TitanHQ™

Navigating the M365 Maze: Insights into IT Administrator Security Challenges.

Microsoft 365 is one of the most popular and trusted brands on the planet. The Office suite covered by M365 includes productivity stalwarts Outlook, Word, Excel, and Microsoft Teams. Millions of companies worldwide rely on M365 to keep their businesses running smoothly.

To use M365 **effectively**, the environment MUST be secure. M365 is a popular brand and business-critical, a perfect mix for cybercriminals who flock to anything that is essential and widely used. However, the M365 environment can be a challenge to administrate. TitanHQ explores these challenges and offers some resolutions.

Why M365 is an admin challenge?

Microsoft 365 is not just composed of point apps; it is an ecosystem that provides an expanded platform for interconnected data communication. Many businesses generate massive amounts of data across the various apps under the M365 umbrella. These data's development, sharing, and storage can easily open security gaps.

These gaps in data flow are compounded when companies utilize collaborative working with third parties and remote workers. It is easy for data to become exposed or cybercriminals to take control of M365 accounts unless a consolidated approach to security measures across the M365 environment is enforced.

However, consolidation is a major challenge in the M365 environment. Sharing permissions and privileges between apps can be complex to enable. This leads to gaps in visibility that cause permissions sprawl and poor audit. Any oversight and governance issues open the chance of accidental or deliberate data exposure. Remediation, too, can suffer from gaps in governance.

It is essential to secure your M365 environment because cybercriminals are exploiting security gaps in the M365 ecosystem.

1.6 million

A 2022 study that surveyed 1.6 million Microsoft 365 users found that 90% had gaps in essential security protections

Why is it important to secure M365?

A 2022 study that surveyed 1.6 million Microsoft 365 users found that 90% had gaps in essential security protections. Many problems occurred because of the difficulty in managing the M365 environment. Some of the issues manifested as poor management of administrator credentials. With these issues in mind, recent security exploits highlighted by M365 users demonstrate the importance of securing M365.

Compromised Teams accounts

Microsoft Teams was used as a ruse in a mass phishing attack on users of the platform. The attack began with a compromised Teams user; the hacked account was used to send over 1,000 malicious Teams group chat invites. If an invite was accepted, the user was then tricked into downloading a malicious file. This file was used to initiate the install of DarkGate malware.

Targeted employees and phishing

In a similar DarkGate-Teams exploit, attackers sent phishing emails to targeted M365 users. The emails looked like HR sent them. The emails contained a link to a malicious remote file. The content of the phishing emails manipulated the recipient's behavior by causing them to feel concerned about a potential vacation clash. Anyone looking forward to vacation will know how concerning a message like this would be. Clicking the link took the recipient to the remote attachment named "Changes to the vacation schedule.zip." The attachment was stored in a Microsoft SharePoint endpoint, making it look legitimate. Downloading the file and opening it triggered a series of programmatic events, resulting in the download of DarkGate Loader and subsequent malware infection.

DarkGate is a malware that can be used to download other malware, steal credentials, execute remote commands, and even hijack a device for cryptomining.

Configuration complexities

In both cases, the attackers exploited a gap in M365 security: external Microsoft Teams users are allowed to message other tenants' users by default. This can be disabled, but it is all part of M365 administration and can be challenging to configure.

The above exploits show the importance of secure configuration in M365. However, this is not the end of the M365 security story. Poor security hygiene measures, even by Microsoft itself, can open gaps in M365 defenses:

Poor authentication hygiene

Another attack compromised Microsoft's executive accounts. The attack was initiated by the Russian hacking group Midnight Blizzard. The hackers used a password spray attack, a type of brute force entry exploit. Because MFA (multi-factor authentication) was not enabled, the attackers were able to access poorly protected accounts. The attackers focused initially on a non-production test tenant account as a way into the M365 environment.

Microsoft was not the only enterprise to suffer from the Midnight Blizzard attack. Hewlett Packard was also a victim of the hacking group, email accounts of cybersecurity employees having data exfiltrated by the group.

