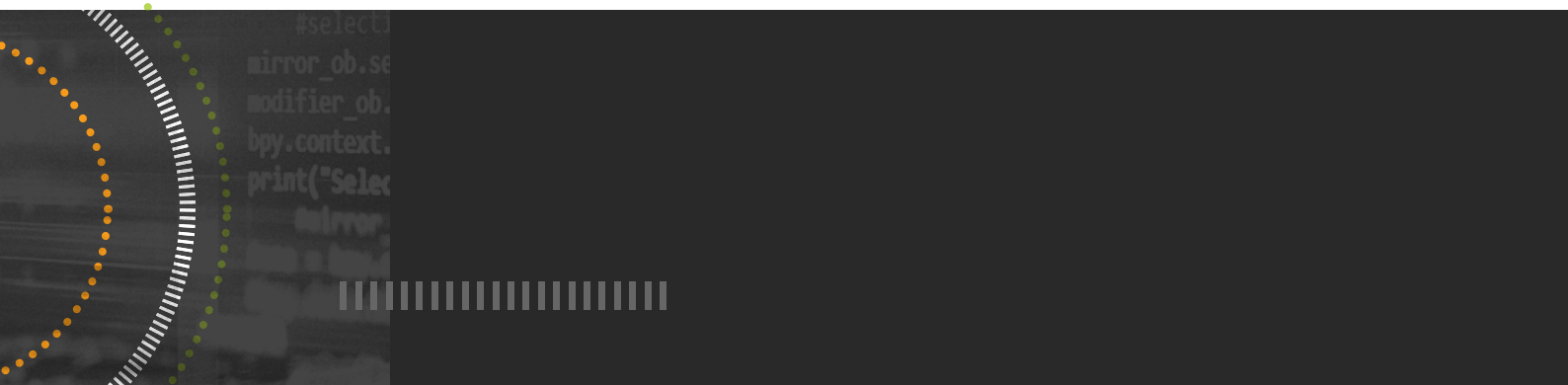
solarwinds msp

LIVRE BLANC

Plan de cybersécurité : édition 2020

Modèle en quatre étapes pour créer une offre de cybersécurité



Plan de cybersécurité : édition 2020

La cybersécurité est devenue une préoccupation majeure pour de nombreuses entreprises. Il y a plusieurs dizaines d'années, les virus étaient de simples nuisances (du moins dans la plupart des cas). Aujourd'hui, des sites Web se retrouvent hors ligne à la suite d'attaques par déni de service distribué (DDoS), des entreprises sont victimes de ransomwares et paient des sommes exorbitantes pour récupérer leurs données, des organisations de toutes tailles font la une des journaux pour des violations de données.

Le grand public est davantage sensibilisé aux cybermenaces, à l'importance de la protection et de la confidentialité des données. En réponse, la réglementation relative aux données s'est durcie—à la fois par secteur et par région. Parmi les nouvelles mesures, le Règlement Général sur la Protection des Données (RGPD) et le California Consumer Privacy Act (CCPA) fixent les règles à suivre par les entreprises en matière de gestion et de protection des informations.

Si vous êtes fournisseur de services informatiques, la prise de conscience du grand public et, par extension, les moyens mis en œuvre par les entreprises, vous ouvrent de nouvelles opportunités. Toutefois, pour faire face à la diversité des menaces actuelles (ransomwares, actes de malveillance en interne, menaces persistantes avancées...) et protéger vos clients, il est indispensable que vous adoptiez une approche de sécurité multicouche. À cela s'ajoute une gestion plus complexe de la sécurité des employés, liée à l'essor du télétravail.

Dans un tel contexte, par où commencer ? Quels outils employer ? Comment évaluer les besoins de vos clients ?

Cet eBook propose un modèle en quatre étapes pour fournir une sécurité multicouche aux clients de services gérés. Il présente une approche adaptée à l'ensemble des réseaux de vos clients (au vôtre également) et indique la marche à suivre pour mettre en place une cybersécurité efficace. Il vous permettra, en outre, d'identifier les besoins en formation de vos employés, ainsi que les outils et processus qu'ils doivent maîtriser.

Table des matières

Les quatre piliers d'une sécurité multicouche

Votre premier réflexe pourrait être de comparer les piliers d'une sécurité multicouche à des outils technologiques à mettre en œuvre pour lutter contre les menaces. Cependant, vous concentrer uniquement sur le déploiement d'outils individuels peut vous détourner de votre objectif global, qui consiste à élaborer une stratégie de cybersécurité cohérente. Bien que des technologies soient évoquées dans chaque section de cet eBook, les quatre piliers présentés correspondent aux quatre grands principes d'une stratégie de cybersécurité typique. En mettant l'accent sur ces concepts plus larges et sur les objectifs que vous souhaitez atteindre pour chacun d'eux, vous pouvez définir une offre de sécurité adaptée à la majorité des entreprises.

Il convient de noter que les technologies individuelles présentées dans chaque section peuvent intervenir à plusieurs niveaux. Par exemple, les outils EDR (Endpoint Detection and Response, détection et correction des menaces sur les points de terminaison) permettent de détecter les menaces et de faciliter la récupération.

1. Préparation

Le premier pilier d'une sécurité multicouche repose sur la supervision des appareils électroniques et de la sécurité physique des locaux de l'entreprise. Il implique de bonnes pratiques en matière de mots de passe et une supervision à distance. Cette couche de sécurité de base peut révéler des signes précurseurs de menaces et vous aider à stopper les attaques avant leur exécution. Sans elle, les défenses des autres piliers de sécurité ne pourraient être mises en œuvre.

2. Détection

Le second pilier comprend de nombreux outils et procédés considérés comme traditionnels : antivirus (AV) pour la détection des logiciels malveillants, technologie EDR pour la détection des menaces sur les points de terminaison au-delà des logiciels malveillants, gestion des mises à jour pour l'identification des logiciels sans correctifs, protection de la messagerie pour la détection des menaces entrantes transmises par e-mail. Ces outils ne sont pas suffisants pour couvrir tous les problèmes, mais ils contribuent à en résoudre un certain nombre.

3. Récupération et chiffrement

Une stratégie de défense doit permettre une récupération rapide en cas de catastrophe. Les deux premiers piliers de sécurité peuvent empêcher de nombreuses attaques, mais ils ne sont pas infaillibles. En mettant en œuvre des solutions de sauvegarde efficaces pour restaurer rapidement les systèmes, une authentification à deux facteurs pour récupérer les comptes et un chiffrement puissant pour empêcher l'accès non autorisé à la propriété intellectuelle, vous pouvez offrir à vos clients l'assurance qu'ils sont protégés contre le vol de données et les temps d'arrêt.

4. Analyse et gestion

Le dernier pilier d'une sécurité multicouche repose sur des stratégies de sécurité avancées ainsi qu'une gestion active. De nombreuses entreprises nécessitent une approche plus approfondie que celle proposée par les trois premiers piliers. Cette dernière phase comprend des tests d'intrusion, des systèmes de gestion des incidents et des événements de sécurité (SIEM) et des centres d'opérations de sécurité (SOC). Elle est souvent prise en charge par des fournisseurs de services gérés de sécurité (MSSP). Même si votre objectif n'est pas de devenir MSSP, il est important de connaître ces pratiques. Vous pouvez également vous associer avec un MSSP afin de fournir ces services avancés aux clients qui en ont besoin.

Avant de mettre en œuvre les pratiques et technologies de ces quatre piliers, il est nécessaire d'évaluer la situation de sécurité de chaque client. Nous vous recommandons d'initier une phase de découverte.

Découverte

Que vous commenciez à travailler avec un nouveau client ou que vous examiniez l'état de sécurité d'un client existant, commencez par faire le point sur les moyens de protection en place. Vous trouverez inévitablement des axes d'amélioration, qu'il s'agisse d'antivirus obsolètes, d'analyses inconstantes, de logiciels non mis à jour ou de sauvegardes inappropriées.

Parcourez cette liste de questions—elle vous aidera à construire votre plan de mise en œuvre des quatre piliers de sécurité multicouche.

