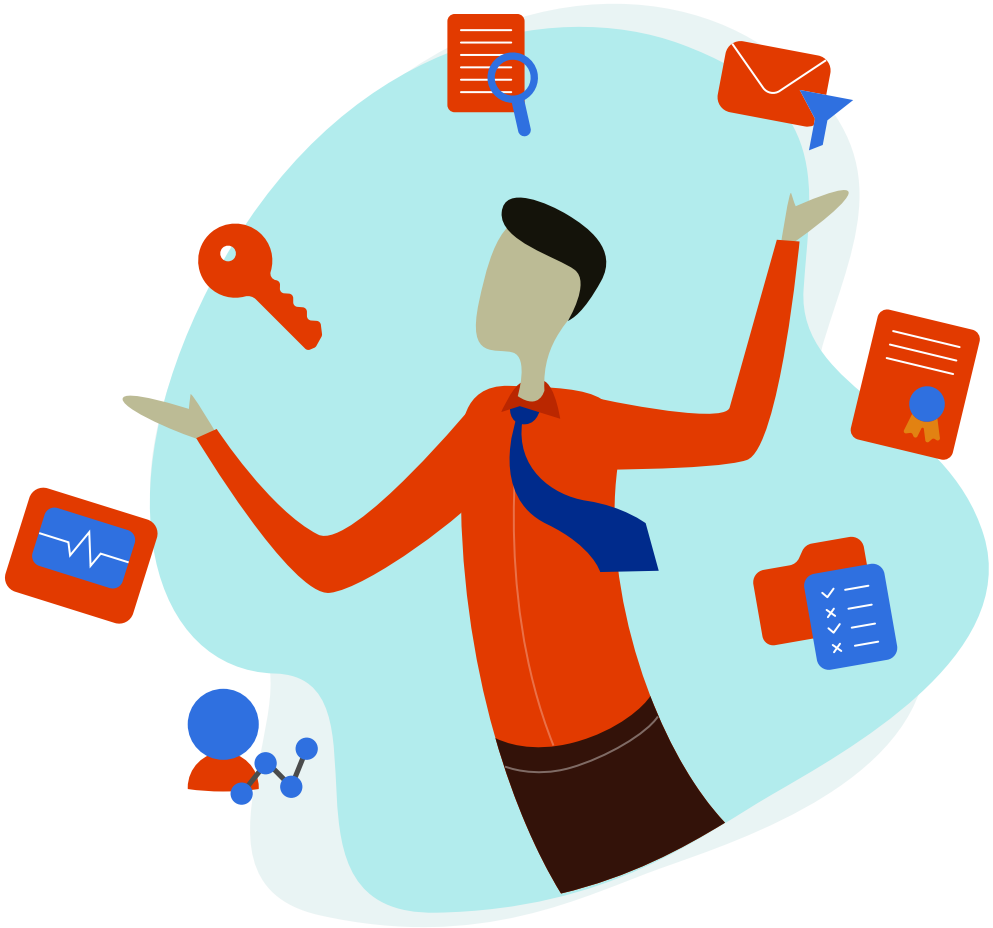
ManageEngine
M365 Manager Plus

Les sept bonnes pratiques pour sécuriser votre Microsoft 365



Introduction

Avec plus de 200 millions d'utilisateurs actifs mensuels dans le monde, Microsoft 365 est la suite d'applications cloud la plus utilisée. Pour de nombreuses entreprises, Microsoft 365 est le point d'entrée dans le cloud computing. Lorsque votre entreprise commence à migrer des données sensibles et critiques vers des plates-formes de cloud computing comme Microsoft 365, plusieurs problèmes de sécurité peuvent vous préoccuper : Les données sont-elles sécurisées ? Qui y a accès ? Que se passe-t-il si des utilisateurs non autorisés compromettent des comptes privilégiés ? Qu'en est-il du respect des exigences de conformité ? En ce qui concerne Microsoft 365, vous pouvez tirer parti des capacités de surveillance fournies par Microsoft et d'autres outils d'administration de Microsoft 365 tels que M365 Manager Plus pour simplifier la surveillance de la sécurité de Microsoft 365. Dans ce livre blanc, nous aborderons les bonnes pratiques de surveillance de la sécurité pour Microsoft 365, notamment les types d'activités à surveiller, les types de menaces à rechercher et les outils que vous pouvez utiliser pour y parvenir.

