HORNETSECURITY

ON-PREMISE VS. CLOUD: WHY YOU SHOULD SWITCH FROM MICROSOFT EXCHANGE TO MICROSOFT 365

AND WHY YOU NEED ADDITIONAL LAYERS OF SECURITY

Content

In January 2021, **four zero-day exploits were discovered in on-premise Microsoft Exchange servers** that gave attackers full access to user emails and passwords on the affected servers, administrator privileges on the server, and access to connected devices on the same network.

A worldwide wave of cyberattacks followed - **an estimated 250,000 servers fell victim to the attacks.** This has once again shown the dangers associated with companies hosting company data and email communication on premise. Read this white paper to learn why **switching from the on-premise Microsoft Exchange solution to Microsoft 365** in the cloud will optimize your uptime.

You'll also discover why you need to boost Microsoft's built-in security with additional layers of protection to **adequately safeguard your organization against security threats.**

MICROSOFT EXCHANGE HACK SHOWS JUST HOW URGENTLY YOU NEED TO MOVE TO THE CLOUD

The Microsoft Exchange Server hack, which affected hundreds of thousands of servers worldwide, is one of the most-serious cyberattacks in recent years. **As of last count, more than 60,000 organizations have fallen victim to the attack.**

High-level authorities such as the White House and the BSI (German Federal Office for Information Security) have urged affected organizations to install security patches in their respective Exchange systems. But patching one's Microsoft Exchange server is not enough if an organization has been compromised; it's like closing the barn door after the horse has bolted.

Attackers may have **already installed backdoors or created accounts to grant themselves high levels of access.**

Affected companies face high costs and loss of sensitive data

Affected companies not only have to face the loss of email communication and the disruption of business operations in the course of the patching process, but are also burdened by far worse damage if the attack was successful.

Hackers can **steal sensitive company data or gain access to critical business processes,** with all the costs, hassles and legal liability that can involve. And even if the Exchange servers are patched, back doors are shut down, and attackers are fully eliminated, that is not the end of it.

A **spate of spear phishing attacks is likely to follow** since the attackers will be able to use the information they collected via the attack, such as emails and other documents. This enables them to craft extremely targeted and credible scam emails.

Cloud versus On Premise – What the experts say

Given the scale of this attack, Hornetsecurity's security experts strongly recommend that companies **replace on-prem deployments of Microsoft Exchange with the cloud-based alternative, Microsoft 365.** Being in the cloud, Microsoft 365 is not vulnerable to this kind of attack or issues caused by bad weather, outages and the like. It additionally includes greater functionality. **Read on to better understand the advantages of cloud-based hosting versus on-prem.**

WHAT'S THE PROBLEM WITH ON-PREMISE HOSTING?

Although cloud computing continues to gain ground in organizations worldwide, companies often ask questions about costs, effort and above all, security when making this decision. After all, sensitive data needs to be protected and smooth operations maintained, especially in relation to something as mission critical as email.

Hosting and operating software on in-house servers offers **various advantages such as full control over one's own systems,** the fact that the entire IT infrastructure is located within the company, local storage of data even without an Internet connection, and high customization options. However, this is countered by several disadvantages, which also come into play with Microsoft Exchange:

The company is responsible for the security of its data and vulnerability management

The company must take care of data security itself. This requires trained IT staff who must be aware of security vulnerabilities and install updates regularly and quickly, prevent system failures and take corrective action in an emergency.

On-prem software is often not up to date, meaning companies become vulnerable

When problems occur in on-premise software and updates are necessary, the company itself is responsible for ensuring that these bugs are fixed. Often, the necessary resources are lacking in this area or staff are unaware of new patches, resulting in crucial delays before the software can be used properly again.

Complete loss of data is possible

Not only does the company need to ensure that on-premise software is up to date, but it also needs to ensure that nothing happens to its hardware. For example, in the absence of backup systems, a fire, flood or technical failure can cause the loss of important data.

On-premise is expensive and time-consuming

Another disadvantage of on-premise software is the high cost. The necessary hardware must be purchased, financed and maintained by the company itself.

Especially vulnerable to ransomware attacks

Data shows that the likelihood of falling victim to ransomware attacks is higher for organizations with on-prem setups. An analysis of data from ransomware leak sites by Hornetsecurity Security Lab found that, among victims whose data was published on these sites, 25 percent of organizations host their email servers on-premise.

In comparison, published information on ransomware leak sites that do not use email as their primary access vector shows that only 13 percent of organizations host their mail servers on-premise. This means that the risk of falling victim to an email-based ransomware attack is twice as high for organizations that self-host their email servers as compared to ransomware attacks that use other attack vectors.

WHAT ARE THE ADVANTAGES OF CLOUD-HOSTED MICROSOFT 365?

Microsoft is seen as the biggest driver of the global move to the cloud and has brought the world's most widely used office suite to the cloud with Microsoft 365. **For companies now weighing the risks of cyberattacks on cloud services against the technological advantages, the list below will prove helpful.**

Latest security updates

Organizations using MS 365 will always automatically have access to the latest version of the solution, without needing to handle any patching themselves. Microsoft delivers updates, and cloud providers focus only on the reliability and security of the system.

This enables their customers' companies to focus on what they do best – their core business. And if there is an attack, the SaaS vendor simply installs the patch themselves. There is no need for every single customer to install their own patches, which simplifies security tremendously.

Latest functions and a variety of additional features

This also means that MS 365 users always have access to its latest features, without needing to lift a finger. Updates are done automatically. Additional features that form part of the package – like Microsoft Teams, OneDrive, SharePoint, etc. – simplify the collaboration within the company and facilitate data exchange.

Easy to use and maintain

The usability of cloud-based applications like Microsoft 365 is less complex. It can be installed in just a few minutes. The company also does not need to handle its maintenance.

Save resources

By using cloud software, companies save not only the expense of operating data centers and server rooms, but also the procurement, installation, configuration, maintenance and updating of software, among other things.

Scalability

Because Microsoft 365 is hosted in the cloud, it's easy to scale the required storage.

Flexibility

Companies who use MS 365 can access documents from any device, anywhere, synchronously.

ISN'T MICROSOFT 365'S BUILT-IN PROTECTION ENOUGH? WHY DOES IT NEED ADDITIONAL LAYERS OF SECURITY?

When considering Microsoft 365 and its many benefits, companies often worry about the security of their data from cyberattacks - this concern is not unfounded, but it is solvable. While Microsoft includes protection mechanisms, **additional levels of third-party protection are necessary for a company to enjoy adequate security.** Here's why:

Microsoft 365 is under massive attack

As Microsoft 365 is the most used office solution by companies of all sizes, it's also the one that's most attacked. For example, in recent years, phishing attacks have increased by 250% percent.

Microsoft itself stated in its latest Microsoft Digital Defense Report that threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot and that threaten even the savviest targets.

Ransomware is the biggest threat

Microsoft underlines that ransomware is the most common-reason behind their incident response engagements from October 2019 through July 2020. The average cost of a ransomware incident is over $84,000.

Microsoft's filters are not perfect - third-party supplementation recommended

A successful attack on Microsoft 365 can be very lucrative for cybercriminals. This is the reason why hackers invest many resources to find vulnerabilities in Microsoft's integrated security systems. It is therefore not surprising that analysts such as Osterman Research recommend additional third-party protection solutions to complement Microsoft's built-in filter.

New study reveals vulnerability of Microsoft 365 accounts

According to Vectra AI, 71% of Microsoft 365 deployments could have been successfully attacked by cybercriminals in 2020. The study also worryingly highlights that upper levels of management overestimate their own defensive capabilities.

Additionally, identifying a Microsoft 365 user is very simple for an attacker, because the MX records and autodiscover entries are visible to the public online. Comprehensive security features are being implemented to prevent possible attacks on Microsoft 365 accounts, but it must be kept in mind that the data in the cloud itself – even in the event of unauthorized access – can be accessed from anywhere. **By using Microsoft 365, an important security aspect is no longer available to companies: the firewall.** If an attacker succeeds in gaining unauthorized access to a Microsoft 365 account, all data is available to them without any restrictions.

HORNETSECURITY

HOW CAN I BOOST MY MICROSOFT 365 SECURITY TO PROTECT COMPANY DATA?

According to statistics, 95% of all successful cyberattacks breach an organization via email. Email communication is considered the main gateway for any cybercriminal methods to access, steal, and encrypt internal company data. The same applies to email communication via Microsoft 365. That's why **Hornetsecurity has developed 365 Total Protection - an industry-unique security and compliance suite designed specifically for Microsoft 365** that provides comprehensive additional protection.

The service combines all the necessary security features required by comprehensive email security management, such as:

- ✓ **Email Live Tracking:** enables an admin to monitor the company's entire email communication in real time.
- ✓ **Threat defense:** multi-stage in-depth analysis and filter systems detect even the latest spam and phishing attacks. Hornetsecurity has the highest detection rates on the market.
- ✓ **Global S/MIME & PGP encryption:** protects the entire email communication from being altered or read by third parties.

The Enterprise version includes even more advanced additional functionality, such as:

- ✓ **Forensic analysis mechanisms:** intelligent filters enable efficient detection and filtering of any cyber threats that breach the company via email.
- ✓ **Detects even advanced threats** like ransomware, business email compromise or CEO fraud.
- ✓ **Malware ex-post alert:** allows admins to delete potentially harmful emails that are detected later.
- ✓ **ATP sandboxing:** offers protection against targeted and blended attacks.
- ✓ **Email archiving:** it is essential to have emails archived - legally and audit-compliant.
- ✓ **URL malware control:** identifies links that may lead to websites offering malware-infested downloads.
- ✓ **Contingency covering:** ensures permanent access to your company's emails even if the Microsoft service is temporarily unavailable.
- ✓ **Global security dashboard:** centralizes all the functions and results of 365 Total Protection and offers a complete overview of your company security.

Try it our for free today on:
www.hornetsecurity.com/us/services/365-total-protection/