La sécurité des e-mails de Microsoft est-elle suffisante ?

Les 7 principales failles en matière de sécurité des e-mails dans Microsoft 365

De nombreuses entreprises se demandent si la sécurité native des e-mails dans Exchange Online Protection ou Microsoft Defender pour Microsoft 365 offre un niveau de protection suffisant pour protéger leurs utilisateurs, leurs données et leurs communications. Malheureusement, le niveau de protection varie en fonction de la licence de chaque utilisateur et, bien que Microsoft ne cesse de parfaire ses capacités en matière de sécurité des e-mails, des failles subsistent. Par conséquent, les professionnels de la cybersécurité doivent déterminer si la sécurité native de Microsoft répond aux exigences de leur entreprise. Nous avons identifié sept points faibles où la sécurité de Microsoft pourrait s'avérer insuffisante.

01 | Protection contre l'usurpation d'identité

La protection contre l'usurpation d'identité dans MS Defender for Microsoft 365 (MSDO) pour les plans 1 et 2, Business Premium (BP) et E5 est basée sur l'intelligence artificielle (IA) qui définit des comportements relatifs aux e-mails et les contacts réguliers des utilisateurs afin de distinguer les messages provenant d'expéditeurs légitimes de ceux provenant d'usurpateurs d'identité.

Les limites de Microsoft

La protection contre l'usurpation d'identité (IP) n'est pas incluse dans Exchange Online Protection (EOP), ce qui signifie qu'elle n'est pas incluse dans Business Basic, Business Standard, E1 ou E3. Elle est disponible dans Business Premium et E5 mais désactivée par défaut. Il existe plusieurs limites liées à l'IP selon que l'expéditeur et le destinataire ont ou non communiqué auparavant, et ne peut pas protéger plus de 350 utilisateurs ou 50 domaines contre l'usurpation d'identité. Les faux positifs proviennent souvent d'expéditeurs ayant des noms courants, des comptes personnels, des comptes internes de fournisseurs et de partenaires et d'anciens employés.

Découvrez comment Barracuda peut vous aider

La protection contre l'usurpation d'identité Barracuda est incluse dans tous les plans et est opérationnelle dès le départ, sans règles ni politiques à spécifier, activer ou configurer, et sans limitation du nombre d'adresses d'expéditeurs, d'utilisateurs ou de domaines.

02 | Backup des données Microsoft 365

Microsoft a pris de nombreuses mesures pour réduire le risque de perte de données en cas de défaillance. Cependant, ils ne peuvent pas vous protéger contre les actions de vos utilisateurs ou contre les menaces indépendantes de leur volonté. Ces risques représentent la majorité des incidents habituels de perte de données. Par conséquent, Microsoft vous recommande de sauvegarder régulièrement vos données ou d'utiliser des applications et services de backup tiers.

Les limites de Microsoft

Selon le modèle de responsabilité partagée de Microsoft, votre entreprise reste responsable en dernier ressort de la protection de vos données. Il peut être difficile de déterminer si un fichier, un dossier, un e-mail ou un site SharePoint est nativement récupérable. Différentes ressources ont des limites différentes, comme les restrictions de type de fichier, les options de point de récupération, les périodes de conservation, les paramètres par défaut ou les maximums configurables, la récupération à partir de la recherche dans les dossiers ou de la recherche e-discovery, ou si l'utilisateur, l'administrateur ou Microsoft lui-même doit effectuer la récupération.

Découvrez comment Barracuda peut vous aider

Barracuda Cloud-to-Cloud Backup permet aux clients de sauvegarder quotidiennement les données critiques au sein d'Exchange Online, OneDrive, Teams, OneNote et SharePoint directement du cloud vers le cloud, vous offrant une évolutivité absolue et sans avoir à gérer quoi que ce soit. En outre, les backups sont intrinsèquement protégés des réseaux de production de Microsoft, et plusieurs copies sécurisées des données sont conservées en différents endroits.

03 | Sandboxing avec pièces jointes Zero-Day

Microsoft Safe Attachments fournit une protection supplémentaire pour les pièces jointes aux e-mails qui ont déjà été analysées par la protection anti-malware dans EOP et est disponible dans le plan MSDO 1 et 2, Business Premium et E5. Concrètement, Safe Attachments active les pièces jointes dans un environnement virtuel pour détecter les menaces de type « zero-day ».

