WHITE PAPER

Securing Office 365

How to Protect against Targeted Email Attacks

An Osterman Research White Paper
Published July 2017

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

Executive Summary

This white paper discusses the growth of Office 365, the cost of the platform and the benefits that it can offer to organizations of all sizes. It also discusses the optimal method of enabling security so as to maximize protection against the growing array of security threats that organizations will encounter, while minimizing the total cost of ownership for an Office 365 environment.

KEY TAKEAWAYS

Email is moving to the cloud: While most business users today are served by on-premises email systems, Osterman Research surveys show that most of these users will be served by a cloud-based system (most often Office 365) by 2018.

Office 365 is less expensive than traditional, on-premises solutions: Email in Office 365 is less expensive than email managed on-premises and by a significant margin: Exchange Online is roughly one-half to two-thirds less expensive than on-premises Exchange when considering all of the costs associated with managing email.

Security threats are real and are getting worse: The vast majority of organizations have experienced some sort of major security problem over the past 12 months, including ransomware, some other form of malware infection, the leak of sensitive or confidential data through email, and CEO Fraud/Business Email Compromise (BEC).

Moving to the cloud can increase security risks: While not always the case, there is the potential that migrating to the cloud can increase security risks among organizations that do not take appropriate steps to secure their infrastructure, their users and their data assets.

Many organizations do not yet have adequate protection in the cloud: Many organizations have not taken the steps necessary to protect their organizations from advanced email attacks, such as low-volume spearphishing and social engineering-based attacks that do not contain a malicious payload and BEC.

There are a number of best practices that organizations should consider undertaking: There are several best practices that decision makers should consider, including the creation of robust security policies, implementing best practices for user behavior, and deployment of a less expensive Office 365 plan in conjunction with a third-party security solution that properly addresses sophisticated attacks like BEC.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Agari – information about the company is included at the end of this paper.

The vast majority of organizations have experienced some sort of major security problem over the past 12 months.

WHY IS OFFICE 365 SO POPULAR?

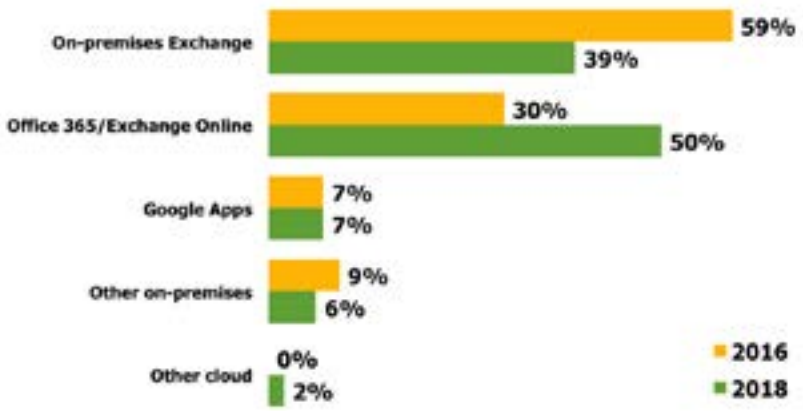
THE MIX IN PLATFORMS IS CHANGING OVER TIME

Office 365 is Microsoft's third major iteration of its hosted/cloud-based email and collaboration offerings and it's by far the most successful of these offerings to date. The company has been (and we anticipate will continue to be) successful in converting much of its base of on-premises users of Exchange and other solutions to Office 365. As shown in Figure 1, the growth of Office 365 will be rapid as on-premises users of Exchange and other platforms move to the cloud.

Figure 1

Deployment of Various On-Premises and Cloud-Based Solutions 2016 and 2018

Source: Osterman Research, Inc.



LOWER COST IS AN IMPORTANT BENEFIT OF OFFICE 365

One of the key benefits of Office 365 and other cloud-based offerings is their potentially lower total cost of ownership relative to on-premises systems, even for large enterprises. Much of the cost savings from cloud-based versions of Exchange, such as Office 365 and Exchange Online, result from the reduction in staffing necessary to support email and other solutions, although savings in power, real estate and related costs also contribute to the cost savings.

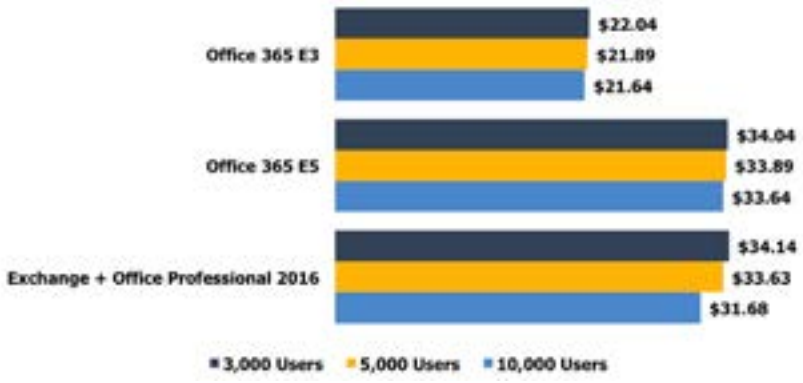
For example, as shown in Figure 2, Office 365 Plan E3 is less expensive than on-premises Exchange. We have included the costs of two leading Office 365 plans that are used in enterprise settings, but it is important to note that these offerings are supersets of the functionality provided by on-premises Exchange and include more functionality (e.g., licenses for desktop productivity applications and other capabilities) that are not included in on-premises Exchange. Consequently, while Office 365 Plan E5 looks to be on par with the price of on-premises Exchange and the on-premises version of Office, Plan E5 provides substantially more functionality.

Figure 2

Monthly Per User Solution and Labor Costs of Various Microsoft Platforms

Note: Assumes a 20% volume discount from list prices for Office 365, Office Professional 2016, and Exchange CALs; assumes three-year replacement cycle.and Exchange CALs; assumes three-year replacement cycle.

Source: Osterman Research, Inc.



THE FINANCIAL BENEFITS OF GOING FROM CAPEX TO OPEX

Switching to cloud services provides organizations of all sizes with a way to gain access to various communication and collaboration services without incurring the capital costs needed to build an on-premises system, nor accepting the responsibility and related costs of managing the resulting infrastructure. Since Office 365 is, for all intents and purposes, rented as a cloud service and the key infrastructure elements are not owned, organizations must continue to pay monthly or annual fees for the service to continue the service. That's not a bad thing, but merely a different way of thinking about shifting the software mindset from one focused on capital expenditures (CAPEX) to one focused on operating expenditures (OPEX).

Among the benefits of operating on-premises systems is the ability to bypass one or two upgrade cycles and so avoid the costs associated with migration from one version of Exchange (or some other platform) to another. For example, many organizations that are switching to Office 365 or Exchange Online are migrating from Exchange 2003 or 2007, never having deployed Exchange 2010 or 2013. These organizations have been able to use products purchased many years ago without incurring the major cost of a migration. Once an organization has shifted to Office 365, that option will no longer be available. However, this also means that software is always up-to-date and current with new standards, file formats, etc. Consequently, by deploying Office 365, organizations can realize the benefits associated with migration to new platforms without incurring the difficulties of going through a migration.

KEY FEATURES AND FUNCTIONS IN OFFICE 365

Office 365 consists of a variety of offerings, some or all of which are offered in the various plans offered by Microsoft: business-grade email, calendaring and scheduling functionality with a 50 Gb mailbox; full copies of Microsoft Office applications, including Word, Excel, PowerPoint, Outlook, Publisher and OneNote on up to five PCs or Macs; Microsoft Office on up to five mobile devices; online versions of Word, Excel and PowerPoint; one terabyte of storage using Microsoft OneDrive for Business per user; Skype for Business, which offers voice, instant messaging and videoconferencing; social media capabilities using Yammer; and various other tools and capabilities, such as corporate intranets, Office Graph, a corporate video portal, business intelligence tools, group policy tools, and various compliance tools, among others.

Office 365 and Exchange Online are offered in a number of plans for commercial enterprises, small businesses, government agencies, educational institutions, students and teachers ranging in price from $4.00 to $35.00 per user per month.

