Email Security: Never more important

In this e-guide

In this e-guide:

Email security remains as important as ever, with the majority of cyber-attacks, including ransomware attacks, still being launched through email using a combination of social engineering, phishing, malicious links and weaponised email attachments.

Email remains the easiest and most effective channel of attack with the number of emails being sent on a daily basis expected to surpass 293 billion by the end of 2019. Despite this, email is the weakest link in most organisations' security strategies, with many failing to address vulnerabilities in popular email platforms such as Office 365.

With the reliance on email and associated threats likely to continue to grow, businesses need to address this threat with a combination of security awareness training and automated tools to reduce the likelihood of infection and speed up the detection of and response to email borne threats. Underlining the importance of email security, it is a core component of the

In this e-guide

UK National Cyber Security Centre's Active Cyber Defence (ACD) initiative.

Warwick Ashford, security editor

In this e-guide

How IT pros are building resilience against email security threats

Nicholas Fearn, guest contributor

Over the past few decades, emails have played an integral role in daily business communication. Whether it is communicating with co-workers and customers, sending marketing campaigns, scheduling meetings or receiving newsletters, they are a useful tool for everyone.

Research from Radicati Group shows that the number of emails sent and received each day will surpass 293 billion by the end of 2019, before reaching 347 billion in 2023. And according to a survey by HubSpot, 86% of professionals say email is their preferred way to communicate for business purposes.

But while the trusty email will no doubt continue to be commonplace in the business world, it has become a core target for hackers. Security threats such as malware, spam, phishing, social engineering and unauthorised access are causing major concern for organisations and IT leaders.

In research compiled by Barracuda Networks, 94% of organisations admitted that email is the most vulnerable part of their enterprise security strategies and

In this e-guide

87% of CIOs expect to see an increase in email security threats over the next 12 months. Business email compromises are particularly damaging, with the US Internet Crime Complaint Center reporting $1.3bn of losses, further underlining the importance for organisations of building resilience against email-borne attacks.

For cyber criminals, email is often an easy way to infiltrate organisations, launch devastating attacks and gain hold of sensitive business information. Paul Rose, chief information security officer at managed service provider Six Degrees, says hackers are increasingly turning to it as their preferred attack vector.

"Not only are email-based cyber-attacks often highly successful, but they can also be deceptively simple," he says. "Targeted attacks against either an entire company – commonly known as phishing – or key persons within that company – spear phishing – can result in significant data breaches or loss of systems and services, whether they utilise malware payloads, social engineering or both."

Rose argues that reducing the risk of a successful attack should include both technology and human considerations. "Effective technology-based security controls such as secure email gateways, attachment scanning and antivirus software are all well and good," he says.

"However, these need to be supported by appropriate people and process controls, including frequent employee training and awareness. As cyber criminals use ever more sophisticated techniques to catch us out, the frequency

of activities designed to raise awareness of these techniques needs to increase in response."

But Rose says awareness should not end at simple PowerPoint presentations and e-learning courses with exams at the end. "Today's enterprises should be exploring the use of internal resources or third parties to carry out phishing simulations across sections of their company," he says. "Continual training and 'real world' testing is essential if the threat from email attacks is to be mitigated in the short, medium and long term."

Chris Ross, senior vice-president at Barracuda Networks, says emails are the weakest security link. "A not insignificant 32% identified customer support as their most attacked department in what could indicate a new emerging trend for would-be attackers," he says. "Brand impersonation also makes up the majority (80%) of email attacks, according to our research earlier this year.

"Without proper employee training, these attacks will continue to succeed. However, training is still hugely lacking across most enterprises we spoke to, with 'once a year' being the most popular response (29%) in terms of how often it is being given. Shockingly, an additional 7% said they either never had training or were not sure."

In this e-guide

Growing threats

As the connected ecosystem continues to expand and people become more reliant on their devices, email threats are likely to grow. Ashley Hurst, international head of tech, media and comms at law firm Osborne Clarke, says there are ever-more convincing phishing attacks in particular.

"Gone are the days of loads of spelling mistakes and obviously fake email addresses," he says. "As people spend more and more time on their mobiles, the fakes can be difficult to spot, despite much more prevalent phishing attack training."

But for Hurst, perhaps even more alarming is what the attackers do once they get a hold of someone's username and password. "We have seen numerous cyber attacks where a single compromised username and password has been used to get into a computer system that has not been updated to use two-factor authentication," he says.

"Once in, the attackers set up email forwarding rules and then review emails, waiting for the opportune moment to change the details on a payment request to divert funds. It can be weeks before the company notices."

Hurst's view is that the answer to these threats is only partly educational. "Companies must continue to refresh cyber security training regularly, particularly around email threats," he says. "But most important is to ensure that

the correct settings are applied to software and that software is updated regularly.

"Small and medium-sized companies with tight IT budgets are particularly at risk and more senior and high-profile individuals tend to be easier targets, particularly if they are vocal about their activities on social media. Every medium to large company needs to have a plan to deal with incidents quickly, even if it is simply knowing which experts to call.

