10 Étapes vers la cyber-résilience de Microsoft 365

Sommaire

La recrudescence des cyberattaques de Microsoft 365

La protection des données Microsoft 365 est un composant essentiel d'une stratégie de cybersécurité moderne. En effet, les applications de la suite sous-tendent les opérations quotidiennes d'innombrables entreprises et activités. Avec sa large gamme d'outils de productivité, y compris Exchange, Teams, SharePoint, OneDrive, etc., Microsoft 365 contient une mine d'informations sensibles et de données d'entreprise critiques. C'est pourquoi de plus en plus d'entreprises investissent dans des solutions tierces ou des services de sauvegarde gérés pour les protéger.[1] Il semble en effet prouvé que les ransomwares sont conçus spécifiquement pour infiltrer Microsoft 365 et d'autres applications SaaS. Selon un rapport de Coalition, les déclarations de cyberincidents liées à des attaques par ransomware ont augmenté de 12 % au premier semestre 2023, avec des demandes de rançons atteignant en moyenne 1,62 millions de dollars.[2] En conséquence de son utilisation généralisée, et alors que de plus en plus d'employés installent et utilisent Microsoft 365 sur des ordinateurs travaillant à domicile, la plate-forme est devenue particulièrement exploitable pour les attaquants capitalisant sur cette infrastructure diversifiée.

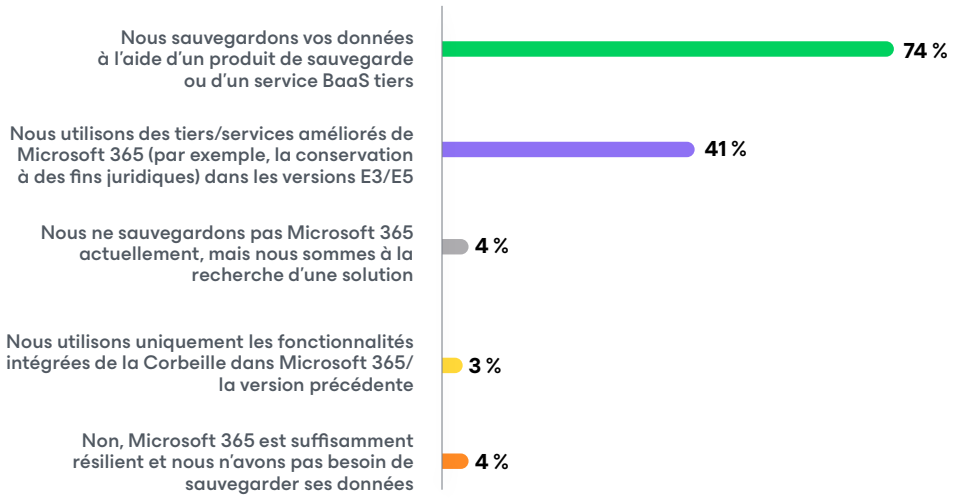
12 %

augmentation des déclarations de cyberincidents au premier semestre 2023

1,62 M$

Montant moyen des demandes de rançons

Votre entreprise sauvegarde-t-elle les données depuis Microsoft 365 ?



[1] Rapport sur les tendances de la protection des données en 2024
[2] Microsoft 365 ransomware : Votre guide complet pour améliorer la compréhension, la prévention et la restauration

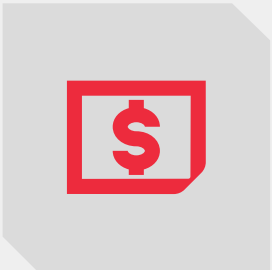
Les risques de perte de données Microsoft 365 sont donc non seulement complexes, mais bien réels. Les pertes de données entraînent de graves perturbations opérationnelles et peuvent causer des dommages financiers importants en raison des temps d'arrêt et des pertes de productivité. Dans un rapport, les responsables informatiques ont estimé le coût des temps d'arrêt à 1 467 $ par minute (88 000 $ par heure)[3], ce qui n'est pas étonnant, au vu du volume important de temps passé et de travail accompli à l'aide de Microsoft 365 dans une journée de travail habituelle. De plus, lorsque des données sensibles sont exposées, les entreprises risquent d'avoir à payer de lourdes pénalités de manquement à la conformité et de voir leur réputation entachée. En effet, en cas d'infractions au RGPD, les amendes peuvent atteindre 21 millions de dollars[4]. Comme les données Microsoft 365 sont extrêmement sensibles pour les entreprises et leurs employés, les incidents de perte de données ont de fortes chances d'éroder non seulement la confiance des clients, mais aussi celle des employés. Ces problèmes sont susceptibles d'entraîner une baisse du chiffre d'affaires et de nuire à la réputation à long terme, à l'intérieur comme à l'extérieur de l'entreprise.

Les conséquences possibles de données Microsoft 365 non protégées ne peuvent être surestimées. Les violations qui exposent les renseignements personnels peuvent entraîner des vols d'identité ou des fraudes, dont les dommages risquent de perdurer bien au-delà de la compromission initiale. Pour les entreprises, la perte de propriété intellectuelle peut éroder leurs avantages concurrentiels et entraîner des batailles juridiques coûteuses ou des amendes. Elles peuvent également faire l'objet de litiges si elles sont jugées négligentes dans la protection des données de leurs clients.

Il n'y a aucun moyen d'y échapper. Une approche proactive de la sécurisation des données Microsoft 365 représente bien plus qu'une idée innovante. C'est un impératif pour s'assurer que les entreprises assurent le maintien de la continuité, assument leurs responsabilités légales et réglementaires et gardent la confiance des clients.

[3] Rapport sur les tendances de la protection des données en 2022
[4] Quelles sont les amendes du RGPD ?

Coût associé aux pertes de données



Le coût des temps d'arrêt est estimé à 1 467 $ par minute (88 000 $ par heure)

En cas d'infractions au RGPD, les amendes peuvent atteindre 21 millions de dollars.

Les violations qui exposent les informations personnelles peuvent entraîner des vols d'identité ou des fraudes.

Les étapes à suivre pour se préparer aux attaques

1. Multi-Factor Authentication

L'authentification multifacteur (MFA) est une mesure de sécurité essentielle qui oblige les utilisateurs à fournir au moins deux facteurs de vérification pour accéder à des ressources numériques, telles que les comptes de messagerie, les applications professionnelles et les services en ligne. La MFA renforce considérablement la sécurité en ajoutant des couches de protection au-delà du simple mot de passe. Cela signifie que même si un cybercriminel obtient le mot de passe d'un utilisateur, il devra toujours contourner les facteurs d'authentification supplémentaires pour y accéder. Ce n'est rien de moins qu'une formidable barrière contre l'entrée non autorisée.

Les avantages de la MFA sont nombreux, en particulier dans le contexte de Microsoft 365 où l'utilisation de données sensibles et les communications d'entreprise sont perpétuelles. MFA peut vous défendre contre les conséquences de cyberattaques courantes telles que le phishing, où les attaquants trompent les utilisateurs pour qu'ils divulguent des informations d'identification. Cette étape d'authentification supplémentaire peut être quelque chose que l'utilisateur connaît (comme un code PIN ou une question de sécurité) ou quelque chose que l'utilisateur possède (comme un smartphone ou du matériel de la société).

Même dans les scénarios où les mots de passe sont compromis en raison de mots de passe faibles ou réutilisés, la configuration d'une authentification multifacteur continuera à protéger le compte contre les accès non autorisés. Ce niveau de sécurité est critique dans les environnements Microsoft 365, où l'accès à distance est courant et où les utilisateurs peuvent se connecter à partir de réseaux non sécurisés ou de périphériques personnels. Le simple fait de savoir que, dans l'ensemble, l'authentification multifacteur crée un mécanisme de défense dynamique qui s'adapte à l'évolution du paysage des menaces est rassurant.

Avantages de l'authentification multifacteur

Protège contre les conséquences des cyberattaques courantes

Continue à protéger le compte contre les accès non autorisés

Crée un mécanisme de défense dynamique qui s'adapte au paysage des menaces

2. Accès basé sur le principe du moindre privilège

Le principe du moindre privilège est la pierre angulaire des pratiques de cybersécurité efficaces, étroitement lié au concept d'architecture Zero Trust, et il est essentiel pour renforcer une organisation contre les cyberattaques potentielles. Une architecture Zero Trust fonctionne en supposant qu'il existe des menaces à la fois à l'extérieur et à l'intérieur du réseau, de sorte qu'aucun utilisateur ou système n'est automatiquement fiable.[5] Cela va de pair avec le principe du moindre privilège, qui veut que les utilisateurs disposent des niveaux minimaux d'accès (ou de permissions) nécessaires à l'exercice de leurs fonctions — et pas plus. Pour Microsoft 365, la mise en œuvre de ces principes peut signifier restreindre l'accès à certains documents, dossiers, sites, paramètres administratifs et applications en fonction du rôle de l'utilisateur au sein de l'organisation.

L'adoption d'un modèle d'accès basé sur le principe du moindre privilège peut améliorer considérablement la posture de sécurité de votre environnement Microsoft 365. Tout d'abord, cela réduit au minimum la surface d'attaque potentielle de la suite pour les cybercriminels. Si le compte d'un utilisateur est compromis, l'attaquant est limité aux droits d'accès de ce compte qui doivent être, dans l'idéal, les plus restrictifs possibles. Par exemple, en cas de vol des informations d'identification d'un utilisateur, l'attaquant ne pourra pas accéder à des informations sensibles ni effectuer des tâches administratives si ces droits ne sont pas associés au compte de l'utilisateur. Cette limitation des dommages crée une zone de quarantaine pour toute violation de la sécurité. Elle est essentielle pour maîtriser la propagation des attaques au sein d'une organisation.

[5] https://www.veeam.com/news/new-zero-trust-data-resilience-model-introduced-by-it-security-and-data-protection-experts.html

3. Sauvegardes régulières

En tant que cible principale des cybercriminels, les sauvegardes sont extrêmement importantes pour Microsoft 365, en particulier au vu du modèle de partage des responsabilités[6] de Microsoft, selon lequel les entreprises sont responsables de la sécurité de leurs données. Ransomware représente une menace importante pour intégrité des données, car les attaquants ont pour objectif de chiffrer les fichiers d'une entreprise et d'exiger un paiement pour les libérer. Néanmoins, les menaces qui pèsent sur les données ne se limitent pas aux attaques malveillantes. Les données peuvent également être compromises par des suppressions accidentelles ou divers autres incidents. Garder les sauvegardes à jour permet à l'entreprise de récupérer rapidement l'accès à ses données, que la perte soit due à un ransomware, à une erreur humaine ou aux nombreuses autres raisons qui rendent le maintien de sauvegardes Microsoft 365 essentiel[7]. Cela permet non seulement de réduire les temps d'arrêt au minimum, mais aussi d'envoyer le message fort que l'entreprise n'est pas une cible facile pour de futures attaques.

Mettre en œuvre une routine de sauvegarde régulière signifie établir un calendrier qui établit un équilibre entre le volume de données traitées et les ressources disponibles pour les opérations de sauvegarde. Cela devrait inclure la sauvegarde des e-mails, documents, contacts, calendriers et toute autre donnée stockée dans la suite Microsoft 365.

Considérez la sauvegarde comme votre police d'assurance. On n'en a peut-être pas besoin tous les jours, mais lorsqu'une catastrophe survient, elle peut faire la différence entre une restauration rapide et une catastrophe mortelle.

