Dell EMC MozyPro® : Empêcher une catastrophe ransomware

L'avantage Mozy

Simple

Gérez de manière transparente la sauvegarde, la synchronization et l'accès mobile dans les environnements de serveurs et multi-utilisateurs à partir d'une console Web unique.

Sécurisé

Vos données sont protégées grâce à un chiffrement d'entreprise, à des datacenters très avancés et à Dell EMC, une entreprise conçue pour durer.

Économique

Réalisez des économies : aucun matériel à acheter et frais supplémentaires minimes.

Contactez Mozy

mozyemeasales@dell.com
0800 91 71 34
www.mozy.fr/pro

Introduction

Ransomware est une menace qui coûte des millions de dollars par an aux entreprises et qui devient malheureusement de plus en plus sophistiqué. Grâce à diverses méthodes d'attaque, y compris des e-mails ciblés et des sites Web infectés, les criminels peuvent injecter des maliciels dans votre réseau, retenant ensuite vos données et d'autres systèmes en otage jusqu'à ce vous payiez une rançon. Il est très difficile de bloquer toutes les attaques de ransomware, alors de nombreux experts, dont le FBI, conseillent aux organisations d'avoir plusieurs niveaux de protection avec des sauvegardes protégées afin de permettre une récupération rapide. Les organisations qui suivent ces conseils se concentrent souvent sur les systèmes internes clés et oublient leurs points d'extrémité — les ordinateurs portables et de bureau — et les applications SaaS, qui contiennent des données critiques au fonctionnement des employés. Heureusement, Mozy et Spanning de Dell peuvent vous aider à mieux protéger vos données avec des solutions de sauvegarde faciles à déployer, efficaces et basées dans le cloud.

L'essor du ransomware

Le premier ransomware connu, Trojan.Gpcoder, est apparu en 2005 et affectait les systèmes d'exploitation Windows. Plus de 10 ans plus tard, il n'y a aucun doute que le ransomware est en plein essor. En fait, la nouvelle croissance du ransomware a augmenté de 58 pour cent durant le deuxième trimestre de 2015, d'après un Rapport sur le paysage des menaces récent de McAfee.[1] Il n'existe aucune raison impérieuse de croire que la menace présentée par ce type de maliciel ne continuera pas à augmenter considérablement. La raison est simple : « Le ransomware est facile à développer, simple à exécuter et réussit très bien à convaincre les victimes de regagner l'accès à leurs précieux fichiers ou systèmes. »[2]

Une analyse récente de Recorded Future a noté des augmentations considérables des infections ransomware en Europe par rapport à il y a un an.[3] Bien que le ransomware ne soit pas limité par les frontières géographiques, les six pays les plus affectés par ce type de maliciel sont les États-Unis, le Japon, le Royaume-Uni, l'Italie, l'Allemagne et la Russie.[4] Considérez l'attaque ransomware suivante qui s'est produite plus tôt dans l'année.

Des cyberterroristes ont pris en otage le système informatique d'un grand centre médical américain, empêchant ainsi l'accès aux données de l'hôpital en les cryptant. À l'origine, les pirates ont demandé 3.6 millions de dollars en échange de la libération des données. Bien que les attaquants ont par la suite réduit leurs demandes à 40

bitcoins (une valeur de 17.000 $ US) en échange d'une clé de décryptage, ils avaient mis au point la réalité suivante : les données des patients et les dossiers médicaux ne sont pas à l'abri des pirates. Après tout, si les informations de cet hôpital de Los Angeles ont été prises en otage, pourquoi pas celles d'un autre hôpital ? Justement, c'est la réalité : tout type d'organisation, dont les organisations médicales, gouvernementales, à but éducatif, industrielles, etc. peuvent faire l'objet d'un complot d'extorsion ransomware.

Qu'est-ce que le ransomware et comment se propage-t-il ?

Le ransomware n'est pas simplement une autre forme de cyber-attaque ; il peut rapidement se propager parmi les dossiers partagés, affectant tant les individus au sein de l'organisation infectée que ceux en dehors de celle-ci. Le ransomware verrouille l'ordinateur (ransomware de blocage) ou crypte les fichiers de l'utilisateur (ransomware crypto), puis exige une somme d'argent de l'utilisateur — normalement un paiement numérique tel que Bitcoin, comme dans le cas du centre médical de Los Angeles — en échange d'une clé de décryptage qui déverrouille l'ordinateur ou les fichiers.

Le ransomware obtient un accès au système informatique au moyen du lien le plus faible d'un réseau, normalement l'e-mail ou un site de réseau social d'un utilisateur. Une fois qu'un utilisateur clique sur un lien malveillant ou ouvre une pièce jointe infectée, le maliciel se propage dans le système. Une fois ouverts, les faux fichiers PDF, les avis FedEx et UPS fabriqués et la correspondance frauduleuse des institutions financières qui sont infectés par un maliciel peuvent rapidement contourner la sécurité du réseau d'une organisation et se propager au-delà du système local au moyen de pilotes de réseau et d'autres points d'extrémités liés aux outils de synchronisation et de partage de fichiers tels que Microsoft OneDrive, Google Drive et Dropbox.

D'après l'équipe US-CERT (United States Computer Emergency Readiness Team), les cybercriminels qui utilisent le ransomware sont tellement efficaces parce qu'ils inspirent la peur et la panique chez leurs victimes, en partie en affichant des messages intimidants tels que « Votre ordinateur a été utilisé pour visiter des sites Web au contenu illégal. Pour déverrouiller votre ordinateur, vous devez payer une amende de 100 $. »[5] Mais le ransomware a également été adopté par de nombreux cybercriminels pour d'autres raisons : sa facilité de création et de déploiement.

L'idée du ransomware est simple : si vous ne payez pas la rançon, vous perdez l'accès à votre ordinateur et aux données qui s'y trouvent. Vous perdez également l'accès des autres individus avec lesquels vous avez partagé des documents et données, ce qui aggrave considérablement l'impact. Malheureusement, les victimes qui paient la rançon risquent tout de même de ne pas récupérer leurs fichiers. La dure réalité est que l'attaquant peut ne pas fournir les clés de cryptage. En fait, une récente enquête a constaté que parmi les victimes de ransomware qui avaient payé la rançon, seulement 71 pour cent ont pu récupérer leurs fichiers.[6]

La réalité du ransomware

Les résultats d'une enquête menée en 2015 par Infosecurity Europe publiée par ESET a constaté que 84 pour cent des personnes interrogées estimaient que leurs entreprises seraient gravement endommagées en cas d'infection par ransomware. Presqu'un tiers d'entre eux (31 pour cent) ont avoué qu'ils seraient forcés de payer les fraudeurs afin de récupérer leurs données décryptées.[7]

Les entreprises comprennent qu'il est très difficile de se protéger contre toutes les menaces, mais le ransomware est particulièrement difficile. Par exemple, «CryptoWall, le leader actuel en matière de ransomware, est hautement sophistiqué et utilise une méthode de cryptage inviolable. Si vous n'avez aucune sauvegarde actuelle, vous êtes cuits... » d'après Stu Sjouwerman, auteur et expert en matière de logiciels anti-espion.[8]

Le ransomware crypto, tel que CryptoWall, représente la majorité de tout le ransomware, d'après le dernier Internet Security Threat Report (Rapport sur les menaces à la sécurité sur Internet). « Jamais auparavant dans l'histoire de l'humanité les individus dans le monde entier n'ont fait l'objet d'extorsion à l'échelle qu'ils le sont aujourd'hui. »[9] Le nombre de types de ransomware crypto s'élevait à 362.000 en 2015 (une hausse de 35 pour cent par rapport à l'année précédente) et atteignait une moyenne de 992 par jour. [10]

Bien que vous et vos données peuvent ne pas devenir victimes de CryptoWall, des millions de nouvelles versions de maliciels sont ajoutées chaque année.[11] 431 millions de versions ont été ajoutées en 2015, une hausse de 36 pour cent par rapport à l'année précédente. Une défense efficace contre le ransomware exige non seulement la détection et la prévention des menaces, mais également une stratégie de sauvegarde et de restauration. Sinon, vous risquez de faire face à des coûts significatifs. Tenez en compte que selon des études récentes, 36 pour cent des participants d'organisations publiques et privées interrogées ont subi des interruptions de systèmes non prévues et/ou des pertes de données en raison d'une violation de la sécurité interne ou externe. Le coût moyen estimé pour chacune de ces organisations ayant subi des interruptions de système au cours des 12 derniers mois est de 555.000 $ US. En outre, le

coût estimé pour chaque organisation ayant subi des pertes de données au cours des 12 derniers mois est de 914.000 $ US. Il est clair que vos données doivent être protégées — et vous devez être confiant dans vos préparations en matière de protection.[12]

Que faire ?

Les données essentielles aux opérations quotidiennes d'une organisation ou qui sont sujettes à la conformité réglementaire doivent toujours être protégées. Les pirates ne se préoccupent pas de savoir à qui appartiennent les informations ; ils feront de leur mieux pour exploiter toute faiblesse de l'infrastructure informatique afin de voler, endommager ou tenir en otage les données d'une organisation. Comme la plupart des criminels, les cybercriminels sont des opportunistes qui recherchent des cibles faciles. Représentez-vous une cible facile ? D'abord, considérez les questions suivantes :

- Vos employés sont-ils conscients des risques que posent les e-mails non sollicités ?
- Vos pare-feu et filtres de mails sont-ils tout le temps à jour ?Utilisez-vous des logiciels antivirus expirés ?
- Synchronisez vous des données entre des points d'extrémité et des systèmes de partage de fichiers synchronisés basés dans le cloud ?

Il est important de noter que les solutions de sauvegarde courantes telles qu'un lecteur USB ou un périphérique de stockage lié à un réseau (NAS) ne sont pas des méthodes fiables de sauvegarder et protéger vos données. Le ransomware se propage normalement parmi l'intégralité du système de fichiers d'une organisation, y compris un disque lié ou un partage de réseau, cryptant à la fois les données de production et les données de sauvegarde.

Une sauvegarde représente la forme de protection la plus fiable dont peuvent profiter les organisations pour protéger leurs données. Plus votre sauvegarde prend en charge les restaurations simples et rapides à l'état existant avant l'infection, moins vous risquez de subir un échec énorme en matière de continuité des opérations. Lorsque vous recherchez une solution de sauvegarde, quels facteurs devez-vous évaluer afin d'assurer que vos données seront protégées ? Tenez en compte les points suivants :

- La sauvegarde est-elle hors site (éloignée de votre site principal) ?
- Pouvez-vous vérifier que les sauvegardes s'effectuent ?
- Pouvez-vous vérifier que les données peuvent être restaurées à leur état d'origine ?
- Dans quel délai pouvez-vous restaurer des données qui ont été prises en otage ?

Le fait d'avoir un plan de sauvegarde et de restauration viable ne constitue pas seulement une bonne pratique opérationnelle, il s'agit également souvent d'une exigence légale ou réglementaire, en fonction de l'industrie ou du type de votre organisation :

- HIPAA exige que les organisations de soins de santé aient un plan de sauvegarde de données et de restauration après sinistre viable en place et testé régulièrement pour assurer la protection électronique des données de santé.[13]
- Deux services d'application financiers et bancaires, l'OCIE et le FFIEC, ont fait de la cybersécurité — dont la capacité de restauration après sinistre — un élément clé de leurs priorités en matière d'application et d'audits.[14]
- Le SEC a rappelé aux entreprises publiques le besoin qui leur incombe d'avoir des cybercontrôles appropriés, dont des fonctions de sauvegarde et de restauration, et leur responsabilité de divulguer tout risque matériel lié à la cybersécurité. Dans le monde actuel, l'incapacité de se remettre d'une menace de plus en plus courante telle que le ransomware pourrait certainement représenter un risque à divulguer.[15]

