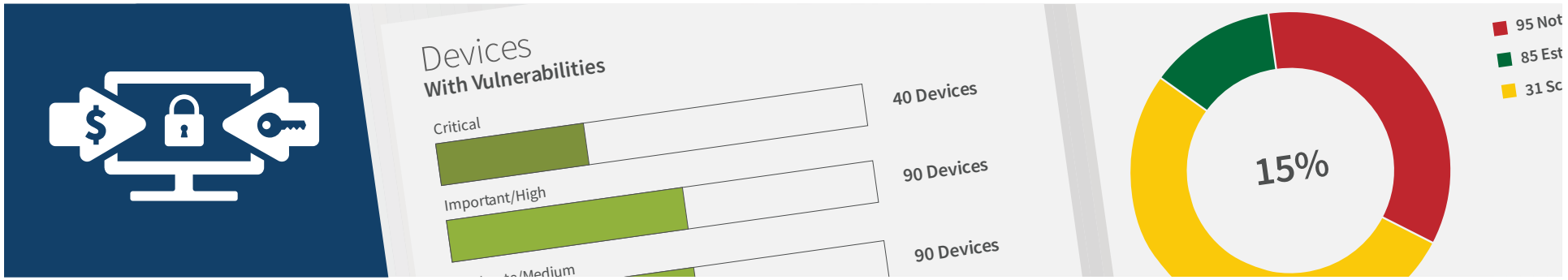
ivanti

9 Étapes pour vous protéger des Ransomwares



Livre Blanc

Table des matières

Introduction

« Contentez-vous de payer la rançon. » C'est ce qu'a déclaré un représentant officiel du FBI lors du Sommet 2015 de la cyber sécurité à Boston.[1] Plus récemment toutefois, le FBI a publié un document officiel qui avertit à propos des ransomwares et établit la liste des meilleures pratiques pour les combattre. D'ailleurs, ce nouveau document dit explicitement : « Le FBI vous déconseille de verser la rançon au criminel. »

Nous savons désormais que la plupart des ransomwares se propagent par le biais de l'hameçonnage ou des e-mails indésirables. Récemment, des utilisateurs de la Chambre des représentants des États-Unis ont été victimes d'une campagne de ransomware conçue, d'après nos informations, pour inciter les utilisateurs à ouvrir une pièce jointe dans un e-mail envoyé à leur compte Yahoo Mail. [2]

Il est toujours très utile de former et de prévenir les utilisateurs finaux, mais il est important de comprendre que les « méchants » sont des professionnels. Ils utilisent un grand nombre d'outils professionnels de marketing et de piratage psychologique pour mieux tromper les utilisateurs, et les amener à ouvrir des e-mails et pièces jointes frauduleux. Par conséquent, il faut partir du principe que même les utilisateurs les mieux formés et les mieux avertis peuvent être trompés. En fait, le dernier rapport Verizon sur les fuites de données montre que 23 % des destinataires ouvrent les messages d'hameçonnage et que 11 % cliquent sur les pièces jointes frauduleuses. [3] Les paris sont contre vous.

Ce livre blanc Ivanti passe en revue les recommandations du FBI et précise les 9 étapes à suivre pour les mettre en œuvre.

Prévention

Il ne sert à rien de mettre en place un modèle « détection et réaction » pour les ransomwares, parce que, dès que le ransomware s'exécute, il est déjà trop tard. C'est pourquoi la prévention est essentielle pour combattre ce type de malware. Le FBI vous suggère de mettre en place les 9 étapes ou méthodes de prévention ci-après, détaillées dans les pages qui suivent :

1. Application de correctifs aux systèmes d'exploitation et applications critiques
2. Vérification de la mise à jour du logiciel antivirus et de la planification d'analyses régulières
3. Application d'une gestion des comptes avec privilèges
4. Protection des fichiers des lecteurs partagés grâce au contrôle d'accès
5. Définition, implémentation et application de règles de logiciel
6. Désactivation des macros dans les fichiers Microsoft Office
7. Création de listes blanches (whitelist) d'applications
8. Restriction des utilisateurs à des environnements virtualisés ou en conteneurs
9. Sauvegarde fréquente des fichiers critiques

1 Application de correctifs aux systèmes d'exploitation et applications critiques

Pour la plupart des entreprises, l'application des correctifs devrait être la première ou deuxième ligne de défense contre les attaques. Cela s'applique également aux ransomwares.

LES CORRECTIFS DOIVENT CONSTITUER LA PREMIÈRE LIGNE DE DÉFENSE.

