FORTRA

LIVRE BLANC (GOANYWHERE)

Rationalisation des opérations:

Exploiter le pouvoir du MFT

Les actualités concernant les atteintes à la protection des données touchent même les organisations les plus importantes et les mieux sécurisées du monde. Malgré leurs mesures de sécurité avancées et leurs systèmes de détection des intrusions, une vulnérabilité importante réside dans la manière dont les données sont partagées.

Les méthodes traditionnelles de transferts de fichiers, telles que le protocole FTP et les courriels, s'accompagnent d'une série de défis en matière de sécurité, de contrôle, d'évolutivité et de conformité.

Les protocoles de transferts de fichiers, comme FTP et HTTP, transmettent les informations d'identification des utilisateurs et les fichiers sans les chiffrer, ce qui les rend vulnérables à l'interception. Ce manque de sécurité incite les entreprises à chercher des alternatives à leurs méthodes de transferts de fichiers non sécurisées.

Le danger des protocoles obsolètes

Le recours à des protocoles obsolètes tels que FTP et le courrier électronique expose les entreprises à des failles de sécurité en raison de l'absence de protocoles solides pour protéger les informations sensibles contre l'interception et l'exploitation éventuelle.

Le FTP natif ne chiffre pas les données : FTP ne dispose pas de mécanismes de chiffrement intégrés, ce qui signifie que les données transférées par FTP sont envoyées dans un format non chiffré. Cela les rend susceptibles d'être interceptées et surveillées par des acteurs malveillants, ce qui peut compromettre des informations sensibles.

Les noms d'utilisateur et les mots de passe sont transférés en clair : Au cours de la procédure de connexion, FTP transmet les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) en texte clair, ce qui rend ces informations vulnérables à l'interception. Cette absence de chiffrement signifie que toute personne ayant accès au trafic réseau peut facilement capturer et déchiffrer les identifiants de connexion, mettant ainsi les données en danger.

Les scripts et les fichiers batch FTP exposent les identifiants et les mots de passe des utilisateurs : Les scripts et les fichiers batch utilisés pour les processus FTP automatisés contiennent souvent des identifiants et des mots de passe en clair. Le stockage d'informations sensibles de cette manière les expose à un accès non autorisé et à une exploitation par des pirates ou des logiciels malveillants. Même si le serveur FTP est sécurisé, le fait de laisser des informations d'identification dans des scripts élargit la surface d'attaque et compromet la sécurité.

Utilisé seul, le protocole FTP ne répond pas aux réglementations en matière de conformité : La plupart des industries et des organisations sont soumises à des exigences réglementaires en matière de sécurité et de confidentialité des données, en particulier celles qui appartiennent à des secteurs fortement réglementés tels que les soins de santé et les services financiers. En raison de son manque inhérent de chiffrement et de sa vulnérabilité aux violations de données, FTP seul, peut ne pas répondre à ces normes de conformité.

Les données transférées peuvent "s'égarer" sur un ordinateur distant : Dans certains cas, notamment lorsque les connexions FTP sont mal configurées ou interceptées, les données destinées à être transférées peuvent être redirigées par erreur vers une autre destination. Cela peut être dû à une mauvaise configuration du réseau, à un accès non autorisé ou à des actions malveillantes. Une redirection non autorisée expose des données sensibles à des parties non autorisées et augmente le risque de violation de données.

FTP ne conserve pas d'enregistrement des transferts de fichiers : Contrairement aux solutions de transferts de fichiers plus avancées, FTP ne dispose pas de fonctions intégrées de journalisation et d'audit. En l'absence d'une journalisation complète, il est difficile pour les administrateurs de suivre et de surveiller les activités de transferts de fichiers, d'identifier les comportements suspects ou d'enquêter sur les incidents de sécurité. Sans traçabilité, il est difficile de maintenir la responsabilité et de garantir la conformité avec les réglementations en vigueur.

Face à ces défis, les entreprises doivent repenser leur approche des transferts de fichiers. Le paysage mondial des transferts de fichiers exige des solutions modernes qui privilégient la sécurité, l'automatisation, l'évolutivité et la conformité pour répondre aux besoins évolutifs des entreprises axées sur les données.

Le coût élevé des solutions de transferts de fichiers non sécurisées

Les méthodes inefficaces de transferts de fichiers peuvent avoir des conséquences financières et opérationnelles importantes pour les entreprises. L'une des conséquences les plus tangibles est le risque de violation de données. Lorsque les fichiers sont transmis à l'aide de protocoles obsolètes ou de canaux non sécurisés, ils deviennent vulnérables à l'interception par des acteurs malveillants. Les conséquences d'une violation de données peuvent être considérables, entraînant des pertes financières, une atteinte à la réputation, une perte de confiance de la part des clients et des responsabilités juridiques.

Les logiciels de transferts de fichiers traitent un large éventail de données, y compris des informations sensibles et exclusives, telles que des dossiers financiers, des secrets commerciaux et des données personnelles. Ces informations sont généralement

confiées au logiciel pour une transmission sécurisée entre les parties. Toutefois, si la sécurité du logiciel de transferts de fichiers est compromise, la confidentialité et l'intégrité des données stockées peuvent être mises en péril.

L'une des principales préoccupations est le risque que le logiciel de transferts de fichiers devienne un point de défaillance au sein de l'infrastructure de sécurité d'une organisation. En tant que pierre angulaire des échanges de données, une faille dans le logiciel peut permettre un accès non autorisé à toutes les informations qu'il contient. Si les attaquants parviennent à franchir les défenses du logiciel, ils peuvent avoir accès à une multitude de données sensibles, ce qui peut avoir de graves conséquences pour l'entité concernée.

En outre, la compromission d'un logiciel de transferts de fichiers peut avoir des implications plus larges que la perte immédiate de données. Elle peut éroder la confiance entre les parties prenantes, nuire à la réputation de l'organisation et entraîner des répercussions juridiques et réglementaires. Les retombées d'une violation peuvent également nécessiter des ressources importantes pour enquêter, remédier à la situation et se rétablir, ce qui aggrave encore l'impact sur l'organisation.

Coûts potentiels au-delà de l'atténuation des brèches

Les amendes réglementaires peuvent se chiffrer en millions, ce qui représente un coût substantiel pour les entreprises qui ne respectent pas les réglementations en matière de protection des données. Dans les secteurs régis par des lois strictes concernant la protection de la vie privée, comme les soins de santé (HIPAA), la finance (PCI DSS) et le Règlement général sur la protection des données (RGPD) de l'Union européenne, la non-conformité peut entraîner de lourdes pénalités. Ces amendes peuvent grimper rapidement, surtout en cas de violation de données causée par des pratiques de transferts de fichiers non sécurisés.

Par exemple, en 2023, Meta Platforms en Irlande a été condamnée à une amende colossale de 1,2 milliard d'euros, après qu'il ait été établi que l'entreprise avait mal traité des données personnelles lors de leurs transferts entre l'Europe et les États-Unis. Deux ans plus tôt, Amazon Europe s'était vu infliger une amende de 746 millions d'euros pour non-respect des principes généraux de traitement des données.

La perte de productivité est une autre de ces conséquences.. Les processus manuels, les erreurs et les retards peuvent entraver les workflows, obligeant les employés à perdre du temps à naviguer dans des systèmes encombrants ou à résoudre des problèmes de transferts. Cela nuit non seulement à la productivité, mais aussi au moral et à l'engagement des employés.

Compte tenu du rôle essentiel que jouent les logiciels de transferts de fichiers dans la facilitation des opérations et de la communication, leur sécurité doit être une priorité pour les entreprises. Les solutions de transferts de fichiers qui utilisent des mesures de sécurité solides, telles que le chiffrement, les contrôles d'accès et les audits de sécurité réguliers, peuvent contribuer à réduire le risque de violation et à préserver la confidentialité des données sensibles.

Augmentation des attaques visant les applications de transferts de fichiers

Ces dernières années, le nombre de cyberattaques visant des applications de transferts de fichiers largement utilisées a augmenté. Ces incidents ont mis en évidence le besoin critique de solutions de transferts de fichiers sécurisés pour protéger les données sensibles et assurer la continuité opérationnelle des entreprises de toutes tailles.

Une attaque importante a exploité une vulnérabilité d'injection SQL précédemment inconnue dans une solution populaire de transferts de fichiers, affectant près de 1 000 organisations dans le monde entier, y compris des entités de haut niveau et diverses agences gouvernementales. Les attaquants ont accédé aux fichiers stockés dans les référentiels et les ont potentiellement manipulés.

Lors d'un autre incident, les auteurs de la menace ont commencé à exploiter une vulnérabilité critique dans une autre application centralisée d'échanges de fichiers que les grandes entreprises utilisent pour transférer de gros fichiers ou de gros volumes à des

vitesses très élevées. Il est intéressant de noter que les attaquants ont activement exploité la vulnérabilité près de quatre mois après la publication initiale du correctif.

Cet incident a mis en évidence la vulnérabilité de ces systèmes et l'importance de mesures de sécurité solides.

Le MFT et les défis d'utilisation de méthodes (FTP) obsolètes

Pour relever ces défis, les entreprises adoptent des solutions robustes de gestion des transferts de fichiers (MFT) pour échanger des fichiers de manière sécurisée et fiable, tant en interne qu'en externe. Les solutions MFT fournissent une plateforme centralisée pour la gestion, la surveillance et le contrôle des transferts de fichiers sur différents réseaux, y compris les environnements cloud, sur site et hybrides.

Les systèmes MFT offrent généralement des fonctions de chiffrement, d'authentification, de pistes d'audit, de planification et d'automatisation pour garantir que les fichiers sont transférés de manière sûre et efficace, tout en respectant les exigences de conformité et les politiques de l'organisation. Cela permet de réduire les risques associés aux violations de données, de garantir l'intégrité des données pendant la transmission, d'offrir aux entreprises une meilleure visibilité et un meilleur contrôle de leurs opérations de transferts de fichiers.

Principales caractéristiques et avantages des solutions MFT

Sécurité renforcée

La sécurité renforcée est un aspect essentiel des solutions MFT pour protéger les données sensibles et atténuer les risques associés aux transferts de fichiers. Cela englobe plusieurs fonctions de sécurité essentielles :

Chiffrement : Les solutions MFT utilisent des algorithmes de chiffrement robustes pour sécuriser les fichiers lors de leur transmission sur le réseau. Ces solutions utilisent généralement des techniques de chiffrement standard, telles que Advanced Encryption Standard (AES), RSA Security ou Triple Data Encryption Algorithm (Triple DES), pour chiffrer les données, garantissant qu'elles restent confidentielles et illisibles pour les parties non autorisées. Le chiffrement convertit les données en texte clair vers du texte chiffré, ce qui les rend indéchiffrables sans la clé de déchiffrement correspondante. Le chiffrement des fichiers pendant la transmission permet de protéger les informations sensibles contre l'interception par des acteurs malveillants, pour ainsi maintenir la confidentialité et l'intégrité des données.

Authentification des utilisateurs : Une solution moderne applique également des mécanismes d'authentification rigoureux pour vérifier l'identité des personnes qui accèdent au système. Les utilisateurs doivent généralement s'authentifier à l'aide d'identifiants tels que des noms d'utilisateur, des mots de passe ou des méthodes d'authentification multifactorielle (MFA). Ces solutions peuvent également s'intégrer aux systèmes de gestion des identités existants afin de centraliser les processus d'authentification des utilisateurs et d'assurer une cohérence au sein de l'entreprise. Cela permet d'empêcher des personnes non autorisées d'accéder à des données sensibles, réduisant ainsi le risque de violation de données et d'accès non autorisé.