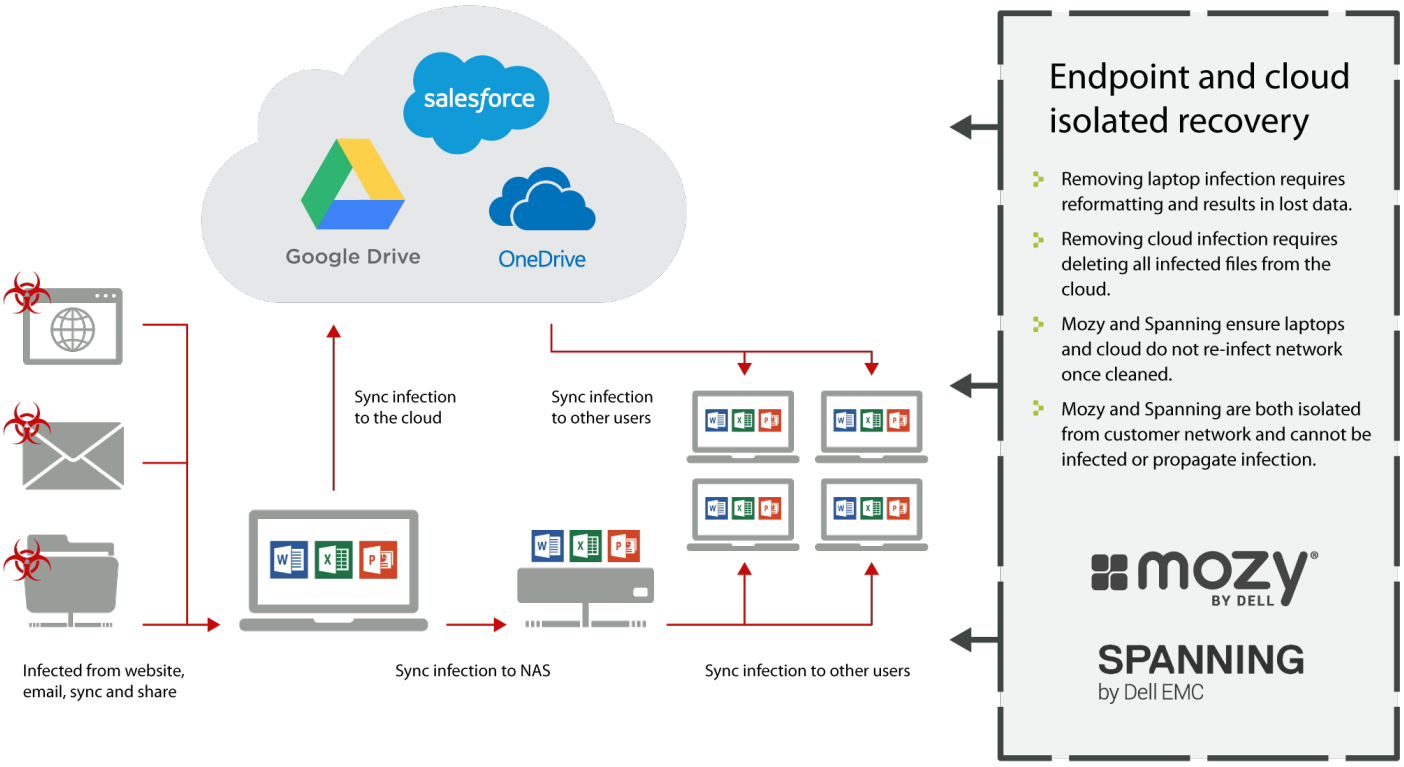
En cas de défaillance matérielle, vol, attaque de virus (y compris un complot d'extorsion ransomware), suppression accidentelle ou catastrophe naturelle ou provoquée par l'homme, si vous avez les bonnes solutions de sauvegarde et de restauration en place, vous pouvez assurer que vos données seront disponibles et seront restaurées à leur état d'origine, et que votre organisation se conforme à la réglementation en vigueur.

Sauvegarder vos données avec Dell

Vous pouvez empêcher une perte de données par ransomware en sauvegardant vos données valables à l'aide de solutions de protection de données de Dell EMC.

Tout commence par les points d'extrémité

La restauration de serveurs ne garantit pas que vous avez éliminé l'infection de votre réseau, car celle-ci est sans doute provenue à un point d'extrémité , comme l'illustre le graphique suivant. Les données sauvegardées avec Mozy et Spanning — tous deux de Dell — sont isolées du réseau client et ne peuvent pas être infectées ou propager une infection.



Protection de données aux points d'extrémité de Mozy de Dell

La solution de sauvegarde dans le cloud Mozy de Dell assure que les fichiers importants de vos points d'extrémité et les données de votre serveur ne peuvent pas être compromis par le ransomware. Grâce à sa technologie back-end, Mozy empêche toute exécution de code au sein des fichiers qui ont été sauvegardés. Mais une simple sauvegarde n'est pas suffisante en elle-même pour assurer que vos fichiers sont protégés contre le ransomware.

Lorsqu'une infection par maliciel est impliquée, la restauration d'un point d'extrémité ou serveur depuis une sauvegarde fonctionne mieux lorsque vous pouvez aisément sélectionner un point dans le temps à partir duquel effectuer une restauration. Par défaut, Mozy conserve les versions de fichiers pendant un maximum d'un an. Si vous avez identifié le point d'infection (utilisateur et fichier) et le moment auquel le maliciel s'est présenté dans l'ordinateur, Mozy peut restaurer tous les fichiers d'un utilisateur précis depuis le moment juste avant l'introduction du maliciel. Par exemple, si le maliciel s'est présenté le 2 juin, vous pouvez restaurer les fichiers de la sauvegarde du 1er juin.

Protection de données Saas de Spanning de Dell EMC

Les plateformes de productivité au bureau SaaS telles que Google Apps ou Microsoft Office 365 sont également susceptibles aux attaques de maliciels, et Google et Microsoft peuvent ne pas pouvoir restaurer rapidement vos fichiers à l'état existant avant l'infection. Les appareils des points d'extrémité infectés peuvent se synchroniser avec ces plateformes, et dans certains cas le maliciel peut automatiquement se propager parmi les disques et dossiers partagés, cryptant les fichiers partagés au sein et même en dehors de votre organisation.

