La sécurité multiniveau facile

Les cyberattaques se multiplient. On en entend sans cesse parler, n'est-ce pas ? Ce n'est pas sans raison. Rien qu'aux États-Unis, on a relevé plus de 500 fuites de données divulguées publiquement en 2016 (près du double de l'année précédente[i]). En février 2017, le cabinet de recherche Opinium a découvert que 78 % des décideurs IT interrogés aux États-Unis et en Europe avaient subi au moins une attaque par ransomware dans leur entreprise au cours de l'année écoulée. Les Shadow Brokers, le groupe de pirates qui a exposé la vulnérabilité ayant favorisé le tristement célèbre WannaCry, a promis d'en divulguer d'autres à intervalle régulier, selon un modèle de « Club du vin du mois ». Le monde entier a maintenant connu sa première rançon de plus d'un million de dollars divulguée publiquement[ii]. Et le virus NotPetya vient de nous montrer à quoi pourraient ressembler les malwares agressifs du futur.

Comment stopper cette vague de terreur ? Sans une stratégie de sécurité ciblée, la multiplication des périphériques coûte cher... et est incontrôlable. Les équipes IT passent bien trop de temps à gérer ces périphériques. Sans parler du manque flagrant de personnel dans le domaine de la cybersécurité... Les entreprises sont contraintes d'optimiser leur personnel en matière de sécurité, et il devient évident qu'une stratégie de sécurité ciblée, qui exploite des technologies exhaustives, qui simplifie la gestion et qui cible les bases de la sécurité les plus efficaces pour vous protéger des attaques « de la vraie vie », est une solution bien plus avantageuse que les autres.

Lorsque l'on sait que 93 % des fuites de données entraînent des dommages pour l'entreprise en seulement quelques minutes, voire moins[iii], il est évident que vous ne pouvez pas vous permettre de faire le mauvais choix pour la sécurisation de votre entreprise.

Commencez par les correctifs

En fait, des correctifs sont déjà disponibles pour un grand nombre de vulnérabilités existantes. Un correctif a été publié en mars 2017 pour la vulnérabilité WannaCry, pour les systèmes d'exploitation Microsoft pris en charge (et Microsoft a depuis publié un correctif même pour ses OS les plus anciens). De nombreuses vulnérabilités existantes telles que celle-ci restent présentes, principalement parce que des correctifs de sécurité disponibles depuis longtemps n'ont jamais été implémentés. En 2015, l'équipe Verizon RISK a constaté qu'un grand nombre de ses vulnérabilités dataient de 2007[iv]. Quant aux 10 principales vulnérabilités connues ? Elles correspondent à 85 % des attaques réussies.[v]

Comment effectuer le suivi de toutes vos vulnérabilités, comment les corriger et comment générer des rapports les concernant, sans que votre budget crève le plafond et sans maux de tête pour le département IT ? Vous devez pouvoir rechercher, évaluer, tester et appliquer des correctifs pour l'ensemble de l'entreprise, en toute facilité. Et comme la majorité des vulnérabilités sont liées aux applications tierces, l'application de correctifs et de mises à jour aux systèmes d'exploitation ne suffit pas.

Gagnez du temps et de l'argent, et concentrez-vous sur les projets essentiels de l'entreprise. En seulement quelques minutes, les outils Ivanti sont installés et opérationnels, et ils vous aident à découvrir, évaluer et corriger les systèmes Windows, macOS, Linux et UNIX dans l'ensemble de votre entreprise, automatiquement et sur la base des stratégies que vous définissez. Nos outils simplifient l'application de correctifs à tous vos systèmes, physiques et virtuels. Trouvez les postes de travail et serveurs en ligne et hors ligne, recherchez les correctifs manquants et déployez-les. Appliquez ensuite les correctifs à tous les éléments de votre installation, des OS aux applications en passant par les machines virtuelles (VM), les modèles virtuels et même l'hyperviseur ESXi, grâce à l'intégration étroite du produit dans VMware.

Ivanti offre également un plug-in pour Microsoft System Center Configuration Manager, qui automatise et simplifie les processus de découverte et de déploiement de vos correctifs d'application tierce via la console SCCM.

La pile API avancée de nos solutions de correctifs s'intègre aux solutions de sécurité, analyseurs de vulnérabilités, outils de configuration comme Chef et Puppet, et autres outils de reporting. Tout en rendant natives les opérations de gestion des correctifs pour un large écosystème de

produits de sécurité, cette intégration vous aide aussi à combler le fossé entre les départements Sécurité, IT et Opérations de développement (DevOps). Par exemple, vous pouvez importer automatiquement la dernière évaluation des vulnérabilités dans le prochain lot de correctifs à tester, ce qui fait du département Opérations IT un partenaire plus efficace dans la protection de l'entreprise. De son côté, DevOps se concentre surtout sur l'amélioration continue et sur l'automatisation. Et l'intégration de ses outils avec la gestion des correctifs permet de concevoir des infrastructures et des systèmes plus résilients et plus cohérents. De plus, vous pouvez exploiter (mode Pull) les données critiques dans des solutions comme Splunk, Reporting Services, Archer et Crystal Reports, afin d'accélérer l'analyse, le traitement et la vitesse de clôture des incidents de sécurité critiques.

Blocage des éléments sans correctif

Par contre, les correctifs ne peuvent pas vous protéger des exploitations « zero-day ». Et que faire si aucun correctif n'est disponible, par exemple, parce que vous utilisez des systèmes plus anciens ou que vous craignez les dommages que les correctifs pourraient infliger à votre environnement ? Vous devez bloquer les applications sans correctif à l'aide d'outils comme les listes blanches d'applications et la gestion des privilèges.

