LIVRE BLANC

DEVENIR FOURNISSEUR DE SERVICES DE SÉCURITÉ GÉRÉS : LA NÉCESSITÉ D'UNE APPROCHE DE SÉCURITÉ MULTICOUCHE

solarwinds msp

INTRODUCTION

Centrer votre activité de services gérés sur la cybersécurité multiplie vos chances d'augmenter vos marges. D'une manière plus significative, en déployant plusieurs couches de sécurité sur les sites de vos clients, vous pouvez réduire les incidents très coûteux. Il est essentiel de comprendre que pour être efficace, une cyberdéfense doit inclure plusieurs couches de technologie. Tout comme il est nécessaire de comprendre qu'une interruption d'activité chez un client représente une perte de revenus pour les fournisseurs de services gérés (MSP).

Les destins des MSP et de leurs clients sont étroitement liés. Les MSP doivent garantir le bon fonctionnement des opérations de leurs clients s'ils souhaitent qu'ils restent satisfaits et qu'ils continuent à honorer leurs factures.

Pour cela, ils doivent fournir des services de sécurité. En intégrant des services de sécurité dans votre offre, vous obtiendrez de nouvelles opportunités de conseil, accéderez à des clients plus importants et fournirez des suites de première catégorie pour la conformité de la sécurité.

La multiplication des cyberattaques, leurs conséquences coûteuses, en particulier lorsqu'il s'agit de ransomwares, vous permettent de tirer des avantages de la mise en œuvre de multiples couches de défense. Vos clients en sortent gagnants, et vous développez vos revenus.

Ce livre blanc présente les types de services sur lesquels les MSP peuvent s'appuyer pour offrir de véritables services de sécurité gérés. Il explore les attaques que les fournisseurs de services peuvent permettre à leurs clients d'éviter, et donne des conseils sur la méthodologie à suivre pour opérer une transition vers cette nouvelle opportunité lucrative de services de sécurité.

TABLE DES MATIÈRES

Les histoires de violations de données font souvent les gros titres et nous expliquent comment, une fois de plus, des entreprises ou organisations ont perdu des informations de clients, vécu des situations embarrassantes ou subi des pertes financières.

RAPPEL HISTORIQUE – POURQUOI FAUT-IL PRENDRE LA SÉCURITÉ AU SÉRIEUX ?

Chaque mois, des histoires de violations de données font les gros titres et nous expliquent comment, une fois de plus, des entreprises ou organisations ont perdu des informations de clients, vécu des situations embarrassantes ou subi des pertes financières à cause d'un incident de cybersécurité. La section suivante fournit quelques exemples de piratages, et présente les faiblesses des infrastructures ayant permis aux violations de se produire. Cette section est particulièrement instructive pour la mise en œuvre d'une solution de sécurité destinée à protéger vos clients.

- **JAPAN AIRLINES**

  La Japan Airlines a remarqué qu'elle avait été piratée seulement après avoir recherché d'où provenait la lenteur des performances de son réseau. La compagnie a découvert que des pirates informatiques s'étaient introduits dans son système et en avaient extrait des informations de clients, notamment les noms, sexes, dates de naissance, adresses, adresses e-mail et lieux de travail des membres de son programme de fidélisation JAL Mileage Bank[1]. 750 000 clients ont été touchés par cette attaque, qui a introduit le programme malveillant sur 23 ordinateurs du réseau. Ce programme malveillant aurait été distribué via un e-mail de phishing.

  VECTEURS D'ATTAQUE :

  - E-mail de phishing
  - Drive-by download (téléchargement involontaire) ou pièce jointe malveillante
  - Cheval de Troie

- **JAPAN PENSION SERVICE**

  Le Service des pensions du Japon (Japan Pension Service) s'est fait dérober 1,25 million de données de clients par des pirates qui ont introduit des logiciels malveillants dans des pièces jointes qu'ils ont fait passer pour des documents du ministère de la santé. Des numéros de pension, dates de naissance et adresses ont été compromis, selon les fonctionnaires du service.

  VECTEURS D'ATTAQUE :

  - E-mail de phishing ciblé
  - Pièce jointe malveillante
  - Cheval de Troie

- **ANTHEM**

  Début 2015, l'organisme d'assurance santé Anthem a perdu les informations personnelles d'environ 80 millions de clients, notamment leurs numéros de sécurité sociale, dates de naissance, adresses postales et numéros de téléphone. Les pirates ont un introduit un logiciel malveillant dans un site Web. Les employés d'Anthem ont été tentés de visiter ce site Web après avoir reçu des e-mails de phishing ciblés, dans lesquels étaient intégrés des liens.

