Office 365

La sécurité dans office 365

Table des matières

Introduction

La popularité croissante du « cloud computing » augmente l'inquiétude de nombreux utilisateurs. La part croissante de contenu maintenant stocké sur le cloud plutôt que localement, où la tâche d'assurer la sécurité de leur contenu revenait principalement aux utilisateurs, augmente l'importance des exigences de sécurité qui s'imposent aux fournisseurs de services de cloud. Les utilisateurs ont besoin de la garantie que leur contenu est sécurisé.

Il est essentiel pour les organisations de contrôler et de personnaliser la sécurité dans les services de cloud. Les outils de productivité couramment utilisés qui nécessitent d'être sécurisés incluent :

- Le courrier électronique
- Les calendriers
- Les systèmes de gestion de contenu
- Les systèmes de collaboration
- Les communications unifiées

Les équipes informatiques doivent permettre d'accéder aux services depuis plus de dispositifs, de plates-formes et de lieux que jamais auparavant. S'il est évident que l'accès aux actifs de l'entreprise depuis de multiples dispositifs est un atout pour les utilisateurs, cet accès élargi rend néanmoins la gestion de la sécurité plus difficile. Chaque point de terminaison représente une surface d'attaque potentielle et un autre point à prendre en compte pour les professionnels de la sécurité. Dans le même temps, les organisations font face à des menaces en constante évolution à travers le monde, et doivent gérer le risque créé par leurs propres utilisateurs lorsqu'ils perdent ou compromettent accidentellement des données sensibles.

Les organisations ont besoin d'un service de cloud disposant de fonctions de sécurité intégrées robustes et de nombreuses fonctions de sécurité personnalisables qu'elles puissent optimiser pour répondre à leurs besoins individuels.

Pour les organisations qui souhaitent étendre les possibilités d'accès à distance tout en conservant les meilleures pratiques de sécurité, il peut s'avérer difficile et coûteux d'ajouter cette combinaison de fonctionnalités de sécurité si leurs services de productivité sont déployés uniquement sur site.

La sécurité dans Office 365

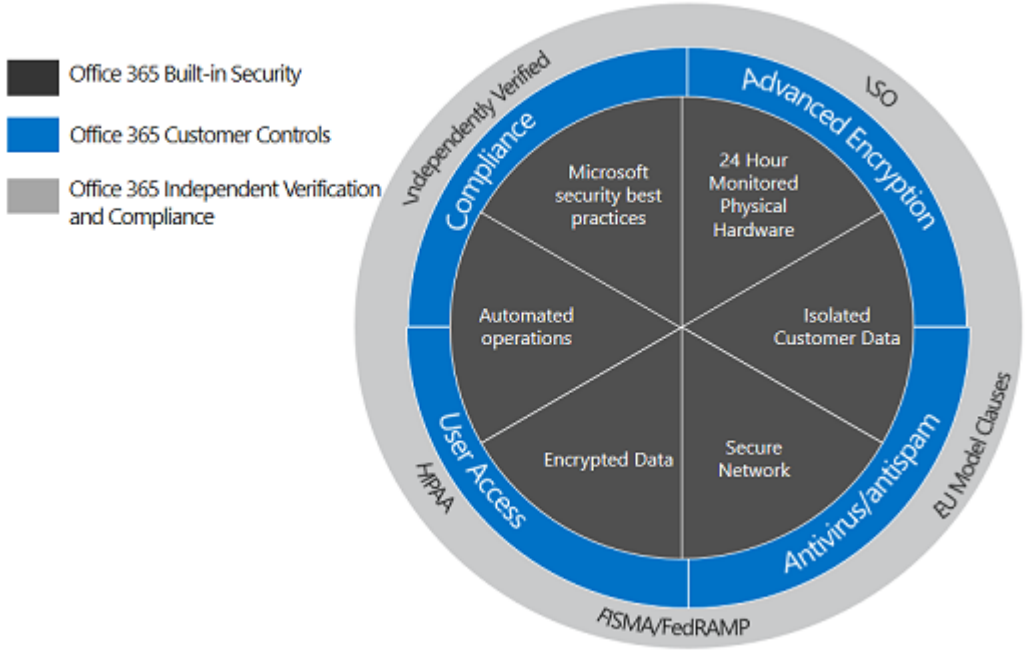
Microsoft est un leader du secteur en matière de sécurité du cloud et met en œuvre des politiques et des contrôles de niveau équivalent ou supérieur à ceux des centres de données internes même des organisations les mieux équipées. La sécurité d'Office 365 repose sur trois piliers :