Supervision

- Quelle solution de supervision générale de la sécurité utilisez-vous ?
- Surveillez-vous l'activité des utilisateurs ?
- Surveillez-vous les dispositifs de sécurité physiques ?
- Surveillez-vous les points d'accès ?
- Surveillez-vous les caméras IP ?

Gestion de la sécurité

- Quelle solution de protection des points de terminaison utilisez-vous ? Disposez-vous d'une solution EDR ? Si ce n'est pas le cas, utilisez-vous un antivirus ? À quelle fréquence effectuez-vous les analyses ?
- Une solution de gestion des mises à jour est-elle installée ? Si c'est le cas, à quelle fréquence mettez-vous à jour vos logiciels ?
- Disposez-vous d'une solution de sécurité de la messagerie ?
- Des paramètres de gestion des mots de passe sont-ils définis ?
- Possédez-vous une procédure complète en cas de départ d'un employé ?

Réduction des risques

- Un programme de gestion des données a-t-il été élaboré ?
- Testez-vous ce programme ?
- Surveillez-vous l'accès des utilisateurs aux données sensibles ?
- Devez-vous vous conformer à des réglementations particulières ?
- À quelle fréquence évaluez-vous votre sécurité ?

Gestion active et analyse

- L'accès des employés est-il limité à certaines données de l'entreprise et zones du réseau ?
- Un contrôle des contenus Internet est-il en place ?
- Formez-vous les employés sur les protocoles de sécurité ?
- Gérez-vous le réseau principal pour éviter toute activité malveillante ?
- Un système de basculement/redondance est-il configuré sur l'ensemble du réseau ?
- Votre entreprise dispose-t-elle d'un directeur technique/directeur de la sécurité en interne ou virtuel ?

Une fois que vous obtenez les réponses à ces questions, vous pouvez mettre en pratique notre modèle. Veuillez noter que ces questions ne sont qu'un point de départ, un examen plus approfondi est nécessaire. Par exemple, vous pouvez découvrir que la formation sur les protocoles de sécurité a lieu uniquement lorsqu'un nouvel employé ou nouveau groupe d'employés arrive dans l'entreprise. Dans ce cas, suggérez la mise en place de sessions de rappel sur une base régulière, de sorte que les employés révisent leurs acquis et mettent à jour leurs compétences sur les nouveaux processus.

Pilier 1 : préparation

Le premier pilier de sécurité consiste à poser les bases. Vous devez préparer votre environnement à limiter les vecteurs d'attaque possibles—et vérifier les mesures mises en œuvre régulièrement.

Tout d'abord, mettez en place des dispositifs de sécurité pour gérer l'accès physique aux bureaux et aux appareils. Par exemple, veillez à ce que seuls les employés en poste puissent entrer dans les locaux. Dressez l'inventaire des badges d'accès de sorte que lorsque des employés quittent l'entreprise, vous puissiez récupérer ces badges ou les désactiver.

Cela est également valable pour le matériel. De nombreux employés tentent de conserver leurs équipements (ordinateur portable, smartphone ou tablette) après avoir quitté leur entreprise. Une solution de supervision et gestion à distance (RMM) permet de garder la trace de chaque appareil grâce à un suivi d'inventaire. Même si vous ne pouvez pas récupérer un appareil après le départ d'un employé, vous pouvez utiliser votre solution RMM pour le verrouiller ou effacer les données qu'il contient, et ainsi éviter que votre ex-employé ne vole ou ne partage la propriété intellectuelle de l'entreprise. Cela est tout aussi important pour les employés qui travaillent à distance. Un équipement fourni par une entreprise est plus facile à dérober s'il n'est pas physiquement dans les bureaux. Assurez-vous donc de pouvoir effacer ces appareils à distance. Faire passer l'ordinateur portable d'un employé en télétravail en pertes pour une entreprise est une chose, subir une violation de données en est une autre.

Vérifiez ensuite la sécurité des webcams. Les pirates informatiques peuvent accéder à des webcams et espionner les employés—ou les réunions importantes en salles de conférence. Les menaces vont au-delà du simple espionnage ; les cybercriminels peuvent utiliser des webcams pour créer un botnet qui servira dans une attaque par déni de service distribué (DDoS). En résumé, surveillez vos webcams—elles constituent un point d'accès plus facile que vous ne le pensez.

