



ConversationalGeek®

5 WAYS to MITIGATE the RISK of Zero Day Attacks Against Microsoft 365





Why Worry About Zero-Day Attacks Against Microsoft 365?

If you're reading this, your organization's users are likely included in the estimated 300 million Microsoft 365 subscribers today¹. The servers within Microsoft 365 – specifically Exchange Online – host contain some of your organization's most sensitive information. These same servers also represent a critical communication medium that organizations simply can't do without for an extended period of time.

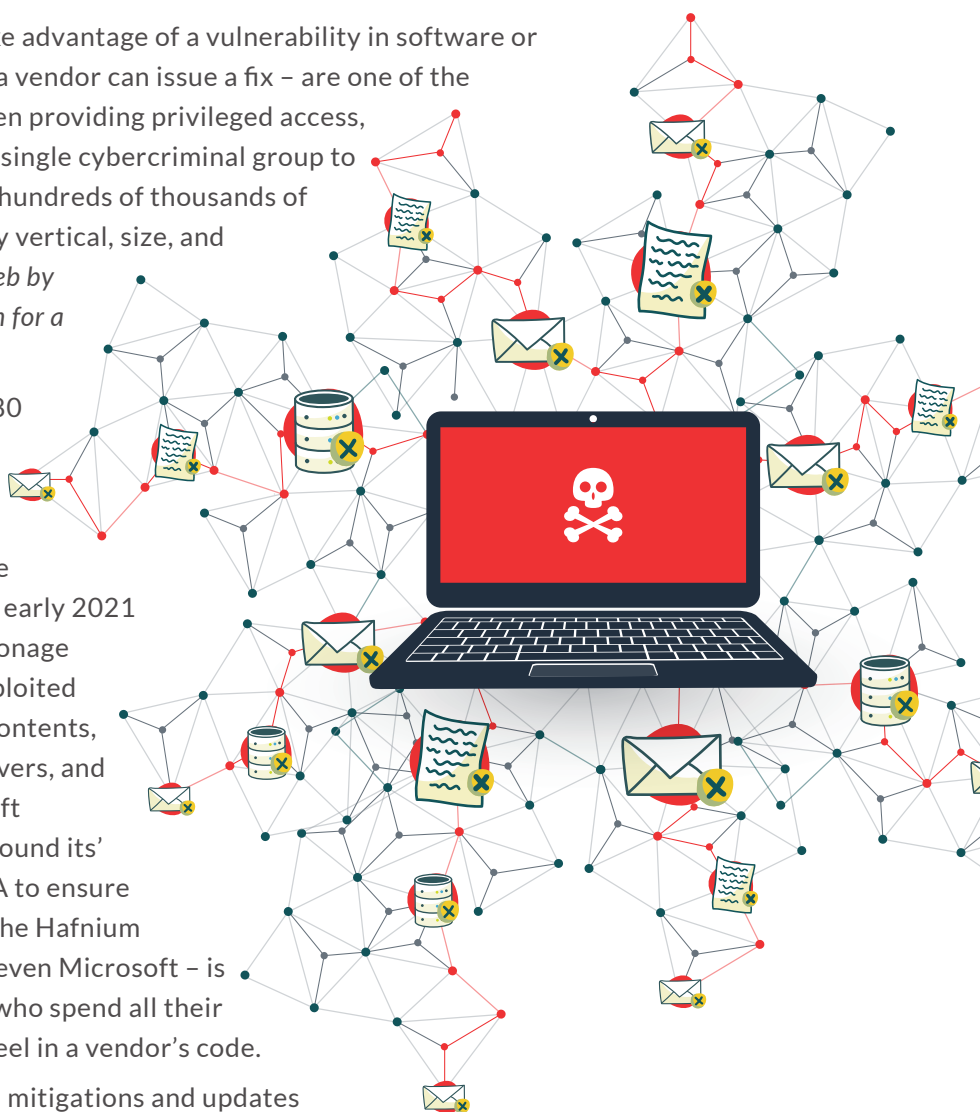
Zero-Day Attacks – those attacks that take advantage of a vulnerability in software or firmware found by cybercriminals before a vendor can issue a fix – are one of the cybercriminal's greatest advantages. Often providing privileged access, Zero-day attacks become the means for a single cybercriminal group to potentially gain access to literally tens or hundreds of thousands of organizations in every geography, industry vertical, size, and country. *There are even posts on the dark web by cybercriminal gangs offering as much as \$3m for a zero-day remote code execution exploit.*

According to recent analysis, there were 80 zero-day vulnerabilities exploited in 2021, a 166% increase from 2020, with Microsoft, Apple, and Google products most frequently targeted². You'll recall the zero-day attack on Microsoft Exchange in early 2021 that originated from a Chinese cyber espionage group, dubbed "Hafnium" and, in total, exploited four vulnerabilities to exfiltrate mailbox contents, gain admin control over compromised servers, and install malicious software. While Microsoft provides a world-class layer of security around its' services, as well as copious amounts of QA to ensure their products are secure from the start, the Hafnium attack is a reminder that no vendor – not even Microsoft – is impervious from very intelligent hackers who spend all their time trying to find a proverbial Achilles' heel in a vendor's code.

And should a zero-day attack occur, initial mitigations and updates generally are not immediately available, putting organizations that are attack targets largely helpless to defend themselves during the time between an attack's discovery and mitigation.

But what happens if the target is Microsoft 365, specifically Exchange Online, as email continues to be? What can you do both proactively and reactively to mitigate the risk a zero-day attack against it includes?

The remainder of this eBook will focus on 5 key risk mitigation steps you can take to protect your operational investment in Microsoft 365.



¹Microsoft Q3 2021 Earnings Call

²Mandiant Threat Intelligence, "Zero Tolerance: More Zero-Days Exploited in 2021 Than Ever Before", April 21, 2022

#1

Harden your email – the most significant attack vector

It's a well-known fact that 90%+ of all cyberattacks start with an email. While we're talking about protecting against zero-day attacks, there's no rule that says a threat actor can't also attempt to take advantage of email to spread malware within an organization. And since this is one of those steps you can more easily address, it makes sense that you need to have a layer of protection that resides logically where an email enters your organization. What's needed is a defense-in-depth approach using third-party solutions that augments any built-in security on Microsoft's part. Microsoft 365 E3 licenses do include Microsoft Defender and Exchange Online Protection to protect against email-based attacks, with E5 licenses including the addition of Microsoft Defender for Identity and for Endpoint. E3 customers have only the essential levels of protection with E5 customers takes the protection and detection of email-borne attacks to an advanced level.

But even so, there are additional layers of your defense-in-depth strategy to harden the email perimeter that can be taken to make it increasingly more difficult for cyberattackers to navigate. The goal is to stop any zero-day attacks that first need to establish a foothold via phishing.



Domain Protection

Several technologies exist today to ensure the validity and integrity of emails received. The Domain-based Message Authentication, Reporting and Conformance (DMARC) defines a policy around what should be done with an email where the sending domain appears to be impersonated. The Sender Policy Framework (SPF) is used within DNS to identify the hostnames and IP addresses of valid email senders for a given domain. Putting these in place helps eliminate the possibility of successful domain impersonation on the part of the cyber attacker.



Virtual Sandboxing

The opening of an email can be simulated within a virtual environment where attachments can be detonated to see whether they perform a malicious action.



URL Protection

Links can be scanned in real-time and blocked from being clicked if deemed malicious.



Credential Harvesting Detection

Sending domains can be validated to ensure phishing emails aren't impersonating a trusted brand, while links and redirects can be intelligently followed to see if they take potential victims to spoofed logon pages to Office 365, Outlook and other Microsoft 365 cloud services. Phishing kits used to quickly prop up an entire fake website front-end for harvesting can also be detected.



Use of Artificial Intelligence

Use of AI focusing on the relationships and connections between senders and recipients, including the strength or proximity of the relationships, can help identify anomalous emails that may be malicious in nature.



Shared Threat Intelligence

A strong defense rests in it being based on shared threat intelligence to ensure the most up-to-date data to increase detections and reduce risk. In addition, the intel gathered through protecting the email perimeter should be shared back to your SIEM to aid in providing a comprehensive view of what's happening on your network.

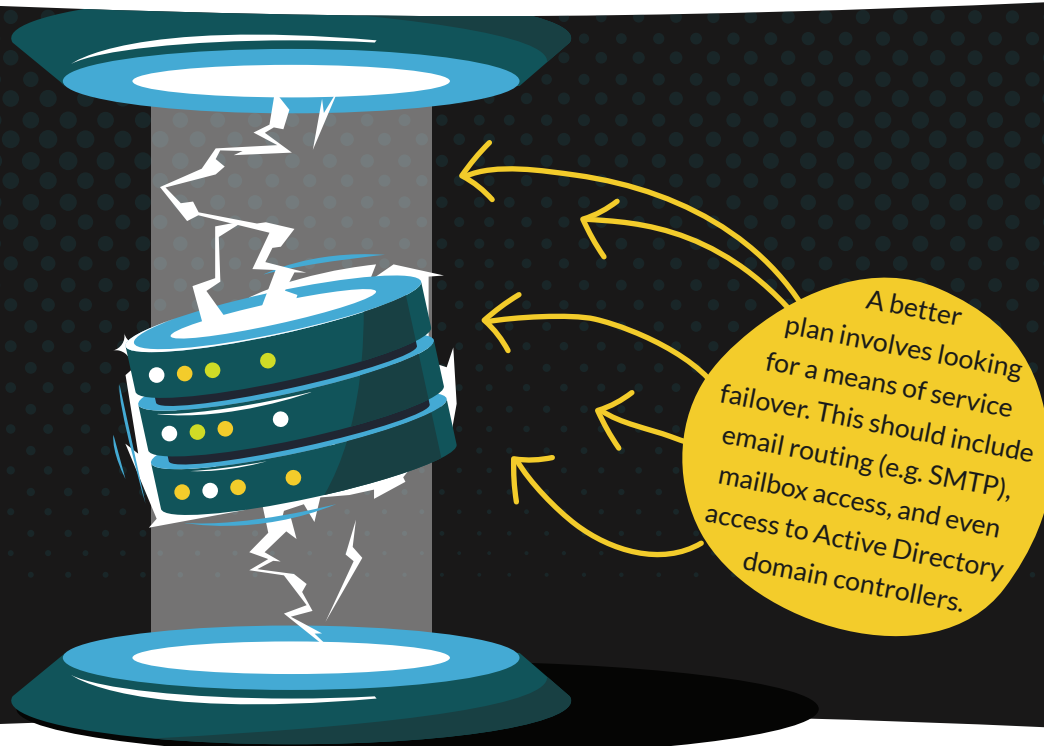
#2

Establishing a continuity plan

While most zero-day exploits do not render the services they compromise completely inaccessible during an attack, it's reasonable to assume that impacted services will need to be taken offline (to eliminate attacker access) while discovered vulnerabilities are being remediated. Should an attack impact Exchange Online servers, remediation may involve the *entire* Microsoft 365 environment, taking

time to update the affected systems, investigate indicators of compromise, and to perform further remediation to remove access, malware, etc.

So, it's necessary to have a continuity plan – one where email services are available and accessible to some degree. In the simplest of working environments, users of the full Outlook client can continue working offline; while not perfect, it does provide some degree of continuity. But that doesn't help with inbound and outbound communications; continuity plans are intent on keeping the business operational.



Depending on which services have been affected (e.g., only an Edge Transport server), it is possible that Microsoft can quickly replace the impacted servers with another and have the affected services reconfigured to point to the new server. However, good risk mitigation practices would dictate you don't plan for such a perfect scenario; you need to be thinking what to do if Exchange Online is down completely.

