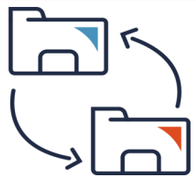
Transférer et téléverser des données en toute sécurité

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Décembre 2022 | ITSAP.40.212



Les données font partie des biens les plus précieux de votre organisation. Elles permettent de prendre de meilleures décisions opérationnelles et de réduire les risques, facilitent la collaboration, favorisent l'innovation et aident votre organisation à répondre aux exigences réglementaires. La quantité de données générées et consultées continue de croître de façon exponentielle. Pour que toutes ces données soient utiles aux organisations, elles peuvent être transférées ou téléversées dans divers systèmes afin d'être partagées, analysées ou conservées en vue d'un stockage. Le présent document fournit de l'information sur la façon de protéger vos processus de transfert de données de sorte à minimiser les risques liés à la cybersécurité auxquels s'expose votre organisation.

Quels sont les **risques** liés aux transferts de données?

Habituellement, les risques liés aux transferts de données peuvent comprendre des menaces pour l'infrastructure, les utilisateurs et utilisatrices, les données, les services et les opérations. Voici comment le processus de transfert de données vers votre réseau ou depuis celui-ci pourrait présenter un grave risque de sécurité pour votre organisation.

- L'utilisation de mécanismes de transfert de données inappropriés pour le traitement de données peut entraîner une fuite. C'est par exemple le cas lorsqu'on emploie une infrastructure de transfert de données non classifiée pour transmettre des renseignements classifiés ou de nature très délicate.
- Une ou un auteur de menace peut profiter des failles des mécanismes de transfert de données pour accéder au réseau d'entreprise et s'y implanter.
- Le téléversement de fichiers sur une plateforme infonuagique non sécurisée peut causer une perte de données ou une atteinte à la protection des données.
- Une ou un auteur de menace peut exploiter d'éventuelles vulnérabilités dans le protocole de téléversement (transfert) de données pour lancer d'autres attaques. Il peut par exemple injecter des maliciels dans le réseau ou modifier des fichiers légitimes et des fichiers de configuration du système.

Quelles sont les **incidences** des risques liés aux transferts de données?

Un processus de transfert de données faisant l'objet d'exploitations peut avoir de graves incidences à long terme sur votre organisation. Parmi les incidences, notons:

- Essuyer une atteinte à la réputation et une perte de la confiance du public résultant d'un incident ou d'une atteinte à la protection des données.
- Être victime de futures attaques contre vos réseaux ou systèmes provenant de l'implantation d'un maliciel à l'état dormant.
- Être incapable d'exploiter pleinement vos biens en raison du goulot d'étranglement de la bande passante réseau alors que votre réseau fonctionne au ralenti.
- Risquer que les opérations soient affectées par une attaque par déni de service distribué (DDoS pour *Distributed Denial of Service*). Une telle attaque pourrait réduire la capacité du système à exécuter de façon simultanée des opérations de données légitimes et des téléversements de fichiers volumineux.
- Subir des peines réglementaires, des poursuites en justice, des engagements financiers ou la suspension des activités commerciales pour une non-conformité aux exigences relatives à la sécurité des données.

Téléversements de données dans le nuage

Le stockage infonuagique est vulnérable aux attaques d'espionnage vu que les données sont stockées et transmises par Internet. Lors d'une attaque d'espionnage, une ou un auteur de menace recourt à un logiciel pour surveiller à distance l'activité entre des machines sur un réseau.

Assurez-vous que votre fournisseur de services infonuagiques (FSI) protège vos données contre la falsification et l'écoute clandestine en:

- chiffrant toutes les données au repos et en transit.
- fournissant des outils pour assurer la protection des réseaux (utilisation de réseaux virtuels, de règles d'acheminement dynamique et de règles sur le flux de données).
- authentifiant tous les accès à votre service infonuagique.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Transférer et téléverser des données en toute sécurité

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Décembre 2022 | ITSAP.40.212

Comment **protéger** les transferts de données?

La liste qui suit propose des mesures qui permettront à votre organisation de resserrer le contrôle de vos processus de transfert et de téléversement de données. Ces mesures aideront à protéger la confidentialité (empêcher un accès non autorisé aux données), l'intégrité (empêcher la falsification des données chiffrées) et la disponibilité (veiller à ce que les bonnes personnes aient accès à la bonne information au moment voulu) de vos données.