For the vast majority of users, email is the most widely used application within Office 365. Email in Office 365 and Exchange Online includes some basic email security capabilities, but more advanced security requires payment of an additional monthly fee for each Office 365 or Exchange Online account. In addition, archiving capabilities are also available that go beyond what is available in the standard offerings.

OFFICE 365 ALLOWS "RIGHTSIZING" CAPABILITIES

A key benefit of Office 365 is its ability to enable "rightsizing" of the tools that are provided to users. For example, if an organization has deployed an infrastructure capable of supporting 1,000 users, but then must undergo a 20 percent reduction in staff, the use of Office 365 enables a significant cost reduction compared to an on-premises system by allowing these now redundant accounts simply to be turned off. In a traditional on-premises solution, the infrastructure to support the 200 users who are no longer with the firm represent a sunk cost that the organization has paid for, but now cannot use until staffing levels return to the previous level. In short, the use of Office 365 provides greater certainty over costs, both in the short term and the long term.

OTHER CONSIDERATIONS

Office 365 benefits from a robust ecosystem of third-party add-on tools that simplify migration, extend use cases, offer security capabilities, and streamline administration tasks. For many, this will be their first migration to Office 365, and using select third-party tools allows them to capitalize on the thousands of hours of experiences that

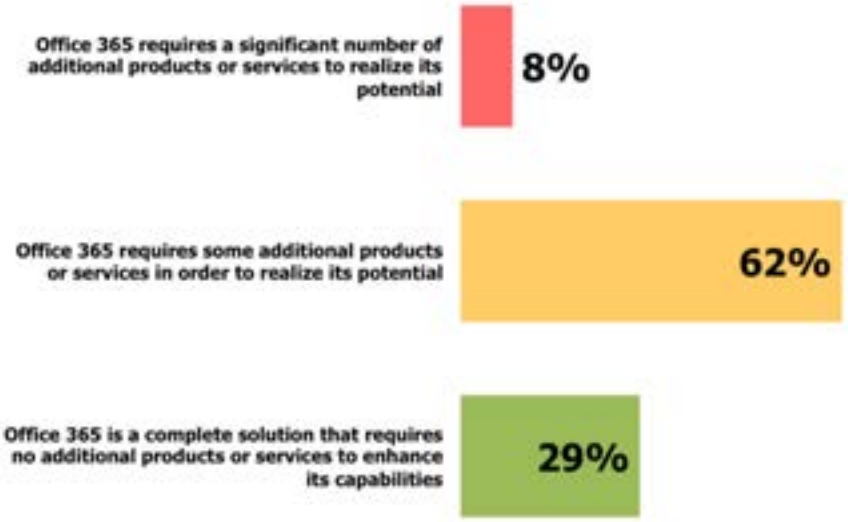
other customers have already gone through: reaping the benefits more quickly, avoiding the pitfalls, and getting to value while mitigating risk. Osterman Research surveys have demonstrated that most current or soon-to-be Office 365-enabled organizations believe they will need third-party solutions to supplement Office 365, as shown in Figure 3.

Figure 3

Views on the Need for Third-Party Solution in Office 365

Among Organizations That Will Deploy Office 365 by 2017

Source: Osterman Research, Inc.



THE DANGERS OF PHISHING, SPEARPHISHING, RANSOMWARE AND CEO FRAUD/BEC

THE THREATS ARE REAL

Osterman Research has found that a wide range of security issues have occurred in mid-sized and large organizations over the past 12 months. As shown in Figure 4, 37 percent of organizations have been the victim of a successful phishing attack that resulted in a malware infection, 24 percent have been the victims of a successful ransomware attack, and 22 percent have had sensitive or confidential information breached through email. In short, at least 75 percent of organizations have been victimized, although this figure may be higher owing to some respondents' reluctance to discuss all of the attacks they have encountered.

Email in Office 365 and Exchange Online includes some basic email security capabilities, but more advanced security requires payment of an additional monthly fee.

Figure 4

Cyber Security Problems That Have Occurred During the Previous 12 Months

Source: Osterman Research, Inc.

