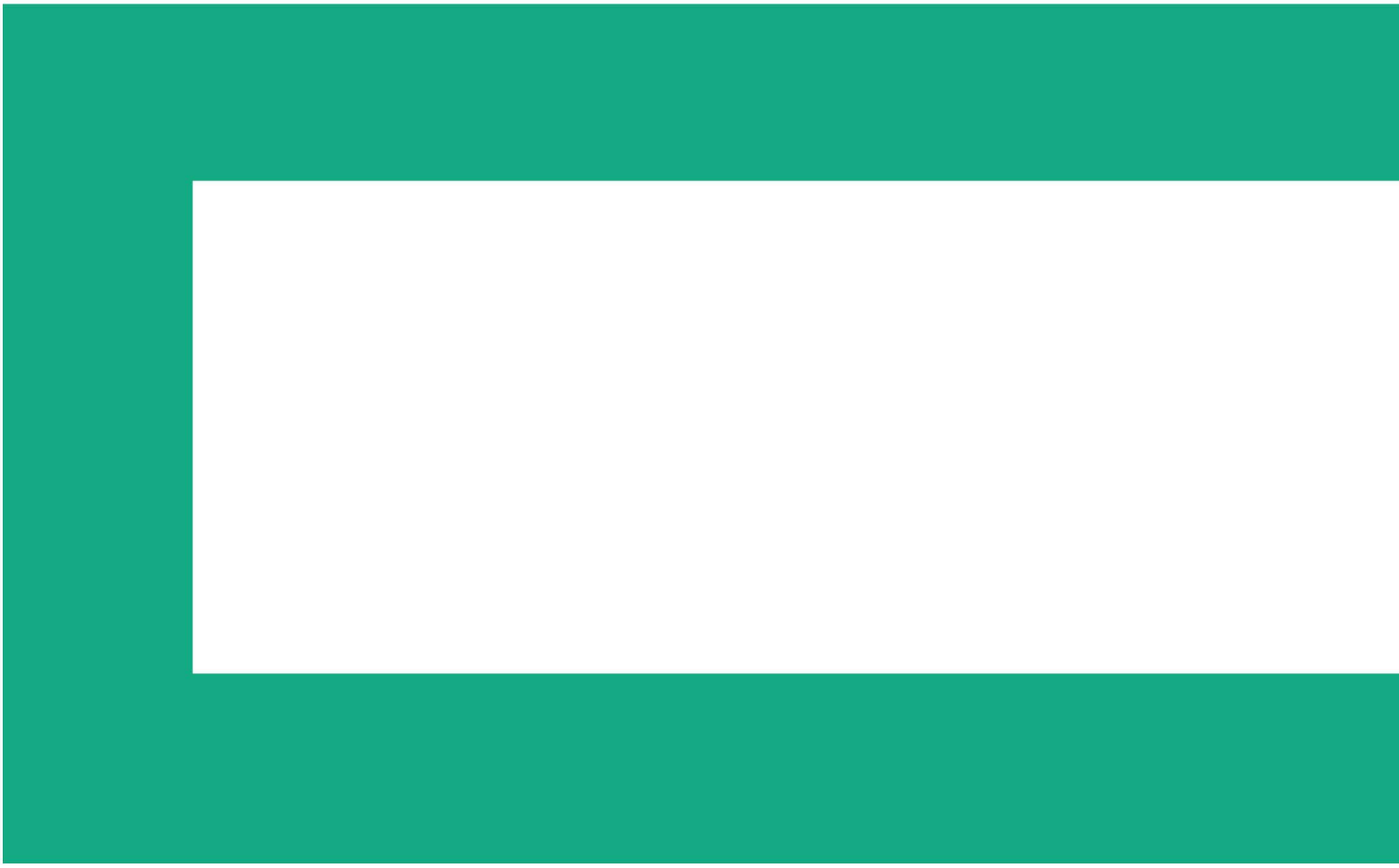
Hewlett Packard Enterprise

SEQUENCE INFORMATIQUE

infrastructure hyperconvergente HPE SimpliVity — Réduire les risques liés au ransomware



Résumé

Le ransomware est rapidement devenu l'une des cybermenaces les plus courantes et les plus dangereuses. Les dernières attaques de ransomware étaient capables d'échapper aux systèmes et pratiques de sécurité d'entreprise les plus stricts et d'envahir toute une organisation, perturbant la productivité des utilisateurs et les opérations commerciales.

Des plans de **sauvegarde et restauration** complets sont absolument essentiels pour lutter contre les menaces de ransomware sophistiquées d'aujourd'hui. En restaurant rapidement les applications infectées et leurs données au dernier état non contaminé, les organisations informatiques peuvent minimiser les incidences d'une attaque de ransomware, limiter les pertes de revenus et restreindre le désagrément subi par les clients.

