avast business
powered by AVG and Avast

Briser le lien entre les utilisateurs et les cybermenaces

Les utilisateurs insouciants, les e-mails infectés et les sites web non sécurisés ou détournés représentent une menace pour les PME. Découvrez comment une Passerelle Web sécurisée peut arrêter les cybermenaces à la source.

IDG CONNECT

GUIDE

Quel est le problème ?

Selon un **rapport**, les cybermenaces sont financièrement plus nuisibles pour les PME (Petites et moyennes entreprises) que les risques d'incendies, d'inondations et de grèves de transport combinés. Cela indique à quel point les cybercriminels considèrent aujourd'hui les PME comme des cibles faciles et lucratives. Alors que la grande majorité des failles de cybersécurité signalées au cours des 18 derniers mois concernaient de grandes entreprises connues à travers le monde, notamment Facebook, Equifax et British Airways, ce sont les PME qui sont de plus en plus ciblées.

Selon une **étude** réalisée par l'institut Ponemon, trois PME sur cinq ont subi une cyberattaque au cours des 12 derniers mois et **une sur trois pense** ne pas être en mesure de se défendre contre une attaque. **Le rapport d'enquête relative aux violations de données** 2018 de Verizon affirme que les PME représentent 58 % des victimes d'attaques de malwares aux États-Unis. Peu de PME ont mis en place des mesures de cybersécurité impénétrables, et les conséquences d'une attaque peuvent être dévastatrices en termes de pertes financières et de réputation.

Selon la Barclays Bank, la fraude cybercriminelle commise contre les PME coûte en moyenne 40 000 euros par entreprise et a causé la perte de 50 000 emplois. Les statistiques sont accablantes et la pression pesant sur les PME pour se défendre contre les menaces en ligne ne fait qu'augmenter. Empêcher les cyberattaques doit être une priorité, mais récemment, la prolifération de sites web infectés utilisant des tactiques SEO (optimisation par moteur de recherche) pour appâter les employés peu méfiants est devenue préoccupante. Les **campagnes d'intoxication SEO** sont de plus en plus sophistiquées dans leur méthodologie.

En migrant vers les réseaux basés sur le cloud, en utilisant des applications numériques, des sites de réseaux sociaux à des fins publicitaires et de formation, des moteurs de recherche pour effectuer des recherches, des diffusions et de la communication en direct, les PME ouvrent une porte potentielle d'accès au réseau de l'entreprise. Un recours croissant au cloud, pour simplifier les opérations et permettre la mobilité, pose également un nombre de défis de sécurité causés par le BYOD (Bring your own device) et les nouvelles techniques d'ingénierie sociale qui dupent les internautes pour qu'ils cliquent sur des sites frauduleux. Mettre fin à ce phénomène devient une priorité.

Contrairement aux grandes entreprises, les PME ne disposent que rarement des ressources nécessaires pour s'équiper de solutions complexes (appareils, logiciels,pare-feu, etc.) afin de contrôler tout le trafic néfaste ou les requêtes provenant de sites malveillants. Il y a aussi le problème du personnel. Sensibiliser et former le personnel demande du temps et des ressources. Un **article** affirmait l'an dernier que la sensibilisation et la vigilance du personnel sont les enjeux clés pour se protéger des attaques. Sept entreprises sur dix pensent que les employés des PME responsables de la cybersécurité font bien leur travail, mais peu d'entre elles dispensent des formations en cybersécurité (20 % des PME) ou disposent de stratégies de cybersécurité (27 %). Un consultant américain a récemment découvert que les comportements sont un problème, affirmant dans son **rapport** que 51 % des dirigeants de petites entreprises déclarent ne pas penser que leur entreprise soit une cible pour les cybercriminels.

Un fait intéressant dans ce rapport est que les sondés admettent utiliser largement les réseaux Wi-Fi et ne pas changer les mots de passe pendant plus d'un an. Penser que les petites entreprises sont invisibles aux yeux des pirates n'est pas seulement erroné, c'est aussi une menace pour la viabilité future de ces entreprises, notamment avec les amendes sanctionnant le manque de protection des données. C'est justement sur ce point que parient les pirates, cette complaisance.

Comme le **suggère** l'entreprise d'analyse de données Fico, 2019 a été déclarée « Année de la cyber-insécurité : 52 semaines au cours desquelles les entreprises de toutes tailles et de tous domaines vont découvrir un nouveau degré de peur, et parfois de panique, en réalisant leur vulnérabilité face aux violations de données, au piratage et autres crimes informatiques. »

Comment les revendeurs et les fournisseurs de services peuvent-ils aider leurs clients PME à améliorer la sécurité, alors que si peu d'entre eux dispensent des formations adéquates à leur personnel ? Comment les aider à implémenter des stratégies, gérer des appareils, et se préparer à toutes les éventualités ?

Nous pensons qu'il y a là une grande opportunité.

Quelles sont les principales menaces ?

- **Ransomware** – Selon l'Évaluation des menaces du crime organisé sur Internet (IOCTA, Internet Organised Crime Threat Assessment) réalisée par Europol, le ransomware provenant du phishing était un problème majeur en 2018 et restera prédominant en 2019.
- **Spear phishing** – L'ENISA rapporte que le nombre d'attaques de phishing/ spear phishing contribuait largement au nouveau record de violations enregistré en 2018.
- **Activités basées sur le cloud** – l'accès à distance au réseau depuis des cafés, des aéroports et même depuis chez soi peut représenter une menace si les appareils ne sont pas gérés.

