Dropbox for Business

Dropbox Entreprises aide les services informatiques à réduire les risques

Les solutions de partage de fichiers utilisées dans le passé avaient été conçues pour garantir la sécurité des données internes. En revanche, elles n'offrent pas de protection dans les situations de partage externe des données et de mobilité des utilisateurs – autant de situations qui peuvent être à l'origine de risques informatiques inattendus. Dropbox Entreprises permet aux utilisateurs de partager des données en interne comme avec l'extérieur, sans limiter le contrôle et la surveillance des flux de données exercés par le service informatique. Grâce aux commandes de partage, aux fonctions d'administration et au suivi de l'activité proposés par Dropbox Entreprises, le service informatique peut plus facilement réduire les risques pour que toutes vos équipes collaborent en toute sécurité.

E-mail

La messagerie électronique est le moyen le plus couramment utilisé pour partager des données en externe. Une enquête réalisée récemment par Dropbox a révélé que 88 % des employés de bureau recouraient à des pièces jointes à des e-mails pour envoyer des fichiers.[1]

Risques

Contrôle des données : dès lors qu'une pièce jointe est envoyée, les données qu'elle contient peuvent être transférées à n'importe qui, ce qui rend difficile tout suivi des personnes qui y ont accès. En outre, il n'est pas possible d'annuler le partage de données envoyées dans une pièce jointe.

Contrôle des versions : quand un document est modifié, un nouveau fichier doit être diffusé. Le suivi des versions devient difficile et les risques de perte ou de fuite des données se multiplient.

Utilisation d'applications : du fait des limites de taille des pièces jointes, les utilisateurs risquent davantage d'utiliser d'autres produits pour envoyer des fichiers volumineux, produits qui ne sont pas contrôlés par le service informatique.

Avantages de Dropbox

Commandes de partage : l'accès aux liens ou dossiers partagés peut être annulé à tout moment si vous ne souhaitez plus partager un document.

Journaux d'audit : grâce aux journaux d'audit de partage, les administrateurs savent quels utilisateurs ont partagé quels documents. Ils peuvent également connaître le nombre de vues des liens partagés, y compris de ceux envoyés à l'extérieur.

Contrôle des versions : grâce aux dossiers partagés, les collaborateurs ont accès en permanence à la version la plus récente d'un fichier. Les liens partagés sont mis à jour dès que les documents correspondants sont modifiés : ainsi, même les utilisateurs externes disposant d'un accès en lecture seule ont les informations correctes.

Utilisation d'applications : les collaborateurs ont à leur disposition plusieurs options de partage de fichiers à l'aide de dossiers et de liens partagés. Ils peuvent notamment le faire directement depuis leur ordinateur, ou même depuis Microsoft Office. Les fonctionnalités de partage de Dropbox sont simples d'utilisation et ne sont assorties d'aucune limite de taille de fichier ; ainsi, les utilisateurs n'ont pas à se tourner vers des solutions non validées par le service informatique.

Dropbox for Business

Dropbox Entreprises aide les services informatiques à réduire les risques

Suite

Serveur FTP sur site

Contrairement aux pièces jointes aux e-mails, les serveurs FTP ne sont assortis d'aucune limite de taille de fichier. Ils renforcent la sécurité et le contrôle des opérations de partage, mais présentent eux aussi des risques.

Risques

Faible taux d'adoption : un serveur FTP ne constitue pas une solution particulièrement conviviale et est parfois mal intégré dans les workflows, ce qui se traduit par un faible taux d'adoption. Les utilisateurs peu satisfaits peuvent se tourner de nouveau vers des solutions non validées par le service informatique, ce qui réduit globalement le contrôle et la visibilité.

Identifiants de connexion partagés : avant de pouvoir utiliser un serveur FTP, les collaborateurs doivent obtenir un compte auprès du service informatique, car ce type de solution n'est pas compatible avec des méthodes telles que l'authentification unique. Il n'est pas rare qu'ils partagent leurs identifiants de connexion pour gagner du temps. Le service informatique voit ainsi ses capacités limitées en termes d'autorisation d'accès et de contrôle de l'accès utilisateur.

Visibilité limitée : il est difficile de savoir précisément qui a accès au serveur FTP et quels sont les fichiers qui y sont placés.

Forte sollicitation du service informatique : la gestion opérationnelle et matérielle d'un serveur FTP nécessite des ressources informatiques non négligeables. En l'absence d'une gestion efficace, des attaques jour zéro et des vulnérabilités non corrigées peuvent créer des failles de sécurité sur le serveur et le réseau de manière générale.

Avantages de Dropbox

Commandes de partage : taux d'adoption élevé : doté d'une interface particulièrement simple d'utilisation et intégrée aux workflows existants, Dropbox Entreprises est immédiatement adopté par les utilisateurs. Le service informatique dispose ainsi d'une plus grande visibilité sur les données et en conserve la propriété.

Des identifiants de connexion pour chaque utilisateur : il suffit de quelques secondes aux collaborateurs pour créer un compte Dropbox Entreprises, ce qui permet de contrôler bien plus facilement l'accès aux données par utilisateur. Les données peuvent n'être partagées qu'avec les destinataires souhaités et les opérations de partage sont accessibles dans l'interface d'administration, ce qui permet de savoir qui a accès à quoi.

Gestion simplifiée : le service informatique n'a aucun matériel à gérer avec Dropbox Entreprises. Les données sont stockées en toute sécurité et bénéficient de plusieurs niveaux de protection. Pour en savoir plus sur les normes et règles de sécurité de Dropbox, consultez la page dropbox.com/business/trust.

Granularité des opérations de connexion : le flux d'activité Dropbox permet de savoir qui a accès aux données et quel usage en est fait.

Dropbox Entreprises aide les services informatiques à réduire les risques

Suite

Clés USB

Une clé USB est un outil très pratique utilisé au quotidien. Elle a été conçue pour simplifier le transfert de données, mais est difficile à gérer par le service informatique. Des solutions plus récentes peuvent offrir davantage de sécurité tout en restant simples d'utilisation.

Risques

Matériel perdu : une clé USB peut être égarée et les données qu'elle contient perdues.

Vulnérabilité : une clé USB peut être infectée par des virus ou des programmes malveillants.

Visibilité limitée : une clé USB n'offre au service informatique aucune visibilité sur l'accès ou le partage des données.

Avantages de Dropbox

Simplicité d'utilisation maintenue : Dropbox Entreprises conserve l'interface "glisser-déposer" des clés USB, fortement appréciée par les utilisateurs pour le partage de fichiers.

Aucun risque de matériel perdu : Dropbox Entreprises offre des niveaux identiques de mobilité et de partage, sans recourir à du matériel physique. Grâce à ses fonctionnalités de récupération de fichiers supprimés et d'historique des versions, aucune donnée n'est perdue.

Visibilité renforcée : l'accès aux clés USB est anonyme. En revanche, Dropbox Entreprises conserve des journaux détaillés des accès aux liens partagés, ce qui permet aux administrateurs de mieux contrôler l'activité des utilisateurs et les opérations de partage de fichiers.

Appareils protégés : quand un collaborateur associe un appareil à un compte Dropbox Entreprises, le service informatique peut protéger les informations stockées sur cet appareil en cas de perte ou de vol.

[1] Source : enquête TNS-Dropbox, "Patterns of Collaboration", février 2015