Au-delà des webcams, veillez à configurer des mots de passe forts pour vos appareils IoT. Avec l'essor du télétravail, la surface d'attaque ne cesse d'augmenter. Chaque appareil connecté à un réseau domestique représente un point d'accès potentiel, qu'il s'agisse de thermostats, de téléviseurs ou d'enceintes connectés. Dès lors que ces appareils sont reliés au Wi-Fi, ils deviennent une porte d'entrée possible pour les cybercriminels. Recommandez aux utilisateurs de définir des mots de passe forts sur leurs appareils, et appliquez le même principe pour toutes les applications et portails Web d'administration associés.

En réalité, le bon réflexe serait de demander à tous les utilisateurs de configurer un mot de passe fort unique pour chaque compte important. Il conviendrait ensuite de configurer des demandes automatiques de renouvellement des mots de passe au minimum tous les 90 jours. Songez à vous équiper d'une solution professionnelle de gestion des mots de passe afin de veiller au respect des bonnes pratiques.

Tout cela nous conduit à un point essentiel : la supervision. Trouvez un outil RMM performant qui vous aide à superviser le trafic entrant et sortant de votre réseau d'entreprise—et qui englobe tous les points d'accès à Internet, y compris les pare-feu, les routeurs et les commutateurs. Surveillez l'ensemble des appareils connectés à Internet, tels que les webcams ou les imprimantes connectées au Web, afin d'identifier tout problème éventuel.

Il est également important de définir des stratégies pour la gestion des employés en télétravail. Vérifiez que ces utilisateurs ont installé un logiciel VPN pour accéder aux ressources de l'entreprise lorsqu'ils sont en dehors du bureau. Cela évitera qu'ils exposent le réseau principal de l'entreprise à une attaque potentielle. De plus, pour les utilisateurs distants qui souhaitent accéder aux systèmes critiques de l'entreprise, essayez de mettre en place une authentification à deux facteurs.

Enfin, souvenez-vous que ce premier pilier sert à poser les bases d'une sécurité efficace. Lors de cette phase, programmez l'installation des mises à jour, l'exécution des sauvegardes et la mise à jour des définitions de virus (si vous utilisez une solution antivirus) à une fréquence régulière, et ce pour tous les périphériques gérés.

Technologies associées au premier pilier

- Logiciel VPN
- Solution professionnelle de gestion des mots de passe
- Outil RMM pour une supervision approfondie et une gestion continue

Pilier 2 : détection

Le deuxième pilier de la sécurité porte sur vos capacités de détection. Lorsqu'une attaque parvient à franchir votre première ligne de défense, qu'il s'agisse d'un phishing ciblé, d'un logiciel malveillant ou d'un ransomware, vous devez être en mesure de la détecter rapidement et de l'arrêter sur-le-champ.

Pendant des années, les antivirus ont été utilisés en première ligne pour se protéger des cyberattaques. Les solutions antivirus restent évidemment utiles. Mais la plupart exécutent des analyses basées sur des signatures pour détecter, mettre en quarantaine ou supprimer les virus. Cela signifie que vous devez mettre à jour les signatures régulièrement, raison pour laquelle nous vous recommandions de programmer les mises à jour dans la section précédente.

La détection des menaces nécessite aujourd'hui une artillerie plus lourde. Les solutions EDR identifient les menaces qui vont au-delà des logiciels malveillants sur les points de terminaison. Au lieu d'une approche basée sur des signatures, les solutions EDR s'appuient sur l'intelligence artificielle et l'apprentissage automatique pour détecter les menaces au niveau des points de terminaison. Si un comportement suspect est identifié, une solution EDR peut signaler ce comportement ou agir automatiquement. Cela est particulièrement important dans les environnements actuels, car les cybercriminels changent leurs modes opératoires pour s'orienter vers des techniques de contournement et des attaques sans fichiers. Si vos clients préfèrent s'en tenir à un antivirus, ce choix sera plus confortable d'un point de vue budgétaire. Mais pour une détection complète, une solution EDR est recommandée.