- ☐ **Traitez tous les fichiers à transférer dans un logiciel antivirus et antimaliciel à jour**.
- ☐ **Faites en sorte que les transferts de fichiers ne puissent être exécutés que par des utilisatrices et utilisateurs authentifiés et autorisés.**
- ☐ **Vérifiez les types de fichiers** à l'aide d'outils d'inspection du contenu plutôt que de vous fier à l'extension, aux indicateurs ou aux en-têtes de type de contenu, car ces indicateurs peuvent facilement être modifiés par une ou un auteur de menace.
- ☐ **N'autorisez que des types spécifiques de fichiers**, comme .PDF, .DOCX et .XLSX, qui sont nécessaires aux fonctionnalités opérationnelles. En limitant la liste des types de fichiers autorisés, vous pouvez éviter le téléversement d'exécutables, de scripts et de fonctions macro malveillants dans les formats de document Microsoft.
- ☐ **Éliminez les menaces intégrées au moyen d'une méthodologie appelée désarmement et reconstruction de contenu (CDR pour *content disarm and reconstruction*).** Des fichiers de type Microsoft Office, PDF ou des fichiers images peuvent contenir des scripts et des macros malveillants cachés qui ne sont pas toujours détectés par un logiciel antimaliciel. Tenez compte de la provenance des données lors de l'analyse de tous les fichiers à transférer.
- ☐ **Appliquez une longueur de nom de fichier et une taille de fichier maximum** qui conviennent au système d'exploitation afin d'éviter de possibles attaques par dépassement ou débordement de mémoire tampon. Un dépassement de mémoire tampon se produit lorsque la quantité de données dans la mémoire tampon dépasse sa capacité de stockage. Une ou un auteur de menace peut exploiter cette erreur de codage pour corrompre la pile d'exécution d'une application Web, exécuter un code arbitraire ou prendre le contrôle d'une machine.
- ☐ **Assurez-vous que les noms de fichier ne contiennent pas de chaînes spécifiques pouvant être considérées par une application comme une commande à exécuter.** Une ou un auteur de menace peut profiter de cette situation pour exécuter un code malveillant ou entraîner de nouveaux comportements susceptibles de compromettre la sécurité ou la stabilité de votre système.
- ☐ **Affichez des messages d'erreur simples** lorsqu'il y a un problème avec le téléversement d'un fichier. Ne donnez pas de renseignements détaillés comme des trajets inter-répertoires, des paramètres de configuration du serveur ou d'autres renseignements qu'une ou un auteur de menace pourrait exploiter pour élargir son accès à vos systèmes.
- ☐ **Mettez en place des mesures de journalisation et de surveillance de réseau**. Consignez toutes les activités liées aux processus de transfert de données, y compris une journalisation détaillée sur l'autorisation du transfert des données, les comptes d'utilisateur permis, le moment de la réception ou du téléversement et les types de données reçues et téléversées. Veillez également à ce que les journaux soient examinés régulièrement pour repérer un emploi malveillant ou des violations des politiques.
- ☐ **Créez une "empreinte" des fichiers avant et après le téléversement** à l'aide d'une fonction de hachage robuste comme SHA 256. Comparez les "empreinte" pour confirmer l'intégrité du fichier. Rendez "l'empreinte" accessible à tous et toutes pour les fichiers téléversés afin d'assurer un contrôle d'intégrité aux personnes qui accèdent aux fichiers.
- ☐ **Définissez des alertes automatiques qui se déclencheront** lors d'événements sensibles, comme des exportations en vrac atypiques de données.
- ☐ **Assurez-vous que les transferts de données effectués avec des périphériques de support amovibles sont chiffrés** au moyen d'une clé USB à autochiffrement, un chiffrement de la couche application ou les deux. Les périphériques de support amovibles doivent être étiquetés, suivis et entreposés en toute sécurité. Les données contenues dans ces périphériques doivent être effacées de manière sécuritaire lorsqu'elles ne sont plus nécessaires.
- ☐ **Chiffrez les fichiers avant de les acheminer** vers le nuage, un support physique ou tous les autres types de supports. Cette mesure permet non seulement de s'assurer que seules les données chiffrées sont transférées, mais aussi d'empêcher une divulgation non autorisée ou accidentelle de vos données. Pour obtenir plus de renseignements, consultez "*Étapes pour gérer les fuites de données dans le nuage (ITSAP.50.112)*."
- ☐ **Mettez en œuvre une solution de protection contre les fuites de données (DLP pour *data leakage protection*)** pour protéger vos données sensibles et les flux de données connexes dans l'ensemble des points de sortie.
- ☐ **Envisagez l'utilisation d'une solution interdomaines (SID) lors du transfert électronique de données entre deux domaines de sécurité distincts.** Cette mesure est particulièrement importante pour empêcher les fuites d'information sensible de réseaux classifiés ainsi que l'introduction de maliciel pouvant compromettre l'environnement classifié. Le "*Guide d'initiation à la sécurité interdomaines (ITSB-120)*" est destiné aux ministères et organismes du gouvernement du Canada.
- ☐ **Concevez votre infrastructure de transfert (téléversement) de données pour qu'elle soit sécuritaire et souple.** Séparez les systèmes de transfert de données des autres sections sensibles de votre réseau, surtout si un accès à distance est autorisé. Mettez en œuvre des contrôles stricts de segmentation et appliquez des politiques de contrôle d'accès rigoureuses.
- ☐ **Favorisez l'utilisation d'une authentification multifacteur (AMF) pour accéder aux systèmes exposés au public afin d'offrir une protection contre des attaques de mot de passe.** Selon les exigences de votre organisation, songez à limiter l'accès à des dispositifs préenregistrés (adresses IP, adresses MAC) ou à utiliser des certificats numériques pour sécuriser l'accès.
- ☐ **Consignez les politiques et les procédures concernant les exigences relatives à l'amorce et à l'achèvement d'un processus de transfert de données.** Les utilisatrices et utilisateurs, les propriétaires de données et les intervenantes et intervenants doivent être formés et être conscients de leurs responsabilités.
- ☐ **Envisagez de recourir à une plateforme de transfert de données spécialisée pour gérer le processus.** Si elle répond au besoin de votre organisation, une plateforme de fournisseur tiers pourrait offrir de meilleures capacités techniques avancées, faire l'objet d'un contrôle indépendant et fournir des mises à jour logicielles ponctuelles pour corriger des vulnérabilités. Sélectionnez un fournisseur ayant de bonnes pratiques en matière de sécurité et utilisant de bons processus de correction et de cycle de vie. Évaluez la solution pour ce qui est des vulnérabilités liées à la sécurité et à la chaîne d'approvisionnement.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada