



La sécurité dans Office 365

Livre blanc

Publication : juin 2011

Table des matières

3	Introduction
3	Enjeux
4	Une base sécurisée
5	Confidentialité et propriété des données
6	Sécurité intégrée
7	Flexibilité pour répondre à des besoins avancés en sécurité
7	Conclusion

Introduction

Ce document présente les pratiques et les technologies qui assurent une sécurité de haut niveau dans Microsoft Office 365 pour les entreprises de toutes tailles. Pour une analyse plus détaillée et plus complète de la sécurité dans Office 365, téléchargez la Description de la sécurité d'Office 365, disponible à l'adresse <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=6c6ecc6c-64f5-490a-bca3-8835c9a4a2ea>.

Microsoft® Office 365 met à la disposition des entreprises, quelle que soit leur taille, la puissance et la productivité du cloud en leur faisant économiser du temps et de l'argent et en libérant des ressources. Office 365 allie la suite de productivité Office bien connue aux versions cloud des tout derniers outils de communication et de collaboration de Microsoft : Exchange Online, SharePoint Online et Lync Online.

En autorisant un prestataire de service externe à stocker et gérer leurs données, les entreprises et organismes doivent prendre en considération la sécurité, la protection, la confidentialité et la propriété des données. Microsoft traite ces sujets avec beaucoup de sérieux et a appliqué l'expérience acquise depuis des années en informatique dans le cloud et sur site pour développer la sécurité et la confidentialité des services Office 365. Microsoft Online Services peut vous apporter les avantages du cloud et la sécurité de haut niveau que vous souhaitez, quelle que soit la taille de votre entreprise. Microsoft adopte une approche très complète pour protéger vos données à la fois au niveau physique (nous avons investi 2 milliards de dollars dans des centres de données à la pointe de la technologie) et au niveau logique (par exemple, nous appliquons pour nos services et nos logiciels des pratiques de conception qui prennent en compte la sécurité).

Office 365 fournit un accès sécurisé aux plateformes et aux équipements, ainsi que des technologies antivirus et anti-spam de grande qualité, automatiquement mises à jour pour assurer la protection contre les menaces les plus récentes. Les fonctions et les services de sécurité sont intégrés dans Office 365, ce qui vous fait gagner du temps et réaliser des économies par rapport à la sécurisation de vos systèmes informatiques. Office 365 vous permet de contrôler facilement les autorisations, les politiques et fonctionnalités via une console d'administration en ligne ; vous pouvez ainsi configurer Office 365 pour qu'il réponde à vos besoins spécifiques dans le domaine de la sécurité.

Enjeux

Les employés devenant de plus en plus mobiles, les informations de votre entreprise sont probablement accédées par plus de personnes, depuis plus d'endroits et à partir d'équipements très divers. Toutefois, ces pratiques augmentent la surface d'attaque de l'infrastructure informatique. Et les attaques deviennent de plus en plus sophistiquées et malveillantes. Aujourd'hui, le cybercrime est pratiqué par des professionnels très organisés, motivés par l'appât du gain. De ce fait, il est indispensable d'adopter une sécurité de haut niveau pour protéger vos systèmes et vos données. L'approche intégrale suivie par Microsoft inclut la conception de logiciels et de services plus sûrs, une surveillance efficace et une réponse rapide aux menaces, et une analyse approfondie des menaces émergentes afin d'adopter des mesures au plus vite, avant que ces menaces ne deviennent des problèmes. En raison de la croissance rapide de la

volumétrie des données générées par le fonctionnement quotidien des entreprises, la sauvegarde et la récupération des données représentent un coût important pour les départements informatiques. Les entreprises ont besoin de solutions abordables et capables de monter en charge, assurant la disponibilité de leurs données 24 heures sur 24, 7 jours sur 7.

En étant conscientes de tous ces enjeux, de nombreuses entreprises découvrent qu'Office 365 peut leur apporter un haut niveau de sécurité pour un coût inférieur à des serveurs installés sur site. Les clients d'Office 365 n'ont plus à gérer en interne le déploiement et l'administration de solutions coûteuses pour la sauvegarde et la restauration des données, et pour la protection antivirus et anti-spam. Office 365 intègre une grande capacité à monter en charge ainsi qu'un mécanisme de reprise après sinistre pour faire face à des volumes croissants de données métier critiques, à un coût fixe et prévisible. Se distinguant nettement des autres offres d'outils de productivité dans le cloud proposées par d'autres acteurs du marché, Office 365 donne la possibilité de gérer temporairement ou de façon permanente un environnement hybride, qui vous permet d'évoluer progressivement vers le cloud ou de conserver certains utilisateurs dans vos systèmes sur site.