Consider third-party solutions that sit externally from your Microsoft 365 environment and during normal operations employs SMTP relays to first accept inbound email and then forward it to Exchange Online within your Microsoft 365 instance. During an outage, email continues to be accepted by the solution and is accessible by special email clients, allowing operations to continue. Once services are restored, any emails that have not yet been forwarded to Microsoft 365, are sent bringing the production instance of Exchange Online current.

This strategy minimizes any downtime caused by the exploit, updates, or incident response activity. It also specifically mitigates *operational* risk of a zero-day attack, keeping the business operational.




#3

Archiving to an independent environment

Along the same vein of thinking as having a continuity plan, those organizations actively relying on an Exchange Online's archiving capabilities need to be thinking about how long the business can operate without an accessible archive, should the Exchange Online server hosting your archive be inaccessible. There are productivity, legal, and compliance-related ramifications should there be no access to an archive for a prolonged period of time, making it necessary to have an archiving strategy that doesn't necessarily put all your archiving eggs in to just the Microsoft 365 basket.

Having a third-party archive that sits outside of Microsoft 365 mitigates the risk that historical data is inaccessible, inaccurate, or is simply gone.

Having an external archive also can assist with any attacks where attackers modify or delete data within a mailbox, as well as attacks holding Exchange data for ransom.



The reality is, on a daily basis, you don't need to keep everything inside Exchange Online. In fact, many organizations offload Inbox contents older than just a few months to an archive to minimize the backup data requirements, thereby speeding up recovery operations.

#4

Ensure Recovery Resilience

Most victims of zero-day attacks experience compromised servers (Exchange servers in the case of Hafnium) and exfiltrated data (whether for extortion, intel, discovery, or espionage). Actions like data deletion, modification, and encryption (as part of a ransomware attack) are very easy to envision as the next step. While separate archives will help with resilience around older email content, organizations need a way to return the environment back – including your data within Exchange Online) to a working state.

In an attack scenario, Microsoft certainly will take the necessary steps to get any affected services back up and running quickly. But Microsoft makes is clear in their Microsoft Services Agreement that protecting the data your organization places within any part of Microsoft 365 (including Exchange Online) is the responsibility of the customer and not Microsoft. Take the following excerpts (with emphasis added):

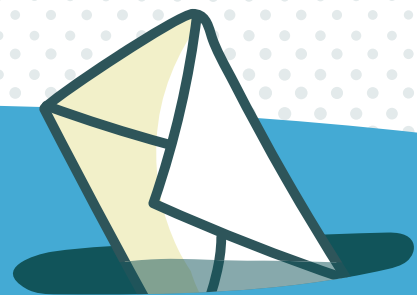
*The Privacy Statement also describes how Microsoft uses your content, which is **your communications with others; postings submitted by you to Microsoft via the Services; and the files, photos, documents, audio, digital works, livestreams and videos that you upload, store, broadcast or share through the Services ("Your Content")**.*

*We don't claim ownership of Your Content. Your Content remains Your Content and **you are responsible for it**.*

So, should an attack result in Exchange Online containing anything less than the email data you expect to see, the data needs to be recovered from backup – *your backup*. So, it becomes necessary to not just be able to recover a mailbox and its' data, but to ensure any recovered data is in a known good *and* known-secure state.

How Do You Solve This?

What's needed is to rebuild a mailbox data from a compliant, independent source that takes the known good historical mailbox data and updates it with a current (and known-secure) copy of all changes.

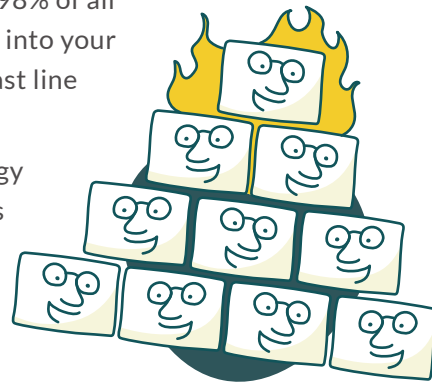


#5

Empower humans and technology to work together to strengthen organizational security

While many zero-day attacks focus on servers and services, users play a material role in most cyberattacks, making them a far larger threat surface for the organization. Oftentimes, we look at users as the weakest link in an organization, as they are prone to fall for phishing scams using sophisticated social engineering tactics – which is used in 98% of all cyberattacks³! But it's possible to turn them into your “human firewall”, where they become your last line of defense for your organization.

