Guide de l'acheteur d'Office 365 : bonnes pratiques de sécurisation d'Office 365

Synthèse

Microsoft Office 365 est aujourd'hui la plate-forme de productivité standard la plus plébiscitée par les petites et grandes entreprises dans le monde. Économique et facile à utiliser, cette solution propose des fonctionnalités de collaboration flexibles qui en font le meilleur choix pour de nombreuses entreprises. Mais la solution Office 365 étant de plus en plus adoptée, elle est aussi devenue une cible de choix pour les cybercriminels qui s'intéressent aux messageries hébergées, aux identifiants des utilisateurs et aux données personnelles/professionnelles précieuses.

Plus de 90 % des attaques ont pour origine des e-mails. Selon le rapport Cisco sur la cybersécurité de 2017, les hackers utilisent l'e-mail comme vecteur principal de propagation des ransomwares et autres malwares. C'est pourquoi les entreprises ne peuvent pas se permettre de lésiner sur la sécurité d'Office 365. La messagerie Exchange Online est vulnérable aux malwares contenus dans les pièces jointes et aux URL malveillantes sources de ransomwares, de compromissions des messageries d'entreprise, de phishing et d'autres attaques.

Bonnes pratiques de sécurisation d'Office 365 : protection contre les menaces et protection des données

Pour la sécurisation d'Office 365, il faut à la fois prendre en compte l'outil de collaboration cloud et la messagerie. Deux types de protection sont requis : la protection contre les menaces et la protection des données.

Sommaire

Pour les personnels en charge de la sécurité, les équipes DevOps et les dirigeants d'entreprise, il est primordial de sécuriser l'utilisation d'Office 365 afin d'améliorer la collaboration et la productivité, de réduire les coûts et de protéger les réseaux. Les entreprises qui utilisent les services Microsoft doivent :

- Détecter les comportements anormaux des utilisateurs, comme les piratages de comptes et la présence d'utilisateurs malveillants
- Appliquer et apporter des preuves de conformité
- Détecter les menaces dans les e-mails entrants
- S'assurer que l'entreprise suit les bonnes pratiques de sécurité
- Identifier les expositions de données résultant d'un excès de partages

Bien qu'Office 365 soit un service fourni dans le cloud, les entreprises sont entièrement responsables de l'utilisation de la plate-forme par leurs employés. Il est important de noter que les solutions de sécurité de Microsoft (incluses dans Office 365 ou vendues via une licence distincte) n'intègrent pas pour le moment de nombreuses fonctionnalités de sécurité essentielles.

Les administrateurs d'Office 365 ne disposent souvent que d'une visibilité limitée sur les activités de leurs utilisateurs, comme les fichiers auxquels ils accèdent, les politiques de ces fichiers et la compromission ou non de ces comptes d'utilisateurs.

Protection contre les menaces : détecter et gérer les menaces

Les cinq principaux éléments à prendre en compte pour la protection des instances Office 365 contre les attaques réseau sont les suivants :

1. Piratage de comptes : « Comment détecter les piratages de comptes ? »
2. Présence d'utilisateurs malveillants : « Des utilisateurs malveillants sont-ils en train d'extraire des données ? »
3. Actions contre les comptes privilégiés : « Les utilisateurs possédant des informations sensibles sont-ils exposés à des risques ? »
4. Manque de visibilité sur les menaces : « Est-ce que je dispose d'une Threat Intelligence complète ? »
5. Manque de visibilité sur les malwares existants : « Une sécurité rétrospective est-elle prévue si un fichier devient malveillant après le point d'inspection initial ? »

Sommaire

1. Piratage des comptes

Les hackers piratent les comptes des applications cloud à un rythme effréné. Microsoft a signalé une hausse annuelle de 300 % des attaques de comptes d'utilisateurs cloud Microsoft. Les attaques ciblées, comme le « spear phishing », ont atteint un niveau de sophistication sans précédent. Il est quasiment impossible de les distinguer des communications légitimes. Dans de nombreux cas d'attaque récents, aucun fichier ni aucune URL malveillante n'ont été utilisés. C'est pourquoi les solutions de sécurité classiques, y compris les outils de protection contre les malwares et le phishing, sont inopérantes face à ces menaces. Bien que les limites traditionnelles de la sécurité aient disparu, beaucoup d'utilisateurs continuent à utiliser les anciennes méthodes d'authentification. Dans le même temps, de nombreuses solutions cloud rendent les réseaux vulnérables à de tout nouveaux modèles d'attaque, comme l'utilisation des identifiants Office 365 des employés pour les connecter à des applications cloud masquées, malveillantes.