Les activités Microsoft 365 que vous devriez surveiller

Savoir par où commencer avec la surveillance de Microsoft 365 peut être un défi. Pour démarrer, vous devez savoir quelles activités surveiller et ce qu'elles peuvent vous apprendre sur votre sécurité informatique. En général, les types d'activités Microsoft 365 que vous devriez surveiller (si vous ne le faites pas déjà) sont les suivants :

Accès des utilisateurs : Découvrez qui accède à votre abonnement Microsoft 365, à quel moment et à partir de quel endroit. Établissez une base de référence pour le comportement normal d'accès des utilisateurs et détectez tout écart pour repérer les tentatives d'attaque. Par exemple, un utilisateur qui essaie de se connecter à partir d'un endroit anormal est certainement suspect et justifie une analyse.

Actions de l'administrateur : Une fois que les pirates ont accès à votre environnement, ils tentent souvent d'élever leurs privilèges pour accéder à vos données sensibles, tout comme les initiés malveillants. La surveillance des modifications apportées aux rôles d'administrateur, de la manière dont les activités de celui-ci sont consignées et des droits d'accès de l'administrateur peut vous aider à détecter les menaces externes et internes potentielles à leur stade le plus précoce.

Modifications des autorisations : La surveillance des modifications apportées aux autorisations et aux politiques de partage de fichiers dans OneDrive for business peut vous aider à repérer les premiers signes d'une violation potentielle des données. En outre, la surveillance des fichiers par utilisateur, notamment lorsqu'ils sont téléchargés, supprimés, modifiés et restaurés, peut vous aider à détecter et à enquêter sur les activités anormales.

Modifications des stratégies Microsoft 365 : Vos stratégies Microsoft 365 définissent les droits d'accès des utilisateurs aux ressources ainsi que les activités que ces utilisateurs peuvent effectuer dans votre environnement Microsoft 365. Toute modification non souhaitée de ces stratégies entraînera une faille de sécurité. C'est pourquoi vous devez surveiller en permanence les modifications apportées aux stratégies, notamment celles concernant les malwares et le filtrage de contenu Exchange. Les modifications apportés à ces stratégies pourraient permettre aux expéditeurs d'envoyer des e-mails de phishing et des pièces jointes malveillantes. Vous devez également garder un œil sur tout changement qui affaiblit les stratégies de mot de passe de votre entreprise.

Activités avec des acteurs malveillants connus : La surveillance de vos activités Microsoft 365 dans le contexte des vecteurs d'attaque connus permet d'atténuer les attaques dès leurs premiers stades. L'identification d'activités telles que le partage de fichiers avec des hôtes malveillants connus et les téléchargements multiples fichiers avec des extensions de fichiers ransomware connues peut vous alerter sur d'éventuelles menaces de sécurité.

Bonnes pratiques pour le contrôle de la sécurité de Microsoft 365

Il existe plusieurs mesures que vous pouvez adopter pour sécuriser votre environnement Microsoft 365. Nous vous présentons ci-dessous sept bonnes pratiques que votre entreprise devrait suivre pour une surveillance complète de la sécurité de Microsoft 365.

Bonne pratique 1:
Configurer les stratégies de mots de passe et l'authentification multifacteur (MFA)

Dans le centre d'administration Microsoft 365, vous pouvez renforcer la sécurité Azure AD en définissant des règles relatives aux mots de passe forts, à l'expiration des mots de passe et l'authentification multifacteur pour l'accès à Microsoft 365. Ce sont de bonnes pratiques de sécurité, mais elles ne sont pas suffisantes. Vous devez également surveiller en permanence les activités de connexion des utilisateurs pour détecter les signes de compromissions des informations d'identification des utilisateurs.

Bonne pratique 2:
Surveiller toutes les activités de connexion des utilisateurs d'Azure AD

Lorsqu'un utilisateur anormal se connecte à votre environnement Microsoft 365, vous devez connaître tous les détails associés à cet incident pour stopper la brèche dans son élan. Par exemple, si votre directeur financier se trouve actuellement à New York mais se connecte depuis la Chine, vous devez le savoir immédiatement. Surveillez toutes les activités de connexion des utilisateurs à Azure AD pour établir une base de référence de l'activité normale des utilisateurs. À l'aide de cette base, vous pouvez identifier les anomalies telles que les connexions inhabituelles en fonction de l'heure, de la fréquence ou du lieu. Surveillez les pics soudains de tentatives d'ouverture de session ou les échecs répétés d'ouverture de session, car ils peuvent être le signe d'une attaque par brute force. Vous pouvez surveiller les activités de connexion des utilisateurs à l'aide des rapports Azure AD ou d'une solution tierce de surveillance de la sécurité de Microsoft 365 comme M365 Manager Plus.

