Guide Enjeux & Perspectives

Gestion & Sécurité Office 365 : enjeux, perspectives et mise en œuvre

Principal vecteur de menaces, l'email est à l'origine de presque toutes les brèches. Un problème accru par Office 365 et sa multiplicité d'accès aux courriers et données de l'entreprise. Cisco Email Security pour Office 365 permet de retrouver contrôle et sérénité en renforçant la sécurité de la messagerie.

L'email est redevenu le talon d'Achille de la sécurité des entreprises. Les sécurités intégrées de Windows 10 et l'usage croissant d'applications SaaS ont, en partie, protégé les utilisateurs contre d'autres formes d'attaque et rendu plus difficile le travail des cybercriminels.
Mais elles ont, parallèlement, redonné à l'email toute sa puissance dévastatrice. 90% des pénétrations dans les systèmes d'information et de vol de données trouvent, aujourd'hui, leur origine avec un email.

Un vecteur de menaces protéiformes

Les attaques par courrier électronique se sont complexifiées. Terminées les grandes campagnes d'emailing identiques à destination de millions d'inconnus connectés. **Les attaques sont, aujourd'hui, ciblées** : elles visent, par exemple, les visiteurs d'un salon à venir, les employés des hôtels et restaurants, les collaborateurs d'une entreprise donnée, les clients d'un service, d'un opérateur ou d'une banque, etc.
Le contenu de l'email est, savamment, conçu, parfois même par des psychologues, pour amener l'utilisateur soit à cliquer un lien dans l'email, soit à ouvrir une pièce attachée :
* Le lien peut conduire à une page de phishing (un site factice qui a tous les atours du site authentique) pour tenter de dérober les identifiants de l'utilisateur sur le service ciblé (iCloud, Gmail, Office 365, OneDrive, Box, Dropbox, Paypal, etc.). Il peut, parfois, pointer vers une page malveillante qui contient du code caché pour analyser les vulnérabilités de l'ordinateur de l'utilisateur et tenter d'en percer les défenses.

* La pièce attachée peut contenir un document Word, Excel, PowerPoint ou PDF contenant soit un lien à cliquer (on retombe, alors, dans le cadre précédent), soit du code malveillant convoyant un logiciel espion (qui va espionner vos activités et saisies) ou un rançongiciel (qui va prendre en otage les données de l'utilisateur voire l'accès à l'ordinateur).

Une ingénierie sociale au service des cybercriminels

Toute la force de ces attaques est de se présenter comme des emails crédibles et non douteux : par exemple, un email provenant d'un collègue avec lequel on travaille souvent, ou un email intitulé « confirmation de réservation » à destination de la réception d'un hôtel, ou alors intitulé « facture en pièce jointe » en visant un employé du service commercial. L'imagination des cybercriminels, en la matière, est sans limites.

L'ingénierie sociale derrière la genèse de telles attaques définit des messages crédibles et des codes couleur alignés sur l'effet recherché : confiance, peur, urgence, etc. Les emails sont rédigés dans la langue de l'utilisateur avec des traductions de qualité (et non du simple Google Translate reconnaissable à vue d'œil, comme cela était souvent pratiqué autrefois). **Les mêmes techniques peuvent être utilisées pour des actions plus perverses encore que le vol d'identifiants ou l'infection des machines.** Typiquement, elles peuvent être adaptées pour amener des employés à déclencher des virements ou des transferts de fonds vers des comptes pilotés par des cybercriminels (attaque BEC).

L'Internet Crime Complaint Center (IC3) estime à 5,3 milliards de dollars le montant extorqué aux entreprises par ce biais entre octobre 2013 et décembre 2016. Des techniques similaires sont, aussi, exploitées pour amener certains utilisateurs à dévoiler des informations ou des documents à caractère hautement confidentiel à des destinataires mal intentionnés.