  VECTEURS D'ATTAQUE :

  - E-mail de phishing
  - Drive-by download
  - Cheval de Troie

Les pirates informatiques utilisent une multitude d'approches et de vecteurs d'attaque dans leur activité frauduleuse.

- **AUSTRALIAN BROADCASTING CORPORATION**

Le diffuseur australien ABC (Australian Broadcasting Corporation) a été frappé par une attaque de ransomware ayant entraîné des perturbations sur sa chaîne d'information ABC News 24. Les pirates ont envoyé au personnel de la chaîne des pièces jointes infectées par un logiciel malveillant, au moyen d'e-mails provenant à première vue de la poste australienne (Australia Post).

En ouvrant les e-mails, les employés apprenaient qu'un colis n'avait pas pu être livré. En ouvrant la pièce jointe pour en savoir plus, ils se retrouvaient infectés par un ransomware[2].

Les crypto-ransomwares sont des menaces pernicieuses croissantes pour les entreprises. Cette catégorie de logiciel malveillant chiffre les fichiers des victimes et ne les déchiffre qu'en échange d'un paiement, généralement en bitcoins. Même si elle est relativement rare par rapport aux autres catégories de malwares, elle se développe rapidement. Selon le rapport Internet Security Threat Report 2015 de Symantec, les crypto-ransomwares infectaient environ 1 000 ordinateurs par jour à la fin 2014[3]. Ce nombre n'a cessé d'augmenter depuis.

VECTEURS D'ATTAQUE :

- E-mail avec une charge utile de ransomware en pièce jointe

- **DRUPAL 7**

En octobre 2014, des pirates informatiques ont trouvé une vulnérabilité dans la célèbre plateforme de gestion de contenu Drupal 7. Ils sont parvenus à envoyer des requêtes spéciales ayant permis d'exécuter du code SQL indésirable, et de compromettre des sites hébergés. La vulnérabilité a pu être utilisée pour prendre le contrôle d'un serveur hébergeant un site Web créé avec Drupal, télécharger l'ensemble des données stockées et transmettre le programme malveillant aux visiteurs du site.

Durant l'attaque, les serveurs infectés de Drupal ont été forcés d'intégrer une « armée de bots ». Les visiteurs des sites Web ont été infectés par un script malveillant, qui s'est ensuite servi d'eux pour trouver d'autres serveurs Drupal vulnérables, et infecter ainsi encore plus de sites Web.

Tout cela aurait pu être évité puisque les développeurs de la plateforme Drupal avaient déjà corrigé la faille. Le problème, c'est que de nombreux administrateurs de sites Web n'avaient pas téléchargé le correctif.

VECTEURS D'ATTAQUE :

- Logiciel non mis à jour
- Injection SQL
- Kit d'exploit automatisé
- Site infecté par une attaque drive-by download

Pour que la protection soit des plus efficaces, les MSP doivent cerner à la fois l'activité de leurs clients et leurs processus clés.

RENDRE VOS CLIENTS DIFFICILES À PIRATER

Les MSP ont la possibilité de servir plus efficacement leurs clients en rendant leurs systèmes informatiques plus difficiles à pirater. Ils peuvent installer une suite d'outils sur leurs propres systèmes, qu'ils utiliseront ensuite pour protéger les ordinateurs et les réseaux de leurs clients.

Pour que la protection soit des plus efficaces, les MSP doivent cerner à la fois l'activité de leurs clients et leurs processus clés. Les systèmes stratégiques doivent être solidement protégés, avec plus de couches de sécurité qu'il n'en faut sur les systèmes communs. Par ailleurs, la protection peut être mise en place à toutes les phases de l'attaque : avant, pendant et après.

- **AVANT**
  Avant une attaque, la priorité consiste à renforcer l'infrastructure informatique et à mettre en application des règles de sécurité strictes. Des outils appropriés doivent être installés (et les employés formés) afin de protéger les clients contre les menaces potentielles. La tâche essentielle consiste ici à mettre en place des sauvegardes fiables, locales et dans le Cloud. La suppression des droits d'administration en local, l'installation des correctifs et l'actualisation des systèmes sont des moyens simples de contrer les attaques courantes.

