solarwinds msp

eBOOK

Guide pratique de la cybersécurité

Comment la sécurité multicouche peut vous aider à protéger vos clients et préserver vos bénéfices

Dans un contexte où les cyberattaques sont plus nombreuses que jamais, les entreprises attendent de leurs fournisseurs de services gérés (MSP) qu'ils leur offrent un niveau de sécurité minimal sur l'ensemble de leur parc informatique. Si à une époque « niveau de sécurité minimal » signifiait « être équipé d'un logiciel antivirus », aujourd'hui, cela ne suffit plus. Une approche multicouche est aujourd'hui nécessaire et doit fournir plusieurs niveaux de sécurité essentiels dans une plateforme unique et intégrée. Cette approche assure une protection plus complète, et aide les MSP à préserver leurs bénéfices.

POURQUOI LA SÉCURITÉ EST-ELLE PLUS IMPORTANTE QUE JAMAIS POUR LES FOURNISSEURS DE SERVICES GÉRÉS ?

Lorsqu'une entreprise est frappée par un ransomware et qu'elle perd ses données financières ou ses informations clients, qui est pointé du doigt ? À tort ou à raison, il s'agit souvent du fournisseur de services gérés.

Pourquoi ? Les cyberattaques telles que les ransomwares sont de plus en plus courantes, et la sécurité se place en tête des priorités pour la plupart des organisations. L'actualité étant sans cesse marquée par des attaques et violations de données, les entreprises s'imaginent que leur conseiller informatique, en qui elles ont confiance, leur garantit un niveau de sécurité suffisant par l'intermédiaire de ses services. Lorsqu'un problème survient, quelle qu'en soit l'origine, le résultat est bien souvent le même : le temps de réaction ainsi que le coût d'intervention minent une partie des profits du MSP. Cela est d'autant plus vrai dans le cadre de contrats à prix forfaitaire.

Selon une étude de 2017, les attaques de ransomwares peuvent nécessiter jusqu'à 12 heures en moyenne pour être corrigées[1].

Le meilleur moyen d'éviter ces problèmes pour les MSP est d'inclure des fonctions de sécurité essentielles dans leur offre de services informatiques gérés. De cette manière, ils assurent à leurs clients une protection contre les menaces courantes. De plus, ils développent leur activité en se démarquant de la concurrence.

LA MULTIPLICATION DES MENACES NÉCESSITE D'ADOPTER PLUSIEURS COUCHES DE SÉCURITÉ

Les entreprises sont plus que jamais confrontées à des risques informatiques, tels que les ransomwares, le piratage, les violations de données, les attaques par déni de service distribué (Distributed Denial of service ou DDos) et l'espionnage industriel. Les points d'entrée de ces attaques sont également plus nombreux : trafic Web et messagerie électronique, clés USB, connexions non sécurisées, appareils tels que les smartphones et les ordinateurs portables, applications et données (en transit ou au repos).

Malgré ce qu'affirment de nombreux éditeurs de solutions de sécurité, il n'existe pas de solution miracle capable de préserver une entreprise de toutes les menaces. Pour véritablement protéger leurs clients, les MSP doivent aller au-delà du simple antivirus, et mettre en oeuvre une approche dite de « défense en profondeur », réunissant plusieurs outils et contrôles de sécurité dans le but de protéger les systèmes informatiques. La clé de cette approche est la redondance : si un contrôle de sécurité échoue ou est ignoré, les autres défenses prennent le relais pour contrer la menace.

Pensez aux diverses mesures de sécurité mises en oeuvre par les particuliers pour protéger leurs maisons. Ils installent des clôtures, verrouillent leurs portes, s'équipent d'une alarme et certains investissent dans des coffre-forts pour mettre leurs biens les plus précieux à l'abri. A cela s'ajoute une dernière couche de sécurité si toutes ces mesures échouent, à savoir leur assurance.

1 *« The 2017 Endpoint Protection Ransomware Effectiveness Report », KnowBe4. Consulté en juin 2018.*

On appelle cela la « sécurité par couches » ou « sécurité multicouche ». La même approche est indispensable en informatique.