"It is astonishing how many substantial companies still don't have effective incident response plans in place, despite all the news about cyber-attacks."

Increasing sophistication

Although education and training can significantly reduce email breaches, the problem is that hackers are constantly finding more sophisticated techniques to target victims. Lewis Henderson, vice-president of threat intelligence at Glasswall Solutions, believes attackers are using techniques that users simply cannot spot.

"Our threat intelligence data is informing us that evasive threats have no malicious payload, and now dominate the top risks so far this year," he says. "We find that most attacks are unique events that are beyond human abilities to detect and prevent, CISOs are forced into a weaker reactive position while

attempting to contain malicious needles in a haystack. It is a challenging scenario to win.

"Example scenario: a supply chain partner is compromised, the malicious actor uses a DDE [dynamic data exchange] or Power Query technique within Microsoft Excel, evades every defence, and an unsuspecting user sees nothing suspicious while the breach is occurring. These are the types of threat where training on its own simply can't help."

Instead of being lost in the noise, Henderson says technology needs to be an enabler for CIOs and CISOs to have a dialogue with the business about file-based threats. "Threat intelligence strengthens their position to push for a change of policy and culture, and this should also influence their decision on which technology can disarm malicious files and attachments of their associated risks," he says.

Neil Thacker, chief information security officer of cloud security firm Netskope, agrees that email threats are growing in sophistication and that organisations need to take a more robust approach to mitigate them. He says effective mitigation needs to come from a comprehensive strategy that covers both education and email and web protection.

"For many years, CISOs have been advising employees not to click on suspicious links," he says. "While phishing simulation exercises do generate

awareness, the simulation exercises are not considered a strategic control that has radically changed behaviour and therefore reduced the threats."

Thacker says phishing for credentials or manipulation of employees are the key objectives for attackers. "However, the attackers have had to mature their processes to ensure they remain covert," he adds. "One example is sending an email with a link followed by activating the malicious payload once the email has been delivered.

"This time-based attack is a common bypass technique that allows for the attack to remain undetected by email security controls. The control in this scenario is therefore better placed at the web inspection layer that inspects links at the point-in-time when the link is clicked on."

Attackers are also exploiting trusted sites and popular cloud applications to host malicious payloads typically trusted by employees, says Thacker. "An email with a link from these locations is typically both trusted by the email security control and therefore also the employee," he says.

"New techniques therefore require a more focused and pervasive approach. Using real email and web security metrics showcasing particularly poor responses to these attacks at department level can be used to educate employees. Running a catch-of-the-day programme, where employees are incentivised to report suspicious emails, is also a good step to help promote and raise awareness on good email security."

Taking action

Steven Furnell, senior IEEE member and professor of information security at Plymouth University, says one of the biggest challenges at present is business email compromise. "This is when an attacker impersonates a senior executive and attempts to fool an employee or other recipient into sending funds or sensitive information, with the legitimate email account having previously been compromised via social engineering or direct intrusion," he says.

To mitigate such threats, Furnell says organisations need to improve awareness among their employees. "The issue of employee education is key in tackling the threat, because it requires message recipients to be aware enough to stop and think about what they are being asked to do, and to double-check that requests are valid, particularly where sensitive data or high-value transactions are involved," he says.

Furnell recommends that employees ask themselves whether an email request seems legitimate and usual; what the value is of the information they are being asked to provide or the task that they are being asked to perform; whether they are confident that the source of the request is genuine; and whether they have to respond right away.

Another increasing threat is ransomware, which is often distributed via email. Avi Raichel, CIO at resilience platform provider Zerto, says: "Attackers can often worm their way in through employee emails, so having the right cyber defences

is key in avoiding a catastrophic situation where customer data, and a whole lot of money, could be at stake.

"Having an extensive tiered security model as well as appropriate role-based access control can help minimise risk. But the attack itself is only half the problem. Without sufficient recovery tools, the outage of the attack will cause loss of data and money, as well as reputational harm and downtime for customers."

Raichel says businesses need to implement tools that enable them to roll back all their systems to a point in time just before an attack. "It works like this: you see the ransomware email, and shut down any impacted computers, servers, and so on," he says.

"You then use a recovery tool to simply roll all of the systems back in time, which takes minutes rather than days, to a point before the company was infected with ransomware. This level of disaster recovery is critical. Emails continue to be at the centre of businesses, they are vulnerable and, inevitably, a standing target for ever-sophisticated cyber criminals."

Emails are a communication standard for most of us in the workplace, but the reality is, security threats often go amiss. A big part of changing this is educating employees about the risks and how they can be mitigated, but organisations also need to ensure they have the systems in place to identify and respond to these ever-growing attacks.

In this e-guide

Email security as important as ever, report shows

Warwick Ashford, security editor

The majority (74%) of businesses that took part in a survey say email-borne cyber attacks are having a major impact and 78% said the cost of email breaches is increasing.

On average, 82% of organisations claim to have faced an attempted email-based security threat in the past year, although the figures differ slightly by global region.

The most common effects cited were loss of employee productivity, downtime and business disruption, recovery costs, loss of data, financial impact, and damage to the reputation of the IT team, according to the *2019 Email security trends report* by Barracuda.