Bonne pratique 3:
Établir une stratégie du moindre privilège

Vous connaissez peut-être déjà cette bonne pratique universelle en matière de sécurité, mais étant donné son importance dans le contexte de la sécurité de Microsoft 365, il est utile de réévaluer les stratégies actuelles de votre entreprise. En général, vous devez accorder à vos administrateurs le moins de privilèges possible, c'est-à-dire suffisamment pour qu'ils puissent accomplir leur travail et rien de plus. Les modifications des privilèges des administrateurs peuvent indiquer qu'un acteur malveillant à l'intérieur de votre environnement tente d'accéder aux données confidentielles de votre entreprise, il est donc important de surveiller en permanence ces activités par le biais des logs d'audit administratifs.

Bonne pratique 4:
Surveiller les logs d'audit des administrateurs Microsoft 365

Par défaut, les administrateurs ont des droits et des autorisations pour accéder aux logs d'audit, surveiller les activités des utilisateurs et détecter les anomalies. Mais il y a toujours un risque qu'un initié malveillant disposant de privilèges d'administrateur tente de modifier les logs d'audit pour masquer ses traces. C'est pourquoi, outre les changements de rôles et d'autorisations, vous devez surveiller toutes les activités des administrateurs.

Vous pouvez auditer ces activités grâce à la fonction de journal d'audit administratif de Microsoft 365 :

• Activités des fichiers et des pages • Activités liées aux dossiers • Activités de partage et de demande d'accès • Activités de synchronisation • Activités d'administration de site • Activités liées aux boîte aux lettres Exchange • Activités Sway • Activités d'administration des utilisateurs Activités d'administration des groupes Azure AD	• Activités de gestion des applications • Activité d'administration des rôles • Activités d'administration des répertoires • Activités eDiscovery • Activités Power BI • Activités Microsoft Teams • Activités Yammer • Activité d'administration Exchange

Bonne pratique 5:
Surveiller toutes les activités des utilisateurs dans OneDrive for business

Il est important de surveiller tous les accès et activités des utilisateurs (suppression, téléchargement, modification, restauration, etc.) aux données critiques pour l'entreprise stockées dans OneDrive for business. En établissant une base de référence de l'activité régulière des utilisateurs, vous pouvez détecter les anomalies qui justifient une enquête. Par exemple, un utilisateur qui restaure un tas de fichiers supprimés dans OneDrive pourrait être un acteur malveillant qui tente de récupérer des données historiques. Bien sûr, il y a toujours la possibilité qu'un employé ait simplement supprimé quelques fichiers importants par accident, mais dans tous les cas, cela vaut la peine d'enquêter.

En outre, la tenue d'un journal de toutes les activités des fichiers d'utilisateurs peut non seulement vous aider à répondre aux exigences de conformité telles que PCI DSS, mais aussi à mener des enquêtes forensiques à la suite d'une violation de données.

Bonne pratique 6:

Surveiller les modifications apportées aux autorisations de partage de OneDrive for business, et le partage de fichiers avec des entités externes.

Lorsque vos utilisateurs partagent des fichiers avec des entités extérieures à votre entreprise, vous devez en être informé. C'est pourquoi vous devez surveiller les modifications apportées à OneDrive for business qui activent les autorisations de partage externes. Avec des outils avancés comme M365 Manager Plus, vous pouvez créer vos propres profiles d'audit et configurer des alertes e-mail en temps réel qui vous seront envoyées chaque fois que les autorisations de partage de fichiers auront été modifiées.

Bonne pratique 7:

Surveiller les modifications apportées aux stratégies de filtrage Exchange Online.

Dans le centre d'administration Microsoft Exchange (EAC), vous pouvez définir la configuration de filtrages de contenus (spam) et de malwares, parmi d'autres configurations. Cependant, la configuration de ces stratégies n'est pas une activité "à faire et à oublier". Vous devez plutôt surveiller en permanence les modifications apportées à ces stratégies qui indiquent une attaque ou une violation de la stratégie. Si des modifications sont apportées et affaiblissent vos stratégies de filtrages de contenu ou de malware, les expéditeurs pourront envoyer du spam,y compris des e-mails de phishing ou des e-mails contenant des pièces jointes chargées de malwares.

