vade

Microsoft 365

Sécurité de l'email dans Microsoft 365 : données et chiffres

Microsoft 365 constitue la principale suite applicative utilisée dans le monde. Cette position en fait une cible de choix pour les hackers intéressés par les données que votre entreprise y stocke. En compromettant ne serait-ce qu'un seul compte à l'aide d'un email, ils peuvent en effet accéder librement à Outlook, SharePoint, OneDrive et Teams. De là, il leur est possible de copier, télécharger et partager des fichiers, mais aussi de poursuivre leurs attaques au sein du système.

D'après le Ponemon Institute, 65 % des PME ont été victimes d'une cyberattaque en 2019, et 53 % ont signalé avoir été confrontées à une tentative de phishing/d'ingénierie sociale. Comme un grand nombre de PME l'ont constaté en 2019, la mise en place d'une solution inefficace peut avoir des conséquences désastreuses ::

53%
PME confrontées à une tentative de phishing [1]

$5,900
Montant moyen des rançons versées [2]

$141,000
Coût moyen du temps d'arrêt [3]

190 Million
Coût moyen de la perturbation des opérations [4]

Le **phishing** est une technique consistant pour le hacker à se faire passer pour une marque à la fois dans l'email à proprement parler, mais aussi sur une page Web. Son objectif ? Pousser sa victime à se rendre sur un site Web frauduleux et à divulguer les identifiants de son compte.

Le **spear phishing** consiste quant à lui à se faire passer pour un collègue ou une connaissance afin de pousser le destinataire de l'email à ordonner un virement, acheter des cartes cadeaux ou modifier des coordonnées bancaires.

Un **malware** est un logiciel malveillant conçu pour compromettre un ordinateur ou un appareil, notamment en corrompant ou dérobant des données et en se multipliant pour infecter d'autres ordinateurs et/ou appareils.

Un **ransomware** est un logiciel malveillant qui bloque un ordinateur. Il affiche à l'écran une demande de rançon en Bitcoins que la victime doit payer pour pouvoir récupérer l'accès à son ordinateur. Si elle ne s'exécute pas, le programme menace de détruire ou de faire fuiter les données.

Attaques par email ciblant Microsoft 365

Rien qu'en 2019, les hackers ont créé plus de 64 331 pages Web de phishing se faisant passer pour des pages de connexion Microsoft. Conçu pour dérober des identifiants, le phishing n'est qu'une des menaces par email auxquelles les entreprises qui utilisent Microsoft 365 sont confrontées.

1 Keeper Security, Ponemon. "2019 Global State of Cybersecurity in Small and Medium Sized Businesses"
2 Datto. "Datto State of Ransomware Report 2019"
3 Ibid.
4 Keeper-Ponemon, 2019.

Sécurité intégrée d'Microsoft 365 (EOP)

Microsoft 365 intègre un système de protection nommé Exchange Online Protection (EOP). Cette solution de sécurité de l'email créée par Microsoft est toutefois connue pour avoir des difficultés à détecter les attaques par email les plus sophistiquées. Lors de tests, les résultats d'EOP se sont avérés médiocres dans des catégories pourtant clés :

Taux de protection	Taux de détection	Taux de précision global [5]
-15%	55%	8%

Pour identifier les emails de phishing et ceux contenant des malwares, EOP y recherche des caractéristiques identifiables correspondant à des menaces déjà détectées précédemment.

- **Adresses IP** connues pour envoyer des emails de spam ou de phishing.
- **Domaines** connus pour héberger des sites ou pages Web malveillants.
- **Pièces jointes** intégrant du code de malwares/ ransomwares connus.

Pour détecter les tentatives de spear phishing, EOP recherche des usurpations du domaine exact, à savoir une réplique d'une adresse email d'une entreprise légitime. Toutefois, EOP ne sait pas reconnaître les autres formes d'usurpation utilisées par les emails de spear phishing:

- **Adresses email d'un domaine voisin,** à savoir des adresses proches d'adresses légitimes, mais non identiques : microsoft.com.company
- **Usurpation du nom affiché,** une technique qui consiste à afficher l'adresse email usurpée en lieu et place du nom de l'expéditeur : microsoftsecurity.com

Vade for M365

Pour protéger Microsoft 365, une solution supplémentaire de sécurité de l'email est nécessaire. Cette solution doit s'intégrer à EOP pour y ajouter un niveau de sécurité supplémentaire venant compenser ses faiblesses. **Vade for M365 bloque les attaques sophistiquées** dès le premier email. Pour ce faire, notre solution s'appuie sur des modèles d'apprentissage automatique qui procèdent à une analyse comportementale en temps réel de l'intégralité de l'email, URL et pièces jointes comprises.

Protection contre le phishing multi facettes réalise une analyse comportementale de l'email et de l'URL.

L'**anti-spear phishing** s'appuie sur une bannière d'alerte et affiche un avertissement si un email semble constituer une tentative de spear phishing..

L'**anti-malware comportemental** voit au-delà des menaces connues. Il analyse les pièces jointes et les codes pour repérer des comportements typiques de malwares/ransomwares.

La **remédiation** élimine les menaces déjà remises à l'utilisateur, soit automatiquement, soit en un clic.

En savoir plus sur Vade for M365

5 SE Labs. "Email Security Services Protection." December 2018.