File sharing scares

The days of paper files are gone. All our information is online or stored on our localized devices — hopefully secured. As part of working remotely and worldwide business partnerships, it is critical that we transfer data one way or another. And with that, we need to ensure that our files are secured while they are stored and in transit.

Secure file sharing

Secure file sharing is when different users or organizations protect the transfer of files. This is usually done by restricting access to the files, only allowing authorized users to view, edit or download the information.

Some ways are more secure than others. A few of the most common methods are using removable media devices, such as USBs; storing files in a centralized server accessible by all employees using the same network; or web-based cloud storage with shareable links.

To ensure the security of these files while stored and during the transfer process, it is critical that they are encrypted. Encryption is when the information is secured by scrambling the content until there has been authorization to access it. When the proper authorization has been granted, the information is converted back to its original form, making it viewable or shareable.

File sharing risks and responsibilities

Organizations try their best to control and secure their information. To help your organization keep data secure, follow all policies and procedures.

One way to do that is to only use company-approved services. If you were to download your own file transfer tool, it is out of your IT department's control, meaning they won't know when updates become available, if there are any security issues or for general support.

Avoid using removable media, if possible. USB devices are easy to use but also easy to hide malware in. It is best practice to only partially trust a removable media device.

If you find a discarded or lost USB drive, report it and hand it over to your IT or security department. They will be able to safely access whatever information is on it. Do not plug it into your computer.

Cloud storage is useful and important but also a target for hackers. To safeguard your information in the cloud, especially while sharing data from one user to another, it is important to grant access and admin rights appropriately.

MOVEit zero-day attack

One of the most popular tools used today is called MOVEit. MOVEit encrypts your data and uses file transfer protocols to send it safely from one server to another. This tool has been around for more than twenty years and is used by major players in tech, healthcare, and even the government.

Recently, hackers attacked MOVEit. Using a technique known as SQL injection, they were able to access and copy the data of MOVEit users.

The breach was discovered, and MOVEit's owners issued a patch. But it was too late. The hackers had already exploited it for a month or even longer.

Takeaways:

- When breaches are discovered, software needs to be patched. Keeping your device, software and apps up-to-date will help keep you from being a target in a breach.
- If you find out that a business or organization you use has been breached by hackers, it's a good time to change your passwords and back up your data.

Cybersecurity roles — Security operations center (SOC) analyst

Have you ever wondered what your friendly cybersecurity team is up to? We'll share a cybersecurity job role each month to give you an inside look!

SOC analyst
A security operations center (SOC) analyst is responsible for analyzing and monitoring network traffic for security events and vulnerabilities. SOC analysts also investigate, document and report on information systems weaknesses.

In the day-to-day, SOC analysts also monitor firewall, email, web and DNS logs to identify and mitigate intrusion attempts.