Quels outils utiliser pour surveiller Microsoft 365 ?

Il existe de nombreux outils et ressources disponibles pour vous aider à sécuriser et à surveiller votre environnement Microsoft 365. En réalité, il peut être difficile de simplement essayer de savoir par où commencer.

Centre de sécurité et de conformité Microsoft 365

Microsoft qualifie son centre de sécurité et de conformité Microsoft 365 de portail unique pour la protection de vos données dans Microsoft 365. Il offre des fonctions utiles telles que l'archivage des boîtes aux lettres, la prévention des pertes de données, la recherche de contenu et les activités des utilisateurs, la gestion des appareils, la signature d'autorisations et la conservation de documents.

Microsoft 365 Cloud App Security

Microsoft propose Microsoft 365 Cloud App Security, précédemment connu sous le nom de Microsoft 365 Advanced Security Management, qui vous donne un aperçu des activités suspectes dans Microsoft 365 afin que vous puissiez enquêter sur les situations potentiellement problématiques et prendre des mesures pour résoudre les problèmes de sécurité lorsqu'ils se présentent. Avec Microsoft 365 Cloud App Security, vous pouvez recevoir des notifications d'alertes déclenchées pour des activités atypiques ou suspectes, voir comment les données de votre entreprise dans Microsoft 365 sont consultées et utilisées, suspendre les comptes d'utilisateurs présentant une activité suspecte et exiger des utilisateurs qu'ils se reconnectent aux applications Microsoft 365 après le déclenchement d'une alerte.

Microsoft 365 Management API et gestion unifiée de la sécurité

Microsoft 365 Management API étend les fonctionnalités de sécurité et de conformité Microsoft 365 aux solutions de gestion de la sécurité dédiées, notamment M365 Manager Plus. Grâce à l'API RESTful, les applications externes peuvent obtenir des informations sur les actions et les événements des utilisateurs, des administrateurs, des systèmes et des stratégies à partir des logs d'activité Microsoft 365 et Azure Active Directory. Cela signifie que vous pouvez gérer la surveillance de la sécurité de Microsoft 365 dans votre plateforme de gestion de la sécurité existante, si elle prend en charge l'API.

Pourquoi envisager l'utilisation un outil tiers de surveillance de la sécurité ?

Alors que Microsoft fournit de nombreux outils, capacités et ressources pour la sécurité et la conformité, trouver où provisionner, configurer et utiliser chaque service peut s'avérer extrêmement difficile. Si l'expérience utilisateur n'est qu'un facteur à prendre en compte, il existe de nombreuses autres raisons pour lesquelles vous devriez envisager d'utiliser une solution de surveillance de la sécurité tierce pour Microsoft 365.

Une couche supplémentaire de surveillance de la sécurité

Une solution de surveillance de la sécurité dédiée peut fournir une couche supplémentaire d'assurance de la sécurité et des capacités de détection des menaces critiques pour votre environnement Microsoft 365, notamment des règles, des alarmes et des analyses prédéfinies.

Visibilité centralisée de l'ensemble de votre dispositif de sécurité

Lorsque vous analysez les activités des utilisateurs dans le centre de sécurité et de conformité Microsoft, vous devez rechercher des informations de sécurité associées dans plusieurs outils et logs pour obtenir le contexte complet de la menace pendant l'enquête et la réponse. Une solution de gestion unifiée de la sécurité démantèle les silos de données en regroupant toutes les données relatives à la sécurité en un seul endroit. Ces données comprennent des informations sur vos actifs, vulnérabilités connues, les activités des utilisateurs et bien d'autres choses encore, ce qui rend les enquêtes sur les incidents beaucoup plus efficaces.

Conserver les logs d'audit au-delà de 90 jours

À partir d'aujourd'hui, Microsoft purge tous les logs Microsoft 365 qui ont plus de 90 jours. Si vous recherchez de meilleures périodes de rétentions des logs pour vous conformer aux réglementations, vous pouvez tirer parti d'une solution comme M365 Manager Plus pour collecter les logs Microsoft 365 et les stocker à l'infini.