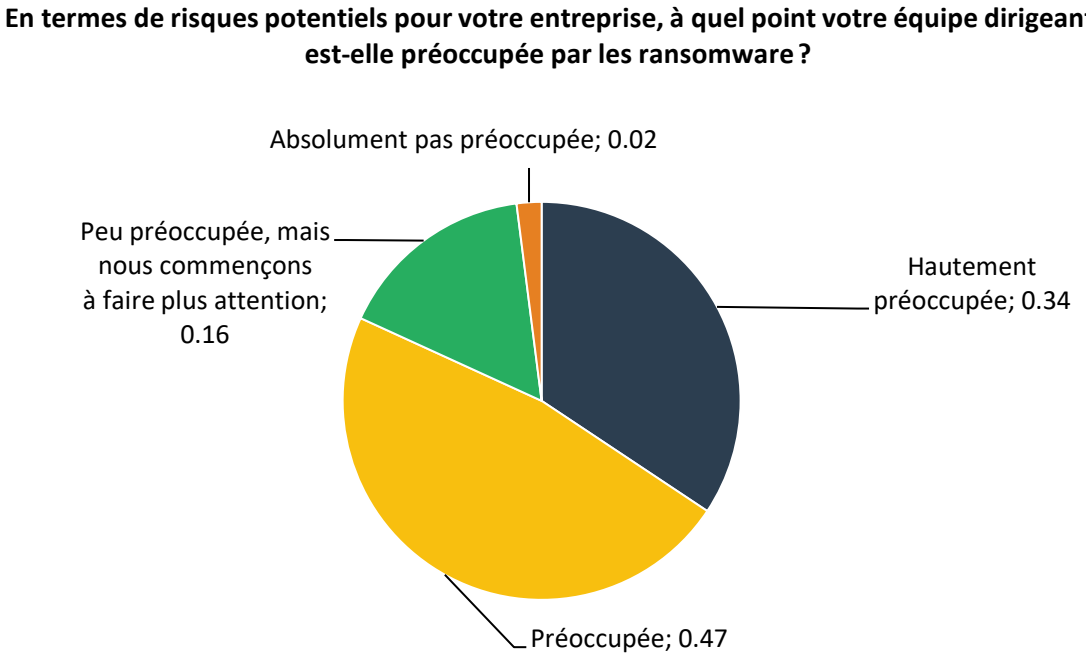


Source : Enterprise Strategy Group

Les cadres dirigeants considèrent les ransomware comme une préoccupation majeure de l'entreprise (voir figure 3).[7] Comme indiqué précédemment, leurs préoccupations sont étroitement liées à leurs priorités en matière de dépenses informatiques. La mise en œuvre de ces priorités entraînera des modifications d'infrastructure et de processus (dans de nombreux domaines) pour aligner les investissements et les ripostes aux ransomware avec la chaîne d'éradication de la cybersécurité.[8] Dans ce contexte, les choix technologiques en matière de sauvegarde et de récupération sont des éléments de protection essentiels.

[6]Source : ESG Research Report, *2018 IT Spending Intentions Survey*, février 2018.
[7] ibid.
[8] La chaîne d'éradication en cybersécurité consiste à identifier chaque étape d'une attaque pour l'arrêter, à savoir : « trouver, réparer, suivre, cibler, engager puis évaluer ».

Figure 3. Niveau de préoccupation de l'équipe dirigeante en matière de ransomware



Source : Enterprise Strategy Group

Les entreprises ont raison de considérer les mesures d'atténuation des risques relatives aux ransomware comme des priorités IT et commerciales majeures. Les ransomware provoquent des interruptions de l'activité qui affectent la disponibilité des données et des applications, avec des conséquences importantes à tous les niveaux.