Une solution EDR est d'ailleurs particulièrement utile lorsque des employés travaillent à distance. Ces employés se connectent à des réseaux offrant différents niveaux de sécurité (dont leurs réseaux domestiques). Une solution de protection des points de terminaison contribue à les protéger et à protéger le réseau de l'entreprise à plus grande échelle.

Une solution de gestion des mises à jour est également nécessaire. Même si la planification de correctifs réguliers a été mentionnée lors de l'étape précédente, assurez-vous de vérifier régulièrement votre solution RMM afin d'identifier les points de terminaison qui ne disposent pas des dernières solutions de sécurité. Au-delà du système d'exploitation, il est important de choisir une solution capable de gérer les mises à jour de logiciels tiers, en particulier celles des programmes connus pour leurs vulnérabilités, tels que les produits Adobe®, Java® et les principaux navigateurs Web.

Vous pouvez également réduire les menaces potentielles en installant une solution de protection de la messagerie. Les e-mails sont le principal vecteur d'attaques. Malheureusement, les options de sécurité natives de la plupart des solutions de messagerie ne suffisent pas. Appuyez-vous sur une solution de sécurité de la messagerie qui utilise la reconnaissance de modèles en temps réel et l'intelligence collective pour détecter les menaces. La sécurité de la messagerie peut garantir une protection contre les menaces les plus courantes. Une solution de sécurité de la messagerie performante doit inclure un antivirus et une protection efficace contre

les courriers indésirables. Certaines solutions s'appuient également sur l'intelligence collective pour aider les utilisateurs à se protéger des attaques actives.

La phase de détection nécessite beaucoup de maintenance active. Si vous gérez des milliers (ou des dizaines de milliers) de points de terminaison, la mise à jour d'un logiciel avec les derniers correctifs ou la maintenance des dernières définitions de virus peuvent rapidement devenir fastidieuses. Pour cette raison, nous vous recommandons de choisir des outils qui vous permettent d'automatiser autant de processus que possible.

Par exemple, une solution de gestion des mises à jour doit vous permettre de définir des règles, telles que lancer un téléchargement, exécuter une mise à jour et effectuer un redémarrage rapide chaque fois qu'un correctif de sécurité critique est disponible pour un système d'exploitation. Toute solution RMM standard propose un certain niveau d'automatisation, mais beaucoup offrent la possibilité de créer des scripts et même des capacités d'automatisation par glisser-déposer.

Technologies associées au deuxième pilier

- Antivirus (bien) ou solution EDR (mieux)
- Gestion des mises à jour pour les systèmes d'exploitation et les logiciels tiers
- Protection de la messagerie

Pilier 3 : récupération et chiffrement

Le troisième pilier de la cybersécurité est axé sur la récupération de compte, la récupération du système et la protection des données. Vos couches de défense précédemment mises en œuvre peuvent éviter de nombreux problèmes, mais elles ne sont pas infaillibles. Sans aller jusqu'au piratage, les erreurs des utilisateurs sont courantes et les catastrophes naturelles peuvent également entraîner des problèmes (allant du simple incendie électrique à l'inondation ou au tremblement de terre majeur).

Avant d'aborder cette étape, tenez compte des réglementations que vos clients sont tenus de respecter. Qu'elles dépendent d'un secteur comme la santé ou la finance, qu'elles relèvent du gouvernement ou découlent d'exigences régionales, comme le Règlement Général sur la Protection des Données (RGPD) ou le California Consumer Privacy Act (CCPA), des normes claires sont imposées et doivent être suivies par de nombreuses entreprises en matière de gouvernance des données. Vous devez vous familiariser avec ces normes si vos clients dépendent d'un secteur ou d'une région réglementés.