The popularity and ubiquitous use of M365 is also its Achilles Heel. Cybercriminals are actively looking for ways to circumvent M365 security. If there is a security gap, it will be found by malicious actors. But as we have seen, the administration of M365 is confounded by complexity and configuration issues.

Attacks and vectors targeting M365 that make administration challenging

The ecosystem use of M365, is part of its attraction for business users. Under one hood, a company can deploy email communications, productivity tools, and collaboration portals. Having this level of interconnectedness brings with it the following issues:

Humans in the middle: M365 is about making employees' working lives easier and more productive. As we have seen, the platform is so popular that Microsoft is winning in this respect. However, people are a favorite exploit for hackers. The human-centric nature of M365 is what attracts cybercriminals. Emails are like a pipeline straight into the middle of a corporation. Email-borne exploits such as phishing are an ideal way for cybercriminals to exploit M365 Outlook. Phishing emails may be mass-delivered or targeted, as in the case of spear-phishing. Even the administrators of M365 are not safe from phishing.

Read more on M365 phishing attacks.

Large interconnected attack surface: M365 covers a large number of apps. Which apps are used by an organization depends on its license. However, even with a basic "Business plan," a company is looking at a potential 28 apps. Many of the apps are interconnected to allow for seamless sharing of data and collaboration /workflow. Many of these apps have separate security configurations. Ensuring all the apps have the correct security settings and the proper user privileges are in place is complicated. Employees must be able to access and share data across these apps. Access from internal users and remote workers means that the attack surface expands and opens security gaps. Add to this joiners and leavers as they come and go in the organization; administration challenges complicate control of those gaps.

Adversary-in-the-Middle (AiTM): AiTM attacks are used to circumvent MFA protection. There are lots of AiTM kits available on the dark web, so this type of exploit is increasingly being seen. The methodology of AiTM requires session tokens to be replayed and/or stolen. The result is the session cookies are stolen allowing hackers to gain access to email accounts. The compromised account is then often used in a Business Email Compromise (BEC) attack. Microsoft recently added new functionality to help mitigate AiTM attacks.

Ransomware focus: M365 Outlook and collaboration tools like Teams are an ideal pipeline into the corporate network. An enlightening report from Coalition Insurance found that, in the context of cyber insurance claims, “Businesses using Google Workspace for email were markedly more secure than those using Microsoft Office 365 (M365) and on-premises Microsoft Exchange.” The report found a 27% increase in ransomware claims. The collaboration capability of M365 and support for remote workers and the broader supply chain have made M365 vulnerable to phishing attacks. These attacks come in via email, and hackers exploit other routes, like messaging systems. The interwoven messaging and communication surface of M365 makes it ideally suited to exploitation. Administering disparate interfaces and channels while ensuring that security gaps are closed is highly complex.

This complexity is compounded by licensing complexities. The Coalition Insurance report noted that the disparity in security between M365 and Google could be due to license agreements. For example, Defender for Office 365 is not included in the Microsoft base E3 license. License complications add to administrator effectiveness in creating a secure M365 environment.

Unauthorized access: As noted in the attacks exploiting executive accounts, unauthorized access is the goal of a cybercriminal. Once access to a system is gained by using either stolen credentials or brute force, the sky’s the limit for fraudsters. Business Email Compromise has become a common outcome of M365-focused attacks. To protect their M365 investments, organizations worldwide are turning to a Defense-in-Depth approach.