[6] Partage des responsabilités dans le Cloud

[7] 7 raisons cruciales de sauvegarder Microsoft 365

4. Sauvegardes inaltérables

L'inaltérabilité joue un rôle essentiel dans la protection des actifs numériques d'une entreprise contre l'altération ou la suppression, qu'elle soit due à des cybermenaces ou à une erreur humaine. Pour Microsoft 365, où de grandes quantités de données sont régulièrement générées, partagées et stockées, veiller à ce que les copies de sauvegarde soient immuables est un aspect essentiel pour une stratégie robuste d'atténuation des menaces. L'inaltérabilité garantit qu'une fois sauvegardées, les informations restent dans leur état d'origine et sont inaltérables pendant une période définie.

Pour les entreprises qui utilisent Microsoft 365, les sauvegardes inaltérables servent de bouclier contre les attaques de ransomware qui visent non seulement les données opérationnelles, mais aussi les cibles de sauvegarde. En fait, selon une étude, presque toutes les attaques par ransomware (93 %) ciblent spécifiquement les sauvegardes.[8] Pour d'autres mesures de sécurité, une copie de sauvegarde inaltérable des données est importante. En créant et en appliquant des stratégies de rétention qui protègent les données de sauvegarde contre l'écrasement ou la falsification, les entreprises peuvent défendre leurs pratiques de continuité contre le chiffrement ou la destruction indésirables des données. L'inaltérabilité garantit qu'en dépit des violations de sécurité qui frappent leurs datastores actuels, l'entreprise peut restaurer ses opérations à partir d'une sauvegarde saine et intacte.

93 %

Des attaques par ransomware ciblent spécifiquement les sauvegardes.

[8] Rapport sur les tendances des ransomwares en 2023

5. Plan d'intervention en cas d'incident

Un plan de réponse aux incidents est un plan bien structuré. Il explique les procédures à suivre lorsqu'une organisation est confrontée à divers incidents de cybersécurité. Il présente ainsi des guides stratégiques pour identifier, contenir, éradiquer les menaces de sécurité, puis rétablir l'activité. Il permet également de s'assurer que tous les acteurs concernés sont informés et prêts à agir.

Pour les entreprises utilisant Microsoft 365, un solide plan de réponse aux incidents comprend l'identification des actifs essentiels au sein de l'écosystème Microsoft 365. Cela signifie indiquer où les données sensibles sont stockées, que ce soit dans OneDrive, SharePoint, Exchange Online ou ailleurs. Une fois ces actifs identifiés, le plan doit définir les menaces potentielles et créer une liste de risques classés par ordre de priorité, ainsi que des stratégies pour les atténuer. Cela comprend l'utilisation d'outils de supervision et de détection intégrés, des stratégies de confinement immédiat, l'éradication des menaces, une communication robuste entre les parties, ainsi que l'identification et la restauration de toutes les données perdues ou compromises.

Le ciment d'un plan de réponse aux incidents est une préparation minutieuse. Cela va bien au-delà des outils techniques, de la formation et de la collaboration des équipes informatiques et de sécurité, car cette préparation s'applique à tous les employés. Les organisations qui utilisent Microsoft 365 doivent organiser régulièrement des sessions de formation adaptées à la complexité de cet écosystème. Les employés qui utilisent des applications au sein de Microsoft 365 telles qu'Outlook et Teams doivent disposer des connaissances nécessaires pour pouvoir discerner et contrer les activités suspectes, qui peuvent prendre la forme de messages apparemment légitimes, de fausses invitations à des réunions de collègues ou d'e-mails de dirigeants de la société d'aspect authentique. Les personnes peuvent constituer une faiblesse en matière de cybersécurité pour n'importe quelle entreprise, mais des employés bien formés ont le potentiel de constituer une formidable barrière contre les menaces.

Un plan de réponse aux incidents commence par

Infrastructure complète de réponse aux incidents

Identification des actifs critiques

Importance de la préparation des employés

6. Audits et tests de pénétration réguliers

Les audits et les tests de pénétration réguliers font partie intégrante du maintien d'un environnement Microsoft 365 résilient. En fait, Microsoft 365 lui-même fournit une gamme d'outils intégrés d'audit et de détection des menaces[9] servant de base de référence pour renforcer son environnement contre diverses menaces de sécurité. Ces pratiques constituent des mesures proactives qui permettent aux entreprises d'identifier et de corriger les problèmes avant qu'ils ne puissent être exploités par des attaquants.

Les audits de l'écosystème Microsoft 365 impliquent un examen systématique de divers aspects tels que les autorisations utilisateur, les contrôles d'accès aux données et les paramètres de sécurité. Bien que parfois compliqués, les audits réguliers permettent de s'assurer que les configurations système restent alignées sur les meilleures pratiques et les politiques de sécurité de l'organisation. C'est une habitude saine à mettre en place et à maintenir. Comme Microsoft 365 englobe différents services, ces audits doivent être complets et couvrir chaque service pour éviter les vulnérabilités inaperçues.[10]

Souvent qualifiés de « piratage éthique », les tests d'intrusion complètent les audits réguliers en permettant aux organisations d'évaluer l'efficacité de leurs mesures de sécurité. Il s'agit de simuler des cyberattaques sur l'infrastructure Microsoft 365 afin d'identifier les faiblesses que de vrais attaquants pourraient exploiter. Pour les entreprises concernées, les tests d'intrusion doivent sonder toutes les couches de leur écosystème Microsoft 365, de la résistance au phishing des employés à la résilience des outils techniques tels que les pare-feu, les systèmes de détection des menaces et les plans de réponse aux incidents. Les enseignements tirés de ces tests aident les entreprises à peaufiner leurs programmes de formation et leurs stratégies de sécurité, afin de pouvoir se défendre de manière plus complète et plus efficace en cas de cybermenace inévitable.

[9] Conseils de sécurité et de conformité pour Microsoft 365

[10] Sécurité native de Microsoft 365 : Déverrouiller les fonctionnalités de conformité et de supervision

7. Politiques de restriction logicielle

La stratégie de restriction logicielle (SRP) est une fonctionnalité de sécurité qui permet aux organisations d'identifier et de contrôler l'exécution du logiciel sur un matériel spécifié. Pour les entreprises qui utilisent Microsoft 365, sa mise en œuvre peut constituer un mécanisme de défense essentiel pour protéger les nombreux appareils dont elles sont responsables. Comme Microsoft 365 contient une multitude d'outils distincts, il invite également à une série de vecteurs de menace distincts et exploitables. En dictant quels logiciels peuvent et ne peuventpas fonctionner sur un système, les SRP réduisent efficacement la surface d'attaque disponible aux acteurs malveillants.

Lors de la création d'un SRP pour un environnement Microsoft 365, l'objectif est de s'assurer que seuls les scripts, les applications et les processus approuvés seront autorisés à s'exécuter. Si nécessaire, cela peut impliquer de tenir une liste blanche et une liste noire des vecteurs de menace. Pour une efficacité maximale, les SRP doivent être configurés en tenant compte du moindre privilège et être régulièrement mis à jour pour refléter les changements apportés aux logiciels utilisés par l'entreprise. Cela comprend les mises à jour des outils Microsoft 365, l'ajout de nouveaux logiciels ou l'arrêt des applications traditionnelles.

En empêchant les logiciels malveillants d'exploiter des techniques d'exploitation courantes, les SRP sont très efficaces pour perturber la chaîne d'infection et maintenir une zone de quarantaine. L'intégration des SRP dans une stratégie de cybersécurité est une approche tournée vers l'avenir. Elle contribue à protéger l'infrastructure d'une organisation contre l'exécution de logiciels non fiables, éventualité grandissante à mesure que les entreprises se développent et embauchent de nouveaux employés.

8. Supervision et journalisation

La supervision et la journalisation constituent une étape essentielle pour assurer la sécurité et l'intégrité de tout environnement Microsoft 365. En gardant un œil vigilant sur les activités du système et en tenant des registres complets des événements, les organisations peuvent détecter les incidents de sécurité potentiels en temps réel, diagnostiquer les problèmes du système, comprendre la portée des violations et améliorer la posture de sécurité globale.

