IDC Analyst Connection

Commandé par :
Vade Secure

Auteur: Konstantin Rychkov

Janvier 2019

Sécurité de l'email : maintenir une protection de haut niveau après la migration vers Office 365

Introduction

La communication et la collaboration sont devenues les pierres angulaires du monde du travail. Mêlant intervenants internes et externes, elles imposent le recours à des solutions souples, conviviales et à même d'assurer la continuité des échanges. Dans tous les secteurs, les plateformes de collaboration et autres outils de messagerie montent en puissance. Pour autant, l'email reste incontestablement le moyen de communication numérique le plus utilisé par les entreprises. En effet, 3,7 milliards de personnes y ont recours, soit plus de la moitié de la planète. Malheureusement, cette popularité fait également de l'email le premier vecteur d'attaque utilisé par les cybercriminels. La raison en est simple et explique également les difficultés que rencontrent les professionnels à sécuriser ce moyen de communication : les utilisateurs accordent une grande confiance au contenu de leur boîte aux lettres. Cette confiance doit reposer sur une sécurité robuste. De nos jours, les infrastructures se tournant toujours plus vers le Cloud, cela signifie quitter les contrôles périmétriques classiques pour adopter des modèles de protection continue sur plusieurs niveaux permettant la détection, mais également la revérification des emails, ainsi que la neutralisation des menaces émergentes.

Vade Secure a interrogé à ce sujet Konstantin Rychkov, responsable de recherche pour IDC European Security Solutions.

Q. L'adoption de la messagerie électronique dans le Cloud - et d'Office 365 en particulier - a-t-elle atteint un point critique, en particulier pour les menaces de cybersécurité ?

R. L'email est le principal moyen de communication utilisé par les entreprises et est devenu indispensable. Le Cloud a permis aux entreprises d'alléger le fardeau pesant sur les équipes informatiques internes en matière de maintenance des serveurs locaux et d'offrir plus de souplesse, d'évolutivité et d'efficacité opérationnelle, tout en réduisant les coûts. Ces raisons expliquent la croissance des dépenses liées à l'email dans le Cloud dans le monde entier : de 22,9 % en 2013, nous sommes passés à 68,4 % en 2018 (80,4 % aux États-Unis et 59,6 % en Europe occidentale). Nous arrivons en effet à un tournant.

Les données d'IDC confirment qu'Office 365 et les applications de messagerie proposées par Microsoft en général sont les plus populaires auprès des entreprises. Elles représentent 54 % du marché des applications de messagerie et 47,6 % des déploiements dans le Cloud au cours du premier semestre 2018 dans le monde.

C'est en 2016 que le Cloud a dépassé les 50 % des nouveaux déploiements, mais IDC prévoit que ce chiffre atteindra 89,4 % en 2022, pour un marché représentant

6,3 milliards de dollars. Les solutions de Microsoft et de Google sont les moteurs de cette croissance. Cette normalisation des plateformes entraîne inévitablement un intérêt accru de la part des cybercriminels et une hausse des risques liés aux déploiements mal pensés. Bien entendu, ce n'est pas pour autant que les entreprises doivent bloquer ou annuler leurs projets de migration. Au contraire, la migration vers le Cloud leur offre l'occasion de réévaluer leur architecture de sécurité de l'email et d'optimiser ainsi la continuité de l'activité.

Q. Comment les attaques sur les messageries électroniques évoluent-elles pour s'adapter aux environnements de type Office 365 ?

R. Au cours des dernières années, les emails sont restés le principal vecteur des attaques : 80 % des attaques commencent par l'envoi d'un email. Le phishing demeure le type d'attaque le plus courant, mais la popularité grandissante du Cloud multiplie les possibilités offertes aux hackers. Par ailleurs, les attaques sont de plus en plus sophistiquées, que ce soit sur le plan du code malveillant utilisé ou de la préparation. Ainsi, dans la droite lignée des attaques de type BEC (Business Email Compromise), on observe une augmentation des usurpations de l'identité de personnes intérieures ou extérieures à l'entreprise.

Les approches classiques reposent sur la protection de la passerelle, qui forme à la fois un point d'entrée et de défense unique. Pour les plateformes dans le Cloud, comme Office 365, cette architecture de sécurité est problématique. En effet, une fois qu'ils ont contourné la passerelle, les hackers ont non seulement accès aux emails, mais aussi aux applications, ce qui leur permet de consulter les données, les fichiers et les contacts qu'elles contiennent. Les emails professionnels hébergés dans le Cloud peuvent ainsi constituer une cible très lucrative.

Comme je l'ai mentionné précédemment, les usurpations d'identité par email montent en puissance. Les données de Vade Secure montrent même que Microsoft est la marque la plus utilisée dans les attaques de phishing depuis trois trimestres consécutifs[1]. Les cybercriminels commencent par se procurer des identifiants Office 365 (ou ceux d'une autre plateforme), puis analysent et imitent les échanges internes ou externes (avec des partenaires et clients) de l'entreprise. Ces attaques en plusieurs phases visent un gain financier direct par le biais de virements bancaires ou du paiement de factures sur des comptes détenus par les malandrins. Un rapport de la SEC (Securities and Exchange Commission américaine) explique ainsi qu'une attaque de ce type a permis le déclenchement de 14 virements sur plusieurs semaines, pour un coût de plus de 45 millions de dollars, une somme que l'entreprise victime ne récupérera jamais[2].

Q. La sécurité native d'Office 365 offre déjà une protection suffisante. Pourquoi adopter un outil de sécurité supplémentaire ?