- Les fonctions intégrées de sécurité
- Les contrôles de sécurité
- La sécurité évolutive

Office 365 est un service à la sécurité renforcée dans lequel les fonctions de sécurité sont intégrées. Les clients Office 365 bénéficient de fonctions de sécurité avancées que Microsoft a intégrées dans le service en s'appuyant sur l'expérience acquise depuis deux décennies de gestion des données en ligne et sur des investissements majeurs dans les infrastructures de sécurité. Office 365 a mis en place des processus et des technologies, qui font encore l'objet d'investissement et d'amélioration, pour identifier de manière proactive et atténuer les menaces de sécurité avant qu'elles ne deviennent des risques pour les clients.

Office 365 propose des contrôles de sécurité qui permettent aux clients de personnaliser leurs paramètres de sécurité. Office 365 jouit de la confiance de clients de toutes tailles dans pratiquement tous les secteurs, y compris des secteurs fortement réglementés tels que la santé, la finance, l'éducation et le gouvernement. Comme Office 365 gère les services de productivité pour une telle diversité de secteurs et zones géographiques, il offre un choix de fonctionnalités que les clients peuvent contrôler pour renforcer la sécurité de leurs données.

Office 365 dispose de processus de sécurité évolutifs qui permettent une vérification indépendante et le respect des normes de l'industrie. Ce document décrit trois aspects de la sécurité dans Office 365.



La sécurité intégrée

Surveillance physique du matériel 24 heures sur 24

Les données d'Office 365 sont stockées dans le réseau des data centers Microsoft, gérés par Microsoft Global Foundation Services et stratégiquement situés à travers le monde. Ces data centers sont conçus à tous les niveaux pour protéger les services et les données contre les dommages causés par une

catastrophe naturelle ou un accès non autorisé. L'accès aux data centers est limité 24 heures sur 24 sur le critère du poste professionnel, de sorte que seul le personnel essentiel ait accès aux applications et services des clients. Le contrôle d'accès physique utilise des processus multiples d'authentification et de sécurité, y compris des badges et des cartes à puce, des lecteurs biométriques, des agents de sécurité sur site, la surveillance vidéo en continu et l'authentification à deux facteurs. Les centres de données sont surveillés à l'aide de capteurs de mouvement, de systèmes de vidéo surveillance et d'alarmes de violation de sécurité. En cas de catastrophe naturelle, la sécurité comprend également des racks antisismiques, si nécessaire, et des systèmes automatiques de prévention et d'extinction des incendies.

Isolation des données des clients

L'une des raisons pour lesquelles Office 365 est à la fois évolutif et peu coûteux est qu'il s'agit d'un service multi-locataire (c'est-à-dire que les données de différents locataires partagent les mêmes ressources matérielles). Office 365 est conçu pour accueillir des locataires multiples de manière hautement sécurisée grâce à l'isolation des données. Le stockage et le traitement des données pour chaque locataire est séparé grâce à l'architecture et aux capacités d'Active Directory spécifiquement développées pour aider à construire, gérer et sécuriser des environnements multi-locataires. Active Directory isole les clients à l'aide de frontières de sécurité (aussi appelées silos). Ce système permet de protéger les données d'un client de telle façon qu'il est impossible aux autres colocataires d'accéder à ces données ou de les compromettre. Il est possible d'utiliser, moyennant le paiement d'un supplément, une version d'Office 365 qui stocke les données sur du matériel dédié.

