AUGMENTT

The 5 Fundamental Best Practices for Microsoft Security

The current surge of high-profile cyber attacks on big enterprise targets has generated lots of buzz around cybersecurity — but the basics of preventing breaches are what the more modestly sized clients of MSPs need to know for optimal Microsoft security.

What’s all the commotion about?

The word “cybersecurity” is on everyone’s lips. We use the term so often and so broadly that it can begin to lose meaning.

There’s so much talk about tips and tricks toward greater cybersecurity but precious little much clarity or context around what exactly we are protecting.

What do small and medium businesses need to know?

MSPs shouldn’t waste time alarming customers with stories about state funded overseas hacking operations that might target their IT.

Only larger modern enterprises should realistically be concerned with criminal attempts to steal company secrets or obtain user logins and sell them on the dark web.

What do small and medium businesses need to know?

The smaller companies that MSPs serve need not worry about "active" threats targetting them specifically.

Instead, it's the "spray and pray" tactics that can do harm, including:

- Millions of phishing emails attempting to obtain employ login credentials
- Millions of fraudulent emails with ransomware files attached or supposedly sent from the company CEO, for instance, asking an employee to purchase gift cards.

These socially engineered email attacks can be clever and opportunistic

For example, a scammer could:

1. Gain access to the M365 account belonging to the CEO or CFO
2. Read emails to identify a large corporate activity in progress
3. Set up email forwarding rules to hide phoney correspondence from the real user
4. Use to the hacked account to email a mid-level finance person about making a large payment related to the ongoing corporate activity
5. Urge the finance person to issue the fraudulent payment by end of day

So, what M365 security do small and medium businesses *really* need?

MSPs should focus their clients' attention on 5 fundamental best practices for preventing M365 breaches.

The 5 fundamental best practices for preventing M365 breaches

1. Implement Multi-factor Authentication (MFA). It’s the single-most important measure against breaches. Microsoft says MFA can block 99.9% of breach attempts.

The 5 fundamental best practices for preventing M365 breaches

2. **Block legacy authentication**. This will close any lingering "back doors" that a cybercriminal might use to circumvent MFA.

The 5 fundamental best practices for preventing M365 breaches

3. Activate all email safeguards, because Outlook email is the most common point of attack for spammers. This includes highlighting external emails, blocking suspicious attachments (e.g., .exe), and more.

Cannot start Microsoft Outlook. Cannot open the Outlook window. The set of folders cannot be opened. The operation failed.

The 5 fundamental best practices for preventing M365 breaches

4. Have a high-quality spam guard product in place, in addition to the standard M365 filtering. These third-party products can vet emails before they reach the inbox, use machine learning to detect emerging threats, and help protect against denial-of-service (DoS) attacks.

The 5 fundamental best practices for preventing M365 breaches

5. Create and implement a thorough user awareness training program to reduce human error while empowering users, increase adoption of MFA and other safeguards, maintain regulatory compliance, and build a security-focused culture.

Augmentt can provide expert guidance

Contact your Augmentt representative today for more about how MSPs can protect their clients' from cybercrime using the fundamentals of M365 security.

AUGMENTT