Exchange Server Breaches Show It's Not Just About Uptime

Early in March 2021, Microsoft announced they had found vulnerabilities that affected their on-premises email platforms. Hackers exploited these vulnerabilities with a series of Exchange Server breaches that have affected hundreds of thousands of organizations. With elevated access, hackers gained the ability to steal data, compromise credentials and plant malware.

Since discovering the vulnerabilities in March, Microsoft has released several security patches. However, in a statement released in May, Microsoft indicated that the initial patches alone would not fully protect their customers. If hackers had already compromised the system before the patch, victims would need to take additional steps to remediate the problem.

This troubling series of events highlights a bigger concern that organizations need to pay more attention to protecting their mail servers. Consider the wealth of information hackers can harvest from email, from personal and financial data to trade secrets. Organizations need to take steps to tighten security around these key assets.

Access Management Just as Critical as Uptime

In general, email service providers focus on uptime guarantees. After all, email plays a critical role in keeping business moving forward, and a downed server can significantly disrupt operations. However, organizations that emphasize availability over security play a dangerous game.

Remote work complicates the situation further, as employees access email using a variety of devices, from laptops to cell phones. With so many devices accessing the system, hackers have a multitude of opportunities to compromise identities. And once they do, the trouble really begins.

To protect their systems, organizations can take several key steps, including a layered approach to access management. Begin with enforcing multi-factor authentication (MFA) for email access. Additionally, implement device-level security. Ideally, employees must use a registered device to access email.

Bite the Bullet and Apply those Patches

In addition to access management, security patches play an essential role in protecting organizations. In the case of the Microsoft Exchange Server breaches, Microsoft has released several patches. However, six months after the breach hit the news, estimates suggest that nearly one third of impacted servers remained unpatched.

Further, as indicated above, organizations that applied only the first patch could still be hosting intruders in their systems. On the other hand, Microsoft customers who immediately applied all patches gained much needed protection. While patch application can prove time-consuming, businesses cannot afford to gamble with their security.

The lesson applies beyond email, as well. Any out-of-date applications or devices increase the risk of attack. From anti-virus to firmware, application software to firewalls, be sure to apply patches in a timely fashion.

Exchange Server Breaches Emphasize Need for Cloud Computing

While the Microsoft Exchange Server breaches have caused widespread security concerns, the problem only affects the on-premises versions of Exchange. Cloud-based Exchange environments remain unaffected.

For many organizations, crises like these underscore the need to migrate to the cloud. On-premises solutions require substantial in-house expertise and frequent patching. Cloud-based solutions, while they bring their own concerns, ease the burden on in-house IT staff and automate the updating process.

Add Experts to Your Security Team

A viral meme claims, "The entire fiasco of Jurassic Park could have been avoided if they hired one more IT guy." Like all jokes, the meme contains an element of truth. Many of the victims of the Microsoft Exchange Server breaches involved small to medium businesses (SMBs) with limited IT staff.

An overstretched IT department will lack the resources to conduct continuous monitoring and server maintenance. They may delay applying critical patches because of lack of manpower. And they may not have the expertise to implement an effective cybersecurity solution.

With a partner like Messaging Architects, businesses have the other IT guy they desperately need. We can customize a security solution to meet business needs, help you implement identity and access management and ensure your systems stay up to date. And when you are ready, we can help you migrate safely to the cloud.