Pour les administrateurs Microsoft 365, l'importation des journaux dans un système performant de gestion des informations et des événements liés à la sécurité (SIEM) peut grandement simplifier le processus. Azure Sentinel, par exemple, est un SIEM natif Microsoft qui utilise un ensemble de connecteurs de données prédéfinis pour transmettre les données de journal d'une entreprise directement dans l'application SIEM. Ces données sont ensuite normalisées pour obtenir des ensembles de données cohérents et surveillées au moyen d'outils d'analyse intégrés.

Une surveillance efficace doit ratisser large pour détecter toute une gamme d'anomalies possibles indiquant une menace pour la sécurité. Il peut s'agir de tentatives de connexion infructueuses (suggérant une attaque en force brute) ou de schémas de téléchargement inhabituels (suggérant une exfiltration de données indésirables), par exemple. Une journalisation complète est tout aussi importante, car elle permet de documenter toutes les activités surveillées. De tels journaux doivent capturer suffisamment de détails pour permettre la reconstitution des événements de l'ensemble d'un incident - avant, pendant et après. Ils représentent une aide inestimable pour l'analyse scientifique post-incident, mais également pour réaliser des audits de conformité et affiner les mesures de sécurité au fil du temps. La journalisation doit être soigneusement configurée pour s'assurer que les données recueillies sont exploitables, fournissant des informations claires et pertinentes sans le bruit qui peut être généré par une portée trop ambitieuse.

Au fil du temps, les informations tirées de la supervision et de la journalisation fournissent aux organisations les données nécessaires pour modifier la stratégie de manière proactive et rationaliser les mises à jour de sécurité.

9. Séparation des données

La séparation des privilèges est une stratégie largement applicable et efficace utilisée par les organisations pour améliorer leur infrastructure de sécurité. Elle est parfaitement adaptée lors de l'intégration de services orientés données tels que Microsoft 365. Les stratégies telles que les architectures mutualisées, les limites administratives et la restriction conditionnelle des comptes se concentrent sur la structuration des données et de leurs privilèges pour réduire les accès non autorisés et limiter les dommages potentiels liés aux violations de la sécurité. En séparant les différents jeux de données et en divisant les réseaux en segments distincts, les organisations peuvent réduire considérablement le risque initial de violations de la sécurité et mettre efficacement en quarantaine les incidents de sécurité éventuels.

L'utilisation de stratégies de séparation des privilèges dans Microsoft 365 permet aux organisations de maintenir des règles d'accès strictes. Comme évoqué dans la section précédente, la meilleure de ces règles consiste à garantir que les utilisateurs, les administrateurs et les services ne reçoivent que les autorisations nécessaires pour effectuer leurs tâches essentielles, et rien de plus. Il s'agit, par exemple, du principe du moindre privilège et du contrôle d'accès en fonction du rôle (RBAC).

Pour les organisations qui exercent leurs activités dans plusieurs juridictions ou possèdent des unités opérationnelles distinctes, la séparation des clients Microsoft 365 via une architecture mutualisée permet d'isoler les données et d'en contrôler l'accès. Il s'agit de la création de limites administratives distinctes pour chaque client. Cela permet d'isoler les environnements avec leurs propres données, comptes utilisateur et contrôles d'accès. Ainsi, les exigences de sécurité et de conformité sont respectées individuellement, et une violation de sécurité ou un problème survenant chez un client ne compromet pas l'intégrité des autres.

À l'intérieur de ces limites administratives, les stratégies d'accès conditionnel et les restrictions de compte ajoutent une couche de défense supplémentaire et peuvent être directement implémentées dans Microsoft 365. Ces stratégies permettent aux organisations de définir et d'implémenter des règles contextuelles pour un compte donné, ce qui permet d'optimiser les règles de sécurité d'une organisation en fonction du niveau de risque, de l'emplacement géographique ou des irrégularités dynamiques telles que les connexions ou les téléchargements suspects.