L'analyse du comportement des utilisateurs et des groupes (UEBA) découvre et analyse toutes les activités des utilisateurs et identifie leurs comportements anormaux. Par exemple, se connecter en très peu de temps depuis différents emplacements géographiques est un comportement suspect. Pour vous protéger contre les connexions malveillantes aux applications, vous devez être en mesure de créer une liste noire et une liste blanche des adresses IP spécifiques. Il est également important d'avoir une visibilité sur toutes les applications connectées, en particulier lorsque les utilisateurs d'Office 365 risquent de se connecter aux applications non autorisées avec leurs informations d'identification existantes. Votre solution doit vous donner le contrôle de votre écosystème d'applications connectées.

2. Présence d'utilisateurs malveillants

Les utilisateurs malveillants déclenchent rarement des alertes de sécurité lorsqu'ils exécutent des tâches nuisibles. C'est pourquoi lé détection de ce type de menace interne est extrêmement difficile. Étant donné la facilité avec laquelle les personnes malveillantes utilisent les applications cloud pour consulter, modifier, distribuer et exfiltrer des données sensibles, il est essentiel de détecter la présence d'utilisateurs malveillants et de réduire les risques associés.

Les utilisateurs malveillants étant difficiles à détecter en interne, il vous faut une solution capable de comprendre et d'établir un point de comparaison avec les comportements habituels des utilisateurs afin de repérer les actions suspectes et d'alerter les administrateurs de la sécurité le cas échéant. La solution doit également repérer les utilisateurs qui téléchargent de grands volumes de fichiers ou accèdent aux comptes Office 365 en dehors des heures normales de bureau.

Sommaire

3. Actions contre les comptes privilégiés

Les utilisateurs privilégiés ont non seulement accès à un grand volume de données sensibles, mais ils ont aussi des droits administratifs, tels que les paramètres de configuration et le provisionnement d'utilisateurs dans les applications. Le piratage d'un compte administrateur Office 365 peut provoquer des dommages considérables, puisque le hacker peut voler, modifier et effacer des données, supprimer des comptes d'utilisateurs et empêcher toute l'entreprise d'utiliser le service.

Il est important de déployer une solution qui surveille ces identités privilégiées dans Office 365 au moins autant, voire mieux que les comptes standard. Elle doit offrir la capacité de séparer les rôles et les responsabilités pour réduire les risques de piratage. La mise en œuvre d'un modèle d'accès avec « privilèges minimaux » permet de définir les privilèges minimum requis par un profil d'utilisateur pour accéder aux comptes Office 365 en fonction des responsabilités professionnelles de cet utilisateur.

4. Threat Intelligence complète

Les attaques contre Office 365 et en particulier la messagerie Exchange Online étant de plus en plus sophistiquées, les couches de sécurité déployées pour s'en protéger doivent l'être également. Comme toute solution de sécurité de la messagerie électronique, Office 365 doit protéger contre les spams, les virus, les logiciels malveillants, les usurpations d'identité et les autres menaces avancées. En outre, pour être efficaces, les solutions de sécurité doivent aller plus loin que les outils de protection du périmètre de base qui inspectent les e-mails à un instant T. Les e-mails étant externalisés vers Office 365, les clients ont besoin d'une solution qui offre une visibilité et un contrôle accrus pour réduire le délai médian de détection d'une attaque et la portée de l'événement et contenir les malwares avant qu'ils provoquent des dégâts.

Pour être efficace, une solution de sécurisation de la messagerie Office 365 doit également fournir un filtrage basé sur la géolocalisation qui protège contre les attaques sophistiquées par spear phishing en contrôlant rapidement le contenu des e-mails en fonction de l'emplacement de l'expéditeur. Elle doit aussi fournir une Threat Intelligence complète pour suivre les menaces nouvelles et émergentes. Les données collectées par la Threat Intelligence proviennent d'un large éventail de sources et doivent être partagées avec plusieurs produits de sécurité pour mettre en corrélation, identifier et détecter rapidement les menaces dans votre messagerie Office 365.