Les limites de Microsoft

Safe Attachments n'est pas inclus dans EOP, ce qui signifie qu'il n'est pas inclus dans Business Basic, Business Standard, E1 ou E3. Il est disponible dans Business Premium et E5. Les boîtes de réception partagées nécessitent une licence pour profiter de Safe Attachments. Microsoft utilise un environnement virtualisé basé sur la technologie de l'hyperviseur MS pour analyser les pièces jointes, que certains types de malwares peuvent contourner.

Découvrez comment Barracuda peut vous aider

Barracuda Email Gateway Defense s'appuie sur plusieurs moteurs antivirus pour bloquer les malwares connus. Les malwares inconnus (zero-day/zero-hour) sont identifiés par une protection avancée contre les menaces à plusieurs niveaux qui exploite l'IA, l'heuristique, l'analyse comportementale et une sandbox dynamique. Contrairement aux sandbox classiques qui reposent sur une infrastructure à hyperviseur, Barracuda émule dynamiquement différentes plateformes à chaque exécution. Les boîtes de réception partagées ne nécessitent pas de licence pour bénéficier de la protection contre les menaces avancées.

04 | Sandboxing des URL en temps réel

Microsoft Safe Links permet de se protéger contre les liens malveillants de phishing et autres attaques. Il est inclus dans les plans MSDO 1 et 2, Business Premium et E5. Les liens dont le profil n'est pas valide sont déclenchés de manière asynchrone en arrière-plan. Cette solution offre également une protection contre les URL malveillantes en temps réel grâce à l'analyse et à la réécriture des URL des messages entrants. Lorsqu'elle est activée, les URL sont analysées avant d'être transmises, que les URL soient réécrites ou non.

Les limites de Microsoft

Safe Links n'est pas inclus dans EOP, ce qui signifie qu'il n'est pas inclus dans Business Basic, Business Standard, E1 ou E3. Il est disponible dans Business Premium et E5 mais désactivé par défaut. Safe Links présente plusieurs limites, notamment en ce qui concerne les malwares sensibles aux hyperviseurs, les modifications apportées par l'utilisateur final, les protocoles de transport non pris en charge, les dossiers publics non pris en charge et le manque de formation « instantanée » de sensibilisation à la sécurité.

Découvrez comment Barracuda peut vous aider

Barracuda Link Protection est inclus dans tous les forfaits de protection des e-mails, est activé par défaut et ne nécessite que peu ou aucune configuration. Les utilisateurs finaux ne peuvent pas ignorer l'écran d'avertissement de Link Protection, et ils sont dirigés vers une formation de sensibilisation à la sécurité grâce à son intégration avec la solution de formation de sensibilisation à la sécurité Barracuda. Les malwares sensibles aux hyperviseurs sont également moins susceptibles d'échapper à la sandbox dynamique de Barracuda, et les protocoles FTP/S et FTP sont pris en charge. Les dossiers publics compatibles avec les e-mails sont pris en charge, et les boites de réception partagées ne nécessitent pas de licences Barracuda Link Protection.

05 | Capacité de détection des menaces

Microsoft Implicit Authentication autorise parfois l'envoi de messages provenant d'expéditeurs qui échouent aux contrôles d'authentification des e-mails (ceux qui n'utilisent pas SPF, DKIM ou DMARC) et peut bloquer les messages valides.

Les limites de Microsoft

Microsoft ne rejette pas explicitement les messages provenant de sources que l'expéditeur n'a pas autorisées, conformément aux rapports DMARC de l'expéditeur. Au lieu de cela, les instructions DMARC de l'expéditeur influencent le verdict, mais ces instructions sont combinées à d'autres données télémétriques de Microsoft. Il peut en résulter des faux positifs et des faux négatifs. En outre, les verdicts inexacts d'Implicit Authentication doivent être continuellement revus dans Spoof Intelligence.

Au premier trimestre 2022, SE Labs a attribué à Microsoft la note AAA pour avoir réussi à bloquer 98 % des messages malveillants. Toutefois, pour obtenir cette note, Microsoft a dû « adapter les contrôles au niveau de protection le plus élevé », ce qui a entraîné le blocage de 14 % des e-mails légitimes. L'effort manuel nécessaire pour autoriser les e-mails bloqués par Microsoft n'est pas une option viable pour la plupart des entreprises.

Découvrez comment Barracuda peut vous aider

Barracuda Email Gateway Defense rejettera les messages provenant de sources que l'expéditeur n'a pas autorisées dans ses rapports DMARC. Barracuda ne supplante pas les directives publiées par l'expéditeur quant à l'acceptation ou au rejet sécurisé des e-mails pour son domaine.