Cet article étudie les évolutions récentes du ransomware, analyse ses incidences et décrit la manière dont l'infrastructure **hyperconvergente HPE SimpliVity** accélère les sauvegardes et les restaurations de données afin de contenir les risques liés au ransomware.

Le ransomware d'aujourd'hui est sophistiqué, destructeur et inévitable

Le ransomware fait partie des principales inquiétudes des organisations informatiques d'aujourd'hui. Dans le monde entier, les attaques de ransomware gagnent en diversité, en complexité et en gravité. Selon un rapport de 2016, le ransomware « est rapidement apparu comme l'une des cybermenaces les plus dangereuses pour les organisations et les consommateurs, avec des pertes mondiales se chiffrant probablement autour de centaines de millions de dollars. »[1] Le ransomware peut affecter toutes les entreprises, quels que soient leur taille et leur secteur, et provoquer des temps d'arrêt et des pertes financières.

Il y a quelques années, le ransomware était encore rudimentaire et relativement bénin. Des attaques dites de « computer locker » ou verrouillage d'ordinateur se contentaient alors de bloquer un ordinateur en désactivant les fonctions du clavier ou de la souris. (En théorie, le cybercriminel débloquait le clavier après réception du paiement de la rançon.) Dans la plupart des cas, les informaticiens pouvaient ignorer les demandes de rançon et restaurer un ordinateur infecté au dernier état de fonctionnement à l'aide d'outils courants d'élimination de malware.

Les choses ont beaucoup évolué ces dernières années. Les attaques de ransomware d'aujourd'hui sont bien plus évoluées et invasives. Les derniers programmes de ransomware sont capables de chiffrer des fichiers de données et d'empêcher les utilisateurs d'accéder à leurs propres données. Le chiffrement peut s'étendre à toute une organisation, bloquer les données dans toute une entreprise et perturber les opérations commerciales. Certaines variantes menacent même de publier des données confidentielles sur Internet si la rançon n'est pas payée.

Il est difficile de prévenir ces attaques ou d'y remédier. Elles sont toutes conçues pour éviter la détection par des applications de sécurité et utilisent des techniques comme le polymorphisme et les serveurs de commande et contrôle jetables. Après l'infection, le malware affecte également les efforts de reprise. Certains logiciels chiffrent les fichiers de sauvegarde Windows® natifs et empêchent la restauration en l'absence d'une clé de déchiffrement. D'autres suppriment la totalité des fichiers de sauvegarde, ce qui rend la reprise impossible.

[1] Symantec ISTR Special Report : Ransomware and Businesses 2016

Le ransomware devient chaque mois plus envahissant, exposant un nombre croissant d'entreprises à un risque. Les attaques de ransomware d'aujourd'hui visent non seulement les machines Windows mais aussi les systèmes Linux® et Mac OS et les appareils mobiles. Et les nouveaux programmes de « ransomware as-a-service » permettent à n'importe quel criminel doté de compétences informatiques élémentaires d'entrer dans l'activité du ransomware. L'auteur du ransomware fournit le malware à d'autres cybercriminels en échange d'un pourcentage sur la rançon versée.

Payer la rançon n'est pas une réponse

Certaines entreprises peuvent être tentées de payer les demandes de rançon afin de restaurer un fonctionnement normal aussi rapidement et facilement que possible. Après tout, le montant moyen d'une rançon est de 679 dollars.[2] Mais les institutions chargées de l'application de la loi comme le FBI encouragent vivement les organisations à ne pas payer de rançon.[3]

Selon le FBI :

- Le paiement d'une rançon ne garantit pas à l'organisation victime qu'elle retrouvera l'accès à ses données. En fait, de nombreuses entreprises ne reçoivent jamais les clés de déchiffrement après le paiement d'une rançon.
- Certaines victimes qui ont payé la rançon signalent avoir été à nouveau visées par des cyberacteurs.
- Après le paiement de la rançon initiale demandée, certaines victimes ont reçu des demandes de paiement supplémentaires pour obtenir la clé de déchiffrement promise.
- Le paiement risque d'encourager ce modèle économique criminel.

Le véritable coût d'une attaque de ransomware — temps d'arrêt du système et manque à gagner

Les attaques de ransomware peuvent faire des ravages dans l'infrastructure d'une organisation. Les temps d'arrêt prolongés des systèmes peuvent affecter la productivité des employés et la satisfaction des clients et impacter le bilan d'une entreprise.

Le coût véritable d'une infection par ransomware inclut des coûts quantifiables comme le manque à gagner mais aussi des éléments moins tangibles comme le dommage causé à la réputation d'une entreprise. Plus l'interruption est généralisée et prolongée, plus les coûts sont élevés. Selon une étude du Ponemon Institute, le coût moyen d'une interruption accidentelle du datacenter approche les 9 000 dollars par minute.[4] La même étude chiffre le coût moyen d'une cyberattaque à 740 357 dollars.