Defense-in-Depth and M365

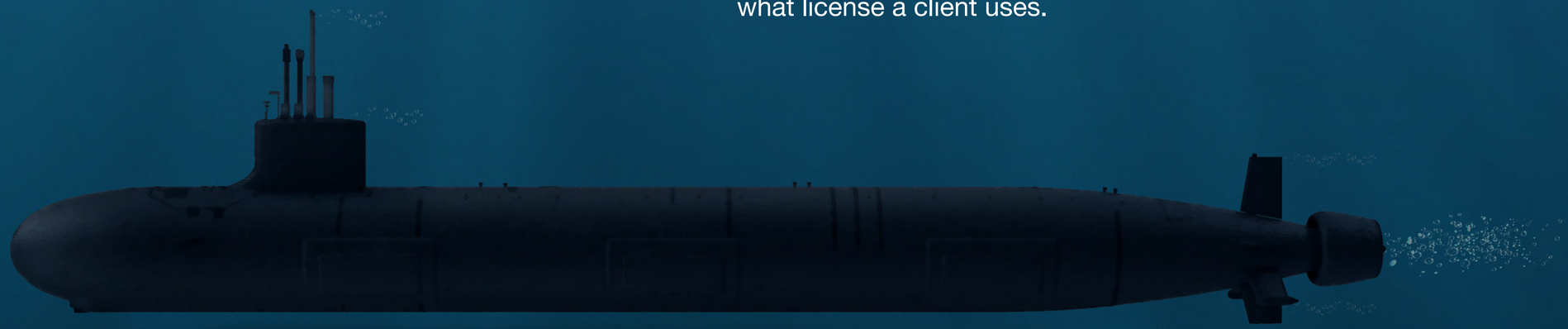
The attack statistics, administration challenges, licensing issues, and expanded attack surface make M365 a candidate for Defense-in-Depth. But what does this mean for Microsoft 365 administrators? Is there a solution to consolidate security?

PhishTitan is an Integrated Cloud Email Security (ICES) solution. Providing multiple layers of protection that can be integrated directly into M365, closes the security gaps. ICES solutions are delivered as cloud-native SaaS solutions. This means that PhishTitan is scalable, easy to deploy, and provides centralized maintenance and management. By integrating with Microsoft 365 native security, PhishTitan's additional advanced protection layers deliver the defense-in-depth approach.

One of the most important layers is to provide intelligent context detection. PhishTitan uses behavioral analytics, AI, and natural language processing (NLP) to augment native Microsoft security. These advanced detection capabilities are designed to detect and prevent advanced phishing threats, like the ones used in M365 exploits. ICES solutions make contextual decisions informed by intelligent pattern detection. It is this contextual analysis that can detect multi-stage attacks such as Business Email Compromise (BEC).

One of the complexities of administration of M365 that leads to security gaps is in the various Microsoft licenses. PhishTitan integrates Defense-in-Depth email security, regardless of the M365 license.

For an MSP this is especially interesting as this adds security above and beyond existing client license restrictions. PhishTitan provides advanced inline phishing protection for advanced zero day and BEC phishing emails, no matter what license a client uses.



PhishTitan's current performance is impressive. For every 80,000 emails received, PhishTitan catches 20 unique and sophisticated phishing attacks, which are otherwise missed by Microsoft's elite and expensive E5 license. PhishTitan automatically adds a security banner to these messages and auto-remediates them to the junk folder.

PhishTitan is an ICES solution that uses a defense-in-depth approach to email security. The intelligent, protective layers, include the following features:

1 **AI-driven threat intelligence:** anti-phishing analysis is based on AI, trained using data from a vast threat corpus. PhishTitan learns to identify patterns, adjusting tactics to capture emerging threats and zero-minute attacks.

2 **Real-time threat analysis:** PhishTitan's AI-driven anti-phishing service follows malicious links in an email to check the website. If the website is found to be legitimate, the email will be released to the user's inbox.

3 **URL rewriting and analysis:** URL analysis validates the security of the URL against multiple curated anti-phishing feeds. This system works with the 'time of click' protection to prevent successful phishing attacks.

4 **Time of click protection:** PhishTitan rewrites URLs and checks the website associated with the link. If the website is a phishing site, the user will be prevented from entering the site.

5 **Link Lock service:** a service that ensures the company remains protected even if a recipient clicks a URL in a malicious email.

6 **Data loss prevention (DLP):** prevents sensitive data from leaving the corporate network, even if by accident or maliciously.

7 **Smart Mail protection:** compares incoming mail with a list of known threats. Curated data from multiple sources of data across the global threat landscape ensures that the most current threats are always part of this list.

8 **Native integration with Office 365 email:** PhishTitan works symbiotically with the native security in M365 to allow a seamless transition from a conventional secure email gateway (SEG) to advanced phishing detection offered by an ICES solution.

Let TitanHQ help you navigate the maze of M365 security.

GET IN TOUCH