Temps d'arrêt des applications et conséquences de la perte de données

Comme indiqué précédemment, l'indisponibilité des données et des systèmes déclenche une réaction en chaîne de conséquences techniques et commerciales. L'étude d'ESG a récemment identifié l'impact des temps d'arrêt et des pertes de données. Une conclusion intéressante indique que 71 % des entreprises interrogées ne pouvaient pas tolérer plus d'une heure d'indisponibilité pour leurs applications hautement prioritaires[9] et ce sont ces mêmes applications qui ont tendance à être ciblées par les ransomware.

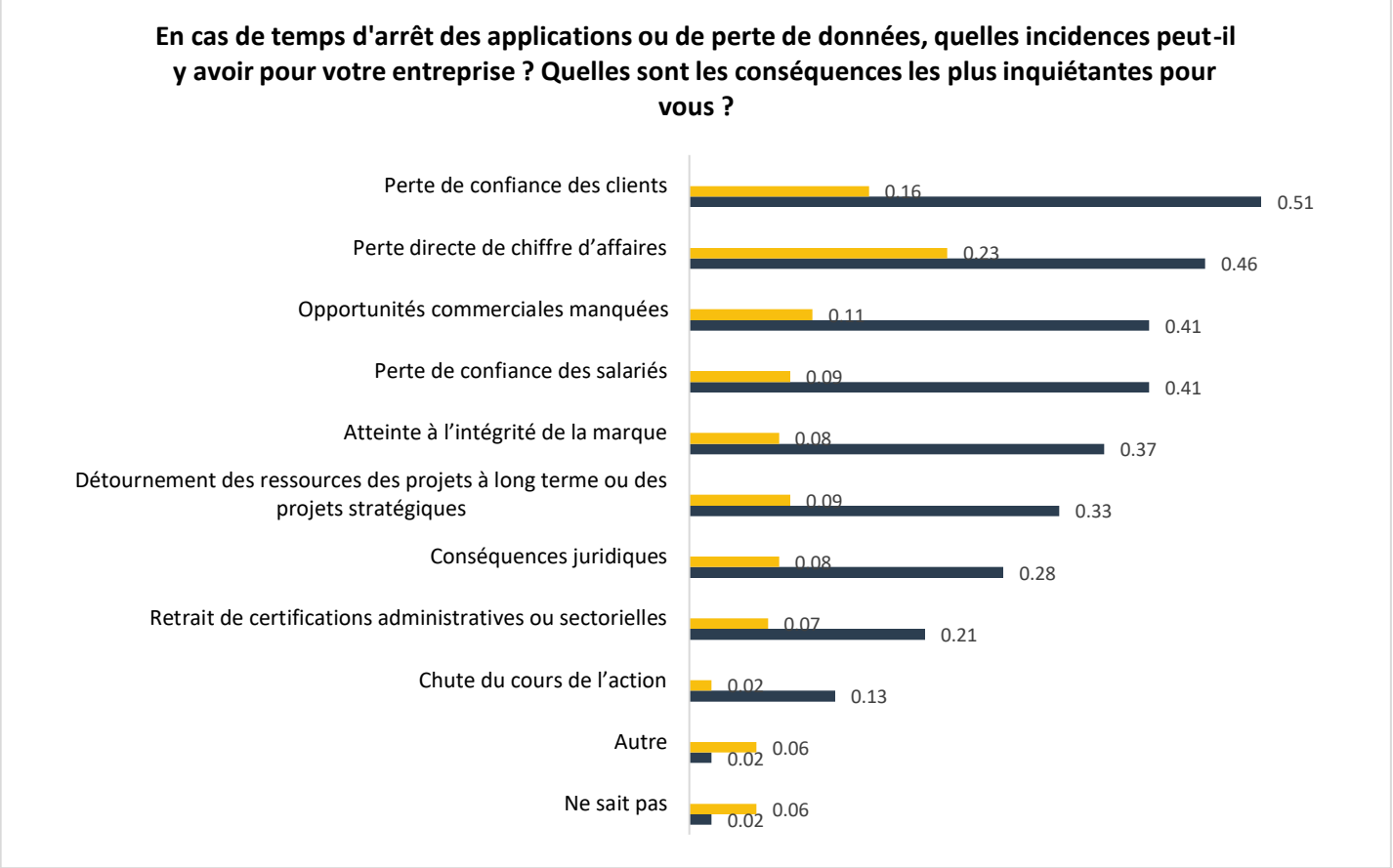
ESG indique également que 24 % des serveurs et services de production entrent dans la catégorie ne tolérant « jamais d'interruption de service », ce qui signifie que les données ou applications qu'ils exécutent doivent être disponibles en permanence ou être mises à disposition via des processus de disponibilité et de restauration tels ceux développés et vendus par Veeam.