La séparation méthodique peut s'appliquer à tous les niveaux hiérarchiques de l'entreprise et constitue une base solide pour sécuriser les données et autres ressources numériques Microsoft 365. Le cloisonnement stratégique atténue non seulement le risque d'accès non autorisé, mais fournit également des garanties et des solutions de repli à plusieurs niveaux contre les atteintes à la sécurité. La séparation des données et des privilèges mérite ainsi, à juste titre, son statut d'approche fiable. Elle permet en effet aux organisations de renforcer leurs cyberdéfenses, de maintenir la continuité de l'activité et au final, de faire de grands progrès vers la cyber-résilience au sein de leur environnement Microsoft 365.

10. Chiffrement

Le chiffrement est une mesure de sécurité fondamentale qui sert de ligne de défense principale dans la protection des informations sensibles, garantissant que seules les parties autorisées disposant de la clé de déchiffrement correcte peuvent accéder aux informations d'origine et s'applique aux données indépendamment de leur utilisation, de leur déplacement ou de leur emplacement. En ce qui concerne Microsoft 365, le chiffrement fournit une couche de sécurité qui aide les entreprises à protéger leurs communications, leurs documents et d'autres données, quel que soit leur emplacement au sein de leur infrastructure cloud.

Les e-mails de phishing et les sites Web infectés sont souvent les précurseurs subtils d'attaques de ransomware graves. Ces dernières années, le ransomware RobbinHood a dévasté les entreprises, leur coûtant des millions de dollars en rançons, en temps d'arrêt et en efforts de restauration, simplement parce qu'un e-mail infecté téléchargé par inadvertance a introduit le logiciel malveillant dans leur système.

Des outils intégrés tels que les étiquettes de confidentialité de Microsoft 365 permettent d'éviter cela grâce au respect de protocoles stricts capables de chiffrer automatiquement les documents et les e-mails. Cela empêche une infection initiale en évitant à l'utilisateur de faire confiance à des e-mails suspects et en lui signalant les expéditeurs potentiellement dangereux. Ces étiquettes peuvent être configurées avec des stratégies de gestion des droits, permettant aux administrateurs de déterminer qui peut accéder aux données etcomment elles peuvent être utilisées. Il s'agit d'un niveau de classificationet deprotection contrôlé de manière centralisée par les entreprises, permettant aux administrateurs informatiques d'arbitrer la remise, le partage etla manipulation des données. Ainsi, les utilisateurs bien intentionnés disposent de plusieurs dispositifs de protection pour empêcher l'introduction ou la propagation de logiciels malveillants (sans entraver les flux de travail dans le processus).

En fin de compte, un chiffrement efficace constitue le fondement sur lequel reposent la confidentialité et la conformité réglementaire. Les entreprises qui utilisent efficacement les fonctionnalités de chiffrement de Microsoft 365 parallèlement à leurs stratégies de sécurité existantes sont bien plus résilientes aux cyberattaques que celles qui ne le font pas. Des pratiques de chiffrement fiables sont essentielles pour protéger les données précieuses contre les ransomwares et les cybermenaces, renforçant ainsi la confidentialité, garantissant la conformité réglementaire et favorisant un espace de travail collaboratif sécurisé.

La cyber-résilience de Microsoft 365 commence par la sauvegarde

Dans le cadre de notre réflexion sur l'avenir de la gestion et de la sécurité des données, la sauvegarde en mode service (BaaS) s'est imposée comme la méthode privilégiée de protection des applications SaaS telles que Microsoft 365. La solution BaaS est une approche basée sur le cloud qui offre aux entreprises un système en ligne et à distance pour sauvegarder et stocker leurs données. L'intégration de BaaS à une stratégie Microsoft 365 répond au besoin de solutions protection des données robustes, évolutif et flexibles, autant d'éléments essentiels pour garantir la résilience de l'entreprise.