NE DEVENEZ PAS L'UNE DES VICTIMES DES RANSOMWARES

DÉJÀ DÉCOUVERTS

Il y a un mois, le ransomware Locky and Cerber a exploité une faille d'Adobe Flash pour se propager et attaquer des postes de travail. [4] Vous pouvez prévenir un grand nombre d'attaques de ce type en vous assurant que le système d'exploitation et les applications tierces requises sont à jour sur chaque système client. Vous devez également faire un effort particulier pour garantir que tous les correctifs et mises à jour critiques des applications comme Adobe Flash, Java, les navigateurs Web et Microsoft Office sont bien à jour. Vous devez en outre définir la priorité des déploiements de correctifs et de mises à jour en fonction des besoins et des stratégies de l'entreprise, et exécuter ces déploiements de façon à ne pas perturber les opérations des utilisateurs ou de l'entreprise.

De nombreuses entreprises craignent que l'application exhaustive et cohérente de correctifs, au bon moment, soit trop complexe à réaliser et à maintenir, ou qu'elle endommage des applications métier critiques. Cependant, l'utilisation des outils de gestion des correctifs les plus récents pour trouver les correctifs manquants et les déployer sur les postes de travail et les serveurs est en réalité une opération assez simple, même dans les environnements les plus complexes.

Ivanti a des années d'expérience dans la fourniture de solutions complètes et adaptables de gestion de bout en bout des correctifs. Nos experts peuvent vous montrer comment utiliser efficacement les solutions Ivanti pour automatiser la gestion des correctifs, et pour déployer ces correctifs critiques sans aucune perturbation (ou presque) pour votre entreprise ou vos utilisateurs.

2 Vérification de la mise à jour du logiciel antivirus et de la planification d'analyses régulières

Si les correctifs constituent votre première ligne de défense, alors l'antivirus (AV) doit être la deuxième. Aujourd'hui, les bureaux d'étude de la sécurité ont montré que la plupart des attaques de ransomware ne peuvent pas être stoppées par les solutions antivirus traditionnelles basées sur les signatures. Pourtant, vous souhaitez sûrement éviter les menaces déjà identifiées et balisées par votre fournisseur d'antivirus.

L'élément essentiel d'une stratégie antivirus efficace consiste à vérifier que votre base de données de définitions de virus est toujours à jour sur tous vos postes de travail. Le logiciel Ivanti de gestion de la sécurité peut automatiser ce processus. Notre solution peut distribuer le fichier de définitions

de virus le plus récent à tous vos postes clients, quelle que soit la taille de votre environnement, en économisant la bande passante. Comme elle prend en charge la plupart des fournisseurs d'antivirus, notre solution fonctionnera probablement avec votre antivirus spécifique. Et si vous choisissez d'utiliser notre solution antivirus, basée sur le moteur antivirus Kaspersky Lab, vous pourrez également automatiser l'analyse et la gestion antivirus depuis une seule console.

3 Application d'une gestion des comptes avec privilèges

La limitation des privilèges est une tactique importante pour vous protéger de différents types de malware, y compris des ransomwares. Par exemple, un ransomware récemment découvert, nommé « Petya », a besoin de privilèges d'administrateur pour s'exécuter. Il sera inoffensif si l'utilisateur ne possède pas ces privilèges. [5]

Il est facile de supprimer des droits d'administrateur, mais il est beaucoup plus difficile de trouver l'équilibre entre privilèges d'accès, productivité des utilisateurs et sécurité de l'entreprise. D'où l'intérêt des solutions de gestion des privilèges.

L'équipe de sécurité Ivanti souligne l'importance de la gestion des privilèges. C'est l'une des raisons qui ont conduit Ivanti à racheter AppSense, fournisseur d'une solution de ce type ayant largement fait ses preuves (entre autres outils performants). AppSense Privilege Management vous aide à définir des stratégies pour limiter les privilèges d'administration aux seuls droits dont les utilisateurs autorisés ont besoin pour travailler.

Il faut cependant tenir compte d'un point pour la protection contre les ransomwares : la plupart des attaques par ransomware passent par de simples fichiers exécutables que les utilisateurs sont poussés à exécuter. Une fois exécuté, ce type de ransomware s'exécute dans l'espace de l'utilisateur actuel et n'a pas besoin de privilèges administrateur pour causer des dommages. Une version plus récente du ransomware Petya (mentionné plus haut) possède un mécanisme de secours qui lui permet de crypter les fichiers sans avoir besoin de privilèges administrateur.

LA LIMITATION DES PRIVILÈGES EST UNE TACTIQUE IMPORTANTE POUR VOUS PROTÉGER CONTRE DES TYPES DE RANSOMWARE SPÉCIFIQUES.

4 Protection des fichiers des lecteurs partagés grâce au contrôle d'accès

Une solution de contrôle d'accès efficace peut vous aider à vous protéger contre les ransomwares. Malgré tout, si cette solution cible principalement (voire exclusivement) les droits d'accès utilisateur, elle sera sans doute totalement inefficace.

Le contrôle d'accès peut s'avérer très utile pour protéger les fichiers stockés sur des lecteurs partagés. En effet, certains utilisateurs ont toujours des droits d'accès légitimes pour consulter et modifier au moins une partie des fichiers de chaque lecteur partagé. Après tout, la plupart de ces fichiers sont des documents créés par des utilisateurs légitimes. Cela signifie qu'un ransomware qui réussit à infecter le système d'un utilisateur doté de droits d'accès légitimes peut crypter et tenir en otages tous les fichiers de tous les lecteurs et dossiers partagés connectés.

Les solutions de sécurité Ivanti offrent un autre type de contrôle d'accès, qui cible les données à protéger plutôt que les droits de ces utilisateurs. Le logiciel Ivanti vous permet de définir des règles qui interdisent à tous les programmes (autres que ceux que vous spécifiez) de modifier les documents ou fichiers critiques ou sensibles. Par exemple, une règle peut autoriser uniquement Microsoft Word à modifier les fichiers .doc et .docx mais interdire toute tentative des ransomwares installés avec succès de crypter ces fichiers.

L'ajout de règles semblables pour protéger tous les fichiers Microsoft Office, Adobe PDF (et autres types de fichier fréquemment utilisés et partagés) constitue la meilleure défense contre les ransomwares. Si vous mettez en place ce type de règle, même si un ransomware s'introduit sur le système d'un utilisateur, il ne pourra pas crypter les fichiers protégés. Les utilisateurs conservent l'accès à ces fichiers et peuvent continuer de travailler sans aucune perturbation (ou presque), et sans avoir besoin de revenir à des versions de sauvegarde plus anciennes et potentiellement obsolètes.

(Notez que certains ransomwares tentent de se faire passer pour des logiciels légitimes et de s'ajouter aux routines de démarrage système. La solution Ivanti le leur interdit.)

CIBLEZ LES DONNÉES

PROTÉGEZ VOS FICHIERS EN MODE PASSIF MÊME SI UN RANSOMWARE A ÉTÉ DÉCLENCHÉ

LES RANSOMWARES EXPLOITENT LES MACROS DES FICHIERS MICROSOFT OFFICE. UTILISEZ LANDESK SECURITY SUITE POUR LES DÉSACTIVER.

Comparée au contrôle d'accès traditionnel, la méthode Ivanti, qui cible la protection des données, constitue une défense plus efficace contre les ransomwares. Elle repose sur la compréhension du comportement des ransomwares, et ne nécessite aucune création ni gestion de règles propres à l'utilisateur (et en constante mutation). Par conséquent, elle est également plus facile à implémenter et à maintenir que le contrôle d'accès basé sur la gestion des droits utilisateur.

5 Définition, implémentation et application de règles de logiciel

Le logiciel Ivanti facilite également la définition, l'implémentation et l'application de règles qui gèrent le comportement des autres logiciels. Les règles peuvent limiter la capacité de certains logiciels à s'exécuter. Elles peuvent aussi interdire la création, la modification ou la lecture de fichiers particuliers ou du contenu de dossiers spécifiques, y compris les dossiers temporaires utilisés par les navigateurs et d'autres programmes. Ces règles peuvent être appliquées au niveau global, ou appliquées à des utilisateurs ou à des groupes spécifiques.

Cependant, avant d'implémenter ce type de règle, il est important de tenir compte de la dégradation de l'expérience utilisateur que ces règles sont susceptibles de provoquer. Par exemple, lorsque vous installez un nouveau logiciel ou une mise à jour, les utilisateurs légitimes doivent parfois décompresser (« dézipper ») ou exécuter des fichiers directement depuis leur navigateur. Les utilisateurs peuvent également avoir besoin de pouvoir créer ou appeler des macros pour travailler. Les règles de restriction des logiciels risquent de bloquer ces activités normalement légitimes.