Incident	% of Organizations
An email phishing attack was successful	37%
One or more of our endpoints had files encrypted because of a successful ransomware attack	24%
Malware has infiltrated our internal systems, but we are uncertain through which channel	22%
Sensitive / confidential info was accidentally leaked through email	22%
One or more of our systems were successfully infiltrated through a drive-by attack from employee web surfing	21%
An email as part of a CEO Fraud/BEC attack successfully tricked one or more senior executives in our organization	12%
An email spearphishing attack was successful in infecting one or more of our senior executives' systems with malware	10%
Sensitive / confidential info was maliciously leaked through email	7%
Sensitive / confidential info was accidentally or maliciously leaked through a cloud-based tool like Dropbox	6%
Sensitive / confidential info was accidentally or maliciously leaked through a social media / cloud application	2%
Sensitive / confidential info was accidentally or maliciously leaked, but how it happened is uncertain	2%
None of the above has occurred or are aware it has occurred	25%

Even a single, successful cyber attack can be very expensive. For example, between October 2013 and May 2016, the FBI recorded 22,143 fraudulent wire transfers resulting from BEC attacks totaling $3.1 billion in losses. While this represents an average of $140,000 per BEC-related loss, some losses are much greater. For example, in 2015, Ubiquiti Networks reported that it had been the victim of several BEC attacks that resulted in a total loss of $46.7 million .

DOES MOVING EMAIL TO THE CLOUD INCREASE THE RISK?

Does moving to the cloud using a shared-tenant architecture – as is the case with most customers of Office 365, Gmail/G Suite and other cloud offerings – increase the risk of an attack? In one sense, cloud-based email is more secure than its on-premises counterpart because it is managed by a carrier-grade staff on a 24x7 basis, large providers can more easily afford redundant infrastructure, software and security flaws are usually patched more quickly, and so forth. However, a case can be made that cloud-based systems are more of a target for cyber criminals, since a cyber criminal that can penetrate a secure email gateway for one customer of a cloud-based email system can perhaps more easily do so for other customers that rely on the same gateway. Moreover, because the email system that a user employs is easily discoverable via MX record lookup, the more users that are on a particular system, the more attractive that target becomes to attackers.

There have been several examples of account takeovers (ATOs) in the cloud, such as the May 2017 Google ATO that used a Gmail plug-in and a similar March 2016 attack against Dropbox users . However, it is important to note that while a similar attack could occur against Office 365 users, always having the latest, patched version of software (which is more likely in the cloud) is likely to be more secure.

CYBER CRIMINALS ARE SHIFTING THEIR FOCUS

Data breaches have been so numerous, and the number of sellers on the "Dark Web" and in underground hacking forums have been so successful, that stolen credit card numbers, health records and other content are no longer as valuable as they once were. As just a couple of examples, the price of a payment card record in 2016 was $6, down from $25 in 2011 . The cost of a health record on the black market dropped from $75 to $100 in 2015 to just $20 to $50 in 2016 .

In short, cyber criminals have inundated the market with so much stolen data that supply is exceeding demand. The result has been a drop in prices for stolen information. Cyber criminals will need to steal more data in order to generate the same level of revenue as they did in the past, or they will need to change their tactics. We are now seeing a shift in emphasis from stealing information to be sold on the black market, where prices are declining, to stealing information and finances directly from those who own it or manage it. Cyber criminals increasingly use ransomware that will extort money from victims, phishing and spearphishing that will install malware like keyloggers that can enable them to transfer money out of corporate bank accounts, and CEO Fraud/BEC that will trick CFOs and others into making large wire transfers directly into cyber criminals' accounts.

CRIMINAL ORGANIZATIONS ARE WELL FUNDED

Cyber criminal organizations are typically well funded and they have good technical resources to publish new and increasingly more capable variants of their malware. For example, ransomware has evolved from locker-type variants that were the norm just a few years ago to more sophisticated, crypto-based variants like CryptoWall (2014), CTB-Locker (2014), TeslaCrypt (2015), Samas (2016), Locky (2016) and Zepto (2016) and WannyCry (2017).

Add to this the fact that there is a growing number of tools designed to help new cyber criminals with minimal knowledge of IT to become "hobbyist" phishers and ransomware producers. This has resulted in an explosion of ransomware and other exploits coming from a large and growing assortment of amateur cyber criminals, adding to the problem from professional cyber criminal organizations driven by the onset of Ransomware-as-a-Service (RaaS) .