La Passerelle Web sécurisée : Cinq raisons d'être idéale pour les PME

Gartner prévoit que 50 % des campagnes de malwares en 2019 utiliseront un type de chiffrement pour dissimuler la diffusion, l'activité de commande et de contrôle ou l'exfiltration de données. Les PME ont besoin de plusieurs couches de sécurité, mais en implémentant une couche principale telle que la Passerelle Web sécurisée (SWG, Secure Web Gateway), les PME peuvent se protéger de leur source, le réseau Internet. Elle aidera les PME à résoudre leurs problèmes de sécurité les plus urgents. Voici quelques avantages clés :

1. **Protection totale à une vitesse maximale –** Protéger tous les appareils à l'intérieur du réseau et les ordinateurs portables à domicile, à l'hôtel, à l'aéroport, ou au café. SWG offre la sécurisation des appareils gérés partout sur le réseau, et les ordinateurs portables et de bureau sous Windows en dehors du réseau. La passerelle recherche des DNS intoxiqués, des liens de phishing, les téléchargements et les sites web infectés avant que le trafic Web n'atteigne le réseau. Elle utilise des recherches basées sur le DNS, qui prennent moins de 2 millisecondes, de sorte qu'elles ne ralentiront pas votre réseau comme les appareils et les serveurs proxy. Le trafic réseau des employés et des utilisateurs à distance est automatiquement dirigé vers le DNS le plus proche, délivrant les meilleures performances.
2. **Facile à mettre en place** – Basé sur le cloud et facile à déployer et à gérer. Prend quelques minutes à mettre en place et configurer.
3. **Facile à utiliser** – Une console simple, centralisée offrant une visibilité globale des ressources. Cela signifie que les PME peuvent avoir une vue d'ensemble de tous les appareils sur le réseau, et alerter à propos de menaces potentielles.
4. **Apprentissage en temps réel** – De nouveaux sites malveillants émergent tous les jours mais la SWG y est préparée en analysant et en apprenant constamment, mettant en sandbox tous les exécutables qui nécessitent une analyse approfondie.
5. **Conçue pour les PME** – La SWG est spécialement conçue pour les PME, offrant une sécurité qui va du terminal jusqu'au réseau. Toutes les PME ne disposaient pas des ressources requises pour déployer des cyberdéfenses sophistiquées, jusqu'à maintenant.

Aperçu des fonctions clés

- **Terminaux intégrés et sécurité Web** – Bloque les téléchargements malveillants et empêche les URL malveillants connus d'accéder au réseau.
- **SSL Intelligent** – Effectue des analyses intelligentes à grande vitesse du trafic SSL, pourtant difficile à inspecter, avec seulement une microseconde de délai.
- **Sandbox Cloud** – Analyse les fichiers et URL suspects dans un environnement virtuel pour détecter le contenu malveillant caché pour tous les fichiers EXE et le trafic DLL.
- **Proxy intelligent** – Inspecte, catégorise et classe un site inconnu suspect en un bon ou mauvais site connu. Vous pouvez ajouter facilement des URL aux listes de blocages/d'autorisations.
- **Filtres de contenu** – Ils vous permettent de choisir, parmi plus de 90 catégories, le niveau de filtrage de contenu que vous souhaitez imposer aux utilisateurs de l'entreprise.
- **Point unique** pour une gestion simple et centralisée.

Ajouter de la valeur pour les fournisseurs de services informatiques

La Passerelle Web sécurisée porte la sécurité par couches à un nouveau niveau dans la plate-forme CloudCare. À partir d'un tableau de bord unique basé sur le cloud, les partenaires peuvent sécuriser à distance de nombreux clients et fournir des services facturés à l'utilisation qui améliorent leur protection et décuplent les marges et les profits.

La Passerelle Web sécurisée est une grande opportunité pour les revendeurs et les fournisseurs de services gérés pour :

- **Ajouter une autre couche de sécurité** pour que les clients se défendent contre le risque croissant de ciblage des PME par les cybercriminels. Cela signifie un nombre réduit d'incidents de sécurité à gérer et une confiance consolidée de la part des clients.
- **Se libérer de la gestion des appareils** et délivrer des solutions de sécurité sur mesure, permettant aux clients de bénéficier d'une cybersécurité sophistiquée quel que soit leur budget.
- **Moduler facilement l'ajout ou le retrait d'utilisateurs** tout au long de l'évolution d'un client, assurant la sécurité et la satisfaction des clients lorsque changent leurs besoins.
- **Augmenter les revenus mensuels récurrents (RMR)** avec une nouvelle offre de sécurité en tant que service (SaaS), qui augmente la rentabilité mais aussi les relations et la fidélisation des clients.
- **Délivrer une sécurité gérée à distance** – besoin moindre d'envoyer des experts coûteux sur le terrain

Le mot de la fin : Solution de cybersécurité de qualité professionnelle entièrement évolutive, qui fournit une protection optimale contre les menaces Web sans la complexité et le surplus de serveurs proxys ou de systèmes locaux.

Nous avons une sécurité des terminaux, alors pourquoi les clients ont-ils besoin de SWG ?

Les systèmes locaux sont d'une efficacité limitée. Les PME ont besoin d'une approche par couches pour assurer leur protection, ce qui signifie plus d'opportunités pour les partenaires.

Quel est le problème des systèmes locaux ?

- Le problème est que les systèmes locaux ont une isolation inadéquate. Les employés à distance peuvent contourner les systèmes locaux et les menaces avancées ne seront pas détectées.
- Et de plus, ils ralentissent tout Étonnamment, 90 % des PME désactivent les inspections SSL à cause d'importantes latences.

About Avast Business

Avast Business provides easy-to-manage, enterprise-grade security and network management solutions for SMBs and IT service providers. Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes securing, managing, and monitoring complex, ever-changing IT environments easy and affordable. The result is superior protection that businesses can count on.

For more information about our managed services and cybersecurity solutions, visit **www.avast.com/business**.