Opérations automatisées

Dans les centres de données Microsoft, l'accès aux systèmes informatiques qui stockent les données client est strictement contrôlé par le contrôle d'accès basé sur les rôles (RBAC) et les processus lockbox. Access. Le contrôle d'accès est un processus automatisé qui obéit au principe de séparation des fonctions et au principe de l'octroi du moindre privilège. Ce processus garantit que l'ingénieur demandant l'accès à ces systèmes informatiques a satisfait aux critères d'admissibilité, tels que la vérification des antécédents, la prise d'empreintes digitales, la formation exigée à la sécurité et les autorisations d'accès. Les ingénieurs demandent l'accès à des tâches particulières dans un processus lockbox. Le processus lockbox détermine la durée et le niveau de l'accès indépendant de l'évaluation du besoin de supervision par un autre ingénieur.

Réseau sécurisé

Dans les data centers Office 365, les réseaux sont segmentés pour fournir une séparation physique des serveurs principaux critiques et des dispositifs de stockage des interfaces accessible au public. La sécurité du routeur périphérique donne la possibilité de détecter les intrusions et les signes de vulnérabilité. Les connexions client à Office 365 utilisent le protocole SSL pour sécuriser Outlook, Outlook Web App, Exchange ActiveSync, POP3 et IMAP. L'accès des clients aux services fournis sur Internet commence sur les sites des utilisateurs et se termine dans les data centers Microsoft. Ces connexions sont chiffrées à l'aide des normes du secteur sur la sécurité des couches de transport (TLS)/SSL. L'utilisation de TLS/SSL établit une connexion client-serveur hautement sécurisée qui contribue à assurer la confidentialité et l'intégrité des données entre l'ordinateur de bureau et le data

center. Les clients peuvent configurer TLS entre Office 365 et les serveurs externes pour le courrier électronique entrant et sortant. Cette fonction est activée par défaut.

Chiffrage des données

Dans Office 365, les données des clients peuvent être dans deux états :

- Au repos, sur les supports de stockage
- En transit sur un réseau entre un data center et un dispositif client.

Tout le contenu de contenu sur disque est chiffré sur le disque à l'aide de Bitlocker, qui utilise l'algorithme de chiffrement Advanced Encryption Standard (AES). La protection couvre tous les disques des serveurs de messagerie et inclut les fichiers des bases de données de boîtes aux lettres, les fichiers de journaux de transaction des boîtes aux lettres, les fichiers d'index de contenu de la recherche, les fichiers de base de données de transport, les fichiers de journaux de transactions de transport, et les journaux de suivi de pagination des disques systèmes et de suivi des messages.

Office 365 assure également le transport et le stockage des messages au format sécurisé Secure/Multipurpose Internet mail extension(S/MIME). Office 365 peut transporter et stocker des messages chiffrés à l'aide de solution de chiffrement de tierces parties, telles que Pretty Good Privacy (PGP).

Les meilleures pratiques de sécurité de Microsoft

La sécurité dans Office 365 n'est pas dans un état figé, mais est un processus continu. Elle est constamment maintenue, améliorée et vérifiée par un personnel expérimenté et qualifié, et Microsoft s'efforce d'utiliser les logiciels et le matériel les plus à jour et perfectionnés grâce à des processus robustes de conception, construction, exploitation et support. Pour que la sécurité d'Office 365 reste la meilleure du secteur, Microsoft s'appuie sur des procédés tels que le Cycle de développement sécurisé (SDL), la limitation du trafic et la prévention, la détection et l'atténuation des violations de la sécurité.

Cycle de développement sécurisé

La sécurité chez Microsoft commence avant même que le public n'entende parler de l'application ou du service concerné. Le Cycle de développement sécurisé (SDL) est un processus global d'assurance sécurité qui imprègne chaque étape de la conception, du développement et du déploiement des logiciels et services Microsoft, y compris Office 365. Grâce à ses exigences de conception, à l'analyse de la surface d'attaque et la modélisation des menaces, le SDL permet à Microsoft de prévoir, identifier et atténuer les vulnérabilités et les menaces avant même le lancement d'un service et pendant la totalité de son cycle de vie de production. Microsoft met le SDL constamment à jour en utilisant les données les plus récentes et les meilleures pratiques pour mieux s'assurer que les nouveaux services et logiciels associés à Office 365 sont hautement sécurisées dès le premier jour.

Limitation de trafic pour empêcher les attaques par déni de service

Exchange Online assure un suivi des bases de référence d'usage et s'adapte aux brusques montées de trafic sans que cela affecte l'expérience utilisateur. Lorsque le trafic en provenance d'un utilisateur dépasse les paramètres types, le trafic est limité jusqu'au retour à une utilisation normale. Que le trafic excessif soit dû au comportement d'un utilisateur ou à une attaque malveillante, par déni de service par exemple, Exchange réagit automatiquement pour permettre aux autres utilisateurs de ne pas être affectés. Office 365 utilise également une plate-forme commerciale tierce de suivi du déni de service offrant des capacités de surveillance et de limitation de trafic.

Prévention, détection et atténuation des violations de sécurité

La prévention, détection et atténuation des violations de sécurité est une stratégie de défense qui vise à prédire et prévenir les violations de sécurité avant qu'elles ne se produisent. Cette approche implique des améliorations continues aux fonctions de sécurité intégrées, y compris le balayage de ports et la remédiation, l'analyse des vulnérabilités du périmètre, les correctifs du système d'exploitation incluant les mises à jour de sécurité les plus récentes, la détection et la prévention des DDOS (attaques par déni de service distribuées) et l'authentification multi-facteurs pour l'accès au service. Cette approche implique des améliorations continues aux fonctions de sécurité intégrées, y compris le balayage de ports et la remédiation, l'analyse des vulnérabilités du périmètre, les correctifs du système d'exploitation incluant les mises à jour de sécurité les plus récentes, la détection et la prévention des DDOS (attaques par déni de service distribuées) et l'authentification multi-facteurs pour l'accès au service. D'un point de vue processus et personnel, la prévention des violations de sécurité implique la surveillance de l'ensemble des accès et des actions des opérateurs/administrateurs, aucune autorisation permanente pour les administrateurs de service, « l'accès et l'élévation juste à temps (JIT) » (c'est-à-dire que l'élévation de privilège est accordée juste à temps et en fonction des besoins) aux privilèges d'ingénieur pour le dépannage du service, et la séparation de l'environnement de messagerie de l'employé et de l'environnement d'accès à la production. Le niveau le plus élevé de privilège est automatiquement refusé aux employés dont les antécédents n'ont pas été vérifiés et cette vérification est un processus très détaillé qui est approuvé manuellement.

La prévention des violations de sécurité implique également la suppression automatique des comptes inutiles quand un employé quitte son emploi, change de groupe, ou n'utilise pas le compte avant son expiration. Chaque fois que possible, l'intervention humaine est remplacée par un processus à base d'outils automatisés, entre autres pour les fonctions courantes telles que le déploiement, le débogage, la collecte de diagnostic et le redémarrage des services. Office 365 continue à investir dans l'automatisation des systèmes qui aide à identifier les comportements anormaux et suspects et à réagir rapidement pour atténuer les risques de sécurité. Microsoft développe en permanence un système très efficace de déploiement des correctifs automatisé qui génère et déploie des solutions aux problèmes identifiés par la surveillance des systèmes, le tout sans intervention humaine. Cela améliore grandement la sécurité et l'agilité du service. Office 365 effectue des tests de pénétration pour permettre l'amélioration continue des procédures de réponse aux incidents. Ces tests internes aident les experts en sécurité d'Office 365 à créer un processus d'automatisation et d'intervention par étapes méthodique reproductible et optimisé.

Contrôles client

Office 365 associe la familiarité de la suite Microsoft Office avec les versions basées sur le cloud de nos services de collaboration et de communications de nouvelle génération : Microsoft Exchange Online, Microsoft SharePoint Online et Microsoft Lync Online. Chacun de ces services offre des fonctions de sécurité personnalisées, que le client peut contrôler. Ces contrôles permettent aux clients de respecter des exigences de conformité, de donner accès à des services et des contenus à des personnes spécifiques dans leur organisation, de configurer des commandes anti-logiciels malveillants/antispams et de chiffrer les données avec une clé détenue par le client.

