6 Ways to Keep Microsoft 365 Data Safe

Hackers recently exploited inadequate security configurations set by organizations. Here are six ways to enhance Microsoft 365 data security.

March 25, 2021 Sanjit Debroy

Recently, Microsoft CEO, Satya Nadella, said “cloud computing has been at the forefront of human resilience against the pandemic.” Indeed, Microsoft’s productivity cloud, Microsoft 365, has helped more than 258 million users across a range of industries build resilience, ensure productivity, reimagine work and tackle unique challenges posed by the pandemic with confidence.

Apart from being one of the most popular productivity suites in the world, Microsoft 365 is also widely used among hackers, as demonstrated by the SolarWinds and Hafnium cyber-attacks.

While these attacks utilized unique tactics, they also exploited inadequate security configurations set by organizations. Microsoft 365 offers plenty of native security features; however, they need to be properly configured to reap the full benefits.

Here are six ways to enhance Microsoft 365 data security:

1. Protect Emails Against Phishing Attacks

Phishing emails, when ransomware is spread via malicious links and email attachments, is one of the foremost data security concerns organizations face today. The first step toward building resistance against such attacks is to provide employees with in-depth phishing prevention training.

However, not all employees will be equally vigilant. As a result, organizations need anti-phishing protection. Microsoft Defender for Microsoft 365, can help organizations protect users from malicious impersonation-based phishing attacks. Advanced Threat Protection scans prevents emails with malicious links and attachments from getting into employees' inboxes, minimizing the inadvertent opening of links or attachments.

2. Add an Additional Security Layer

Typically, employees type in a username and password to verify their identity when logging into Microsoft 365. However, organizations can't always trust their employees to be diligent enough to safeguard their passwords at all times.

Microsoft's Multi-Factor Authentication (MFA) is an effective way to increase the Microsoft 365 data security of your organization. It delivers a two-step verification process that is widely used in many consumer applications today, including online banking. MFA protects Microsoft 365 users from cyberattacks that target accounts with weak or stolen passwords. Having this feature turned on provides an additional layer of security for collaboration tools.

3. Secure Administrative Accounts

The administrative accounts your organization uses to oversee the Microsoft 365 environment include various elevated privileges. When an administrative account is compromised, the consequences can be much worse than breaches to personal accounts. However, many organizations get lazy and grant admin privileges because it is easy.

That is why Microsoft has added read-only admin accounts to help organizations grant requisite permissions while ensuring security.

Additionally, organizations can leverage the Privileged Identity Management (PIM) service to manage, control and monitor access to important resources in an organization. Such resources may include Azure AD, Microsoft 365 and Microsoft Intune.

With this service, your organization can minimize security risks by enabling the decision-makers to assign temporary admin status to specific users. The access can be controlled based on the information needed and the length of time a user would require admin privileges.

4. Safeguard Business Data in Rest and Transit

The volatile online cybersecurity landscape has made it imperative for organizations to take actions to protect sensitive information either at rest or during transit.

Microsoft 365 features several built-in data encryption capabilities. BitLocker is a powerful data encryption feature that supports the encryption of hard drives on Microsoft devices. It ensures that if any device is lost or stolen the ability to fetch data will be difficult to impossible.

Additionally, TLS connections can be leveraged to secure files on SharePoint Online or OneDrive for Business through best-in-class encryption.

Office Message Encryption is another great feature that allows an organization to send and receive encrypted email messages between people both inside and outside of an organization. These

encrypted messages can only be accessed by recipients after signing in with a Microsoft account, a Microsoft 365 account or entering a one-time passcode.

5. Deliver Secure Browsing Across Devices

Device management is essential for every Microsoft 365 tenant, especially in times when an organization's data and resources are accessed from various devices such as mobile phones, tablets, smartwatches and laptops.

With Microsoft 365's Mobile Device Management (MDM), organizations can ensure secure browsing and a consistent end-user experience across various devices and platforms. MDM allows the Microsoft 365 users to enroll their devices, install internal business applications, and manage their mobile devices through a web portal. The goal of this tool is to enable everyone to be more productive and secure on almost any device, from anywhere.

Additionally, organizations can also leverage Microsoft Intune for MDM and Mobile Application Management (MAM) too. Intune offers more in-depth security than the built-in Microsoft 365 MDM service.

6. Utilize Data Loss Prevention (DLP) Policy

Every organization, regardless of industry or size, needs to have a Data Loss Prevention (DLP) policy in place to prevent business data from being improperly accessed or deleted. With an effective DLP policy in the Microsoft 365 Security & Compliance Center, organizations can identify and segregate documents containing sensitive information across different locations, including SharePoint Online, Microsoft Teams, Exchange Online and OneDrive.

Secondly, the policy averts the accidental sharing of sensitive information via email by automatically blocking the email before being sent. The DLP policy also monitors and protects all sensitive files in the desktop versions of Word, Excel and PowerPoint.

It's essential for Microsoft 365 tenants to continuously focus on establishing a strong culture of Microsoft 365 data security across an organization.

Educating users about how to ensure password privacy, recognize phishing emails, understand the security aspects of mobile devices or laptops and how every aspect of an organization's data security stance is important. Organizations should remember that security training is not a one-time task, it's an ongoing requirement.