LES COMPOSANTS ESSENTIELS DE LA SÉCURITÉ INFORMATIQUE

Les MSP qui envisagent d'intégrer des services de sécurité dans leur offre de services informatiques doivent commencer par les éléments de base suivants :

GESTION DES MISES À JOUR

De nombreuses violations sont les conséquences d'un piratage informatique qui exploite des logiciels ou des systèmes non mis à jour. Les MSP doivent s'assurer que chacun des appareils qu'ils gèrent dispose des derniers correctifs logiciels. Plus leurs clients sont nombreux, plus la tâche est difficile à accomplir. Un logiciel de gestion des mises à jour offre une visibilité complète sur l'état des correctifs. De plus, des fonctionnalités d'automatisation et de programmation permettent d'exercer un contrôle précis sur les stratégies de mise à jour.

ANTIVIRUS MANAGÉ

La manière dont un MSP gère un antivirus est aussi importante que sa façon de le déployer. Les meilleures solutions antivirus protègent contre les logiciels malveillants connus et nouveaux (en associant un système traditionnel de signatures avec des vérifications heuristiques et des analyses comportementales). Elles offrent également une grande flexibilité en proposant des stratégies de quarantaine personnalisables. Un antivirus intégré (ou managé) permet aux MSP d'accéder à un tableau de bord unique, à partir duquel ils peuvent simplifier les déploiements en bloc sur plusieurs sites et serveurs, programmer des analyses automatisées à des heures qui ne perturbent pas les utilisateurs dans leur travail, etc.

PROTECTION WEB

Souvent, pour ne pas dire toujours, les attaques de phishing, les téléchargements involontaires et autres menaces via le Web se produisent parce que des utilisateurs peu méfiants tombent sans le vouloir sur un site malveillant. Les MSP doivent pouvoir bloquer les URL malveillantes, afin d'empêcher les connexions à des domaines connus pour être utilisés par des pirates informatiques. Les logiciels de protection Web offrent cette possibilité, tout en permettant aux MSP de définir leurs propres stratégies de filtrage de contenu, listes noires de sites Web, stratégies de navigation, etc.

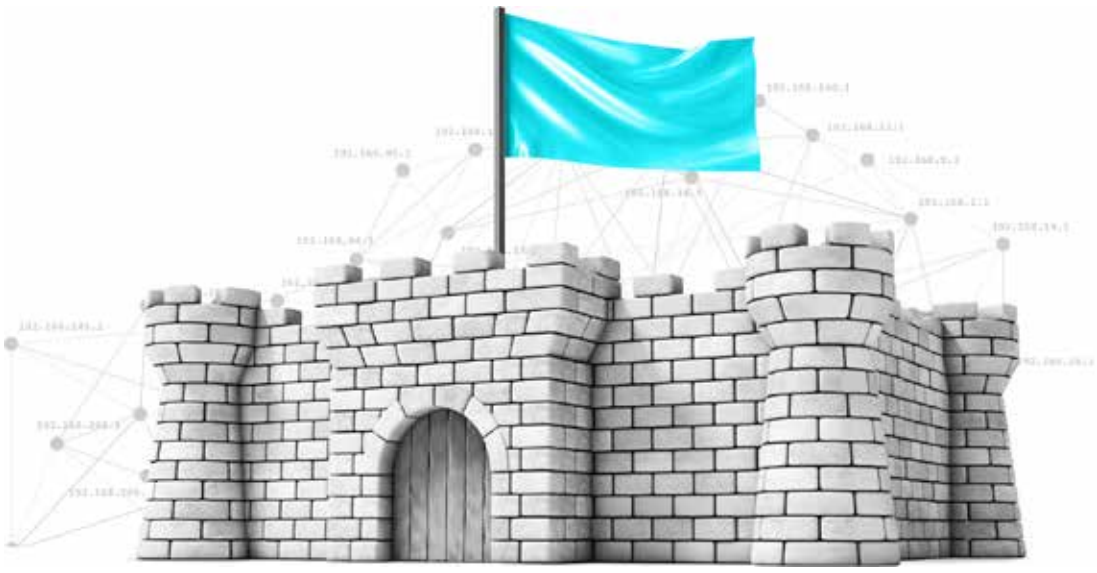
FILTRAGE DE LA MESSAGERIE

La majorité des menaces de sécurité font leur entrée par la messagerie électronique. En recherchant dans les e-mails entrants et sortants les pièces jointes, scripts, domaines, URL et chaînes de texte potentiellement dangereux, les logiciels de filtrage de la messagerie facilitent la protection des clients contre le courrier indésirable, les tentatives de phishing et les logiciels malveillants. Ils permettent également aux MSP de contrôler entièrement leurs stratégies de liste noire, liste blanche et quarantaine.

SAUVEGARDE

La sauvegarde ressemble beaucoup aux assurances : nous n'en avons pas toujours besoin, mais quand c'est le cas, elle nous sauve la vie. Une solution de sauvegarde et reprise après sinistre basée dans le Cloud offre la meilleure protection contre les attaques de ransomwares. Elle permet aux entreprises de se remettre au travail en restaurant facilement et rapidement leurs fichiers corrompus ou chiffrés. Au minimum, les MSP doivent proposer une solution qui sauvegarde les documents de leurs clients. S'ils gèrent leurs serveurs, ils doivent aussi penser à sauvegarder ces systèmes.

Dans l'idéal, de tels services de sauvegarde doivent être intégrés dans chaque offre proposée par les MSP. Ils pourront ainsi s'assurer que tous leurs clients bénéficient d'un niveau de protection minimal et approprié face aux risques.



LA SÉCURITÉ MULTICOUCHE EN ACTION

Opter pour une stratégie de sécurité multicouche est essentiel. Pensez en effet aux moyens utilisés par un logiciel malveillant pour s'introduire dans le réseau informatique d'une organisation[2] :

73 %
Pièces jointes d'e-mails

54 %
E-mails de phishing

28 %
Sites Web compromis ou malveillants visités par les utilisateurs

La messagerie électronique et l'utilisation du Web sont de loin les points de départ les plus courants des attaques de ransomwares. Dans la plupart des cas, les utilisateurs consultent sans le vouloir un site Web malveillant ou compromis. Ils sont attirés par un lien ou une pièce jointe en apparence légitime, et cliquent dessus.

Les informations les plus exposées dans les attaques de ransomwares sont les données financières (62 %), suivies des informations clients (61 %).

Diverses méthodes permettent de détecter les attaques de ransomware. Les plus courantes sont les outils de sécurité des points de terminaison, les passerelles de messagerie et les passerelles Web, ou les systèmes de détection des intrusions (pare-feu de réseau) :

83 %
Anti-malware/antivirus/ outils de sécurité des points de terminaison

64 %
Passerelles de messagerie et passerelles Web

46 %
Système de détection des intrusions

Si le client d'un MSP se fie uniquement à un antivirus, près d'un ransomware sur cinq passera entre les mailles du filet. Mais si plusieurs contrôles de sécurité sont exécutés à la suite, une menace non détectée par l'antivirus et introduite dans le réseau pourra toujours être identifiée lors de ses déplacements d'un appareil à l'autre, ou de ses tentatives de contact avec un serveur de commande et de contrôle malveillant.

Dans un système de sécurité multicouche, chaque composant est destiné à compléter les autres (voire à compenser les lacunes des autres), dans le but d'intercepter les menaces de sécurité avancées. La gestion des mises à jour installe les derniers correctifs de sécurité sur les logiciels et les systèmes d'exploitation, afin qu'aucune vulnérabilité ne puisse être exploitée. L'antivirus détecte et bloque de nombreuses menaces connues. Le filtrage de la messagerie et du Web met en quarantaine les e-mails suspects, et empêche les communications vers des sites de commande et de contrôle. Les sauvegardes de données facilitent la récupération en cas de pertes subites. Grâce aux sauvegardes, 54 % des entreprises ont déclaré avoir pu reprendre leur activité dans les 24 heures ayant suivi une attaque de ransomware[2].

2 *« Ransomware Report 2017 », Bitdefender, Cybersecurity Insiders, Information Security Community on LinkedIn, Crowd Research Partners. Consulté en juin 2018.*

UNE APPROCHE SIMPLIFIÉE DE LA SÉCURITÉ MULTICOUCHE AVEC SOLARWINDS

Une offre de sécurité multicouche ne doit pas nécessairement être complexe ou coûteuse.