Même si cela devrait déjà avoir été fait en amont, demandez aux utilisateurs d'activer l'authentification à deux facteurs (2FA) sur leurs comptes et appareils. Il est possible qu'en dépit de vos recommandations, les utilisateurs se servent du même mot de passe pour tous leurs comptes. Si leurs comptes sont compromis dans un autre environnement, l'entreprise court un risque important. L'authentification à deux facteurs alerte les utilisateurs en cas de tentative d'accès à leurs comptes. De plus, elle permet de rationaliser le processus de réinitialisation des mots de passe

lorsqu'un compte est verrouillé et que l'utilisateur ne peut plus y accéder. Vous pouvez envisager de proposer un portail de réinitialisation des mots de passe en libre-service aux utilisateurs finaux afin d'alléger la charge de travail de votre équipe.

Définissez ensuite des règles pour encadrer l'installation de logiciels. Les employés installent souvent leurs propres programmes. Cela vous expose à des problèmes de sécurité et de responsabilité. Deux options s'offrent à vous :

1. Créer une liste noire de logiciels pour empêcher les employés de les installer sur leurs systèmes.
2. Bloquer toutes les installations de logiciels, sauf si elles sont approuvées et effectuées par un administrateur. Cette deuxième option implique davantage de gestion, mais le jeu peut en valoir la chandelle à long terme.

Évaluez ensuite la qualité des solutions de sauvegarde de vos clients. Choisissez de préférence une solution « Cloud-first ». Ces solutions ont recours à la déduplication, à la compression et à l'optimisation WAN pour vous permettre de sauvegarder les données dans le Cloud (puis de les restaurer) en toute simplicité. Les fenêtres de sauvegarde sont plus courtes, vous pouvez ainsi sauvegarder vos fichiers plus souvent sans devoir vous soucier de l'utilisation des ressources ni de l'interruption de l'activité. Cela vous permet de disposer de sauvegardes récentes en cas d'incident.

La plupart des solutions « Cloud-first » proposent également un système de sauvegarde sur site, sans pour autant devoir vous équiper d'un équipement de sauvegarde coûteux. Il vous suffit de créer une copie de sauvegarde sur le matériel à votre disposition, par exemple, une clé USB ou un disque dur externe. Ces solutions facilitent le respect de la règle de sauvegarde « 3-2-1 ».

Votre solution de sauvegarde doit vous donner la possibilité d'automatiser autant de processus que possible. Vous devez également pouvoir vérifier toutes vos tâches de sauvegarde à partir d'une seule console Web. Lorsqu'un problème survient, il est essentiel de vérifier les journaux système rapidement afin de s'assurer que des données n'ont pas été compromises. Cherchez une solution qui permette de sauvegarder les serveurs, les postes de travail et les documents professionnels importants à partir d'un seul tableau de bord. Vous gagnerez du temps dans le traitement de votre base clients.

Nous avons précédemment évoqué l'utilisation de solutions EDR pour détecter les menaces. Certaines solutions EDR sont également utiles dans le processus de récupération. Par exemple, après une attaque de ransomware, SolarWinds® EDR (basé sur la technologie SentinelOne®) peut automatiquement restaurer un point de terminaison à un état de sécurité connu, minimisant ainsi les perturbations pour l'utilisateur final. Au-delà d'une récupération rapide, SolarWinds EDR vous permet de comprendre ce qui n'a pas fonctionné et de corriger la vulnérabilité.

Un plan de reprise après sinistre doit par ailleurs être fourni. L'élaboration de ce type de plan peut faire l'objet d'un livre blanc à part entière, nous n'entrerons donc pas dans les détails ici. Notez cependant qu'un plan de reprise après sinistre doit couvrir à la

fois la récupération des données et des équipements, qu'il ne doit pas se limiter aux problèmes liés à la cybercriminalité, les catastrophes naturelles et l'erreur humaine ayant souvent un rôle majeur dans les incidents. Que vous fournissiez ce plan vous-même, que vous travailliez avec l'équipe informatique interne de vos clients ou que vous sous-traitiez cette tâche à un tiers, vos clients ont besoin d'un manuel décrivant les incidents les plus probables et les étapes à suivre pour assurer la continuité (et le déroulement normal) de l'activité.

La création d'un plan de reprise après sinistre peut prendre du temps et nécessiter un certain niveau de détail. N'hésitez pas à faire appel à une entreprise spécialisée pour offrir ce service.