De plus, du point de vue du délai optimal de reprise d'activité (RPO), 51 % des organisations interrogées par ESG indiquent que le délai maximum de perte de données qu'elles peuvent tolérer pour leurs applications hautement prioritaires n'est que de 15 minutes avant de subir un impact significatif sur l'activité.

[9]Source : ESG Master Survey Results, *Real-world SLAs and Availability Requirements*, mai 2018.

Les temps d'arrêt des applications et la perte de données ont des effets dévastateurs et le rétablissement d'une exploitation normale peut prendre des mois, voire des années. La perte de confiance des clients et la perte directe de chiffre d'affaires viennent en tête des conséquences graves possibles (voir figure 4).[10]

Figure 4. Effets potentiels de l'indisponibilité des applications et des pertes de données sur une entreprise



Source : Enterprise Strategy Group

Les exemples d'attaques par ransomware qui interrompent des services privés ou publics pendant des durées largement supérieures à 15 minutes sont légion. À bien des égards, les ransomware créent la catastrophe absolue. Ils sont omniprésents. Ils ont une grande force de destruction. Ils deviennent plus opérationnels. Ils ont des conséquences importantes sur l'activité. Et leur fréquence s'accélère

Bien qu'il n'existe pas de solution miracle, il est possible d'adopter des mesures IT systématiques et résilientes ainsi que de meilleures pratiques en tirant parti d'infrastructures de protection des données robustes pour limiter les dangers techniques et commerciaux des ransomware.

[10] ibid.

Les meilleures pratiques et technologies sont nécessaires

Cybersécurité

Pour repousser les attaques par ransomware, ESG recommande plusieurs meilleures pratiques et technologies de cybersécurité, de sauvegarde et de restauration. Voici un récapitulatif général des facteurs et des activités à privilégier :

- Formation des utilisateurs finaux, tests d'intrusion et simulations de phishing menées par un partenaire cybersécurité tiers constituent tous de bons points de départ. Avec un personnel moins expérimenté, la formation des utilisateurs finaux ne doit pas être oubliée.

- Les contrôles e-mail et Web sont cruciaux, étant donné le risque d'infection provenant de ces vecteurs. Pour établir une première ligne de défense de l'infrastructure, utilisez des outils permettant d'identifier et de bloquer les e-mails de spear-phishing, d'analyser les ransomware ou les programmes malveillants connus dans les courriers électroniques et d'isoler les pièces jointes aux fins d'analyse. Cet effort doit englober les applications cloud natives telles qu'Office 365. Les contrôles Web peuvent être utilisés pour analyser la réputation d'un site, bloquer les mauvaises adresses URL connues et examiner les téléchargements suspects et les codes malveillants ciblant les navigateurs. Des techniques supplémentaires telles que le sandboxing contribuent également à limiter l'expansion de malware nouveaux ou inconnus.

- Les postes de travail sont souvent le vecteur d'attaque pour injecter un ransomware et ils nécessitent un ensemble de contre-mesures robustes. Les contrôles de sécurité des systèmes d'extrémité qui ont recours à plusieurs technologies de détection pour empêcher les ransomware basés sur les fichiers ou sans fichiers ainsi que d'autres types de logiciels malveillants sont essentiels. Pour les systèmes à fonction fixe et pour ceux avec moins d'écarts de configuration et de mode d'utilisation, le contrôle des applications est très efficace. Autoriser uniquement les logiciels connus sur les postes de travail des employés réduit considérablement le risque qu'un exécutable fasse des ravages sur l'ordinateur puis se répande à travers le réseau. De plus, la surveillance comportementale avec analyse dynamique via sandboxing pour détecter les conduites suspectes (chiffrement, connexions aux lecteurs mappés, etc.) est un complément indispensable à la protection des postes de travail.