Contrôle d'accès : Les mécanismes de contrôle d'accès granulaire, qui permettent aux entreprises de définir et d'appliquer les autorisations d'accès aux fichiers, constituent une autre caractéristique essentielle de toute solution MFT robuste. Les administrateurs peuvent spécifier les droits d'accès et les privilèges par utilisateur ou par groupe, en déterminant qui peut visualiser, modifier ou supprimer des fichiers et des répertoires. Les contrôles d'accès aident les entreprises à appliquer le principe du moindre privilège, en n'accordant aux utilisateurs que les autorisations strictement nécessaires à l'accomplissement de leur travail. Certaines solutions MFT prennent également en charge le contrôle d'accès basé sur les rôles (RBAC), ce qui permet aux administrateurs d'attribuer aux utilisateurs des rôles assortis d'autorisations prédéfinies en fonction de leur poste ou de leurs responsabilités.

Amélioration de la visibilité et du contrôle

L'amélioration de la visibilité et du contrôle est un autre avantage indéniable des solutions MFT, car elles sont cruciales pour les organisations qui cherchent à améliorer la surveillance, la sécurité et l'efficacité de leurs opérations de transferts de fichiers. Il s'agit notamment de :

Surveillance : De solides fonctions de surveillance en temps réel permettent aux administrateurs de suivre de près les activités des transferts de fichiers sur le réseau de l'entreprise. Grâce à des tableaux de bord intuitifs et à des alertes personnalisables, les administrateurs peuvent obtenir une visibilité instantanée sur les opérations, notamment sur l'état des transferts, la taille des fichiers, les taux de transferts et les parties concernées. La surveillance en temps réel facilite la résolution rapide des problèmes tels que les échecs de transferts, les surcharges ou les activités inhabituelles, ce qui aide les administrateurs à prendre des mesures correctives immédiates et à minimiser les interruptions.

Pistes d'audit : En maintenant des pistes d'audit complètes pour détenir des informations détaillées sur chaque aspect des transferts de fichiers, des métadonnées essentielles telles que les horodatages, les identités des utilisateurs, les noms de fichiers, les protocoles de transferts, les adresses de source et de destination sont enregistrées. En outre, les pistes d'audit documentent les événements du système, les changements de configuration et les activités liées à la sécurité, fournissant ainsi un historique complet des opérations de transferts. Ces données constituent des preuves légales précieuses dans les enquêtes sur les incidents de sécurité ou les audits de conformité, aidant les entreprises à démontrer qu'elles respectent les exigences réglementaires et les politiques internes.

Automatisation des workflows : Grâce à l'automatisation des tâches répétitives et de workflows, les solutions MFT permettent aux entreprises de rationaliser les processus de transferts de fichiers. Les administrateurs peuvent définir des flux automatisés qui spécifient la séquence des actions à effectuer pendant les transferts de fichiers, telles que le chiffrement, le déchiffrement, la compression, la validation des fichiers et l'acheminement, sur la base d'un ensemble de critères prédéfinis. Les flux automatisés permettent également aux entreprises de programmer des transferts à certains moments ou en réponse à des événements déclencheurs, tels que la disponibilité de nouveaux fichiers ou des changements de conditions.

Augmentation de l'évolutivité et de la fiabilité

L'évolutivité et la fiabilité accrues sont d'autres avantages des solutions de MFT modernes. Ces avantages sont essentiels pour les organisations qui doivent faire face à des volumes de données croissants et à des demandes de plus en plus nombreuses pour des opérations de transferts de fichiers efficaces. Pour bénéficier de ces avantages, la solution MFT doit présenter les caractéristiques suivantes :

Gestion centralisée : Une plateforme centralisée pour gérer tous les aspects des opérations de transferts de fichiers permet de gagner du temps et d'économiser des ressources. Au lieu de s'appuyer sur des outils disparates et des interventions manuelles éparpillées dans différents services ou sites, les entreprises peuvent consolider leurs processus de transferts de fichiers dans un système unifié. Cette approche permet de rationaliser les tâches de gestion, de réduire la complexité, d'améliorer la visibilité et le contrôle des activités de transferts de fichiers. Les administrateurs peuvent définir des politiques standardisées, des contrôles d'accès et des paramètres de surveillance à partir d'une console centrale, ce qui garantit la cohérence et la conformité dans l'ensemble de l'entreprise.