06 | Archivage des e-mails

Une archive Microsoft est une boîte de réception spécialisée qui apparaît à côté de la boîte de réception principale de l'utilisateur dans Outlook. Les politiques de backup peuvent déplacer automatiquement les éléments vers les archives pour gagner en place et optimiser les performances de la boîte de réception.

Les limites de Microsoft

Les archives de toutes les boîtes de réception standard et partagées sont limitées à 50 Go pour Business Basic, Standard et E1. La capacité de stockage des archives commence à 100 Go pour Business Premium et E3/E5. Par défaut, le contenu des archives n'est pas immuable, et seules les boîtes de réception autorisées et autorisées pour la mise en suspens juridique peuvent conserver les messages supprimés au-delà d'une période de 14 jours. Les archives d'utilisateurs sans licence dépassant 50 Go ou celles placées en suspens juridique nécessitent une licence payante pour le plan 1 Exchange Online et une licence complémentaire d'archivage ou un forfait Exchange Online 2. Les archives de 100 Go sont parfois encore annoncées comme « illimitées », mais ne peuvent en réalité pas dépasser 1,5 To après activation de l'extension.

Pour les boîtes de réception de 100 Go, l'option d'auto-expansion autorise un maximum virtuel de 1,5 To. Microsoft Purview détermine automatiquement quels dossiers d'archives sont déplacés vers chaque nouvel incrément de 100 Go, le nombre de sous-dossiers à créer et les éléments à répartir dans ces dossiers afin de pallier synthétiquement au plafond initial de 100 Go. Il existe de nombreuses contraintes, notamment un taux de croissance quotidien maximum, des restrictions en matière de taille d'importation et de type de fichier, des restrictions en matière de recherche, des restrictions en matière d'utilisation appropriée, quand l'archive peut être augmentée, le délai pour chaque augmentation,

si les dossiers peuvent être supprimés après une expansion, si les dossiers peuvent être récupérés après une suppression, l'imprécision de la lecture/non lecture, et d'autres contraintes liées aux environnements hybrides sur site ou sur le cloud.

Découvrez comment Barracuda peut vous aider

Barracuda Cloud Archive Service fournit un véritable espace de stockage illimité moyennant un coût modéré et prédéfini par utilisateur. Les données archivées sont immuables et stockées indépendamment des données de production. Il n'y a pas de segments de stockage intermédiaires à créer tous les 100 Go. Aucune limite. La conservation des données dans les boîtes de réception inactives est gratuite, quelle que soit leur taille ou la nécessité d'une mise en suspens juridique.

07 | Accès conditionnel

Microsoft propose un accès conditionnel par utilisateur dans Azure Active Directory Premium P1 et P2. L'accès conditionnel rassemble divers éléments basés sur l'identité afin de prendre les bonnes décisions et d'appliquer les politiques de l'entreprise.

Les limites de Microsoft

L'accès conditionnel est disponible uniquement dans Business Premium et Microsoft 365 E3 et E5 ; il n'est pas disponible dans Business Basic, Standard et Office E1/E3/E5. L'authentification native sans mot de passe basée sur un certificat n'est pas disponible. Les politiques de l'accès conditionnel sont appliquées après cette confirmation d'authentification. Les entreprises doivent utiliser Intune pour vérifier l'identité du périphérique et le niveau de sécurité lors de l'authentification, mais les utilisateurs finaux (en particulier BYOD) et les sous-traitants ne veulent pas adhérer à des systèmes de gestion des périphériques mobiles (MDM) comme Intune.

Découvrez comment Barracuda peut vous aider

Barracuda Zero Trust Access optimise la mise en œuvre de l'authentification multifactorielle (MFA) en utilisant l'authentification basée sur les certificats dans Barracuda CloudGen Access. CloudGen Access vérifie l'identité de l'utilisateur et du périphérique avant que l'utilisateur ne soit connecté ou n'obtienne une autorisation d'accès aux applications ou aux ressources internes. Les points de terminaison constituent un niveau de défense supplémentaire contre les comptes Microsoft compromis, car un pirate ne disposant que des identifiants ne pourra pas se connecter. Les certificats de dispositifs sécurisés sont stockés dans le TPM ou les modules SEP de chaque dispositif ; il est pratiquement impossible de les extraire, de les copier ou de les cloner ; leur distribution et leur gestion ne nécessitent aucun matériel spécifique.

Contournez les limites de la sécurité native des e-mails de Microsoft 365 grâce à Barracuda Email Protection. Strength in Security (Renforcer la sécurité)

Barracuda
Your journey, secured.