R. Depuis quelques années, Microsoft procède à des investissements massifs dans ses fonctions de sécurité, et il est tout à fait correct de dire que les protections

[1] https://www.vadesecure.com/fr/classement-phishers-favorites-microsoft-domine-toujours-le-classement/
[2] https://www.sec.gov/litigation/investreport/34-84429.pdf

intégrées dans les messageries sont efficaces. Malheureusement, les fonctions natives d'Office 365 et d'Exchange Online Protection (EOP) sont principalement conçues pour filtrer le spam et intercepter les malwares connus. Les techniques anti-spoofing par authentification composite (combinaison des protocoles SPF, DKIM et DMARK) ne sont disponibles que pour la version E5 d'Office 365 et ATP, même si certaines de ces fonctions sont également proposées dans EOP depuis fin 2018[3].

Les solutions basées sur la réputation sont redoutablement efficaces contre les menaces connues, mais la sophistication croissante des attaques visant les messageries impose d'adopter une défense sur plusieurs niveaux permettant de neutraliser les menaces inconnues, les attaques très dynamiques et les usurpations d'identité de type BEC. Cette dernière technique permet d'attaquer l'entreprise sous de nouveaux angles. Ainsi, si l'analyse des emails internes était un bonus dans le cadre d'un environnement sur site, elle est absolument indispensable dans le Cloud

Les filtres de sécurité de l'email dans le Cloud d'Office 365 et G-Suite, les deux plateformes de messagerie dans le cloud les plus utilisées (et de loin), sont robustes, mais pas infranchissables. De plus, les hackers multiplient les stratégies pour contourner les mécanicismes de protection natifs. Il est donc recommandé de renforcer la protection native des déploiements Office 365. Ce niveau de sécurité supplémentaire, dans la droite ligne des approches classiques des architectures sur site, doit venir compléter cette protection, sans la remplacer.

Q. Quelles problématiques ou limitations les entreprises disposant déjà d'une passerelle de messagerie doivent-elles prendre en compte ?

R. Il est intéressant de noter que l'étude mondiale d'IDC CloudView 2018 (avril 2018, n = 5 740) a relevé que 7,5 % des entreprises ont choisi de quitter le Cloud et de revenir à des applications/charges de travail de messagerie sur site (8,7 % en Europe occidentale). Par ailleurs, la sécurité fait partie des trois priorités des déploiements SaaS, PaaS et multicloud. La problématique de la sécurité de la migration est donc un axe central de la transformation des entreprises.

Les passerelles de messagerie sécurisées font partie des technologies classiques auxquelles cette étude fait référence. Cette architecture repose sur un modèle binaire (positif/négatif) et a fait ses débuts sur le marché dans les années 90, lorsque la passerelle se trouvait dans les DMZ (zone démilitarisée). L'adoption rapide du Cloud remet ce modèle en cause, car les contrôles de la passerelle sont insuffisants ou entraînent au contraire un flux important de faux positifs qui interrompt les activités.

Par ailleurs, une passerelle de messagerie sécurisée impose de modifier l'enregistrement MX et pose donc les limites suivantes :

- Intégration efficace à la sécurité native d'Office 365 impossible, car elle rend inutiles les défenses basées sur la réputation (ex. pour EOP) ou

[3] https://docs.microsoft.com/fr-fr/office365/securitycompliance/protect-against-threats

nécessite une sophistication additionnelle pour être intégrée en toute transparence.

- Impossibilité d'analyser les emails internes, car la passerelle est placée dans le flux d'emails.
- Mise en place et (re)configuration de la quarantaine des spams externes, induisant ainsi un surcroît de travail de gestion pour le service informatique interne.
- Formation additionnelle potentiellement nécessaire pour les utilisateurs finaux.
- Visibilité du produit au travers d'une simple recherche MX ; les hackers peuvent utiliser cette information pour personnaliser leurs attaques selon le fournisseur et contourner ainsi cette défense.

Q. Aucun produit de sécurité de l'email ne peut bloquer toutes les menaces. Ceci étant posé, quelle est la meilleure méthode à adopter pour gérer les faux négatifs ?

R. À vrai dire, l'élimination des faux négatifs n'a jamais été le point fort des solutions de sécurité de l'email, ceci en raison de l'approche traditionnelle de la protection des messageries. Le traitement des faux négatifs impliquerait des technologies supplémentaires de détection et de réponse qui devraient s'intégrer dans la globalité des solutions de sécurité pour obtenir une unification en la matière.

La dépérimétrisation de l'infrastructure de l'entreprise, mue par une acceptation et une utilisation plus larges du Cloud et conjuguée au panel des menaces dynamiques auxquelles les entreprises font face de nos jours, fait peser un fardeau de plus en plus lourd sur les épaules des équipes en charge de la sécurité. La taille des entreprises et la rapidité de leur activité requièrent en premier lieu une automatisation de la neutralisation des menaces et des réponses qui y sont apportées, qui nécessitent elles-mêmes une certaine visibilité. Il en va de même pour la sécurité de l'email en particulier. Comme indiqué, la protection continue des emails est un véritable must pour toute infrastructure basée sur le Cloud, ce qui impose des mises à jour dynamiques des règles.

Autre élément clé d'une élimination efficace des faux négatifs : l'intégration dans les outils et les workflows SOC et/ou SIEM, de façon à ce que les résultats de détection des menaces puissent être mis à profit pour mettre à jour les stratégies de réponse aux incidents en sus des ajustements des règles.

IDC France

13 rue Paul Valery
75016 Paris, France
+33 1 56 26 26 66
Twitter: @IDCFrance
idc-community.com
www.idc.com

A propos d'IDC

IDC est un acteur majeur de la Recherche, du Conseil et de l'Évènementiel sur les marchés des Technologies de l'Information, des Télécommunications et des Technologies Grand Public. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1100 analystes proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologies dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale de la société IDG, leader mondial du marché de l'information dédiée aux technologies de l'information.