Data transfer and upload protection

CANADIAN CENTRE FOR CYBER SECURITY

December 2022 | ITSAP.40.212

Data is one of your organization's most valuable assets. It enables better business decisions and reduces risks; facilitates collaboration; drives innovation, and assists your organization in meeting regulatory requirements. The amount of data generated and consumed continues to grow exponentially. For all this data to be meaningful to organizations, it may be transferred or uploaded to various systems to be shared, analyzed or retained for storage. This document offers information on how to secure your data transfer processes to minimize potential cyber security risks to your organization.

What are the **risks** with data transfers?

Generally, risks with data transfer can include threats to your infrastructure, users, data, services, and operations. Here is how the process of transferring data into or out of your network could present a critical security risk to your organization.

- Using data transfer mechanisms inappropriate for data processing can lead to data leakage. For example, using an unclassified data transfer infrastructure to transmit classified or highly sensitive information.
- Threat actors can exploit gaps in the data transfer mechanisms to gain entry to the corporate network and gain a foothold within the network.
- Uploading files to an unsecure cloud platform can lead to data loss or data breaches.
- Threat actors can exploit vulnerabilities that may be present in the data upload (transfer) protocol to perform additional attacks. This includes injecting malware into the network, or modifying legitimate files, and system configuration files.

What are the **impacts** of data transfer risks?

An exploited data transfer process can have significant and long-lasting impacts to your organization. Some of the potential impacts can include:

- Reputational damage and loss of public confidence as a result of an incident or data breach.
- Possibility for future attacks against your networks or systems from a malicious implant in a dormant state.
- Inability to use your assets to their full potential with network bandwidth bottleneck as your network slows down.
- Operations could be affected by a Distributed Denial of Service (DDoS) attack, which could reduce your system's capacity to simultaneously execute legitimate data operations and large file uploads.
- Regulatory penalties, lawsuits, financial liability or business suspension for non-conformance with requirements for maintaining data security.

Data uploads to cloud environments

Cloud storage is vulnerable to snooping attacks as data is stored and transmitted over the internet. In a snooping attack, a threat actor uses software to remotely monitor activity between machines on a network.

Check that your cloud service provider (CSP) protects your data against tampering and eavesdropping by:

- encrypting all data at rest and in-transit.
- providing tools for network protection (use of virtual networks, dynamic routing rules, and data flow rules).
- authenticating all access to your cloud service.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Data transfer and upload protection

CANADIAN CENTRE FOR CYBER SECURITY

December 2022 | ITSAP.40.212

How to **protect** data transfers?

The following is a list of measures that will enable your organization to tightly control your data transfer and upload processes. These measures will help to protect the confidentiality (prevent unauthorized access to the data), integrity (prevent tampering of the encrypted data), and availability (ensure that the right people can access the right information when needed) of your data.

□ **Run all files to be transferred through an up-to-date anti-virus and anti-malware software**.

□ **Allow file transfers to be executed only by authenticated and authorized users.**

□ **Verify file types** with content inspection tools rather than based on the extension, flags, or content-type headers as these indicators can easily be spoofed by threat actors.

□ **Allow only specific file types** such as PDF, .DOCX, and .XLSX that are required by business functionality. By restricting the list of allowed file types, you can avoid malicious executables, scripts and macro functions within Microsoft document formats from being uploaded.

□ **Remove possible embedded threats using a methodology called content disarm and reconstruction (CDR).** Files such as Microsoft Office, PDF and image files can contain hidden malicious scripts and macros that are not always detected by anti-malware software. Consider the data's provenance when scanning all files to be transferred.

□ **Enforce a maximum file name length and file size** that is appropriate to the OS to prevent potential buffer overflow or buffer overrun attacks. Buffer overflow occurs when the amount of data in the buffer exceeds its storage capacity. Threat actors can exploit this software coding error to corrupt a web application's execution stack, execute arbitrary code or take over a machine.

□ **Validate that file names don't contain specific strings that can be evaluated by an application as a command to be executed.** Threat actors can exploit this to execute malicious code, or cause new behaviours to compromise the security or stability of your system.

□ **Display simple error messages** when there is an issue with the file upload. Do not include detailed information such as directory paths, server configuration settings or other information that threat actors could potentially leverage to gain deeper access into your systems.

□ **Implement audit logging and network monitoring measures.** Actively log all activities related to your data transfer processes including detailed logging on how data transfer is authorized, which user accounts are allowed, as well as when and what data was received or uploaded. Ensure the logs are also reviewed regularly to identify malicious use or policy violations.

□ **Create a "fingerprint" of files before and after uploading** using a strong hash function such as SHA 256. Compare "fingerprints" to confirm the integrity of the file. Make the "fingerprint" publicly available for uploaded files to provide an integrity check for those accessing the file.

□ **Set up automated alerts to be triggered** in response to sensitive events, such as atypical bulk exports of data.

□ **Ensure that data transfers utilizing physical, removable media devices are encrypted** using self-encrypting USB drive, application-layer encryption or both. Removable media devices should be labeled, tracked, and stored securely. Data contained within these devices should be securely wiped when it's no longer required.

□ **Encrypt files prior to transmission** to cloud environments, physical media and all other media types. This ensures only encrypted data is transferred, as well as prevents unauthorized and inadvertent disclosure of your data. For more information, see "*Steps to address data spillage in the cloud (ITSAP.50.112)*."

□ **Implement a data leakage protection (DLP) solution** to safeguard your sensitive data and associated data flows across egress points.

□ **Consider using a Cross-Domain Solution (CDS) when transferring data electronically between two different security domains.** This is particularly important to prevent leakage of sensitive information from classified networks as well as introduction of malware that could compromise the classified environment. For Government of Canada departments and agencies, see "*Cross domain security primer (ITSB-120).*"

□ **Architect your data transfer (upload) infrastructure to be secure and resilient.** Separate data transfer systems from other sensitive parts of your network especially if remote access is enabled. Implement strict segmentation controls and enforce strict access control policies.

□ **Encourage the use of multi-factor authentication (MFA) to access publicly exposed systems to protect against password attacks**. Depending on your organizational requirements, consider restricting access by pre-registering devices (IP addresses, MAC addresses) or using digital certificates to secure access.

□ **Document policies and procedures to guide all stakeholders on required expectations for initiating or completing a data transfer process.** Users, data owners, and stakeholders should be trained and be aware of their responsibilities.

□ **Consider using a dedicated data transfer platform to manage the process.** If suitable to your organizational needs, a third-party vendor platform may offer better advanced technical capabilities, may be independently audited, and can provide timely software updates to address vulnerabilities. Select a vendor with good security practices and patching/lifecycle processes. Evaluate the solution for security and supply chain vulnerabilities.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada