ipswitch

Secure. Control. Perform.

UN LIVRE BLANC D'IPSWITCH

7 étapes vers la conformité avec le RGPD

Comment le règlement général relatif à la protection des données (RGPD) s'applique aux transferts externes de fichiers

ipswitch

Introduction

Pour les cybercriminels, le vol de données personnelles génère un marché noir florissant à l'échelle mondiale. Définies généralement comme tout type de données permettant d'identifier un individu, les données personnelles font de toute organisation qui recueille des informations (mots de passe, numéros de carte de crédit, données de santé ou adresses) une cible privilégiée pour les cybercriminels. Sans surprise, depuis 2013 les violations de la sécurité représentent près de 6 milliards de données volées à l'échelle mondiale.

En réponse à cette menace croissante, la Commission européenne met en place le règlement général relatif à la protection des données (RGPD), qui a été accepté par le Parlement européen et le Conseil et sera adopté le 25 mai 2018. Le RGPD remplace la directive sur la protection des données en place depuis 20 ans, renforce de nombreuses clauses déjà présentes dans ladite directive, et définit des normes plus sévères pour la protection des informations personnelles des résidents de l'Union européenne.

Aujourd'hui le transfert de données personnelles est un processus opérationnel central des services informatiques dans un large éventail de secteurs d'activité. Sur le plan de la sécurité, les données en transit sont menacées car elles représentent une occasion unique d'être interceptées au cours de la transmission, ou lorsqu'elles sont stockées et traitées sur le lieu de destination.

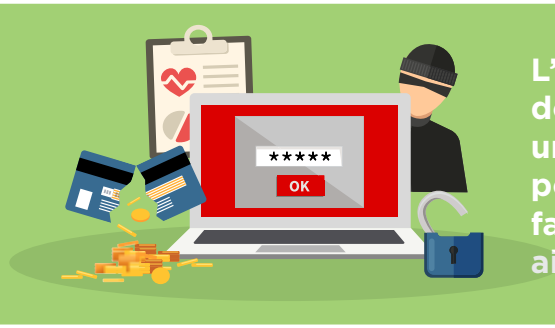
Dans le cadre de leur préparation au RGPD, les services informatiques gérant des transferts externes de données personnelles doivent revoir les sept contrôles de sécurité décrits dans ce livre blanc. Ils sont généralement reconnus comme des pratiques exemplaires visant à garantir la sécurité, avant, pendant et après le transfert externe de données protégées.

La menace

La définition courante des données personnelles est la suivante : il s'agit de toutes informations qui, en propre ou combinées avec d'autres données auxquelles leur propriétaire peut accéder, permettent d'identifier un individu. Pour un cybercriminel, la collecte, le traitement et le transfert de données personnelles font des organisations d'un grand nombre de secteurs d'activité des cibles lucratives en matière d'attaques sous la forme de : hameçonnage, déni de service, ransomware (faux logiciel de décodage et de protection) et menaces avancées persistantes.

Depuis 2013, les violations de la sécurité enregistrées officiellement comptent pour plus de 5,8 milliards de données perdues dans le monde. Il s'agit de mots de passe, dossiers de santé, adresses de facturation et informations de crédit.

Même si aucune industrie dont les acteurs collectent et enregistrent des données personnelles n'est à l'abri, selon des sources telles que le Breach Level Index, 80 % des violations se produisent dans les secteurs de la technologie, de la vente au détail, des



L'importance accordée aux données personnelles génère un marché noir florissant pour les outils et le savoir-faire des cybercriminels, ainsi que le vol de données.

ipswitch

finances et de la santé. Si votre organisation recueille, enregistre, partage, traite ou transmet des données personnelles, vous êtes une cible probable des attaques.

Une partie importante de ces données volées sont écoulées sur un marché noir sur lequel les prix varient en fonction de leurs type et âge (date à laquelle elles ont été subtilisées). Par exemple, les prix par enregistrement pour les mots de passe varient entre 0,10 et 0,20 €, alors que les numéros de cartes de crédit volées récemment peuvent atteindre entre 30 et 50 €.

Si votre organisation collecte ou traite les données personnelles de résidents de l'Union européenne, qu'elle y soit implantée physiquement ou pas, vous êtes soumis au RGPD. Aux termes du RGPD, la perte de données en raison de l'insuffisance de règles et de mesures de protection adéquates peut générer des amendes pouvant représenter 4 % du chiffre d'affaires mondial d'une entreprise.

Depuis 2013, les **violations de la sécurité** au niveau mondial comptent pour **5,8 milliards de données perdues.**

Source : Breach Level Index

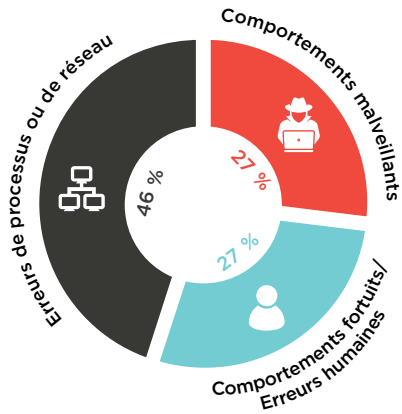
L'ennemi

Qui est responsable des violations et vols de données ? Alors que les médias nous font croire que les états nations et les cybercriminels sont majoritairement à l'origine de nos problèmes, la vérité est beaucoup moins évidente qu'elle n'y paraît. Une étude récente d'Ipswitch portant sur 255 professionnels de l'informatique a montré que seulement 27 % des violations de données résultent de comportements malveillants. Les comportements accidentels ou les erreurs humaines comptent également pour 27 % des violations de données. Quant aux erreurs de processus ou réseau, elles ne représentent pas moins de 46 % de l'ensemble des failles de sécurité ! Nous savons qui est l'ennemi et cet ennemi, c'est nous.

En fait, les pertes de données se produisent principalement du fait qu'un employé au sein de l'organisation ou chez le partenaire ne respecte pas les règles. Ainsi la transmission de données par des moyens non sécurisés (pièces jointes d'e-mails ou services Web grand public), ou les attaques d'ingénierie sociale via une messagerie ou les médias sociaux, illustrent ces défaillances.

Bien sûr dans certains cas, de nombreux enregistrements sont volés par le biais d'attaques avancées persistantes de cybercriminels, mais même dans ce scénario, une part de la chaîne implique habituellement la participation involontaire des employés ou partenaires.

Causes des failles de sécurité



Votre exposition au danger

Le RGPD définit les « contrôleurs » et les « opérateurs » comme deux types différents d'organisations auxquelles la réglementation s'applique. Le contrôleur détermine le comment et le pourquoi du traitement des données personnelles alors que l'opérateur agit au nom du contrôleur. Par exemple, si vous êtes une banque qui sous-traite les processus de transmission électronique des chèques pour le portail en ligne de votre client, le sous-traitant est un opérateur.

Le RGPD impose des obligations légales spécifiques aux opérateurs, notamment le devoir de mettre en place un chemin d'audit des activités de traitement des données. Aux termes du RGPD, les opérateurs engagent bien davantage leur responsabilité qu'auparavant sous la directive sur la protection des données, lorsque survient une violation de la sécurité.

Si vous êtes un contrôleur, le RGPD vous impose des obligations plus lourdes pour garantir que les opérateurs agissent en conformité. Vous n'êtes pas dégagé de vos obligations sur la protection des données si une faille éclate dans le réseau d'un opérateur.

ipswitch

Lors d'une récente attaque en escroquerie par e-mail, les employés d'un organisme de santé ont été invités à répondre avec leurs noms d'utilisateur et mots de passe EFSS – **60 % s'y sont pliés.**

Il s'agit d'un facteur important concernant l'application de règles de sécurité au transfert de données personnelles entre les contrôleurs et les opérateurs. Non seulement le transfert doit être sécurisé, mais les données doivent aussi être protégées lorsqu'elles sont traitées. Dans certains cas le RGPD peut également être utilisé pour certifier qu'une fois le traitement terminé, l'opérateur doit supprimer toutes les données personnelles qui ne sont plus nécessaires.

La première étape dans l'évaluation de votre état de préparation à la conformité au RGPD doit consister à mesurer votre exposition au risque de perte de données via des échanges contrôlés et ad hoc avec des intervenants externes. Les trois aspects à prendre en compte sont les suivants :

- La protection de vos principaux processus de transfert de fichiers.
- Le risque de transmissions ad hoc de données personnelles via des pièces jointes par les employés.
- La prévalence/protection de la transmission de fichiers basée sur le cloud.

LES PRINCIPAUX PROCESSUS DE TRANSFERT DE FICHIERS

Très probablement vos principaux processus de transfert de fichiers, notamment ceux impliquant des données personnelles, sont déjà centralisés à l'échelle d'un petit groupe de serveurs FTP hautement sécurisés. Avec un peu de chance, ils utilisent SFTP ou FTPS qui exploitent les mécanismes SSH ou SSL pour assurer des transmissions et authentifications cryptées. Si tel n'est pas le cas, vos problèmes sembleront peut-être trop importants pour être abordés par ce livre blanc, mais nous vous recommandons de lire ce document dans tous les cas.

Si tel est le cas, vous devez savoir que même les processus de transfert de fichiers sécurisés (SFTP/FTPS) ont des limites qui vous exposent à un risque accru de failles de la sécurité et de non-conformité. Parmi les éléments majeurs non répertoriés dans les critères des meilleures pratiques, citons l'automatisation, la visibilité, la journalisation sécurisée et verrouillée et la non-répudiation.

Les risques relatifs à la sécurité/conformité qui pèsent sur FTP sont les suivants :

- **Absence de cryptage :** Si le serveur n'est pas compatible SFTP ou FTPS, les transmissions de fichiers sont au format texte brut (non cryptés) et vulnérables au vol lors du transit via un certain nombre de technologies faciles à utiliser. L'exposition des données personnelles formatées en texte brut sur l'Internet public est sans aucun doute une violation grave du RGPD.
- **Automatisation insuffisante :** Les transferts de fichiers répétitifs représentent un processus lourd dans la plupart des environnements FTP, avec pour corollaire des risques d'erreur humaine et de pertes de données pour les organisations. L'automatisation des workflows de transferts de fichiers fournit un mécanisme de gouvernance visant à réduire les risques de pertes de données et d'amendes pour non-conformité.
- **Manque de visibilité :** Les serveurs FTP n'ont pas le niveau de visibilité et de journalisation requis pour obtenir la certification de conformité. Les journaux doivent être verrouillés et consigner la date de transfert des fichiers, indiquer s'ils ont été reçus par le destinataire prévu et s'ils ont été supprimés par la suite.
- **Évolutivité insuffisante :** Souvent les organisations s'appuient sur leur service informatique pour développer un ensemble de scripts propriétaires permettant d'automatiser leurs activités de transfert de fichiers. À mesure que les besoins de l'organisation évoluent, la gestion de ces scripts devient lourde et complexe, ce qui peut générer des failles de sécurité imprévues.

Les services informatiques doivent être particulièrement vigilants face à l'utilisation de technologies de partage de fichiers non sécurisées telles que les transferts FTP, la transmission d'e-mails et les services de cloud grand public par les employés et les partenaires externes.

ipswitch

TRANSFERTS DE FICHIERS AD HOC ET TRANSMISSIONS BASÉES SUR LE CLOUD

Afin d'assurer la conformité avec la réglementation sur la protection des données, votre organisation doit mettre en œuvre des processus qui garantissent un traitement sécurisé des données personnelles, et contrôler qu'ils sont respectés. Comme vulnérabilité notable, citons la probabilité qu'un employé envoie des données réglementées via un canal non sécurisé (pièce jointe d'un e-mail ou service de partage de fichiers grand public basé sur le cloud, par exemple).

Risques pour la sécurité/conformité générés par les e-mails et les partages de fichiers basés sur le cloud

- **Cryptage :** Les fichiers ne sont probablement pas cryptés sur les postes de travail des utilisateurs et en transit.
- **Distribution :** Il n'y a pas de garantie que les données transmises soient reçues par, et seulement par, le destinataire visé.
- **Durée de vie des données :** Les fichiers peuvent ne pas être supprimés du serveur de messagerie ou du référentiel du cloud et les données risquent d'être exposées pendant des mois après l'échange initial.

Contrôles de sécurité de transfert de fichiers

Au final, la protection des données devient une affaire de gouvernance, d'application de règles et de mise en œuvre d'obligations spécifiques en matière de sécurité. La norme internationale ISO/IEC 27001 est largement reconnue comme étant la meilleure pratique de référence en matière d'obligations de sécurité par les organismes réglementaires du monde entier. Son influence sera sans doute forte pour déterminer les certifications de conformité au RGPD. Le tableau ci-dessous met en évidence sept des meilleures pratiques de contrôle de la norme ISO/IEC 27001 les plus pertinentes concernant les opérations de transfert externe de fichiers.

Obligation de sécurité	ISO 27001	RGPD/DPD	Contrôle de transfert de fichiers
1. Conformité	A.18	Oui	Automatisation
2. Protection des communications	A.13	Oui	Contrôle et visibilité
3. Politiques de sécurité des informations	A.5	Oui	Protection des informations
4. Contrôle d'accès	A.9	Oui	Authentification
5. Cryptographie	A.10	Oui	Cryptographie
6. Protection physique et de l'environnement	A.11	Oui	Architecture sécurisée
7. Protection de la continuité des activités	A.17	Oui	Basculement

ipswitch

1

AUTOMATISATION

Les workflows de transfert de fichiers couramment utilisés doivent être automatisés afin de minimiser la portée des erreurs humaines qui pourraient entraîner des pertes de données. Vos outils de transfert de fichiers doivent prendre en charge des fonctions telles que le renvoi automatique, la correction d'erreurs et la confirmation de réception de tous les transferts de données.

2

CONTRÔLE ET VISIBILITÉ

Le contrôle et la visibilité des flux de données sont des critères déterminants pour une gestion efficace de la sécurité, et essentiels pour valider la conformité. Vos outils doivent faciliter la visibilité et le contrôle à un niveau central, ainsi que l'autorisation préalable de tous les transferts de fichiers. Les journaux doivent être conservés dans une base de données verrouillée afin d'assurer l'intégrité des chemins d'audit.

3

PROTECTION DES INFORMATIONS

Vos technologies, outils ou processus doivent assurer des contrôles d'intégrité des fichiers, la suppression des données après réception, ainsi que la non-répudiation (l'expéditeur et le destinataire doivent tous deux être autorisés et authentifiés pour accéder aux données). L'existence d'un chemin d'audit verrouillé permettant d'établir un suivi de l'intégrité, de la diffusion, de l'authentification, de la non-répudiation et de la suppression des fichiers transmis en externe après leur transfert représente un aspect important de la conformité.

4

AUTHENTIFICATION

L'authentification des utilisateurs et des administrateurs constitue un aspect essentiel de la sécurité et de la conformité. Vos systèmes de transfert de fichiers doivent être capables de prendre en charge un ensemble de mécanismes de contrôle d'accès, notamment l'intégration aux annuaires centraux des utilisateurs, le contrôle d'accès basé sur des règles et l'authentification unique comme l'authentification à plusieurs facteurs.

5

CRYPTOGRAPHIE

Les algorithmes de chiffrement ont une durée de vie limitée. Souvent les normes de conformité ne permettent pas l'utilisation de systèmes fragilisés. Par conséquent, il est essentiel que vos systèmes de partage de données utilisent de puissants mécanismes cryptographiques à la pointe de la technologie afin de permettre la sélection, la distribution et la protection sécurisées des clés de chiffrement. Pour anticiper le futur renforcement de la législation sur la protection des données, vos systèmes doivent garantir la protection et l'intégrité permanentes des données, qu'elles soient en transit ou à l'état de stockage.

6

ARCHITECTURE SÉCURISÉE

L'architecture de vos systèmes doit s'intégrer avec les infrastructures et applications de sécurité existantes. Les systèmes doivent également garantir qu'aucune donnée non cryptée ne se trouve sur le serveur DMZ, ou résilier les demandes entrantes d'authentification et de transfert de données avec un serveur passerelle proxy au niveau du DMZ.

ipswitch

7

BASCULEMENT

La continuité de l'activité en mode sécurisé est l'une des principales obligations de nombreuses réglementations sur la protection des données. Cette exigence vise à protéger la confidentialité, l'intégrité et la disponibilité des transferts de fichiers à tout moment en cas d'erreur, d'accident ou de panne. Une solution redondante automatique et sécurisée est essentielle pour garantir que les transferts de fichiers ont abouti ou sont relancés jusqu'à ce qu'ils soient terminés.

Fonctions de conformité d'Ipswitch® MOVEit

MOVEit® est un système de transfert de fichier automatisé qui vous permet de gérer, de visualiser et de contrôler les échanges de données sensibles avec des interlocuteurs externes en respectant les lois sur la protection des données. Le tableau ci-dessous indique comment MOVEit met en application chacune des sept principales meilleures pratiques visant à garantir la conformité à la législation sur la protection des données.

Exigences de sécurité	MOVEit Control
Conformité	MOVEit contribue à garantir que les transferts de fichiers sont sécurisés, que les données sont protégées en permanence, et que les enregistrements de transferts sont protégés dans des chemins d'audit verrouillés pendant la durée légale, avant leur destruction assurée.
Protection des communications	MOVEit permet une visibilité et un contrôle à un niveau central, l'autorisation préalable de tous les transferts de fichiers, ainsi que le cryptage, la traçabilité et la non-répudiation des transferts, y compris la protection des chemins d'audit des événements importants. MOVEit est structuré pour s'intégrer à l'infrastructure, aux règles et aux applications de sécurité existantes, et assure qu'aucune donnée non cryptée ne se trouve sur le serveur DMZ, éliminant ainsi toute obligation pour les accès externes.
Politiques de sécurité des informations	MOVEit chiffre les fichiers à l'état de stockage et en transit, permet la non-répudiation et des contrôles d'intégrité des fichiers. Ipswitch fournit des accès via différents canaux (messagerie, Web, appareils mobiles) et des clients de bureau qui, combinés à la solution MOVEit, permettent aux utilisateurs d'accéder en toute conformité aux transferts de fichiers.
Contrôle d'accès	MOVEit offre un large choix de mécanismes d'authentification, notamment des intégrations aux systèmes existants, et une palette de fonctions complète dédiée à la gestion des accès des utilisateurs : listes noires et listes blanches, et outils pour aider les administrateurs à sélectionner les paramètres adéquats afin de respecter les politiques de sécurité.
Cryptographie	MOVEit utilise de puissants mécanismes cryptographiques et permet la sélection, la distribution et la protection sécurisées des clés de chiffrement et de déchiffrement, en cohérence avec les dispositions légales et réglementaires internationales.
Protection physique et de l'environnement	L'architecture de MOVEit se caractérise par une mise en œuvre suffisamment flexible pour s'adapter aux exigences de votre organisation en termes de sécurité physique.
Protection de la continuité des activités	MOVEit protège la confidentialité, l'intégrité et la disponibilité des transferts de fichiers à tout moment en cas d'erreur, d'accident ou de panne. Ipswitch Failover peut assurer les transferts de fichiers sans interruption.

À propos d'Ipswitch

Ipswitch permet de résoudre des problèmes informatiques complexes avec des solutions simples. Des millions de personnes dans le monde font confiance à ses logiciels pour transférer des fichiers entre leurs systèmes, avec leurs partenaires et leurs clients, mais aussi pour surveiller leurs réseaux, applications et serveurs. Ipswitch a été fondée en 1991. Son siège social est situé à Lexington, dans le Massachusetts, et l'entreprise dispose de bureaux aux États-Unis, en Europe et en Asie.

Pour plus d'informations, visitez le site **https://fr.ipswitch.com**.

Frost & Sullivan a attribué à Ipswitch MOVEit son prix 2016 du leadership en matière de produits de transfert de fichiers sécurisé.

Dans le cadre de leur enquête sur les meilleures pratiques dans le secteur, MOVEit a été reconnue comme la solution la plus performante pour répondre aux principaux besoins des clients et de l'industrie en termes de sécurité, flexibilité et évolutivité, tout en offrant une expérience client sans égale et une grande facilité d'utilisation.

ipswitch

Demandez-nous une VERSION D'ESSAI GRATUITE de Ipswitch MOVEit pendant 30 jours ›