- **PENDANT**
  Renforcer un système contre les attaques n'empêchera pas les cybercriminels de tout mettre en œuvre pour s'introduire dans les environnements de vos clients et accéder à leurs données. Les MSP doivent être capables de détecter une attaque dès son apparition, de l'empêcher d'endommager les systèmes ciblés et, enfin, d'éviter d'autres intrusions de l'attaquant. Des règles de pare-feu appliquées au trafic sortant (aidant à déceler les comportements inhabituels au niveau des postes de travail et serveurs) et une journalisation des événements sont essentielles pour la détection des activités malveillantes. Un antivirus, un filtrage des e-mails et une protection Web sont également des technologies utiles pour enrayer les cyberattaques.

  Par exemple, pour contrer une attaque de type « zero-day », vous pouvez mettre en place des vérifications au niveau des journaux d'événements, afin de détecter les activités suspectes sur les réseaux de vos clients.

  Une vérification spécifique pourrait rechercher les fichiers Acrobat.exe et Flash.exe présentant des failles de protection sur les ordinateurs du réseau. Si Adobe Reader cesse de fonctionner lorsqu'un client ouvre un PDF ou clique sur une vidéo en ligne, cela peut signifier qu'un problème s'est produit au niveau du logiciel, et qu'il s'agit probablement d'une attaque de type « zero-day ».

  L'ordinateur est utilisé comme point d'entrée pour accéder aux autres parties du réseau et lancer une attaque de grande ampleur.

Comprendre ce qu'il faut faire une fois l'attaque terminée (et comment en tirer les meilleures leçons) est une phase importante du processus.

· APRÈS

Un MSP au service de multiples clients peut être témoin de nombreuses attaques au cours d'une année. Comprendre ce qu'il faut faire une fois l'attaque terminée (et comment en tirer les meilleures leçons) est une phase importante du processus. Une fois l'attaque contrée, assurez-vous d'en mesurer l'étendue et de maîtriser les dommages afin qu'aucun autre système ne soit touché, puis réparez les dégâts déjà provoqués. Dans la plupart des cas, cela implique une restauration de données et/ou d'une image système. Les MSP doivent garantir la résilience de l'activité de leurs clients.

Enfin, recueillez toutes les informations possibles sur les systèmes touchés. Vous pourrez ensuite vous appuyer sur vos connaissances pour renforcer vos systèmes. De cette manière, vous tirez sans cesse des enseignements et continuez à améliorer vos services. Ne vous précipitez pas systématiquement sur une solution technologique. Parfois, les attaques sont contenues simplement en supprimant le logiciel fautif (par exemple, Adobe Flash) ou en appliquant des droits d'accès sur les logiciels téléchargés. Il suffit de retirer aux utilisateurs la possibilité d'installer des logiciels pour éviter de nombreuses cyberattaques courantes.

Comme les cambrioleurs, de nombreux pirates informatiques sont opportunistes : ils vont là où l'accès est le plus simple.

POURQUOI ADOPTER UNE APPROCHE DE SÉCURITÉ MULTICOUCHE ?

Derrière ce processus de sécurité complet se cache une approche multicouche. Cette approche combine plusieurs lignes de défense dans le but de repousser les attaques potentielles. Son principe : une protection unique, quelle qu'elle soit, ne suffit pas pour arrêter un cybercriminel déterminé.

Pour mieux comprendre l'approche de sécurité multicouche, imaginez que votre système informatique soit une maison. Dans votre maison se trouvent vos objets de valeur. Vous pouvez facilement installer un verrou sur votre porte d'entrée afin d'empêcher toute intrusion pendant que vous dormez. Mais cela ne vous aiderait pas à verrouiller votre porte lorsque vous sortez de chez vous. Vous pouvez donc décider de monter une serrure de type à pêne dormant.

Il vous reste toujours les fenêtres, faciles à briser et proches du sol. Des barreaux de fer les protégeraient davantage. Mais pour plus de sûreté, vous pouvez choisir d'installer une alarme, au cas où un voleur trouverait un autre moyen d'entrer. Enfin, l'installation de luminaires à l'arrière de la maison permettrait d'empêcher les cambrioleurs de se tapir dans l'obscurité et les dissuaderait d'agir. À ce niveau, il est vraisemblable que le cambrioleur se tourne vers une autre maison, moins bien protégée.