ATTACKS ARE BECOMING MORE SOPHISTICATED

From the early days of crude phishing emails that tried to trick gullible users into clicking on a malicious link or open a malicious attachment, attacks have morphed into sophisticated BEC attacks that can more easily fool users into sending wire transfers, sharing confidential tax information, and the like. These more sophisticated attacks are aided by hackers' infiltration into an organization's network and their learning business processes with the goal of creating successful attacks aimed at specific senior executives. In short, BEC and other forms of attack are going to get worse without the right solutions and processes to protect against them.

A targeted email attack, such as BEC, is designed to bypass an organization's security defenses using sophisticated social engineering techniques that attempt to trick potential victims.

PREVENTING ADVANCED EMAIL ATTACKS IS CRITICAL

A targeted email attack, such as BEC, is designed to bypass an organization's security defenses using sophisticated social engineering techniques that attempt to trick potential victims into sharing sensitive or confidential information. This can occur through a variety of means, such as a bogus sender that spoofs an email address, sends an email using a look-alike domain or attempts to deceive recipients using a valid domain name. However, a bogus sender can also employ an authentic account that has been compromised.

Email is the threat vector of choice because it's so pervasive and such an easy target in most organizations. Cyber criminals' goals include stealing credentials for corporate banking accounts so that funds can be stolen; stealing intellectual property; gaining access to sensitive systems like military databases or other highly valuable content; or simply to gain access to various backend systems to search for information that might be sensitive or confidential. The fundamental goal is to locate, exfiltrate and monetize victims' data and intellectual property without the victim finding out.

Every organization must prevent advanced email attacks because of the enormous issue that spearphishing attacks leveraging identity deception has become. Because attackers have the advantage of stealth, identity deception is a key area on which decision makers must focus. In short, a new paradigm is needed to address the problem.

MANY ARE NOT PERFORMING SUFFICIENT DUE DILIGENCE

One of the problems in addressing advanced email attacks is the lack of due diligence on the part of many organizations. That's not to say that IT managers, security teams, CISOs, CIOs and others are not doing their job – the vast majority are – but they're being overwhelmed by a combination of inadequate security controls and reliance on practices and processes that will not address sophisticated threats that attempt to use deceive recipients. For example:

- Some organizations have insufficient processes and testing in place to address key application and system vulnerabilities.
- Some organizations lack strong internal control processes that will allow them to adequately address zero-day and other threats.
- Many current defense technologies are not sophisticated enough to significantly reduce the level of threats that organizations are experiencing. For example, numerous Osterman Research surveys have found that for many organizations their problems with more advanced threats are actually getting worse over time.
- Finally, the problem with advanced threats can get worse in the cloud.

IMPORTANT ISSUES TO CONSIDER

There are a number of important issues for decision makers to consider as they focus on addressing advanced threats in the context of their current or planned use of Office 365:

No solution can be all things to all customers

While Office 365 is a robust offering that offers a wide range of capabilities offered at attractive price points, it is important to remember that the platform is designed to satisfy the needs of a broad market. Consequently, there will be specific requirements around security, archiving, eDiscovery and compliance that Office 365 will not be able to fully satisfy, necessitating the use of enhanced functionality from third parties.

Office 365 may become a prime target for attackers

By virtue of its large and growing user base (86+ million as of May 2017), the platform may become a prime target for cyber criminals. Since the majority of Office 365 customers are supported using a shared-tenant model, cyber criminals capable of penetrating Office 365 defenses may be able to attack a large number of customers at one time, making the platform a magnet for targeted attacks. That's by no means a knock on Microsoft or Office 365, but merely an acknowledgement that popular platforms draw significant cyber criminal activity.