6 Désactivation des macros dans les fichiers Microsoft Office

La désactivation des macros des fichiers Office bloque de nombreux types de malware, y compris des ransomwares. Par exemple, Locky est un ransomware de cryptage relativement nouveau, qui se multiplie principalement par le biais de spam avec des pièces jointes. Il pousse les utilisateurs à activer des macros dans les documents Word pour télécharger le malware sur les machines.

Ivanti Security Suite permet aux administrateurs IT de définir une stratégie qui désactive les macros. Le déploiement de cette stratégie pour les collaborateurs qui n'ont pas besoin d'utiliser des macros interdit efficacement l'exécution de ce type de ransomware.

Autres considérations

Le FBI a émis des recommandations supplémentaires visant à renforcer la protection de votre environnement. Elles sont conçues pour vous aider à vous défendre contre plusieurs types de malware et d'autres attaques. Si vous les utilisez correctement, elles vous protègeront également des ransomwares.

7 Création de listes blanches (whitelist) d'applications

Cette solution interdit en fait aux ransomwares de s'exécuter, puisqu'aucun ransomware n'est un logiciel de confiance. Cela garantit que seules les applications connues et marquées comme « de confiance » peuvent s'exécuter sur un poste client. Les aspects les plus complexes, concernant la réussite des listes blanches (whitelist), sont la création de la liste initiale des applications de confiance, et le fait de maintenir cette liste à jour, exacte et complète.

Les solutions Ivanti, notamment AppSense Application Management, comportent plusieurs options permettant de créer des listes blanches exhaustives, flexibles, efficaces et directes. De plus, Ivanti facilite la création et la maintenance de vos listes blanches. Par exemple, la solution Ivanti « découvre » automatiquement toutes les applications en cours d'exécution sur les systèmes « propres » et vérifie l'intégrité des applications par rapport à sa propre base de données de réputation des applications. L'ajout de règles afin de faire confiance aux applications sur la base de leur propriétaire (ex. : administrateurs autorisés) et de leur fournisseur (ex. : Microsoft, Oracle) réduit encore le nombre d'opérations de configuration nécessaires pour créer la liste des applications de confiance.

INTERDISEZ DÈS LE DÉPART L'EXÉ-CUTION DES RANSOMWARES

CRÉEZ DYNAMIQUEMENT DES LISTES BLANCHES (WHITELIST) DE VOS APPLIS

8 Restriction des utilisateurs à des environnements virtualisés ou en conteneurs

Dans la plupart des cas, le ransomware est distribué sous forme d'une pièce jointe d'e-mail. En limitant les utilisateurs à des environnements virtualisés ou en conteneurs, vous garantissez que les ransomwares qui parviennent à accéder au système d'un utilisateur ne pourront pas nuire à l'environnement de travail principal de cet utilisateur.

Bufferzone, partenaire Ivanti One, fournit une solution élégante d'isolement des menaces, qui s'intègre aux solutions de sécurité Ivanti . Pour en savoir plus sur Bufferzone, visitez le site https://www.ivanti.fr/partners/ivanti-one/bufferzone .

9 Sauvegarde fréquente des fichiers critiques

Le document du FBI recommande d'utiliser des sauvegardes fréquentes des fichiers critiques pour assurer la continuité des activités. Si vous les utilisez correctement, les sauvegardes peuvent être votre planche de salut si vous êtes victime d'un ransomware. Cependant, si vous implémentez les défenses préconisées par cet eBook, en particulier les fonctions de contrôle d'accès de Ivanti, vous n'avez pas besoin de compter uniquement sur les sauvegardes pour combattre les ransomwares.

Les attaques par ransomware se multiplient. Battez-vous !

Avec les solutions Ivanti, vous pouvez gérer et protéger tous les postes clients, vous prémunir des menaces (anciennes ou nouvelles) et passer à un niveau de protection supérieur.

POUR PLANIFIER UNE DÉMO DES SOLUTIONS DE SÉCURITÉ IVANTI

CONTACTEZ NOTRE ÉQUIPE AU +33 1 49 03 77 80

Références

1. http://www.businessinsider.com/fbi-recommends-paying-ransom-for-infected-computer-2015-10
2. http://www.computerworld.com/article/3068623/security/ransomware-attacks-on-house-of-representatives-gets-yahoo-mail-blocked.html
3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
4. https://threatpost.com/latest-flash-zero-day-being-used-to-push-ransomware/117248/
5. https://blog.malwarebytes.org/threat-analysis/2016/04/petya-ransomware/.