Chiffrement avancé

Un des atouts majeurs d'Office 365 est la possibilité de permettre au client d'utiliser des fonctionnalités de chiffrement intelligent comme mesure de sécurité supplémentaire. Office 365 offre cette possibilité à l'aide du Service de gestion des droits RMS. L'utilisation de RMS offre aux utilisateurs, où qu'ils se trouvent, la flexibilité de sélectionner les éléments qu'ils souhaitent chiffrer, quel que soit l'endroit où est situé ce contenu. En outre, une caractéristique unique de RMS est d'offrir la possibilité de raisonner sur le contenu pour fournir une protection intelligente. Un utilisateur peut chiffrer du contenu et lui appliquer un traitement intelligent, tel que l'identification des personnes autorisées à accéder à ce contenu et le type d'accès dont elles disposent. Par exemple, Alice peut autoriser un petit groupe de personnes à voir du contenu, mais pas à modifier ou transmettre ce contenu à quelqu'un d'autre. Le chiffrement des courriers électroniques envoyés à des utilisateurs non-fédérées est disponible sous Office 365, permettant des services de chiffrement ad hoc avec n'importe quel destinataire. Office Professionnel Plus permet une sécurité avancée avec un support natif pour l'agilité cryptographique grâce à l'intégration dans les interfaces le Chiffrement de nouvelle génération (CNG) pour Windows. Les administrateurs peuvent spécifier les algorithmes cryptographiques à utiliser pour chiffrer et signer les documents.

Permettre l'accès utilisateur

Les données et les services Office 365 sont sécurisés au niveau data center, réseau, logique, stockage et acheminement. De plus, il est essentiel pour les clients de pouvoir contrôler qui peut accéder aux données et comment ces personnes autorisées utilisent des données. Office 365 utilise Windows Azure Active Directory comme plate-forme d'identité sous-jacente. Cela permet d'offrir aux utilisateurs d'Office 365 de puissantes options d'authentification avec un contrôle granulaire de la façon dont les professionnels du service informatique et les utilisateurs peuvent accéder au service et l'utiliser. Office 365 permet également l'intégration avec Active Directory dans l'environnement d'entreprise ou les autres magasins d'annuaires ou systèmes d'identité d'identité tels que Active Directory Federation Services (AD FS), ou des systèmes de jetons sécurisés (STS) pour permettre l'authentification sécurisée, basée sur les jetons de services.

Fédération d'identité côté client et système de sécurité à authentification unique

Les administrateurs peuvent fédérer sur site Active Directory ou d'autres magasins d'annuaires avec Windows Azure Active Directory, la plate-forme d'identité utilisée par Office 365. Une fois la fédération configurée, tous les utilisateurs d'Office 365 dont l'identité est dans le domaine fédéré peuvent utiliser leurs connexions d'entreprise existantes pour un accès authentifié à Office 365. La fédération permet une authentification sécurisée à base de jetons. Elle permet également aux administrateurs de créer des mécanismes d'authentification additionnels tels que :

- L'authentification à deux facteurs
- Le contrôle d'accès basé sur le client, ce qui permet aux organisations de contrôler comment les utilisateurs accèdent aux informations depuis des dispositifs spécifiques ou des lieux spécifiques ou une combinaison des deux (par exemple, en limitant l'accès à partir d'ordinateurs publics ou d'un réseau Wi-Fi ouvert).
- Le contrôle d'accès basé sur les rôles, une procédure similaire à la procédure du contrôle d'accès aux data centers Microsoft décrite ci-dessus dans la section « Opérations automatisées ».

Grâce à la fédération des messages instantanés, les utilisateurs de Lync Online peuvent envoyer des messages instantanés dans un environnement hautement sécurisé à des utilisateurs de Lync Online dans d'autres organisations, du serveur sur site Lync Server 2010, ou même du réseau public de messagerie instantanée Skype. Toutes les communications fédérées entre les systèmes de messagerie instantanée sont chiffrées à l'aide de serveurs proxy d'accès. En outre, Lync Online permet aux administrateurs d'enregistrer les conversations de messagerie instantanée.