La solution de sauvegarde Spanning protège entièrement les données stockées et générées dans Google Apps et Office 365 et vous permet de restaurer rapidement des données depuis un point dans le temps antérieur, avant le cryptage des fichiers par le ransomware.

Le fait de sauvegarder et protéger les données critiques de votre organisation avec les solutions de sauvegarde Mozy et Spanning

vous offre une tranquilité d'esprit, sachant que vous pourrez rapidement et aisément restaurer vos données exactement à l'état dans lequel elles étaient à n'importe quel point dans le temps en cas de l'occurrence d'une perte de données. De cette façon, vos donnés sont protégées, sécurisées et disponibles à tout moment. Ces solutions assurent votre capacité à réagir et à vous remettre d'une attaque, puis à restaurer rapidement vos données à leur état d'origine pour la continuité des opérations et afin de satisfaire les objectifs de délai de restauration et de point de restauration (RTO et RPO).

Conclusion

D'après ESET Ireland, le ransomware devient de plus en plus agressif avec de nouvelles capacités et des vagues continues de variantes.[16] Bien que la prévention et la détection soient critiques, une sauvegarde mise à jour régulièrement qui permet une restauration rapide et précise représente la dernière ligne de défense. « ...L'utilisation de fichiers de sauvegarde est un moyen efficace de minimiser l'impact du ransomware et... la mise en œuvre de pratiques d'excellence en matière de sécurité informatique est le moyen le plus efficace d'empêcher les infections ransomware. Les individus ou entreprises qui sauvegardent régulièrement leurs fichiers sur un serveur ou périphérique externe peuvent effacer leur disque dur pour éliminer le ransomware et restaurer leurs fichiers depuis une sauvegarde. Si tous les individus et entreprises sauvegardaient leurs fichiers, le ransomware ne serait pas une activité rentable pour les cybercriminels. »[17]

Les organisations dépendent plus que jamais sur les données numériques. Ainsi, toutes les organisations — des plus petites sociétés aux grandes entreprises — doivent prendre les mesures nécessaires pour assurer la sauvegarde sécurisée et la restauration rapide de leurs données à leur état d'origine.

Pour en savoir plus sur la prévention d'une catastrophe ransomware à l'aide d'une protection de données des points d'extrémité, visitez http://mozy.fr/protection/ransomware. Pour découvrir comment protéger vos données SaaS, visitez www.spanning.com.

[1] McAfee Labs Threat Report, page 33, Intel Security Group, August 2015.
[2] Ransomware a Favorite of Cybercriminals, Matthew Rosenquist, McAfee Blog Central; September 1, 2015.
[3] Locking Up Europe With Ransomware: Origination, Targeting, and Payment, Recorded Future, Inc., 2016.
[4] The evolution of ransomware, Version 1, page 5; Kevin Savage, Peter Coogan, Hon Lau; Symantec; August 6, 2015.
[5] Ransomware and Recent Variants, United States Computer Emergency Readiness Team; March 31, 2016.
[6] Crypto-Ransomware: Survey of IT Experts, page 16, Jeffrey Henning, Researchscape International; February 4, 2016.
[7] UK Companies Commonly Held Hostage by Hackers, Urban Schrott, ESET Ireland; June 29, 2015.
[8] Ransomware victims: Just pay up, grin, and bear it, says the FBI, The Register; October 27, 2015.
[9] Internet Security Threat Report, Volume 21, page 58, Symantec, April 2016.
[10] Ibid., page 8.
[11] Ibid.
[12] EMC Global Data Protection Index, independent research by Vanson Bourne, March–April 2016.
[13] HIPAA Security Rule, 45 CFR 164.308(7).
[14] National Exam Program Risk Alert, Volume IV, Issue 8; September 15, 2016.
[15] Emerging SEC guidance and enforcement regarding data privacy and breach disclosures, Joseph D. Masterson, Inside Counsel; June 25, 2015; and Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks, Paul Weiss; September 30, 2015.
[16] Jigsaw and how ransomware is becoming more aggressive with new capabilities, Urban Schrott, ESET Ireland; May 4, 2016.
[17] U.S. Department of Justice, Federal Bureau of Investigation, Letter to Senator Ron Wyden, February 8, 2016.

05/17, Livre Blanc, H16432-FR