Contrairement aux produits de sécurité indépendants qui imposent parfois d'avoir une solide expertise et d'utiliser plusieurs consoles, SolarWinds offre une intégration complète de ses principales fonctionnalités de sécurité dans une seule et même console de gestion.

Depuis leur tableau de bord simple d'utilisation, les MSP s'assurent que leurs stratégies de sécurité sont définies et appliquées systématiquement sur tous les appareils gérés, y compris les serveurs. Ils bénéficient d'une fenêtre unique, à partir de laquelle ils configurent et automatisent de façon rapide et simple leurs stratégies dans divers domaines : mises à jour, antivirus, protection Web, filtrage de messagerie, sauvegarde, etc. Leurs prestations de services sont rationalisées, leur rentabilité augmente, le tout sans effort supplémentaire.

Dans certains cas, ces principales fonctionnalités de sécurité peuvent être activées depuis la plateforme de supervision et de gestion à distance du MSP. Dans d'autres, elles doivent être achetées séparément, puis activées. Quoi qu'il en soit, avec SolarWinds, elles peuvent être gérées et automatisées rapidement et facilement, depuis un seul tableau de bord. Les MSP peuvent ainsi faire de la sécurité un élément essentiel de leurs offres informatiques de base (ou s'ils préfèrent, la proposer sous forme de module complémentaire à un prix attractif par appareil), et permettre à leurs clients d'avoir l'esprit tranquille grâce à des services de sécurité simples, performants et efficaces.

Les MSP peuvent ainsi faire de la sécurité un élément essentiel de leurs offres informatiques de base… et permettre à leurs clients d'avoir l'esprit tranquille grâce à des services de sécurité simples, performants et efficaces.

UNE SITUATION GAGNANTE POUR TOUS

En choisissant une approche multicouche, et en intégrant les fonctionnalités essentielles de sécurité dans leur offre de services informatiques gérés, les MSP sont en mesure de répondre aux principales attentes de leurs clients en matière de sécurité.

Les clients ont l'esprit libre : ils savent qu'ils courent moins de risques d'interruption d'activité liés à des menaces courantes et en constante évolution. Par ailleurs, des clients bien protégés permet de réduire le temps passé par les techniciens à résoudre des problèmes routiniers en matière de sécurité et à intervenir suite à des attaques. Lorsque les principaux contrôles de sécurité sont automatisés et facilement gérés, les techniciens sont en mesure de fournir un support à davantage de clients. Ils peuvent se concentrer sur des tâches à plus forte valeur ajoutée, répondant aux objectifs à long terme de l'entreprise. Les MSP développent leurs comptes, élargissent leurs services facturables et renforcent leurs relations avec leurs clients. À mesure qu'ils acquièrent plus d'expérience et de connaissances en matière de sécurité, ils offrent des services plus poussés et génèrent davantage de revenus récurrents.

Vous souhaitez en savoir plus sur la protection de vos clients ? Consultez le Security Resource Center de SolarWinds MSP afin de découvrir les dernières alertes de sécurité informatique, ainsi qu'une bibliothèque complète d'articles, de rapports et de livres blancs à propos des tendances et des problèmes de sécurité actuels.

SolarWinds est un acteur majeur dans l'offre de logiciels de gestion d'infrastructures informatiques performants et abordables. Nos produits permettent aux organisations du monde entier, quels que soient leur type, leur taille ou la complexité de leurs infrastructures, de superviser et de gérer les performances de leurs environnements sur site, dans le cloud ou hybrides. Nous travaillons en permanence avec tous les types de spécialistes des technologies—professionnels des opérations informatiques, professionnels DevOps, fournisseurs de services gérés (MSP)—afin de comprendre les défis auxquels ils font face pour maintenir la disponibilité et les performances de leurs systèmes à un niveau élevé. Destiné aux MSP, le portefeuille de produits SolarWinds MSP propose des solutions de gestion de services informatiques évolutives, fondées sur une sécurité multicouche, une intelligence collective et une automatisation intelligente. Ces produits sont conçus pour permettre aux MSP d'offrir des services informatiques externalisés très efficaces à leurs PME clientes, et de mieux gérer leur propre activité. Pour en savoir plus, consultez le site solarwindsmsp.com/fr.