- Les contrôles du réseau ont un rôle vital à jouer dans la prévention de la propagation des ransomware. Cette initiative commence par la mise en place d'une protection sur tous les ports et protocoles et par la surveillance de tout le trafic du réseau physique ou virtuel. La supervision du réseau contre les ransomware connus (au moyen d'une combinaison de techniques telles que la correspondance de modèles et l'émulation de scripts) peut être complétée par des méthodes de détection comme l'analyse sandbox pour les ransomware nouveaux et inconnus.

- Les serveurs, en particulier les serveurs de base de données, sont également devenus la cible des attaques par ransomware. Les serveurs requièrent l'utilisation de technologies permettant d'analyser les ransomware et d'autres formes de programmes malveillants et des contrôles pour maintenir l'intégrité du système. Faire preuve de diligence pour assurer la discipline en matière de correctifs est une meilleure pratique évidente, mais elle a une incidence opérationnelle pour de nombreuses entreprises et n'empêche pas les attaques « zero-day ». Le patching virtuel via détection et prévention des intrusions sur l'hôte (HIDS/HIPS) est une efficace couche de sécurité centrée sur l'identification des codes malveillants afin que ce trafic n'atteigne jamais l'application du serveur. Le renforcement des serveurs, la surveillance de l'intégrité des fichiers (FIM) et l'analyse des applications sont également des contrôles de sécurité importants qui permettent de maintenir les états connus et approuvés des workloads.

Enfin, comme pour toute interruption informatique majeure, il faut en priorité réagir aux incidents et s'y préparer pour contrecarrer les ransomware et/ou rétablir une exploitation normale après une attaque. Les entreprises doivent tester leurs plans d'intervention en cas d'incident, y compris leur capacité à restaurer efficacement les systèmes et données de production si une compromission survient.

Sauvegarde et restauration

Au-delà des meilleures pratiques en matière de cybersécurité, la sauvegarde et la restauration sont des éléments importants pour garantir la disponibilité et ils doivent être examinés et optimisés avec soin. Les meilleures pratiques peuvent inclure les actions suivantes :

- La formation du personnel informatique, une activité aussi essentielle que la formation des utilisateurs finaux. Elle peut s'avérer encore plus critique étant donné la proximité des administrateurs informatiques et leur accès à une infrastructure sensible. Il convient d'accorder une attention particulière à la formation de l'équipe de sauvegarde et de lui offrir un enseignement régulier sur les meilleures pratiques en matière de sécurité, de mise en réseau et de stockage.

- Le respect de la règle du 3-2-1 selon laquelle trois copies des données sont sauvegardées sur deux supports différents, avec une de ces copies stockée hors site. Veeam ajoute un « 1 » supplémentaire à la règle du 3-2-1, dans laquelle une copie du support de stockage doit être conservée entièrement hors ligne, c'est-à-dire sans connexion directe à Internet, à aucun réseau informatique, ou à tout autre ordinateur.

- La gestion des contrôles d'accès, en utilisant différentes informations d'identification pour les rôles de sauvegarde et les autorisations d'accès à l'application de sauvegarde, au datastore/à la cible et au réseau. C'est une activité vitale pour « protéger le protecteur ». C'est donc une activité cruciale pour la restauration des données et des systèmes. L'utilisation d'un système de fichiers différent pour le stockage de sauvegarde peut également contribuer à limiter la propagation des ransomware.

- À la recherche d'une solution dotée de fonctionnalités d'alerte comportementale. Les alertes comportementales sont une fonctionnalité qui peut s'avérer très avantageuse dans une application de sauvegarde et de restauration, en particulier lorsqu'elle informe un administrateur d'une éventuelle activité de ransomware telle que la détection de multiples opérations de chiffrement, une utilisation intensive du CPU ou un nombre d'I/O très élevé.

La Veeam Availability Platform à la rescousse

La Veeam Hyper-Availability Platform et les composants associés du portefeuille global de Veeam offrent aux entreprises la disponibilité des données, où qu'elles se trouvent : sur site, dans le datacenter principal, dans les bureaux distants, sur des périphériques individuels ou à n'importe quel endroit dans le cloud. Elle est parfaitement adaptée à la protection contre les ransomware et met l'accent sur les datacenters et les postes de travail.

Au niveau du datacenter, Veeam permet aux organisations de restaurer les données infectées par un ransomware à un état connu comme satisfaisant au moyen de la Veeam Hyper-Availability Platform. Les utilisateurs finaux peuvent tirer parti de Veeam Availability Suite pour effectuer des opérations de restauration rapides et granulaires relatives à leurs bases de données, applications, fichiers et systèmes d'exploitation. Dans de nombreux cas, des restaurations complètes seront nécessaires pour rétablir le fonctionnement normal des systèmes affectés par le ransomware. Veeam fournit également une protection avancée des applications en ligne les plus répandues telles que Microsoft Office 365.

La suite offre des fonctionnalités de restauration de fichiers en un clic pour les snapshots de baie de stockage qui peuvent s'avérer particulièrement utiles pour la récupération rapide de fichiers critiques. Au cours de ces dernières années, Veeam a également réalisé des intégrations avec de nombreux fournisseurs de stockage afin d'accroître ses performances et ses capacités de restauration.

Ce document a déjà mentionné l'utilisation des « bacs à sable » dans le contexte de la cybersécurité. Dans le contexte de la sauvegarde et de la restauration, Veeam emploie un concept similaire pour les tests de reprise après incident. Cette approche consiste à utiliser le dernier point de restauration correct avec Veeam On-Demand Sandbox. Cette capacité est très importante dans le contexte de la gestion et de la planification de la réponse aux ransomware.

Comme indiqué, les postes de travail peuvent constituer une première ligne de défense du point de vue de la cybersécurité, car ils représentent souvent le principal vecteur des attaques par ransomware. Disposer d'un outil de sauvegarde performant pour les ordinateurs portables et les postes fixes tel que Veeam Agent *pour Linux* ou Veeam Agent *pour Microsoft Windows* est un impératif. Ces solutions fournissent une sauvegarde et une restauration en mode image pour les systèmes non virtualisés.

La grande vérité

Les ransomware continueront à sévir et deviendront une menace encore plus présente pour les entreprises du monde entier. La vaste surface d'attaque des ransomware et la créativité à la fois criminelle et technique de ses instigateurs suscitent des défis en constante évolution pour les professionnels de la cybersécurité et de la protection des données.

Les ransomware sont véritablement devenus un risque économique potentiellement dévastateur. Celui-ci doit être géré grâce à une combinaison de meilleures pratiques et d'outils couvrant un large éventail de technologies et d'activités. Même les entreprises les mieux préparées sont vulnérables aux défaillances de disponibilité des données et des systèmes causées par la cybercriminalité. Cela rend le rôle des technologies de sauvegarde et de restauration et des meilleures pratiques qui y sont associées encore plus central et plus visible.

L'optimisation de la disponibilité des données et des systèmes nécessite une planification minutieuse et un ensemble complet d'outils permettant de restaurer rapidement de précieux actifs et services avec des pertes très limitées. C'est précisément ce que réalise l'Hyper-Availability Platform de Veeam. Et elle a déjà aidé de nombreuses organisations à rétablir une exploitation normale après des attaques malveillantes.

Enterprise Strategy Group est une société de conseil stratégique et d'analyse informatique qui offre des informations sur le marché à la communauté IT mondiale.