Comme les cambrioleurs, de nombreux pirates informatiques sont opportunistes : ils vont là où l'accès est le plus simple. La mise en œuvre de multiples systèmes de défense peut décourager les intrusions. Mais l'analyse des points faibles d'un environnement informatique est parfois plus complexe que le relevé des points d'entrée possibles de votre maison. L'approche multicouche permet d'y remédier.

Une stratégie de défense multicouche efficace comporte sept éléments. Tous ces éléments sont complémentaires, et forment un filet de protection autour des systèmes de vos clients.

Une technique courante des cybercriminels consiste à cibler les logiciels qui n'ont pas été mis à jour, et ne sont donc pas protégés contre les vulnérabilités connues.

DÉFINITION D'UNE APPROCHE DE SÉCURITÉ MULTICOUCHE

1. GESTION DES MISES À JOUR

Une technique courante des cybercriminels consiste à cibler les logiciels qui n'ont pas été mis à jour, et ne sont donc pas protégés contre les vulnérabilités connues.

De nombreuses attaques exploitent ces logiciels, même lorsque les failles sont identifiées depuis longtemps. Les failles logicielles sont répertoriées dans la base de données CVE (Common Vulnerabilities and Exposures) maintenue par la société MITRE. Selon Verizon, 99,99 % des exploits opérés en 2014 s'appuyaient sur des vulnérabilités disposant d'un numéro CVE depuis au moins un an[4].

En fait, c'était même pire que cela. Le rapport de Verizon montre que plus de 30 failles responsables de violations de données en 2014 figuraient dans la première édition de la base CVE, parue en 1999. Vous avez bien lu, des entreprises continuent de perdre des données à cause de failles identifiées avant l'apparition du virus ILOVEYOU. L'importante des mises à jour logicielles est telle que le service de renseignement australien ADS (Australian Signals Directorate) les énumère comme une obligation pour limiter les intrusions[5].

Si les correctifs système avaient été correctement installés par la plupart des administrateurs de sites Drupal 7 (voir plus haut), leurs sites Web n'auraient pas été compromis et les visiteurs n'auraient pas été infectés. Les pirates, qui ont élaboré une attaque exploitant une faille connue de Drupal, ont profité de l'absence de mise à jour corrective de la part des administrateurs pour agir.

Après avoir détecté une faille dans un composant logiciel spécifique (système d'exploitation, moteur de base de données, cadre d'applications, application logicielle), les cybercriminels peuvent facilement créer des scripts afin de chercher sur Internet les versions exécutées du logiciel, puis lancer leurs attaques. Des kits d'exploits, conçus pour la recherche sur la cybersécurité, contiennent des catalogues de failles régulièrement actualisés, ainsi que le code permettant de les exploiter. Ils fournissent des armes prêtes à l'emploi aux utilisateurs sans scrupules.

La gestion des mises à jour est une pratique accessible pour les administrateurs informatiques. Ils peuvent, jusqu'à un certain point, automatiser l'installation des correctifs à l'aide de scripts ou de systèmes plus sophistiqués qui documentent, téléchargent, testent et gèrent les correctifs de multiples éditeurs de logiciels

Il peut être judicieux de consulter les forums avant de télécharger les correctifs, mais aussi de tester ces derniers sur un système pendant une journée avant de les déployer. Parfois, malgré les tests réalisés par l'éditeur, les correctifs peuvent être insatisfaisants. Même si une mise à jour est susceptible d'entraîner des problèmes sur le site d'un client, il est de loin préférable de gérer une mauvaise mise à jour plutôt qu'une cyberattaque, car vous connaissez exactement la cause du problème.

Face à un tel nombre d'attaques utilisant des programmes malveillants comme points d'entrée sur les réseaux d'entreprise, les antivirus ne sont pas une option, mais une obligation.

2. ANTIVIRUS

Les services antivirus doivent être un élément clé de l'arsenal des MSP. Même s'il ne permet pas de contrer à lui seul les attaques, l'antivirus est une ligne de défense utile contre les programmes malveillants utilisés par les cybercriminels pour s'immiscer dans les systèmes des entreprises. Toutes les directives de meilleures pratiques et les exigences de conformité imposent des systèmes de protection contre les logiciels malveillants. Les cybercriminels emploient souvent des chevaux de Troie et programmes malveillants déjà « connus » pour attaquer leurs cibles. Par conséquent, un antivirus à jour peut détecter et supprimer ces menaces, à condition de disposer des définitions les plus récentes.

La technologie antivirus a récemment évolué. Elle intègre désormais des fonctions heuristiques et autres capacités avancées permettant de détecter des virus et chevaux de Troie jusqu'alors inconnus. De plus, avec les mises à jour de signatures depuis le Cloud, les éditeurs de solutions de sécurité peuvent protéger directement les clients des MSP contre les nouveaux échantillons de programmes malveillants, à mesure qu'ils apparaissent.

Face à un tel nombre d'attaques utilisant des programmes malveillants comme points d'entrée sur les réseaux d'entreprise, les antivirus ne sont pas une option, mais une obligation.

3. PROTECTION WEB

La technologie antivirus n'est pas parfaite. Elle peut identifier une signature de logiciel malveillant, ou non. Elle peut détecter le comportement suspect d'une application, ou passer à côté. De nombreux programmes malveillants sont diffusés au moyen d'un navigateur. C'est pourquoi la protection Web occupe également une place essentielle dans la stratégie de défense multicouche.

Avec cette technologie, les MSP peuvent identifier les sites Web consultés par les employés de leurs clients en entreprise (ou les sites consultés sans autorisation par les machines infectées). À l'instar des logiciels antivirus, les services de protection Web reçoivent des mises à jour régulières de noms de domaine et adresses IP en lien avec des activités malveillantes. Ces données peuvent être utilisées pour interdire l'accès à certains sites en entreprise.

Les services de protection Web donnent également la possibilité aux MSP d'offrir une valeur ajoutée supplémentaire à leurs clients. Ils peuvent être employés comme des mécanismes de détection afin d'identifier les activités suspectes sur Internet indiquant une attaque possible. Ils permettent également d'empêcher les employés de consulter des sites légitimes mais indésirables, tels que des sites sportifs ou de divertissement. Les MSP aident ainsi leurs clients à préserver la productivité de leurs employés.

Selon le rapport Data Breach Incident Report (DBIR) de Verizon, 54 % des infections de logiciels malveillants sont liées à des activités sur le Web. L'utilisation des navigateurs est largement supérieure à celle des logiciels de messagerie. De plus, les utilisateurs y ajoutent souvent des modules tiers afin de bénéficier de fonctionnalités supplémentaires. Les navigateurs offrent ainsi une plus grande surface d'attaque, et deviennent des cibles particulièrement attrayantes.

La messagerie étant l'un des outils les plus importants d'une entreprise, elle reste l'un des principaux vecteurs d'attaque des pirates.

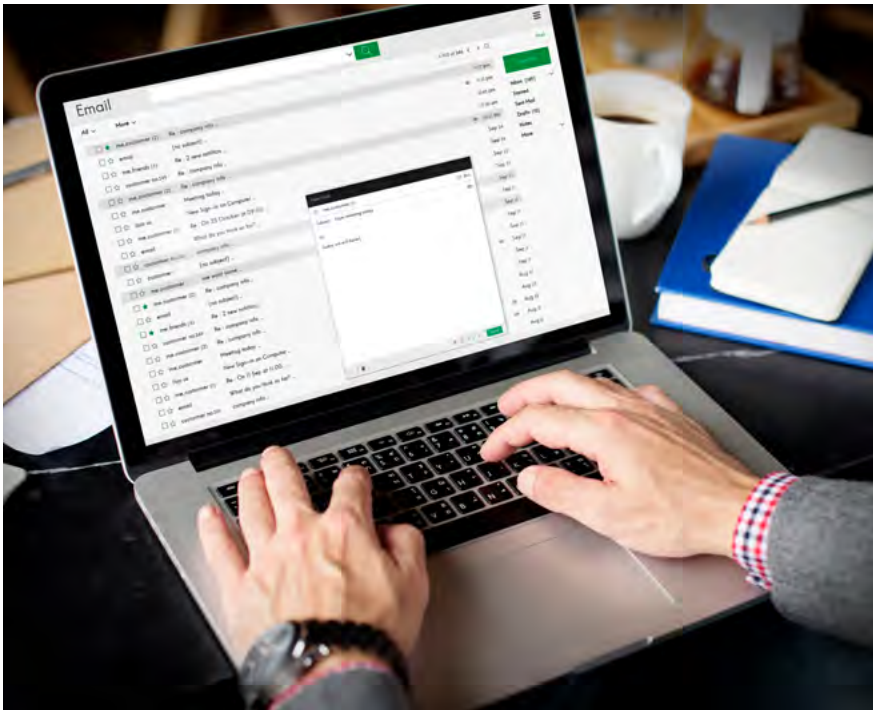
4. PROTECTION DE LA MESSAGERIE ÉLECTRONIQUE

La messagerie étant l'un des outils les plus importants d'une entreprise, elle reste l'un des principaux vecteurs d'attaque des pirates. Ils s'en servent pour envoyer des liens vers des sites Web malveillants ou des pièces jointes infectées directement aux employés. Les e-mails sont un vecteur potentiel d'ingénierie sociale : pour augmenter leurs chances de réussite, les pirates observent l'entreprise et insèrent des détails pertinents dans leurs messages.

Avec une offre de services de protection de la messagerie, les MSP procurent des avantages significatifs à leurs clients, au-delà de simplement les rassurer. En étudiant de grands volumes de courriers indésirables et en identifiant des modèles, les MSP développent des connaissances précieuses sur les types d'attaques qui visent leurs clients. Par exemple, si un nombre important d'e-mails est envoyé à des employés précis, ils peuvent en déduire qu'il s'agit d'un acte malveillant.

Les MSP peuvent également améliorer les performances des réseaux de leurs clients et potentiellement réduire leurs coûts de bande passante en proposant un service de protection de la messagerie basé dans le Cloud. Les flux de messagerie sont alors collectés puis filtrés par leurs soins avant d'être transmis à l'entreprise. Ce service évite d'encombrer les réseaux des clients avec du courrier indésirable. Les clients peuvent également configurer leurs réseaux afin que seuls les e-mails provenant du service Cloud du MSP soient acceptés, et ainsi renforcer leur protection.

Selon le rapport Data Breach Incident Report (DBIR) de Verizon, 77 % des infections sont liées à la réception d'un e-mail contenant une pièce jointe ou un lien malveillant(e). Un service de protection de la messagerie fiable, dans le Cloud, offre une solide couche de défense supplémentaire.



5. SAUVEGARDE

Une sauvegarde efficace est le dernier service essentiel d'une stratégie de sécurité multicouche. Protéger vos clients contre les attaques peut leur assurer une certaine tranquillité d'esprit en termes de sécurité. Mais la cybersécurité n'est pas une science exacte, même les meilleurs systèmes de protection peuvent être compromis. La menace d'une attaque, et le risque de perte de données qui l'accompagne, font de la sauvegarde un composant stratégique de tout service de cybersécurité.

Les MSP doivent veiller à tester leur service de sauvegarde. Des sauvegardes fréquentes et incrémentielles dans le Cloud sont plus faciles à tester et à garantir auprès des clients. De plus, l'absence de supports physiques réduit le risque de vol, perte ou corruption des données sauvegardées.

Personne n'est jamais trop prudent en matière de sauvegarde. Avec l'explosion des attaques par ransomwares, vos clients ont besoin de sauvegardes à la fois locales et Cloud. La sauvegarde Cloud permet de répondre aux exigences de conformité et meilleures pratiques imposant une sauvegarde quotidienne hors site. De plus, la technologie utilisée est difficilement accessible par les ransomwares. Vous pouvez ainsi restaurer vos fichiers si une attaque parvient à déjouer vos défenses.

La sauvegarde locale permet une restauration plus rapide des fichiers volumineux ou de quantités importantes de fichiers. Associée à une sauvegarde redondante dans le Cloud, vous évitez le stress lors d'un incident. Confiants de la validité de leurs sauvegardes, les MSP réagissent efficacement en cas d'incident pour rétablir les opérations de leurs clients.

Ne vous méprenez pas, ces incidents peuvent être coûteux et nuire à votre réputation

6. VENDRE LA SÉCURITÉ MULTICOUCHE

Les MSP qui appliquent un tarif par équipement ou par utilisateur devraient envisager la mise en œuvre d'un maximum de couches de sécurité. Lorsqu'un MSP est contraint de gérer un incident de sécurité informatique pour un client, il s'agit rarement d'une tâche simple ou rapide. De plus, un déplacement sur site est souvent nécessaire. Pour la plupart des entreprises informatiques au planning bien rempli, le calcul est simple : un excellent retour sur investissement s'obtient par un travail que l'on peut facturer, et non par l'élimination de logiciels malveillants sur des systèmes, la restauration de données ou la réinstallation de systèmes d'exploitation. Moins vous passez de temps à traiter des appels complexes liés à la sécurité, mieux c'est.