This is accomplished by combining technology and employees together through continuous security awareness training. By using engaging content, users can be taught to have a vigilant mindset, understanding what kinds of attacks are occurring, the tactics used, how to spot them in the middle of doing their job, and to avoid becoming a victim.



But not every employee retains training the same, so organizations need a feedback loop to understand where their greatest human risk exists (that is, which users are most likely to continue to fall for phishing attacks). The feedback loop for security awareness training is phishing testing, where users are sent, in essence, fake phishing emails to see who falls “victim” to the phish and who spots it.



By utilizing phishing simulation tests, organizations can gain visibility into which employees pose a higher risk of falling victim to actual phishing scams, are ignoring obvious signs of impersonation and social engineering, and are clicking links or opening attachments without a using a scrutinizing eye. These employees represent the greatest risk and can be “patched” through further security awareness training and subsequent phishing testing. This same data can also be used as the basis of assessing the current security stack to find ways that further strengthen defenses.

³Purplesec, Cyber Security Trends Report (2021)

What if I'm not yet on MICROSOFT 365?

First off, it's important to realize there *will be a next time* when it comes to zero-day attacks – likely even for Microsoft. The harsh reality is the threat actors are becoming more sophisticated and it's necessary to build cyber resilience to be prepared when (not *if*) attacks occur.

Those organizations currently using on-premises instances of Microsoft 365 may be wondering if it's more secure to stay where they are. The answer is a resounding “no”; the very same concerns outlined in this eBook are even more relevant to Exchange on-prem as Microsoft 365 has a far better layered defense-in-depth in place, more staff dedicated to protecting, monitoring, and remediating security issues, etc.

So, the obvious answer for those organizations still on-premises is to migrate to Exchange Online within Microsoft 365 – keeping in mind all the risk mitigation steps raised within this eBook once you get there. But a blind lift and shift of your on-premises Exchange data isn't the right answer; should you look to migrate to Microsoft 365, there needs to be a de-risking of the move, including:



Archive Before Migrating

Microsoft 365 only needs to house current business email and content. So, looking to archive *before* the migration minimizes the amount of data the needs to be pushed into the cloud. Having a solution that can archive your on-premises Exchange pre-migration and then be pointed to Microsoft 365 post-migration is an effective answer.



Plan Licensing

Once you put something in the cloud, there is an immediate monthly cost. Take count of how many employees need licenses, which licenses they need, etc.



Address Support Headcount

Staffing needed to support both the move and the subsequent ongoing management may look different than it does today. Consider headcount needs for administration, backups, licensing, and support.



Take Care of Backups

Microsoft is a firm believer in the shared responsibility model, and backups of all data within Microsoft 365 – including Exchange Online – are the customer's responsibility. Have a solution in place and a backup strategy ready once you begin your migration.



Considering What Else Should be Consolidated

Because the organization will likely take advantage of other services such as Teams, OneDrive for Business, SharePoint Online, and more, there may be a similar opportunity to consolidate which data gets moved to those new platforms.



Assess the risk of "good enough"

Microsoft offers plenty of supporting solutions around Microsoft 365 to address archiving, security, compliance, and more. Assess the risk that may be introduced by relying on a single vendor (something pointed out a few times in this eBook) and consider the need for additional third-party solutions to offset the risk.



Mimecast was born in 2003 with a focus on delivering relentless protection initially for email. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security and resilience challenges together. But we haven't stopped there, we are the company that built an intentional and scalable design philosophy that addresses the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technical failure; and to lead the movement toward building a more resilient world.

For more information, visit: www.mimecast.com