Office 365 security is fairly solid, but it has some shortcomings
Microsoft has included some robust capabilities in Office 365 from a security perspective, but there are some limitations with regard to:

- Targeted and more advanced threats
- Reporting for response to threats
- Threat intelligence that is not as sophisticated as it could be
- Data loss prevention capabilities
- Delays in its sandboxing capabilities
- The ability for attackers to evade Office 365's sandboxing
- Shortcomings in its URL technologies
- Delays in attachment handling
- Lack of robust detection of deception techniques

Consider the use of third party offerings
Organizations considering Office 365 should seriously consider the use of third party offerings to supplement native Office 365 security capabilities, particularly for security and encryption. Office 365 security is good and its encryption functionality works, but third party offerings combined with it can significantly enhance an organization's security posture.

User training is important, but it will not solve every security problem
Osterman Research strongly recommends that every organization implement a security awareness training program that will make users more aware of phishing attempts, instruct them not to open attachments or click on links unless they are certain of the sender's identity, and so forth. However, security awareness training is not effective for targeted attacks, situations where sophisticated attackers can successfully impersonate valid senders or in situations where users do not have enough information to make an informed decision about the validity of a sender's identity. Instead, organizations need to invest in protection technologies that will prevent users from receiving dangerous emails or that will at least warn them of the danger in the emails they receive. The ideal situation is one in which every targeted attack, as well as less sophisticated ones, are prevented. While security awareness training is important and useful and can significantly reduce poor user behavior, it cannot stop all of it.

THE PROS AND CONS OF VARIOUS APPROACHES FOR SECURING OFFICE 365

There are five basic approaches that an organization can take with regard to securing Office 365:

Retain the existing secure email gateway using a hybrid approach
Even if organizations have migrated some or all of their users to Office 365, they can continue to maintain their existing, secure email gateway to protect whatever assets remain on-premises, as well as their cloud-based users. The modest advantage of this approach is that security is maintained inside the organization perimeter, offering a relatively simply approach to IT and IT security.

Organizations considering Office 365 should seriously consider the use of third party offerings to supplement native Office 365 security capabilities.

However, this approach is not recommended: remote workers are more difficult to secure because many network level defenses are unavailable in "desktop" forms. And, while IT can force the use of VPN and backhaul all traffic through the organization's data center to mitigate some of the risks of this approach, it can introduce additional IT challenges.

Add another cloud-based layer as an initial hop

Another approach to securing Office 365 is to add another cloud service to supplement the native security available in the platform. An important advantage of this approach is that as soon as a cloud security provider makes available mitigations to new threats, their customers are protected immediately. The cloud security provider is high motivated to ensure that no threats get through, hence rapid time-to-mitigation, and organizations don't have to patch or update internal systems before being protected.

However, relying on multiple cloud providers to deliver IT capabilities, and thus having several cloud service-aligned security solutions, can make unified visibility into threats across a collection of disparate cloud services more labor intensive and more prone to risk. Moreover, this approach means that Office 365-enabled organizations are paying double for secure email gateway functionality, since capabilities like spam filtering and anti-malware are already included in Office 365 offerings like Plan E3.

Purchase additional security from Microsoft

An adjunct to the approach above is to supplement the security available in Office 365 with Microsoft's Advanced Threat Protection (ATP), which offers better protection than is available with the Exchange Online Protection (EOP) included in Office 365. ATP provides defenses against more advanced threats, such as real time examination of links that users click in email attachments. ATP is available as an add-on for most Office 365 plans.

However, ATP does not address most BEC or targeted zero-day attacks, leaving organizations vulnerable to these attacks.

Implement training/user awareness programs

Another option is to provide robust security awareness training to users so that they are more likely to spot phishing attempts. However, it is important to note that security awareness training is not a panacea for all security problems, since users can still make mistakes, and some threats (such as WannaCry) are not spread via user interactions.

Fill the gap in email defense

Another approach is to implement another layer of email defense that offers a better way to determine the true identity of a sender and then either block bogus emails or, at a minimum, warn recipients that the sender may be suspect. Using a system that enables more insight into the identity of senders will stop attacks, such as BEC attempts, more effectively than conventional methods. Because sophisticated attacks like BEC attempts will impersonate a trusted sender, are low volume in nature, and often will not carry any sort of malicious payload or a link to a source of malicious content, an email defense layer focused on accurately determining sender identity will be more effective than conventional methods like EOP.

