Barracuda
Your business, secured.

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 Office 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 | Efficacité la détection des menaces

Microsoft 365 seul ne fournit pas une protection adéquate contre les attaques e-mail avancées bloquées par la solution Barracuda Impersonation Protection alimentée par l'IA. Pour mesurer l'efficacité de détection de Barracuda par rapport à Microsoft, nous avons traité plus de 10 milliards d'e-mails distribués à des comptes Microsoft, tous types de licences confondus.

Les limites de Microsoft

Microsoft 365 présente un taux moyen d'échec de détection de 47 % pour les attaques e-mail avancées, comme le détournement de conversation, le phishing et les usurpations d'identité. Pour les attaques plus sophistiquées, comme le détournement de conversation, ce taux d'échec atteint 88 %. Les fonctionnalités de sécurité natives de Microsoft 365 sont insuffisantes pour permettre aux organisations de protéger leurs utilisateurs contre les menaces complexes actuelles.

4,2 M	1,99 M	47 %
D'ATTAQUES BLOQUÉES PAR BARRACUDA	D'ATTAQUES MANQUÉES PAR MICROSOFT	TAUX D'ÉCHEC DE MICROSOFT

Découvrez comment Barracuda peut vous aider

Barracuda offre une sécurité complète pour Microsoft 365 avec une protection efficace alimentée par l'IA contre le phishing, les attaques BEC et le piratage de comptes. Grâce à un puissant moteur d'IA utilisant les métadonnées des e-mails historiques provenant d'expéditeurs internes et externes, combinées au traitement du langage naturel, Barracuda Impersonation Protection améliore la sécurité des utilisateurs Microsoft 365 avec une efficacité de détection supérieure.

02 | Sauvegarde 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 des pièces jointes zero-day

Microsoft Safe Attachments fournit une couche de protection supplémentaire pour les pièces jointes déjà analysées par la protection antimalware dans EOP et est inclus dans les offres MSDO Plan 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 avec EOP, ce qui signifie qu'il n'est pas inclus dans les offres Business Basic, Business Standard, E1 ou E3. Il est inclus dans les offres 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 d'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 offres MSDO Plan 1 et 2, Business Premium et E5. Les liens sans réputation valide sont analysés en arrière-plan de manière asynchrone. La solution ajoute également une protection en temps réel contre les URL malveillantes avec l'analyse et la réécriture des URL dans les messages entrants. Lorsqu'elle est activée, les URL sont analysées avant la distribution, qu'elles soient réécrites ou non.

Les limites de Microsoft

Safe Links n'est pas inclus avec EOP, ce qui signifie qu'il n'est pas inclus dans les offres Business Basic, Business Standard, E1 ou E3. Il est inclus dans les offres Business Premium et E5, mais il est 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 l'absence de formations de sensibilisation à la sécurité « ponctuelles ».

Découvrez comment Barracuda peut vous aider

Barracuda Link Protection est inclus dans tous les plans 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 | Protection contre l'usurpation d'identité

La protection contre l'usurpation d'identité dans Microsoft Defender for Office 365 (MSDO) Plan 1 et 2, Business Premium et E5 est une intelligence artificielle qui analyse les schémas d'e-mail avec les contacts fréquents des utilisateurs afin de distinguer les messages légitimes des usurpations.

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 les offres Business Basic, Business Standard, E1 ou E3. Elle est incluse dans les offres Business Premium et E5, mais désactivée par défaut. Elle présente plusieurs limitations selon que l'expéditeur et le destinataire ont déjà communiqué ou non, et ne peut protéger plus de 350 utilisateurs ou 50 domaines contre l'usurpation. Des faux positifs surviennent fréquemment avec des noms courants, des comptes personnels, des comptes de partenaires ou fournisseurs internes, 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.

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 sous licence et où la conservation pour litige est activée peuvent conserver les messages supprimés au-delà de 14 jours. Les archives d'utilisateurs sans licence dépassant 50 Go ou conservées pour litige nécessitent une licence Exchange Online Plan 1 payante et une licence de module d'archivage, ou Exchange Online Plan 2. Les archives de 100 Go sont parfois encore présentées comme « illimitées », mais ne peuvent en réalité pas dépasser 1,5 To après extension.

Pour les boîtes de 100 Go, l'auto-expansion permet un maximum artificiel de 1,5 To. Microsoft Purview détermine automatiquement quels dossiers d'archive sont déplacés à chaque incrément de 100 Go, combien de sous-dossiers créer et comment répartir les éléments afin de contourner la limite initiale. De nombreuses limitations existent : croissance quotidienne maximale, restrictions sur la taille et le type de fichiers importés, limitations de recherche, restrictions d'usage, délais d'extension des archives, suppression et récupération des dossiers après l'extension, erreurs de statut lu/non lu, ainsi que des limitations dans les environnements hybrides sur site/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 | Réponse et résilience limitées après la distribution

La sécurité des e-mails ne s'arrête pas à la livraison du message. Les attaques modernes reposent sur une exécution différée, des actions utilisateur compromises et des piratages de comptes après réception dans la boîte. Dans ces cas-là, les organisations doivent rapidement comprendre l'ampleur de l'attaque, en contenir l'impact et restaurer les utilisateurs et les données affectés. Elles ne doivent pas se contenter d'identifier le message d'origine.

Les limites de Microsoft

Defender pour Office 365 se concentre principalement sur le filtrage avant livraison et la protection au moment du clic. Lorsque des menaces e-mail contournent ces contrôles, la réponse se limite essentiellement à des alertes et à des actions isolées comme la suppression de messages. Defender pour Office 365 ne fournit pas nativement de workflows coordonnés d'investigation, de confinement ou de récupération pour les utilisateurs, les identités et les éléments impactés en aval. Les équipes informatiques doivent donc évaluer manuellement la situation, réinitialiser les comptes et restaurer les données via des outils et processus séparés.

Découvrez comment Barracuda peut vous aider

Barracuda étend la protection des e-mails à un modèle de sécurité axé sur la résilience. En corrélant les menaces e-mail avec les activités post-livraison, Barracuda Managed XDR Cloud aide les équipes à comprendre le contexte complet d'un incident et à y répondre plus efficacement. Lorsque les attaques entraînent une compromission de comptes ou des impacts sur les données, Barracuda Cloud-to-Cloud Backup et Entra ID Backup permettent de restaurer les e-mails, les données collaboratives et les configurations d'identité. Cette approche aide les équipes aux ressources limitées à réduire l'impact des attaques et à restaurer les opérations lorsque la prévention seule ne suffit pas.

Contournez les limites de la sécurité native des e-mails de Microsoft 365 grâce à Barracuda Email Protection.

Barracuda
Your business, secured.