Le troisième pilier de sécurité implique également de chiffrer les données sur tous les appareils. Certains clients penseront que ce n'est pas utile. Pourtant, le chiffrement permet de protéger les données si elles sont extraites d'un ordinateur portable, d'une tablette ou d'un smartphone volés par un utilisateur malveillant. Le chiffrement peut également s'avérer nécessaire dans le cadre de certaines obligations réglementaires. Une fois encore, vérifiez les lois applicables aux secteurs de vos clients.

Technologies associées au troisième pilier

- Solution de sauvegarde
- Outil EDR
- Authentification à deux facteurs
- Portail de réinitialisation des mots de passe
- Chiffrement des appareils

Pilier 4 : analyse et gestion

Le dernier pilier de sécurité porte à la fois sur la gestion quotidienne et l'analyse à long terme. Cette phase englobe de nombreuses tâches et de nombreux outils sophistiqués qui peuvent dépasser le domaine de compétences des MSP. Cependant, il est important de se familiariser avec ces outils et pratiques—et de sous-traiter certains aspects si nécessaire—afin de fournir des services complets à vos clients. Ces services relevant souvent du domaine des MSSP, vous pouvez vous associer avec l'un d'eux afin de proposer l'offre globale recherchée par vos clients.

Tout d'abord, équipez-vous d'un pare-feu plus puissant pour protéger vos clients. Une solution UTM (Unified Threat Management, gestion unifiée des menaces) vous fournira un pare-feu de qualité professionnelle ainsi que plusieurs technologies utiles telles qu'un antivirus, un anti-spam et une détection des intrusions sur le réseau.

Recherchez ensuite une solution SIEM (Security Information and Event Management, gestion des événements et des informations de sécurité). Une solution SIEM comprend à la fois une base de données de grande envergure et des outils avancés d'analyse des données pour vous aider à évaluer les tendances de sécurité. Les outils les plus performants proposent des outils d'investigation numérique (recherche et analyse de données), une « threat intelligence » qui signale les hôtes dangereux, une

surveillance des périphériques externes ajoutés (comme les clés USB) et même des rapports de conformité.

Si vous disposez d'une solution SIEM et des connaissances nécessaires pour l'exploiter, utilisez les données de cette solution pour bloquer les domaines et les sites Web malveillants que vous rencontrez. De nombreuses solutions de filtrage de contenu Web contiennent une liste par défaut de sites malveillants connus, dont l'accès est bloqué aux utilisateurs. Vous pouvez néanmoins personnaliser les règles définies et ajouter plus de sites à la liste—ou bloquer certaines catégories, telles que les réseaux sociaux ou les sites de jeux en ligne, afin que les employés restent productifs pendant les heures de travail. Les solutions de filtrage Web contribuent à protéger les utilisateurs de plusieurs problèmes majeurs, tels que les téléchargements furtifs, les sites de phishing et le détournement d'URL.

Ces systèmes peuvent néanmoins être complexes à prendre en main et à maintenir. Nous avions envisagé d'intégrer les outils SIEM dans le pilier « détection », mais leur mise en œuvre nécessite une analyse et une gestion actives, ainsi que des connaissances spécifiques. Il ne s'agit pas d'outils prêts à l'emploi comme les solutions EDR. De plus, l'analyse et le stockage des données requièrent des compétences spécialisées—ce qui signifie que ce niveau de service est souvent associé aux entreprises disposant de budgets de sécurité importants. Les menaces devenant plus coûteuses et plus fréquentes, de nombreuses entreprises de taille moyenne commencent à se tourner vers des fournisseurs SIEM.

Pour passer au niveau supérieur, proposez à vos clients les services d'un centre d'opérations de sécurité (SOC). La mise en œuvre d'un SOC nécessite généralement l'intervention de spécialistes de la sécurité. Ils offrent une surveillance des menaces 24 h/24 et 7 j/7 pour les incidents de cybersécurité et des recommandations de corrections pour les équipes chargées des réponses aux incidents. Ces services peuvent être excessifs pour de nombreux clients, mais certaines réglementations, telles que la norme PCI DSS, exigent la mise en place d'un SOC. Nous vous recommandons de vous associer à un MSSP offrant des services SOC si vous ne disposez pas des compétences en interne.