It is important to note that the five options above are not mutually exclusive: organizations can implement multiple approaches to provide the most effective security posture for their organizations. For example, while security awareness training is useful to attune users to the importance of not clicking on attachments or links in phishing attempts, a solution that accurately determines sender identity is needed to prevent BEC attempts and similarly dangerous threats from reaching end users.

BEST PRACTICES AND TECHNIQUES TO CONSIDER

APPRECIATE THE SECURITY RISKS YOU FACE

Every decision maker needs to understand the risks that his or her organization faces from phishing, spearphishing, CEO Fraud/BEC, ransomware and other forms of malware, and address them as a very high priority. While that may seem obvious, many decision makers give mental assent to these problems, but they fail to put that understanding into action by training users appropriately and implementing a sufficiently robust security infrastructure. Cyber crime is an

industry with sophisticated technical expertise, enormous funding, and a rich target environment of potential victims, and it must be dealt with as such. In short, the number of opportunities for successful threat infiltration is increasing and Office 365 represents a new set of security challenges that must be understood.

CONDUCT A COMPLETE AUDIT OF CURRENT SECURITY TOOLS, TRAINING AND PRACTICES

Decision makers should undertake a complete audit of their current cyber security infrastructure, including their security awareness training regimen, the security solutions they have in place, and the processes and practices they have implemented to detect and remediate security incidents. This is a key element in identifying the deficiencies that may (and probably do) exist, and it can be used to prioritize spending to address problems.

ESTABLISH GOOD POLICIES

It is essential to develop thorough and detailed policies for all of the email, web, collaboration, social media, mobile and other solutions that IT departments have deployed, or that users are allowed to employ. As a result, Osterman Research recommends the development of detailed and thorough policies focused on the tools that are used today or probably will be in the future. Policies should focus on legal, regulatory and other obligations to encrypt emails if they contain sensitive or confidential data; monitor all communication for malware that is sent to blogs, social media, and other venues; and control the use of personal devices that access corporate systems that contain business content.

While policies, in and of themselves, will not prevent cyber security threats, they can be useful in limiting the number of solutions that employees use when accessing corporate systems. These limitations, in turn, can be helpful in reducing the number of ingress points for ransomware, other forms of malware, phishing and spearphishing attempts, and other content that might pose a security risk.

IMPLEMENT BEST PRACTICES FOR USER BEHAVIOR

Decision makers should establish a number of best practices to address any cyber security gaps may exist. Some of these might include:

- Employees should use login credentials that match the sensitivity and risk of the corporate assets they are accessing. These passwords should be changed on a schedule to be established by IT.
- Communication “backchannels” should be created for staff members that will be involved with corporate finances or sensitive information. For example, if a CEO asks that his CFO transfer funds to an established supplier, the CFO should have a way of verifying the authenticity of the CEO’s request before initiating the transfer, such as texting or calling the CEO’s smartphone.
- Employees should be reminded and required to keep software and operating systems up-to-date so that application and system vulnerabilities can be addressed in a timely fashion. IT can help through management and enforcement of these updates.

Decision makers should establish a number of best practices to address any cyber security gaps may exist.

- Ensure that every employee maintains good anti-malware defenses on their home computers and personal devices if there is any chance that these devices will be used to access corporate resources, such as corporate email or databases with sensitive corporate information.
- Employees, especially senior executives who are more likely to be the target of a CEO Fraud/BEC attack, should be reminded on a regular basis about the dangers of oversharing information on social media. Employees' friends might be interested in the latest personal information that gets posted on Facebook, for example, but this information can provide cybercriminals with the information they need to create a believable spearphishing email.
- Employees should be tested regularly to determine if their security awareness training has been effective, and to identify those employees that might need additional training.

SHOULD YOU USE A HIGHER-LEVEL OFFICE 365 PLAN OR A LOWER-LEVEL PLAN WITH THIRD-PARTY SECURITY PROTECTION?

As organizations consider the deployment of Office 365, or as they re-evaluate their current Office 365 deployment, there is an important choice to make with regard to advanced security:

- Should you choose the more expensive Enterprise Plan E5 that includes ATP, which provides sandboxing or URL rewriting capabilities at an additional cost (approximately $2.00/user/month), or
- Should you choose the less expensive Enterprise Plan E3 and supplement it with ATP, or
- Should you choose the less expensive Enterprise Plan E3 in conjunction with a third party security solution like Agari Advanced Threat Protection?