Les services de sauvegarde permettent aux entreprises d'externaliser leurs besoins en sauvegarde à des fournisseurs spécialisés. Ceux-ci leur proposent des solutions de bout en bout capables d'automatiser les processus de sauvegarde, de réduire la quantité d'infrastructures locales nécessaires et de fournir une sécurité de premier ordre, tout en leur permettant d'accéder à leurs données et de les contrôler directement. Pour les utilisateurs de Microsoft 365, la solution BaaS se traduit par davantage de sécurité des données, d'efficacité opérationnelle et de tranquillité d'esprit.

La sécurisation d'un écosystème Microsoft 365 est une entreprise à multiples facettesqui nécessite que les entreprises mettent en œuvre des mesures de prévention stratégiques et des plans de réponse aux incidents efficaces. La démarche vers la cyber-résilience de Microsoft 365 se poursuit et nécessite un engagement en faveur d'une utilisation efficace des progrès technologiques. Heureusement, il existe des fournisseurs de sauvegarde spécialement conçus pour les données Microsoft 365.

Veeam Data Cloud *for Microsoft 365*

Veeam Data Cloud *for Microsoft 365* permet une résilience totale des données Microsoft 365, avec une touche moderne. Veeam Backup *for Microsoft 365*, la meilleure solution de sauvegarde du marché pour Microsoft 365, est désormais proposée en mode service.

Simplifiez votre stratégie de sauvegarde à l'aide d'un logiciel, d'une infrastructure de sauvegarde et d'un stockage illimité dans un service cloud tout-en-un qui vous permet de tirer parti de puissantes technologies de protection des données et de sécurité au sein d'une expérience utilisateur simple et transparente.

Veeam Data Cloud *for Microsoft 365* est un service de sauvegarde qui offre une protection et une restauration complètes des données pour **Microsoft Exchange, SharePoint, OneDrive for Business et Teams**, et vous laisse une maîtrise totale de votre environnement Microsoft 365.

→ Demander une démonstration de Veeam Data Cloud for Microsoft 365

Avec **Veeam Data Cloud *pour Microsoft 365***, vous obtenez :

- **Une technologie fiable et phare du marché :** La solution de protection des données la plus complète, avec plus de 10 ans d'innovation à grande échelle.
- **Plateforme moderne, sécurisée et intuitive :** Créez facilement des tâches de sauvegarde, effectuez des restaurations et obtenez des informations sur Microsoft 365 depuis une interface utilisateur Web moderne.
- **Service tout compris :** Logiciel, infrastructure de sauvegarde et stockage illimité regroupés avec une maintenance continue assurée par des experts.

Préparez-vous, restez informés

Votre parcours vers la cyber-résilience de Microsoft 365 ne s'arrête pas là : ce n'est que le début. Élargissez vos connaissances, affinez vos stratégies et gardez une longueur d'avance en 2024. Laissez-nous vous aider à transformer les difficultés en opportunités grâce à notre vaste collection de ressources :

- 8 avantages d'un service de sauvegarde pour Microsoft 365
- Sauvegarde Microsoft 365 pour les nuls
- Microsoft 365 : meilleures pratiques de restauration

À propos de Veeam Software

Veeam®, le leader mondial de la protection des données et de la restauration après une attaque par ransomware, s'est donné pour mission d'aider toutes les entreprises à se relever après une panne ou une perte de données et, surtout, à aller de l'avant. Avec Veeam, les entreprises assurent la résilience totale en garantissant la sécurité des données, la restauration et la liberté des données de leur cloud hybride. La Veeam Data Platform offre une solution unique pour les environnements cloud, virtuels, physiques, SaaS et Kubernetes et garantit aux décideurs informatiques et responsables de la sécurité que leurs données et applications sont protégées et toujours disponibles. Basé à Seattle et possédant des bureaux dans plus de 30 pays, Veeam protège plus de 450 000 clients dans le monde, dont 74 % des entreprises du Global 2000, qui font confiance à Veeam pour le maintien de leur activité. La résilience totale commence avec Veeam. Pour en savoir plus, rendez-vous sur www.veeam.com ou suivez Veeam sur LinkedIn @veeam-software et X @veeam.