Se protéger d'attaques aussi sophistiquées est devenu complexe. Même avertis et formés, les utilisateurs peuvent à tout moment se laisser piéger. Inattention, maladresse, validation dans la précipitation sont des comportements humains dont les cybercriminels savent tirer profit…

Dans un tel contexte, les utilisateurs sous Office 365 constituent des cibles privilégiées puisque les cybercriminels connaissent leur attachement à l'email, leur utilisation des outils bureautiques Microsoft, leur habitude d'être face aux écrans d'authentification d'Office, OneDrive, etc.

Des solutions simples et immédiates

Les entreprises ne sont, heureusement, pas totalement démunies face à de telles attaques. Office 365 est, certes, un logiciel SaaS, hébergé dans le Cloud et opéré par les équipes de Microsoft, il est aussi - et peut-être avant tout - une vraie plateforme ouverte et extensible.

Une opportunité que des acteurs majeurs de la sécurité comme Cisco peuvent mettre à profit pour y greffer de nouvelles solutions originales et innovantes. Également hébergées dans le Cloud, ces solutions ne nécessitent aucune infrastructure interne et aucun investissement d'infrastructure.

Détecter les attaques…

La solution Cisco Email Security pour Office 365 s'appuie à la fois sur l'analyse de milliers d'emails, sur des techniques innovantes à base de Machine Learning, sur l'intelligence collective du Cisco Threat Grid, et sur la compétence des experts de Cisco Talos, une des plus importantes équipes mondiales de chercheurs en cybermenaces.

Ces derniers fournissent de nouvelles mises à jour de sécurité toutes les 5 minutes en moyenne.

L'association de ces technologies et compétences procure à cette solution **une rare aptitude à identifier les menaces inconnues et les transformations de fichiers.** Des filtres et analyseurs réalisent une inspection approfondie des liens présents dans les emails et les pièces attachées pour remonter jusqu'à la menace et la détecter.

Ils évaluent en temps réel tous les liens afin de détecter les sites compromis qui, soudainement, passent d'un statut sain à un com-

portement malveillant. Des techniques FED (Forged Email Detection), qui cherchent à comprendre la formulation des courriers ainsi que la validité des expéditeurs et des adresses de réponses, détectent les attaques de « spear phishing » y compris celles les plus élaborées réalisées non pas au travers d'un seul email, mais d'une succession d'envois.

Les stopper en amont

L'objectif premier de toutes ces techniques avancées de détection est d'être en mesure de stopper **les attaques utilisant des liens Web compromis ou des pièces dangereuses** non seulement avant qu'elles n'atteignent la boîte de réception des utilisateurs de l'entreprise, mais également avant que ces menaces ne se propagent à vos partenaires et clients.

La solution multiplie les boucliers pour contrer phishings, attaques BEC, malwares, mais aussi le spam et la saturation des boîtes email par des courriers inutiles, synonymes de pertes de temps et de productivité en berne.

Empêcher les fuites

Cisco Email Security pour Office 365 ne se focalise pas, uniquement, sur les emails entrants. Différents boucliers assurent, également, un contrôle des emails sortants, à commencer par une surveillance comportementale afin de détecter les comptes compromis.

Une analyse et une limitation des flux sortants sont, aussi, appliquées afin d'éviter l'utilisation des ressources de l'entreprise pour la diffusion de spams qui, non seulement, nuisent à l'image de l'entreprise auprès des clients et partenaires, mais font aussi courir le risque de voir le domaine de l'entreprise blacklisté (ce qui pourrait conduire à la perte de prospects et de contrats juste par l'interruption des échanges).
Cisco a, également, intégré **sa technologie DLP (Data Leak Prevention) qui analyse contenus, contextes et destinations des emails** pour identifier les éventuelles fuites d'information, qu'elles soient accidentelles ou volontaires.
L'entreprise peut même, précisément, contrôler qui est accrédité pour transmettre tel ou tel type d'information. Plus de 100 règles prédéfinies accélèrent la mise en œuvre du bouclier antifuite et le respect des directives de conformité.

Agir et remédier

Détecter et bloquer sont deux étapes essentielles, mais elles ne suffisent pas à assurer une messagerie 100% sécurisée. Dès qu'un malware, une attaque de phishing ou une URL malveillante est détecté, l'entreprise a, non seulement, besoin de comprendre l'impact de cette attaque, mais également de mesurer son ampleur et y remédier rapidement.