Une base sécurisée

Microsoft fournit des services en ligne depuis de nombreuses années. Microsoft Global Foundation Services (GFS), le groupe responsable de l'hébergement d'Office 365 et de tous les services en ligne de Microsoft, est né en 1994 avec la mise en place de MSN. Il s'est rapidement développé et est devenu au fil des ans l'une des entités les plus importantes d'Internet. L'infrastructure des services en ligne de GFS est régulièrement contrôlée et auditée par des organismes renommés, extérieurs à Microsoft. En raison de notre approche globale et complète de la sécurité et de la confidentialité, Microsoft Global Foundation Services a obtenu les certifications ISO 27001 et EU Safe Harbor, et a réussi l'audit SAS 70 Type II. Office 365 est basé sur une technologie qui a fait ses preuves ; c'est la dernière version de notre produit précédemment nommé BPOS (Business Productivity Online Services), qui compte des centaines de milliers de clients satisfaits. Avec Office 365, vous bénéficiez de toute notre expérience dans le cloud.

Microsoft sait que la sécurité est un travail permanent, pas un état figé. La sécurité doit en permanence être maintenue, améliorée et vérifiée par du personnel expérimenté et formé ; elle nécessite des technologies de mises à jour des logiciels et des matériels ; elle est assurée par les processus très fiables que nous avons mis en place pour la conception, la construction, l'exploitation et la maintenance de nos services.

Les données Office 365 sont stockées dans le propre réseau de centres de données de Microsoft, offrant une haute disponibilité et stratégiquement répartis dans le monde entier. Ces centres sont conçus dès le départ pour protéger les services et les données contre tout risque, qu'il s'agisse d'une catastrophe naturelle ou d'un accès non autorisé. Nous appliquons les meilleures pratiques pour assurer la sécurité physique : matériel très haut de gamme, accès sécurisés, alimentations redondantes, réseaux de fibres redondés, et de nombreuses autres techniques. En raison de la redondance mise en place, les mises à jour peuvent être déployées sans que nos utilisateurs ne constatent l'arrêt de nos systèmes. Nos systèmes sont

protégés au niveau logique par une isolation très forte des données, un contrôle permanent et par de nombreuses pratiques et technologies ayant fait leurs preuves. Toutes les tâches relatives à la sécurité physique et logique sont effectuées par notre personnel dans nos centres de données, ce qui allège d'autant votre charge de travail pour le maintien de la sécurité de vos données et systèmes.

Depuis 2002, Microsoft a développé l'Initiative pour l'Informatique de confiance, qui vise à promouvoir en interne comme sur le marché l'adoption des meilleures pratiques dans le domaine de la sécurité. Une part importante de l'Initiative pour l'informatique de confiance réside dans la conception des logiciels qui prennent en compte la sécurité dès le début de leur conception. Ainsi, les produits et les services qui composent Office 365 — Microsoft Exchange Online, Microsoft SharePoint® Online, Microsoft Lync® Online et Microsoft Office Professional Plus — ont été conçus en respectant toutes les pratiques rigoureuses de sécurité définies dans le Microsoft Security Development Lifecycle (SDL). SDL est en permanence mis à jour et communiqué gratuitement à l'industrie du logiciel afin de mettre en place de meilleures pratiques dans le domaine de la sécurité, quels que soient les fournisseurs et les plateformes.

Vous souhaitez que vos données métier soient en permanence disponibles pour vos utilisateurs. En raison de l'expérience de Microsoft dans les services d'hébergement, et de l'étroite relation qui existe entre Office 365 et les équipes produits et support Microsoft, Office 365 peut répondre à la demande des clients pour une haute disponibilité des services. Les technologies et les protocoles utilisés permettent à Office 365 de redémarrer rapidement, même après un incident grave.

Confidentialité et propriété des données

Microsoft a mis en place une politique cohérente, fiable et transparente pour le respect de la confidentialité, afin que vous restiez totalement propriétaire de vos données. Le [Trust Center](#) vous explique en détail comment nous gérons et utilisons les données collectées lors de vos interactions avec Microsoft Online Services. Si vous décidez d'arrêter votre utilisation d'Office 365, nous vous offrons 90 jours supplémentaires de fonctionnalités réduites, afin de vous permettre d'exporter toutes vos données vers vos propres systèmes. Microsoft vous avertit aussi de nombreuses fois avant d'effacer des données clients.

Isolation des données

Office 365 est un service mutualisé, ce qui signifie que les données sont réparties sur différentes ressources matérielles. Par conséquent, vos données peuvent être stockées sur le même matériel que celles d'autres clients. C'est ainsi qu'Office 365 peut vous être proposé à un coût intéressant, avec de fortes capacités de montée en charge. Bien sûr, Microsoft a conçu cette architecture mutualisée afin qu'Office 365 apporte toutes les garanties de sécurité et de respect de la confidentialité des données. Ainsi, le stockage et le traitement des données sont parfaitement cloisonnés de façon logique entre les clients via la technologie Active Directory spécialement conçue pour cet objectif. Pour les entreprises qui

souhaitent une isolation supplémentaire, il existe une version spécifique d'Office 365 qui stocke vos données sur un matériel dédié.