Le fait de sauvegarder et de restaurer rapidement les données est essentielle à la continuité des activités

Malheureusement, même les meilleurs systèmes et pratiques de sécurité n'offrent pas une protection complète contre les attaques de ransomware sophistiquées d'aujourd'hui. Les derniers programmes sont spécifiquement conçus pour échapper à la détection basée sur la signature. Il est absolument essentiel de disposer d'un plan de sauvegarde et restauration des données complet pour la restauration des opérations en cas d'infection.

La meilleure manière de minimiser l'impact d'une attaque de ransomware est de restaurer les services aussi rapidement que possible, avec des pertes de données minimales. Une solution de sauvegarde et restauration hors ligne rapide et efficace est vitale.

[2] Internet Security Threat Report, Volume 21, Symantec, avril 2016

[3] Ransomware Prevention and Response for CEOs, Federal Bureau of Investigation, 2016

[4] Cost of Data Center Outages, Data Center Performance Benchmark Series, Ponemon Institute, janvier 2016

HPE SimpliVity accélère la récupération des données et réduit les risques liés au ransomware

Une entreprise peut prendre certaines mesures pour minimiser les pertes de données et les temps d'arrêt causés par une cyberattaque. Une première étape importante consiste à définir des objectifs de temps de reprise (RTO) et des objectifs de point de reprise (RPO). Les administrateurs informatiques doivent déterminer pendant combien de temps leur entreprise peut se permettre d'être arrêtée pendant l'exécution de la restauration, et combien d'heures de données stratégiques pour l'entreprise elle peut se permettre de perdre.

La stratégie de protection des données doit alors être centrée sur une solution capable de remettre l'infrastructure en état dans le délai prescrit. Une solution hyperconvergente HPE SimpliVity consolide l'infrastructure informatique et simplifie à la fois le plan de protection des données et le processus de reprise, en particulier pour les entreprises devant support plusieurs bureaux distants. Des solutions offrant des fonctions intégrées, comme une protection des données intégrée, contribuent à soulager la charge supportée par les bureaux distants et améliorent la protection dans toute l'entreprise.

L'infrastructure hyperconvergente HPE SimpliVity fournit un composant 2U modulaire, évolutif de ressources x86, qui offre toutes les fonctionnalités d'une infrastructure IT traditionnelle – y compris des capacités d'hyperviseur, de calcul, de stockage et de protection des données – dans un device unique, avec une interface d'administration unifiée, centrée sur les machines virtuelles. La fonctionnalité de protection des données intégrée HPE SimpliVity accélère les opérations de sauvegarde et de restauration des données et aide les organisations IT à se remettre rapidement des attaques de ransomware. La solution réduit les coûts et la complexité de l'équipement et des opérations en éliminant ou en allégeant considérablement le recours aux outils dédiés de sauvegarde et restauration de données, aux solutions de déduplication et aux appliances d'optimisation WAN.

L'efficacité des données HPE SimpliVity permet de réaliser des sauvegardes plus fréquentes pour une protection des données quasi continue, pour des périodes de conservation plus longues et une reprise plus rapide. HPE SimpliVity permet de sauvegarder et de restaurer des machines virtuelles d'un téraoctet en moins d'une minute, même via des connexion WAN à bande passante limitée. En cas d'infection par un malware, une machine virtuelle et toutes ses données peuvent être restaurées rapidement et facilement, ce qui minimise le temps d'arrêt du système, les interruptions d'activité et la perte de revenus.

Conclusion

Les programmes de ransomware contemporains peuvent échapper aux systèmes de sécurité des entreprises, paralyser l'infrastructure IT et perturber les applications stratégiques. Une solution de sauvegarde et restauration hors ligne complète est essentielle pour répondre aux infections par ransomware et limiter l'exposition.
L'infrastructure hyperconvergente HPE SimpliVity avec protection des données intégrée a démontré qu'elle accélérait les fonctions de sauvegarde et restauration et réduisait les risques liés au ransomware. Avec HPE SimpliVity, les organisations peuvent restaurer rapidement et facilement leurs applications stratégiques, ce qui réduit la perturbation des activités et la perte de revenus.

Pour en savoir plus, consultez les sites
hpe.com/info/simplivity

a00038991FRE, janvier 2018

Conclusion

Les programmes de ransomware contemporains peuvent échapper aux systèmes de sécurité des entreprises, paralyser l'infrastructure IT et perturber les applications stratégiques. Une solution de sauvegarde et restauration hors ligne complète est essentielle pour répondre aux infections par ransomware et limiter l'exposition.
L'infrastructure hyperconvergente HPE SimpliVity avec protection des données intégrée a démontré qu'elle accélérait les fonctions de sauvegarde et restauration et réduisait les risques liés au ransomware. Avec HPE SimpliVity, les organisations peuvent restaurer rapidement et facilement leurs applications stratégiques, ce qui réduit la perturbation des activités et la perte de revenus.

Pour en savoir plus, consultez les sites
hpe.com/info/simplivity

a00038991FRE, janvier 2018