Sommaire

5. Sécurité rétrospective et inspection d'URL en temps réel

Aujourd'hui, les attaques sont de plus en plus sophistiquées, y compris celles qui ciblent les utilisateurs d'Office 365. Une pièce jointe entrante apparemment inoffensive peut se transformer en malware plusieurs, heures, jours ou semaines après avoir pénétré dans un environnement. La sécurité rétrospective avertit les administrateurs lorsqu'un fichier devient malveillant. Elle joue donc un rôle déterminant pour identifier les options de sécurité d'Office 365. En outre, la fonction de correction automatique de la messagerie supprime automatiquement ces pièces jointes malveillantes, faisant gagner plusieurs heures de travail aux équipes et les aidant à bloquer les menaces avant qu'elles provoquent plus de dégâts.

En plus de la protection continue contre les pièces jointes, l'analyse d'URL en temps réel au moment du clic est requise. Cette fonction bloque les URL suspectes chaque fois qu'un utilisateur clique dessus. Comme avec les pièces jointes, les hackers savent qu'ils peuvent échapper à l'analyse des URL à un instant T en reportant leurs attaques après ce moment.

Votre solution doit analyser en permanence les pièces jointes et les URL après le point initial d'inspection à un instant T proposé par la plupart des produits de sécurité pour messageries électroniques. La sécurité doit être assurée en permanence.

Protection des données : détecter et gérer la perte de données

Bien que la protection contre les menaces soit un élément essentiel de la sécurisation d'Office 365, la protection contre la perte de données est tout aussi importante. Des informations critiques sont stockées dans Office 365. Il s'agit non seulement d'informations sensibles, comme les dossiers médicaux, les fiches de paie ou les données de cartes de crédit, mais aussi d'e-mails et de pièces jointes contenant des données sensibles. Par le passé, ces données étaient contrôlées et réparties dans les différentes couches de sécurité de l'entreprise. Désormais, les données sont exposées dans les couches de sécurité définies au sein d'Office 365. Vous pouvez compenser cette perte de visibilité en augmentant les contrôles et la visibilité dans Office 365.

Les acheteurs doivent prendre en compte plusieurs éléments pour éviter toute perte de données lors de la sécurisation de leurs instances Office 365. Voici les cinq principaux :

1. Politiques utilisateur peu claires : « Mes utilisateurs sont-ils parfaitement informés des bonnes pratiques ? »
2. Manque de visibilité sur les données sensibles : « Est-ce que je sais ce que mes utilisateurs téléchargent ? »
3. Risque d'exfiltration des données : « Est-ce que je sais ce que mes utilisateurs partagent ? »
4. Perte de données via des e-mails sortants : « Est-ce que je sais ce que mes utilisateurs envoient par e-mail ? »
5. Chiffrement des e-mails : « Mes utilisateurs chiffrent-ils correctement les données sensibles envoyées par e-mail ? »

Sommaire

1. Politiques utilisateur claires

Formez les utilisateurs d'Office 365 afin qu'ils comprennent que si les applications cloud sont très pratiques, elles s'accompagnent néanmoins d'un risque de sécurité accru. Cette formation doit être obligatoire. Il est essentiel de leur donner des directives claires sur la façon de gérer les contenus créés dans Office 365, ainsi que les e-mails et les pièces jointes aux e-mails.

2. Visibilité sur les données sensibles

Les utilisateurs chargent souvent des informations sensibles dans Office 365, des numéros de carte de crédit aux informations sur leur santé, en passant par les programmes de développement des produits. Les systèmes classiques de prévention des pertes de données (DLP) sur site se limitent au trafic sur le réseau. Il leur est impossible de détecter les informations sensibles que les utilisateurs transfèrent ou créent dans les services cloud.

Office 365 requiert un moteur DLP cloud pour identifier les informations sensibles stockées dans les environnements cloud qui sont en infraction avec la politique. Cet outil doit se concentrer sur les types courants d'informations sensibles, comme les numéros de carte de crédit et les informations protégées en matière de santé. Il doit aussi créer des politiques pour identifier les données propriétaires, comme la propriété intellectuelle.

Le moteur DLP cloud doit constamment surveiller Office 365 afin de détecter et de protéger les informations sensibles par le biais de politiques globales prêtes à l'emploi, ainsi que de politiques personnalisées hautement paramétrables. Une entreprise qui déploie des fonctionnalités DLP pour Office 365 doit aussi s'assurer que les politiques DLP seront suivies à l'avenir et que des analyses rétroactives seront effectuées afin de garantir leur pleine conformité aux politiques.