Les mécanismes de réponses automatiques de Cisco Email Security évitent aux équipes IT de coûteux temps d'investigation et de réparation des dégâts. **Grâce à l'autoremédiation rétrospective des boîtes email, les menaces sont automatiquement nettoyées à l'échelle de l'entreprise.**

Des analyses de réputation dynamiques donnent davantage de visibilité sur l'origine des malwares et des menaces ainsi que sur les systèmes et boîtes affectés.

Cette autoremédiation s'applique, également, aux techniques DLP : outre, le simple blocage ou la notification de l'utilisateur, elle propose soit de mettre l'email anormal en quarantaine, soit de le chiffrer, soit d'envoyer des copies carbone à des personnes accréditées, soit d'ajouter simplement des « disclaimers » en fin de mails (notamment lorsque l'email ne divulgue pas d'informations confidentielles, mais doit comporter des éléments impératifs pour respecter une législation).

Un déploiement quasi instantané

La force première de la solution proposée par Cisco, c'est la simplicité de sa mise en œuvre.

Il suffit de rediriger le domaine MX pour que le courrier de toute l'entreprise soit intégralement protégé en quelques minutes. Cisco Email Security pour Office 365 est disponible sous forme d'abonnement et accessible à tous les profils d'entreprises à partir de 100 boîtes aux lettres.
Plusieurs options de déploiements sont proposées. La plus simple consiste à se reposer, intégralement, sur le service Cloud en mode SaaS. Toutefois, les entreprises aux contraintes particulières peuvent opter pour un déploiement local « on-premises » sous forme d'appliance. Elles peuvent, aussi, choisir un déploiement hybride dans lequel les emails les plus critiques et sensibles sont supervisés en local avec des filtres renforcés, le reste étant protégé via le Cloud.

Quelle que soit la forme de déploiement adoptée, les fonctionnalités restent identiques et le niveau de protection maximal.

Bien évidemment, quelle que soit l'option choisie, les utilisateurs sont protégés sur tous les appareils qu'ils utilisent pour accéder à leurs emails, qu'il s'agisse d'ordinateurs contrôlés par l'entreprise, de notebooks personnels autorisés par l'entreprise en mode BYOD, de smartphones, de tablettes, d'accès Web depuis des terminaux d'hôtels.

Au final, on retiendra que l'adoption d'Office 365 n'engendre pas de perte de contrôle et de sécurité pour les entreprises dès lors qu'elles s'équipent de solutions de protection spécialement pensées pour le service cloud de Microsoft.

Cisco Email Security pour Office 365 permet de retrouver de la sérénité, de l'efficacité, du contrôle et de la visibilité tout en profitant de l'agilité et de la fluidité opérationnelle du Cloud.

Insight, l'accompagnement avec un partenaire expert de confiance

Mieux vaut ne pas s'aventurer seul.
Une stratégie de sécurité performante nécessite expériences et compétences et ne laisse aucune place à l'improvisation. Pour mieux accompagner ses clients, Insight a mis en place des pôles de compétences reconnus et s'appuie sur son équipe d'experts, afin de former, délivrer et déployer Office 365 chez ses clients.

Insight propose une offre de services gérés pour Office 365 réduisant ainsi les contraintes associées à la prestation d'une assistance pour les outils de productivité Microsoft.

« Des partenaires comme Insight sont essentiels pour s'assurer que les clients comprennent bien toute la richesse de l'offre, puissent mettre en œuvre cette richesse et bénéficient d'un accompagnement personnalisé ».

Insight offre les conseils et les expertises indispensables pour sélectionner, mettre en œuvre et gérer des solutions technologiques complexes afin d'atteindre les objectifs des entreprises. Grâce au réseau international, à ses partenaires, services et solutions, Insight aide les organisations à fonctionner plus efficacement.

Découvrez-en plus sur https://fr.insight.com

Conception éditoriale & réalisation : Agence COM4MÉDIAS www.com4medias.com - crédit photos : Shutterstock