To answer that question, Osterman Research evaluated the capabilities and threat coverage, as well as efficacy results of the following platforms:

- Office 365 Enterprise E5
- Office 365 Enterprise E3 with ATP or a leading secure email gateway
- Office 365 Enterprise E3 in conjunction with Agari Advanced Threat Protection

While the higher level Office 365 plan does offer enhanced security and greater protection than lower level plans, Osterman Research recommends for the vast majority of organizations that they implement a lower level plan, but supplement it with a more capable, third party security offering.

Figure 5

Comparison of Office 365 + ATP vs. Office 365 + Agari

▲ Full coverage/support

△ Partial coverage/support

Source: Osterman Research, Inc.

Threat	Office 365 E5	Office 365 E3 + ATP or SEG	Office 365 E3 + Agari
Spam	▲	▲	▲
Malware	▲	▲	▲
Spoof	△	△	▲
CEO Fraud/BEC			▲
Cost of ownership	Highest	13% less	31% less

We believe that deploying a solution focused on thwarting sophisticated attacks on top of the native functionality that Microsoft already provides in Office 365 is a best practice because it will reduce overall risk and protect against the advanced threats that Office 365 does not adequately address, particularly those threats relying on identity deception.

SUMMARY

The deployment of Office 365 is growing by leaps and bounds, and for good reason: Microsoft offers a robust set of communication and collaboration tools in a reasonably priced array of offerings, enabling lower total cost of ownership for organizations of all sizes compared to traditional, on-premises solutions. However, the security in Office 365 cannot address all threats as well as some third-party solutions, and so the use of a less expensive Office 365 plan in conjunction with a more robust third-party security solution can typically offer the highest level of security and the lowest total cost of ownership.

ABOUT AGARI

Agari is the best line of defense against identity deception--the common thread enabling today's most costly and damaging email attacks—including ransomware, spear phishing, and business email compromise. While other security companies focus on securing networks, applications, and data by searching for malicious content, Agari focuses on defending against attacks on the most vulnerable part of your network: human perception. Drawing on visibility into more than 10 billion legitimate messages each day and 70% of global inboxes, Agari is constantly perfecting its artificial intelligence engines that model what authentic, trustworthy communications look like. With no user intervention or training required, Agari blocks attempts at digital deception at massive scale and speed. No other security solution is able to do what Agari does, and our solution only gets smarter every day.

Agari is trusted by leading Fortune 1000 companies—including 6 of the top 10 banks and 5 of the world's leading social media networks—as well as government agencies, to protect their organizations, partners, customers, and constituents from advanced email attacks.

AGARI SOLUTION FOR OFFICE 365

Designed specifically to elevate advanced security controls while preserving operational benefits of Microsoft Office 365, Agari provides simple, seamless, and secure protection for Office 365 email environments. Integrating via a secure APIs, Agari is far more cost effective than deploying a largely redundant second-layer gateway. More importantly, Agari is a superior choice to sandboxing, URL rewriting, or other content-focused approaches that are constantly one step behind attackers and degrade the user experience.

Benefits of Agari for Office 365:

- **Stops attacks others miss –** Complete protection from advanced email threats, including spearphishing, ransomware, CEO/CFO wire fraud, business email compromise and more.
- **Keeps users and admins productive –** No reliance on rule creation, user training, out of band content analysis, or other productivity drains
- **Easy to deploy –** No software to install, seamless integration with existing infrastructure

For more information, visit: https://www.agari.com/office-365/

REFERENCES

https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm

http://www.businessinsider.com/google-doc-phishing-worm-affected-fewer-than-01-of-gmail-users-2017-5

http://www.mailguard.com.au/blog/dropbox-scam-new-phishing-attack

Source: Intel Security as noted in the Verizon 2016 Data Breach Investigation Report

http://www.healthcareitnews.com/news/cybercriminals-poised-launch-more-ransomware-attacks-black-market-price-health-data-drops

https://www.enterprisetimes.co.uk/2016/05/20/clever-cerber-ransomware-attack-spotted/