Optimisation de la bande passante : Une solution MFT robuste intégrera des techniques avancées pour optimiser l'utilisation de la bande passante lors des transferts de fichiers. L'une de ces techniques est la compression des données, qui réduit la taille des fichiers avant leur transmission, minimisant ainsi la quantité de données transférées sur le réseau et accélérant les temps de transferts. Certaines solutions mettent en œuvre des mécanismes de

limitation de la bande passante afin de réguler le taux de transmission des données, d'éviter la surcharge du réseau et de veiller à ce que les transferts de fichiers gourmands en bande passante ne perturbent pas les processus commerciaux essentiels. La solution MFT comprendra également des techniques de haute disponibilité et de cluster, afin de garantir une utilisation efficace des ressources ainsi qu'un accès ininterrompu aux services, en répartissant le trafic réseau sur des systèmes redondants. La fiabilité et les performances des applications critiques s'en trouvent améliorées.

Conformité

Un autre avantage du MFT réside dans la gestion efficace des exigences réglementaires au sein d'une organisation, en particulier dans le contexte d'activités de transferts de fichiers. Cette approche comporte deux éléments clés :

Rapports automatisés : Une bonne solution MFT est dotée de fonctionnalités de reporting robustes qui génèrent automatiquement des informations détaillées sur les activités des transferts de fichiers, l'état de conformité et les incidents de sécurité. L'automatisation du processus de reporting permet aux entreprises de gagner du temps et d'économiser des ressources, car les tâches de reporting manuelles sont sujettes aux erreurs et peuvent nécessiter une main-d'œuvre importante.

Prise en charge des normes industrielles : Tout outil de transferts de fichiers solide aura été conçu pour adhérer à divers protocoles et normes industrielles tels que SFTP, FTPS, PGP, HTTPS, AS2/AS3/ AS4. En s'alignant sur ces normes, les entreprises peuvent s'assurer que leurs processus de transferts de fichiers répondent aux exigences légales et réglementaires de leur secteur. Il s'agit notamment de mettre en œuvre des protocoles de chiffrement, des contrôles d'accès, des pistes d'audit et d'autres mesures de sécurité exigées par les organismes de réglementation.

Le MFT répond aux besoins évolutifs des entreprises

Les solutions de gestion des transferts de fichiers offrent des fonctionnalités qui permettent aux entreprises d'échanger des fichiers en toute sécurité, d'améliorer leur efficacité opérationnelle et de se conformer aux exigences réglementaires.

En adoptant des solutions de MFT robustes, les entreprises peuvent atténuer les risques de sécurité, améliorer la visibilité et le contrôle des données et optimiser les processus de transferts de fichiers pour répondre aux besoins changeants de leurs opérations.

A propos de GoAnywhere

GoAnywhere® Managed File Transfer est une solution de transferts de fichiers sécurisés, qui rationalise et chiffre les échanges de données entre les systèmes, les employés, les clients et les partenaires commerciaux. Elle offre un point de contrôle unique et convivial avec des paramètres de sécurité étendus, plusieurs modules de collaboration, des pistes d'audit, des rapports détaillés, ainsi que des agents à distance.

Quels sont les avantages des transferts de fichiers sécurisés pour votre entreprise ?

Découvrez les nombreuses fonctionnalités et les paramètres de sécurité du MFT grâce à une démonstration personnalisée de notre solution GoAnywhere MFT.

www.goanywhere.com/demo

goanywhere.sales@fortra.com
www.goanywhere.com

FORTRA®

À propos de Fortra

Fortra est une entreprise de cybersécurité pas comme les autres. Nous créons un avenir plus simple et plus fort pour nos clients. Nos experts de confiance et notre portefeuille de solutions intégrées et évolutives apportent équilibre et contrôle aux organisations du monde entier. Nous sommes les artisans du changement positif et vos alliés infatigables pour vous apporter la tranquillité d'esprit à chaque étape de votre parcours en matière de cybersécurité. Pour en savoir plus, rendez-vous sur fortra.com.

fta-sft-wp-0924-79dev