Enfin, des tests d'intrusion périodiques peuvent vous aider à préparer la sécurité. Un logiciel de tests d'intrusion vous aidera à simuler plusieurs scénarios d'atteinte à la sécurité. Ces tests permettent de voir comment les pirates informatiques parviennent à atteindre un objectif, qu'il consiste à accéder à des données sensibles ou à détruire un réseau. Vous pouvez vous appuyer sur les résultats pour corriger les vulnérabilités et renforcer votre sécurité. Il est utile d'exécuter ces tests au moins une fois par trimestre pour mettre à jour vos défenses.

Technologies associées au quatrième pilier

- UTM
- SIEM
- SOC
- Logiciel de tests d'intrusion

Les fournisseurs de services informatiques peuvent-ils se permettre de ne pas fournir de sécurité multicouche ?

Les cybercriminels ne sont pas voués à disparaître. Leurs méthodes deviendront de plus en plus pénalisantes à mesure qu'elles évoluent pour répondre aux nouveaux protocoles et aux nouvelles normes de sécurité. Les entreprises qui hébergent des données sensibles (en d'autres termes, pratiquement toutes les entreprises) seront toujours confrontées à un certain niveau de menace.

Quelles sont les conséquences pour l'avenir ?

La gravité des cybermenaces de ces dernières années conduit de nombreux fournisseurs de services informatiques à proposer des services de sécurité. Lorsque vos clients rencontrent un problème informatique (quel qu'il soit), ils s'adressent à vous, leur MSP, pour le résoudre. Peu importe que vos clients soient victimes d'une erreur humaine ou que leurs systèmes soient verrouillés à cause d'un ransomware, ils souhaitent simplement que leur problème soit résolu.

Pour la plupart des services proposés dans cet eBook, notamment la gestion des mises à jour, la détection et la correction des menaces sur les points de terminaison (EDR) et la sauvegarde, de bons outils de gestion et d'automatisation suffisent. Il s'agit de la cyber-hygiène de base, et tous les MSP doivent être en mesure de fournir ces services. Cependant, le contexte actuel des cybermenaces peut vous contraindre à proposer des services plus avancés, tels que ceux mentionnés dans le quatrième pilier. Fort heureusement, vous n'êtes pas obligé de faire cavalier seul : un partenariat avec un MSSP vous permettra de fournir ces services plus facilement.

Prendre plus de responsabilités dans le domaine de la sécurité peut vous sembler décourageant si vous n'êtes pas un fournisseur de services gérés de sécurité à part entière. Vous pouvez néanmoins suivre le modèle présenté dans cet eBook et développer progressivement votre stratégie de sécurité multicouche. En plus d'augmenter la satisfaction de vos clients, vous renforcerez leur confiance.

solarwinds msp

Pour en savoir plus, consultez le site ***solarwindsmsp.com/fr***

SolarWinds (NYSE:SWI) est un acteur majeur dans l'offre de logiciels de gestion informatique performants et abordables. Nos produits permettent aux organisations du monde entier, quels que soient leur type, leur taille et leur complexité, de superviser et de gérer leurs services, infrastructures et applications informatiques sur site, dans le Cloud ou hybrides. Nous travaillons avec les spécialistes des technologies — professionnels des opérations et des services 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 infrastructures et applications informatiques 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 leurs propres activités.

© 2020 SolarWinds MSP Canada ULC et SolarWinds MSP UK Ltd. Tous droits réservés.

Les marques de commerce SolarWinds et SolarWinds MSP sont la propriété exclusive de SolarWinds MSP Canada ULC, SolarWinds MSP UK Ltd. et de leurs filiales. Toutes les autres marques de commerce citées dans ce document appartiennent à leurs propriétaires respectifs.

Ce document est fourni à titre d'information uniquement. SolarWinds n'offre aucune garantie expresse ou implicite et n'assume aucune responsabilité légale quant à l'exactitude, l'exhaustivité ou l'utilité des informations contenues dans ce document.