L'authentification à deux facteurs

L'authentification à deux facteurs renforce la sécurité dans un environnement multi-dispositifs et dans un monde organisé autour du cloud. Microsoft propose une solution en interne pour l'authentification à deux facteurs avec l'option téléphone et prend également en charge les solutions tierces d'authentification à deux facteurs. La solution d'authentification à deux facteurs Microsoft basée sur le téléphone permet aux utilisateurs de recevoir leurs codes PIN sous forme de messages sur leur téléphone, puis d'entrer leur PIN qui sert de second mot de passe pour se connecter à leurs services.

Conformité

Office 365 offre toute une série de fonctions de conformité, y compris des fonctionnalités de prévention de la perte des données (DLP), de découverte électronique et d'audit et établissement de rapports. Cette offre de fonctionnalités préserve l'expérience utilisateur et n'affecte en rien sa productivité, ce qui se traduit par une plus grande acceptation des utilisateurs. Cette offre de fonctionnalités préserve l'experience utlisateur et n'affecte en rien sa productivité, ce qui se traduit par une plus grande acceptation de l'utilisateur.

Prévention de la perte des données (DLP)

Bien que les logiciels malveillants et les attaques ciblées puissent provoquer des violations de données, les erreurs des utilisateurs sont en fait une source de risque de perte de données bien plus importante pour la plupart des organisations. Exchange Online fournit une technologie de prévention des pertes de données (DLP) qui identifie, surveille et protège les données sensibles et aide les utilisateurs à comprendre et à gérer les risques de perte de données. Par exemple, DLP identifie proactivement les informations sensibles contenues dans un message de courrier électronique, telles que les numéros de sécurité sociale ou de cartes de crédit, et alerte les utilisateurs via des « conseils de politique » avant d'envoyer le message. Les administrateurs disposent d'une gamme complète de contrôles et peuvent personnaliser le niveau de restrictions pour leur organisation. Par exemple, les utilisateurs peuvent simplement être avertis sur les données sensibles avant l'envoi, l'envoi de données sensibles peut exiger une autorisation, ou l'envoi de données sensibles par les utilisateurs peut être complètement bloqué. Les fonctions DLP analysent les messages de courriers électroniques comme leurs pièces jointes, et les administrateurs ont accès à des rapports complets sur qui envoie quelles données.

Politiques d'audit et de conservation

Les politiques d'audit Office 365 permettent aux clients de journaliser les événements, y compris la visualisation, l'édition et la suppression des contenus tels que les messages de courrier électronique, les documents, les listes de tâches, les listes de problèmes, les groupes de discussion et les calendriers. Lorsque l'audit est activé dans le cadre d'une politique de gestion de l'information, les administrateurs peuvent visualiser les données d'audit et résumer l'usage courant. Les administrateurs peuvent utiliser ces rapports pour déterminer comment l'information est utilisée dans l'organisation, gérer la conformité, et enquêter sur les sujets de préoccupation.

eDiscovery

Facile à utiliser, le nouveau centre de découverte électronique eDiscovery peut être délégué à des utilisateurs spécialisés, tels que le responsable conformité ou le personnel des ressources humaines, pour mener des tâches de découverte électronique sans générer de coûts supplémentaires pour le département informatique. L'utilisation d'eDiscovery permet aux clients d'extraire du contenu à l'aide d'Exchange Online, SharePoint Online, Lync Online, et même du partage de fichiers. Le centre eDiscovery intégré à Office 365 permet aux clients de bénéficier d'une expérience unique pour la recherche et la conservation du courrier électronique, des documents et des boîtes aux lettres du site. Avec eDiscovery, les clients peuvent préciser spécifiquement ce qu'ils veulent rechercher et conserver. La possibilité pour les clients de trouver que ce qu'ils veulent et rien de plus peut contribuer à une réduction des coûts de découverte. Le processus eDiscovery ne représente aucune charge pour l'utilisateur pour la préservation et la recherche de données, parce que tous ces processus sont exécutés en arrière-plan.

Gestion du déversement des données

Office 365 dispose de fonction de conformité pour aider les clients confrontés à un « déversement » de données. Par exemple, si un client du gouvernement fédéral devait transmettre des données

confidentielles dans Office 365, il existe des moyens pour le client de supprimer eux-mêmes les données. Les responsables conformité et sécurité disposant de privilèges RBAC appropriés peuvent utiliser eDiscovery pour rechercher le message ou le document et le supprimer définitivement. Les disques durs utilisés pour stocker les données « déversés » ne sont jamais réaffectés, réparés ou déplacés pour toute autre raison hors de la zone physiquement sécurisée du data center d'Office 365. Ils sont détruits s'ils ne sont plus utilisés dans l'infrastructure d'Office 365.