Il est essentiel que les utilisateurs reçoivent uniquement les applications dont ils ont besoin pour être productifs, et qu'ils ne puissent pas introduire d'applications non autorisées susceptibles de nuire à la stabilité du poste de travail, d'avoir un impact sur la sécurité, de compromettre la conformité des licences, de provoquer des périodes d'inactivité utilisateur et d'augmenter les coûts de gestion des postes de travail.

Cependant, même si le verrouillage des postes de travail limite les risques, cela réduit aussi fortement la qualité de l'expérience des utilisateurs finaux. Les utilisateurs frustrés par une mauvaise expérience produisent moins et font plus souvent appel au centre de support. Ces utilisateurs peuvent également réagir au verrouillage de leur système en se tournant vers des solutions de rechange en « Shadow IT », générant ainsi des risques de sécurité supplémentaires.

Ivanti propose des solutions leaders du marché, qui vous aident à interdire l'exécution du code non autorisé sans que le département IT ait à gérer manuellement des listes interminables, et sans nuire à la productivité des utilisateurs. Trusted Ownership™ interdit automatiquement l'exécution de tout le code, même inconnu, introduit par un utilisateur non marqué comme « De confiance » (compte d'utilisateur standard, par exemple). Vous gérez tout aussi facilement les privilèges utilisateur et les stratégies, de manière très détaillée, tout en autorisant l'utilisateur à augmenter son niveau de privilèges en cas d'exception. Nos solutions vous permettent d'accorder très facilement aux utilisateurs uniquement les privilèges nécessaires pour remplir leur rôle... Ni plus ni moins.

Nous étendons également la prise en charge de l'environnement SCCM au contrôle des applications. Contrôlez les applications et les actions des utilisateurs finaux sur le poste client à l'aide d'une console centralisée. Et utilisez System Center Operations Manager (SCOM) pour collecter les événements « Contrôle des applications » et les détails d'audit.

Alignement sur la gestion de la sécurité

La plateforme Ivanti Endpoint Security combine la gestion automatique des correctifs et le contrôle des applications avec une gestion intégrée puissante de la sécurité du poste client : stratégies globales, diagnostics de sécurité, contrôle à distance du poste client, tableaux de bord et rapports de sécurité, etc.

À ce niveau, Ivanti ajoute des fonctions avancées d'antivirus et d'antimalware à votre solution de sécurité. Nos solutions assurent également le contrôle des périphériques (contrôle de l'utilisation des périphériques amovibles, et obligation de cryptage des périphériques amovibles et des disques durs) et la protection avancée contre les attaques sans fichier (désactivation des scripts téléchargés depuis Internet, apprentissage du comportement des applis, autorisation de l'exécution des scripts uniquement pour les applis de confiance, protection contre les attaques en mémoire, etc.). De plus, vous pouvez limiter l'accès aux réseaux ou aux adresses IP autorisés, ou bien personnaliser la configuration de pare-feu pour chaque système ou groupes de systèmes, y compris en configurant les derniers pare-feux Windows. De plus, vous pouvez détecter les tentatives de cryptage des fichiers sur la machine locale, bloquer le processus de cryptage et avertir tous les autres ordinateurs du réseau, afin de mettre le malware sur liste noire. L'attaque est ainsi tuée dans l'œuf.

Une interface unique très pratique vous permet de gérer facilement les paramètres et les tâches des composants et services de sécurité intégrés. En outre, les puissantes fonctions de contrôle à distance vous permettent d'isoler, d'examiner et de nettoyer des postes client sur l'ensemble du réseau. Prenez le contrôle des machines dont l'exécution est trop lente ou qui présente un autre souci de sécurité. Obtenez des informations en temps réel pour trouver rapidement la cause première du problème (affichez des informations sur la réputation des applications, la durée de découverte/d'exécution, et autres métadonnées) et la corriger depuis une seule et même console. Enfin, l'intégration avec vos outils de gestion des systèmes renforce l'efficacité et le contrôle de votre environnement IT.

Rapports et tableaux de bord en temps réel

En fin de traitement, Ivanti vous aide à consulter les résultats.

Comme il n'existe pas de vraie sécurité sans connaissance approfondie de l'environnement, Ivanti Xtraction vous permet de créer des rapports à l'aide d'une simple case à cocher. Il fournit des données à la demande, et vous permet de créer facilement de nouveaux tableaux de bord et rapports pour apporter les données voulues à la Direction, aux responsables, aux chargés de gamme de produits (LOB) et aux propriétaires d'application.

Avec nos connecteurs prédéfinis compatibles avec presque tous vos outils (centres de support, outils de surveillance et d'ITAM, systèmes téléphoniques, etc.), vous n'avez besoin d'aucun codage, gourou du Business Intelligence ou feuilles de calcul... Et aucun silo de données n'est créé. En outre, Xtraction peut être personnalisé pour se connecter à encore plus de systèmes, si bien que tous les utilisateurs peuvent voir les données de l'ensemble de l'entreprise en contexte. La masse énorme des informations se transforme en données critiques importantes, pour une prise de décisions plus rapide, plus pertinente et plus facile.

i Privacy Rights Clearinghouse

ii https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/

iii Verizon 2016 Data Breach Investigations Report (DBIR)

iv Verizon 2015 DBIR

v Verizon 2016 DBIR