Au final, tout est une histoire de chiffres. Les menaces des cybercriminels sont constantes, allant de simples attaques par force brute contre un VPN, le protocole RDP, Outlook Web Access ou tout autre service exposé, à des attaques plus sophistiquées comme le phishing ciblé (spear phishing). Les MSP doivent combiner un maximum de services de sécurité tout en veillant à leur rentabilité, afin de réduire les risques d'incidents entraînant des interruptions d'activité.

Selon Gartner et d'autres cabinets d'analyse, le modèle de « sécurité sous forme de service » prend réellement de l'ampleur sur le marché actuel. Un logiciel de sécurité vendu sous forme d'abonnement est le moyen le plus rentable de réduire les risques d'incidents de sécurité chez vos clients. Ne vous méprenez pas, ces incidents peuvent être coûteux et nuire à votre réputation.

7. LA RÉPUTATION EST LA BASE DE TOUT

Toute interruption d'activité, qu'elle soit liée à un logiciel malveillant ou à une autre cause, est perçue comme un manquement de la part du MSP. Cela peut sembler rude, mais si votre client n'est plus en mesure de travailler et que vous vous agitez dans tous les sens pour essayer de rétablir ses systèmes, vous risquez, avec le modèle MSP, de perdre ce contrat. Parmi tous les services abordés, il en est un qui présente une importance majeure : la sauvegarde. Cette couche de sécurité est la plus essentielle car elle offre une protection contre toutes les menaces : physiques, clients, MSP et cybercriminels.

L'objectif ultime d'une offre de services de sécurité gérés est de rendre le piratage de vos clients difficile. Il serait inexact et injuste de promettre à vos clients une sécurité à 100 %, mais vous pouvez leur proposer une armure solide pour un forfait relativement bas.

La mise en œuvre de services de sécurité pour vos clients peut garantir leur satisfaction et leur productivité. Face à la multiplication des menaces, le déploiement de plusieurs couches de sécurité semble la meilleure réponse. Ainsi, en tant que MSP, vous pouvez vous concentrer sur la réalisation des projets et le développement de votre activité, plutôt que de passer votre temps à répondre à des appels coûteux liés à des problèmes de sécurité sur site.

EN CONCLUSION

Les services de sécurité gérés représentent une nouvelle activité lucrative pour les MSP. En réalité, avec l'augmentation croissante des cyberattaques, les MSP qui n'offrent pas de services de sécurité risquent de perdre des contrats au profit de ceux qui en proposent. Pour fournir de véritables services de sécurité, vous devez adopter une approche multicouche. En proposant des services de filtrage de virus, de gestion des mises à jour et de protection Web, vous rendrez le piratage de vos clients difficile. En les complétant d'un service de sauvegarde et de restauration, vous faciliterez la restauration des données et la continuité d'activité en cas de cyberattaque.

En résumé, offrir une sécurité multicouche à vos clients vous apportera non seulement de nouveaux revenus, mais garantira aussi la satisfaction des entreprises sous votre protection. Et un client heureux, c'est un client fidèle.

RÉFÉRENCES

1. http://www.wsj.com/articles/japan-airlines-reports-hacker-attack-1412053828
2. http://www.csoonline.com/article/2692614/malware-cybercrime/ransomware-attack-knocks-tv-station-off-air.html
3. http://www.symantec.com/security_response/publications/threatreport.jsp
4. http://www.verizonenterprise.com/DBIR/2015/
5. http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

SÉCURITÉ MULTICOUCHE **INTELLIGENCE COLLECTIVE** **MULTIPLATEFORME**

SolarWinds MSP donne la possibilité aux MSP, de toutes tailles et du monde entier, de développer une activité hautement rentable, efficace, assortie d'un avantage concurrentiel mesurable. Ses solutions intégrées axées sur l'automatisation, la sécurité, la gestion de services et de réseaux, sur site et dans le Cloud, et accompagnées de recommandations pratiques, aident les MSP à réaliser leurs tâches plus facilement et plus rapidement. SolarWinds MSP aide les MSP à se concentrer sur l'essentiel, à respecter leurs accords de niveaux de service et à créer une activité rentable.

Pour plus d'informations, visitez le site
www.solarwindsmsp.com

RMWP00087FR0617

solarwinds msp