3. Risque d'exfiltration des données

Office 365 facilite le partage et la collaboration, mais crée aussi des risques supplémentaires en termes d'exfiltration des données. En quelques clics, un utilisateur peut mettre des données à disposition depuis n'importe où sur Internet. Les cybercriminels et les utilisateurs internes malveillants ou négligents peuvent facilement exploiter Office 365 pour exfiltrer ou exposer des informations sensibles.

Vous avez besoin d'une solution qui identifie toutes les données sensibles stockées dans Office 365. Elle doit mettre en évidence les informations qui, selon les politiques créées par votre entreprise, sont partagées ou exposées de façon inappropriée. La fonction de gestion automatisée des incidents doit être capable d'éliminer les risques en cas d'infraction à la politique, y compris d'informer les administrateurs et les utilisateurs, de supprimer des collaborateurs ou même d'annuler le partage de fichiers et bien plus encore. Ces contrôles sont essentiels pour réduire l'exposition des contenus sensibles et les risques d'exfiltration des données.

Sommaire

C07-740121-00 01/18

4. Perte de données par le biais d'e-mails sortants

Les solutions de sécurité pour la messagerie électronique doivent détecter, bloquer et gérer les risques associés aux e-mails sortants. Elles doivent donc fournir une protection contre les contenus malveillants envoyés aux clients et aux partenaires commerciaux et empêcher les données sensibles de quitter l'environnement cloud, intentionnellement ou par inadvertance. En plus d'entraîner la perte de propriétés intellectuelles critiques, les comptes de messagerie piratés qui contiennent des malwares risquent de propager un virus en déclenchant soudainement l'envoi de spams en rafale. Le risque est que le domaine de messagerie de l'entreprise soit placé sur liste noire, même lorsque les e-mails sont signés. La messagerie électronique Office 365 ne fait pas exception.

Pour votre messagerie électronique Office 365, vous avez besoin d'une solution qui comporte des couches de sécurité pour les e-mails sortants. Elle doit inclure l'analyse comportementale pour détecter les comptes piratés, la limitation de débit du trafic sortant et l'analyse antispam et antivirus, pour éviter que les machines ou les comptes piratés finissent sur listes noires dans les messageries.

Il est par ailleurs indispensable qu'elle fournisse des informations sur le contenu, le contexte et la destination pour empêcher la perte de données volontaire ou accidentelle, assurer la conformité et protéger votre marque et votre réputation. Vous contrôlez qui est autorisé à envoyer des informations, quels types d'informations, vers quelle destination et sur quel support. Il convient de mettre en place des politiques prédéfinies pour éviter la perte de données et vous conformer aux normes de sécurité et de confidentialité prévues par les réglementations gouvernementales et du secteur privé.

5. Chiffrement des contenus sensibles dans les e-mails sortants

Les utilisateurs d'Office 365 doivent pouvoir se fier à des communications sécurisées pour mener leurs activités professionnelles sans crainte d'être piratés, en particulier lorsqu'ils envoient des contenus sensibles. Le chiffrement est l'une des couches de sécurité critiques pour la protection des données. Il préserve les informations sensibles, telles que les données financières et personnelles, les informations sur les concurrents ainsi que la propriété intellectuelle à des fins de protection et de conformité.

Pour gérer l'enregistrement des destinataires des e-mails, l'authentification et les clés de chiffrement par message/par destinataire, les utilisateurs d'Office 365 ont besoin du service de clé de chiffrement le plus avancé disponible. La solution doit aussi permettre aux responsables de la sécurité et de la conformité de contrôler et d'avoir une visibilité sur les données sensibles envoyées, notamment avec des tableaux de bord de reporting personnalisables qui affichent le trafic des e-mails chiffrés.

Résumé

Les outils cloud de collaboration comme Office 365 sont aujourd'hui utilisés par le grand public. Les clients bénéficient d'un accès permanent et étendu aux données dont ils ont besoin pour exercer leur activité, et ils peuvent utiliser ces solutions facilement. Mais ils doivent aussi examiner en détail les solutions de sécurité qui perpétuent ce confort tout en assurant la protection requise. Cisco s'adapte à ces nouvelles technologies cloud et procure la sécurité complète qui est essentielle pour bénéficier de ces avantages. Pour en savoir plus sur les bonnes pratiques de sécurisation d'Office 365, contactez votre responsable de compte Cisco ou consultez le site www.cisco.com/go/cloudsecurity.