Sécurité intégrée

Contrairement à une installation sur site protégée par un pare-feu et accessible via un réseau privé virtuel (VPN), Office 365 est conçu spécifiquement pour être accédé de manière sécurisée depuis Internet. Il existe deux options pour l'identification de l'utilisateur : un identifiant Microsoft Online et un identifiant fédéré. Dans le premier cas, l'utilisateur crée un compte Microsoft Online Services pour accéder à Office 365. Avec un seul identifiant et un seul mot de passe, l'utilisateur accède à tous les services Office 365. L'application de signature unique assiste l'utilisateur pour le choix et l'utilisation d'un mot de passe fort, ce qui renforce la sécurité des services.

Dans le cas de l'identification fédérée qui s'appuie sur Active Directory Federation Services (un service de Microsoft Windows Server 2008) déployé sur le réseau interne, chaque utilisateur d'Office 365 s'authentifie avec son identifiant et son mot de passe d'entreprise habituels. Dans ce cas, les identités sont gérées uniquement en interne. Cela permet aussi aux entreprises d'utiliser une authentification à deux facteurs (comme une carte à puce ou un système biométrique en plus du mot de passe) afin de renforcer la sécurité.

Quelle que soit la méthode d'authentification utilisée, les connexions établies avec le service Office 365 à travers Internet sont chiffrées via le protocole standard SSL/TLS à 128 bits. Office 365 implémente d'autres mesures de sécurité pour protéger les informations sensibles, comme S/MIME (Secure/Multipurpose Internet Mail Extensions) pour le chiffrement à clés publiques et les signatures numériques, ainsi que la protection par Information Rights Management pour restreindre l'accès et les actions possibles sur les documents, emails et même les messages vocaux.

Avec Office 365, vous accédez à tout votre environnement comme vos boîtes aux lettres, vos sites Web SharePoint et vos stockages de documents. Vous gardez le contrôle sur les politiques de sécurité et les comptes utilisateurs. Ce degré de contrôle vous permet d'appliquer de façon efficace les politiques de sécurité et de confidentialité de votre entreprise. Les politiques et les utilisateurs s'administrent via une console Web ou via Remote PowerShell pour l'automatisation des tâches routinières.

Forefront Online Protection for Exchange

Pour protéger les emails entrants, sortants et internes ainsi que les fichiers partagés contre les virus et le spam, Office 365 inclut Microsoft Forefront® Online Protection for Exchange. Cette solution antivirus/anti-spam conçues sur plusieurs niveaux, utilise simultanément plusieurs moteurs d'analyse pour identifier de façon très précise les menaces éventuelles et les bloquer, en minimisant les « faux positifs » qui peuvent conduire au blocage inopiné d'emails. Les technologies Forefront incluses dans Office 365

sont constamment mises à jour avec les dernières signatures de menaces, afin de vous protéger contre les nouvelles menaces sans que vous ayez à intervenir.

Flexibilité pour répondre à des besoins avancés en sécurité

Certaines entreprises sont soumises par la réglementation à des contraintes particulières ou à des impératifs de sécurité interne qui dépassent les possibilités d'un environnement mutualisé. Par exemple, des restrictions peuvent s'appliquer sur les pays où peuvent être stockées les données. Dans certains cas, toutes les données du client doivent être stockées dans un pays en particulier. Microsoft a conçu Office 365 pour fournir une flexibilité maximale aux entreprises qui peuvent choisir leur style de déploiement. Par exemple, vous pouvez déployer aujourd'hui Microsoft Exchange Server, Microsoft SharePoint® Server et Microsoft Lync® Server en interne, puis envisager de passer au cloud par la suite. Vous pouvez choisir de conserver certains utilisateurs sur site tout en plaçant les autres dans le cloud grâce à la coexistence possible entre les serveurs sur site et ceux d'Office 365 ; les utilisateurs continuent de partager leurs informations de présence et leurs calendriers, et de communiquer entre eux comme s'ils étaient tous hébergés dans la même infrastructure.

Conclusion

Placer les services de productivité dans le cloud impose la prise en compte de manière sérieuse des questions de confidentialité et de sécurité. Office 365 a été conçu pour vous apporter une sécurité de très haut niveau pour que vous puissiez migrer vers le cloud en toute confiance. Nos centres de données sont conçus, construits et administrés en respectant une stratégie de défense en profondeur tant au niveau logique que physique et tous nos services sont développés en appliquant les principes de SDL (Security Development Lifecycle). Pour les utilisateurs comme pour les administrateurs, Office 365 simplifie l'accès et l'utilisation des données et des services tout en respectant les bonnes pratiques recommandées dans le domaine de la sécurité. Nous avons conçu nos services de productivité dans le cloud en pensant à vous, afin que vous puissiez bénéficier des avantages du cloud comme vous le souhaitez et à votre rythme.

Ressources

Office 365 : <http://office365.fr>

Microsoft Global Foundation Services : <http://www.globalfoundationservices.com>

Vidéos des centres de données Microsoft

<http://www.globalfoundationservices.com/infrastructure/videos.html>

Informatique de confiance Microsoft : <http://www.microsoft.com/about/twc/en/us/default.aspx>

SDL (Security Development Lifecycle) : <http://www.microsoft.com/security/sdl/default.aspx>

Forefront Online Protection for Exchange : <http://technet.microsoft.com/en-us/forefront/cc540243>