Activation des contrôles anti-logiciels malveillants/antispam

Les clients disposent d'options de configuration pour les contrôles anti-logiciels malveillants/antispam dans le service. Les clients ont également le choix d'utiliser leur propre service anti-logiciels malveillants et un service tiers pour l'acheminement de et vers Office 365. Office 365 utilise une analyse anti-logiciels malveillants multi-moteurs pour protéger les messages entrants, sortants et internes contre les logiciels malveillants transmis par courrier électronique.

Office 365 évalue les messages reçus et attribue une valeur de niveau de confiance du courrier indésirable (SCL). Les messages ayant une valeur SCL élevée sont supprimés à l'entrée, tandis que les messages avec des valeurs SCL plus faibles sont déposés dans la boîte de réception des utilisateurs. Les messages avec des valeurs SCL limites sont placés dans les dossiers de courrier indésirable des utilisateurs, où ils sont automatiquement supprimés après 30 jours. Les administrateurs peuvent utiliser le Centre d'administration d'Office 365 pour gérer les contrôles anti-logiciels malveillants/antispam, y compris des options avancées de traitement du courrier indésirable et des listes d'expéditeurs approuvés et bloqués à l'échelle de l'organisation. Les utilisateurs peuvent gérer leurs expéditeurs approuvés et bloqués depuis leurs boîtes de réception Microsoft Outlook ou Microsoft Outlook Web App.

Les contrôles de contenu et l'analyse anti-logiciels malveillants multi-moteurs contribuent également à éliminer les documents contenant du code malveillant. Office 365 se base sur les extensions de noms de fichiers pour empêcher certains types de fichiers qui peuvent contenir du code malveillant d'être téléchargés sur le service ou d'y être récupérés. Office 365 utilise un filtre de message instantané intelligent (IIMF) pour aider à protéger le service et les réseaux des clients contre les logiciels malveillants et le spam envoyés par messagerie instantanée. Microsoft a développé l'IIMF en s'appuyant sur des années d'expérience dans l'exploitation de systèmes mondiaux de messagerie instantanée sécurisée.

Vérification indépendante et conformité

Office 365 a mis en oeuvre la sécurité sous forme d'un processus évolutif capable de s'adapter rapidement aux nouvelles tendances en matière de sécurité et aux besoins spécifiques de votre secteur. Microsoft effectue régulièrement des analyses de gestion des risques, et développe et maintient un

cadre de contrôle de sécurité qui répond aux normes les plus récentes. Le cycle de vie utile d'Office 365 intègre des examens internes et des audits externes par des organismes reconnus. Des relations de travail étroites avec les autres équipes Microsoft permettent une approche globale de la sécurisation des applications dans le cloud.

L'exploitation d'une infrastructure de cloud globale entraîne la nécessité de satisfaire à des obligations de conformité et de passer des audits menés par des tiers. Les obligations en matière d'audits émanent des demandes du gouvernement et du secteur, des politiques internes et des meilleures pratiques du secteur. Office 365 garantit que les attentes en matière de conformité sont constamment évaluées et intégrées. En conséquence, Office 365 a été vérifié de manière indépendante, y compris lors d'audits conformes aux normes ISO 27001 et SSAE16 SOC 1 (Type II), peut transférer des données à l'extérieur de l'Union européenne dans le cadre de l'accord Sphère de sécurité (Safe Harbor) entre les États-Unis et l'UE et des Clauses contractuelles types de l'UE, accepte de signer un Accord de partenariat HIPAA BBA avec l'ensemble des clients, a reçu l'autorisation d'exploitation pour opérer auprès d'une agence fédérale des États-Unis aux termes de la loi FISMA et a dévoilé ses mesures de sécurité dans le registre public de la Cloud Security Alliance. Office 365 étend les contrôles mis en place pour répondre à ces normes aux clients qui ne sont pas nécessairement soumis à ces lois ou contrôles spécifiques.

ISO 27001

Le service Office 365 a été conçu pour répondre aux normes ISO 27001 et a été le premier grand service de productivité cloud public pour entreprises à avoir mis en œuvre cet ensemble rigoureux de normes mondiales couvrant les contrôles physiques, logiques, et les contrôles de processus et de gestion.

FISMA

Office 365 a obtenu une autorisation modérée FISMA pour l'exploitation par plusieurs agences fédérales. L'exploitation aux termes de la loi FISMA exige la transparence et des rapports de sécurité fréquents à nos clients fédéraux aux États-Unis. Microsoft applique ces processus spécialisés dans l'ensemble de son infrastructure pour améliorer encore ses Services de sécurité en ligne et son Programme de conformité au profit des clients qui ne sont pas soumis aux exigences FISMA.

HIPAA BAA

Office 365 est le premier grand service de productivité cloud public pour entreprises à proposer un Accord de partenariat HIPAA BAA à tous ses clients. HIPAA est une loi des États-Unis qui s'applique aux organismes de soins de santé ; elle régit l'utilisation, la divulgation et la sauvegarde des informations de santé protégées, et impose aux organismes concernés de signer des Accords de partenariat avec leurs fournisseurs ayant accès à ces informations protégées.

Clauses contractuelles types de l'UE

Office 365 est devenu le premier grand service de productivité cloud public à signer les clauses contractuelles standard créées par l'Union européenne (connu sous le nom de « Clauses contractuelles types de l'UE ») avec tous ses clients. Les Clauses contractuelles types de l'UE concernent le transfert international de données. Office 365 est l'un des très rares services de cloud, sinon le seul, à avoir été

largement validé par les autorités européennes chargées de la protection des données (APD) pour son approche des Clauses contractuelles types de l'UE, y compris les APD de Bavière, du Danemark, de France, d'Irlande, du Luxembourg, de Malte et d'Espagne.

Cloud Security Alliance

Office 365 répond aux exigences de conformité et de gestion des risques telles que définies dans la Matrice de contrôle du Cloud (CCM) de la Cloud Security Alliance (CSA). La CCM est publiée par un organisme sans but lucratif, dirigé par ses membres, qui regroupe d'éminents praticiens du secteur et dont l'objectif est d'aider les clients à prendre les bonnes décisions lors du passage au cloud. La matrice fournit une compréhension approfondie des concepts de sécurité et de confidentialité et des principes conformes aux lignes directrices de la Cloud Security Alliance dans 13 domaines. Office 365 a publié un résumé détaillé de ses capacités par rapport aux exigences de la CCM qui illustre comment elles répondent à ces exigences et fournit aux clients des informations approfondies lui permettant d'évaluer les différentes offres sur le marché aujourd'hui.

Conclusion

Aujourd'hui, les entreprises ont besoin de services de productivité qui aident les utilisateurs à en faire plus à partir de pratiquement n'importe où, tout en maintenant la sécurité face à des menaces en constante évolution. Office 365 prend en charge ces deux types de besoins avec une plate-forme de productivité très sécurisée et basée sur le cloud. Les informations concernant la sécurité, la confidentialité, la conformité, la transparence et la continuité du service dans Office 365 se trouvent dans Office 365 Trust Center, le Centre de confiance et de transparence d'Office 365. La plate-forme Office 365 intègre la sécurité à tous les niveaux, du développement d'applications à l'accès de l'utilisateur final en passant par les data centers physiques. Aujourd'hui, de moins en moins d'organisation ont la capacité de maintenir un niveau de sécurité équivalent sur site à un coût raisonnable.

Surtout, les applications Office 365 incluent à la fois des fonctionnalités intégrées de sécurité qui simplifient le processus de protection des données et une flexibilité qui permet aux administrateurs de configurer, gérer et intégrer la sécurité d'une façon adaptée a leurs besoins d'affaires uniques. En choisissant Office 365, les entreprises choisissent un partenaire qui comprend vraiment les besoins de sécurité de l'entreprise et a obtenu la confiance de sociétés de toutes tailles dans presque tous les secteurs et zones géographiques.