The report, based on a survey of 660 IT security professionals globally at small, medium and large enterprises in a wide range of industry sectors, indicates that although most (63%) IT professionals are more confident about their email security systems than they were a year ago, email attacks continue to have a significant impact on businesses.

In this e-guide

A top concern is widespread phishing, particularly spear phishing, with 43% of organisations reporting spear phishing attacks in the past 12 months.

Asked about the impact of spear phishing attacks, 43% of respondents said machines had been infected with malware, 33% reported stolen credentials, 20% reported monetary loss and 17% said sensitive or confidential data had been stolen.

Ransomware is another top concern because ransomware attacks that encrypt critical business data and demand payment in return for a decryption key are often sent to individuals in organisations by email.

A recent report by security firm SonicWall indicated a resurgence of ransomware around the world in the first half of 2019, attributed in part to the emergence of ransomware as a service (RaaS) providers in hacker forums.

Other email-borne threats that businesses are worried about include malware, viruses, data loss, spam, smishing, email account takeover and vishing. Only 7% of organisations polled said they are not worried about any of these risks.

Breach costs and monetary losses are on the rise, the report shows, with 78% of organisations saying the financial impact of email breaches is increasing dramatically due to costs associated with identifying and remediating threats, communicating with those affected, business interruptions, and productivity losses.

In this e-guide

As a result, 66% of organisations claimed that attacks have had a direct monetary cost to their organisation in the past year, with nearly a quarter saying attacks have cost $100,000 (£80,400) or more.

While 88% of respondents said their organisations had virus and malware filters in place and 85% said they had spam filters, only 68% said they had email authentication measures in place, and 55% said they had security training. Fewer still had sandboxing technology (29%), automated incident response (25%), spear phishing protection (23%) and account takeover protection (22%).

Spending on email security is a positive sign, the report said, underscoring the fact that organisations understand the seriousness of current threats. The survey shows 48% of organisations are spending more than last year, 45% are spending the same, and only 7% are spending less.

The increased investment in email security tools reflects the growing sophistication of the attacks and the need to protect against potential damage from evolving threats, said the report.

However, the report noted that organisations are underinvesting in tools designed to protect email beyond the traditional security gateway, such as automated incident response, spear phishing protection and tools to prevent account takeover.

In this e-guide

Only 4% of respondents rated their organisation's remediation capabilities to address malicious emails as "excellent", while 58% said their organisation was "very good" but could do better, 35% said its capabilites were "acceptable" but miss some advanced attacks, and 3% said their organisation's capabilties were "inadequate" and most attacks were missed.

The amount of time spent investigating and remediating attacks is also cause for alarm, the report said, with 55% of firms admitting they take more than an hour to do so.

"A delayed incident response could be enough time for hackers to infect an entire organisation with ransomware or steal sensitive data," said the report. "Organisations increasingly need automated incident response to cut through complexity, accelerate time-to-detection and free up stretched and stressed security staff."

Based on the success and proliferation of email-based attacks, the report said IT security professionals will need to stay focused on the evolution and escalation of phishing, ransomware and other threats and improve email security that goes beyond the traditional gateway.

Next Article

In this e-guide

Email still top security vulnerability, survey shows

Warwick Ashford, security editor

Despite email being used since the 1990s and a high level of awareness of the associated risks, 94% of organisations surveyed admit that it is still the top security vulnerability.

At the same time, email threats are expected to increase in the coming year, according to 87% of the 280 decision-makers in Europe, the Middle East and Africa polled by security firm Barracuda, with 75% reporting a steady increase in email attacks in the past three years.

Almost half (47%) of respondents said they had been hit by email-borne ransomware attacks, 31% were victims of a business email compromise attack, but the majority (75%) said they had been hit by brand impersonation attacks, also known as brandjacking.

The high proportion of brand impersonation attacks, the researchers said, supports the findings of a recent Barracuda report on spear phishing, which found that 83% of all the email attacks analysed focused on brand impersonation.

Finance departments are the most targeted by email-borne cyber-attacks, according to 57% of respondents. However, 32% said customer support was their most attacked department, which could indicate a new trend for would-be attackers, according to researchers at Barracuda.

"Without proper employee training, these attacks will continue to succeed," the researchers said in a blog post, noting that training was still hugely lacking across most organisations surveyed.

The largest group (29%) said they received security training only once a year, while 7% said they had either never had training or that they weren't sure.

The lack of regular, in-depth security training, the researchers said, is leaving employees either confused or unaware of security protocols, with 56% of respondents stating that some employees do not adhere to security policies, and 40% of those saying their employees used "workarounds".

Despite these findings, the researchers said there were indications that some organisations are taking measures to reduce email threats, even among the 62% of organisations that expect their security budgets to either remain the same or decrease.

Just over a third (36%) of respondents, for example, said they were implementing instant messaging applications such as Slack or Yammer to reduce email traffic. However, the researchers warned that while they have not

seen attacks using messaging platforms such as Slack, this may well change in the future.

“Any organisation going down this route should do so with care, as if we know anything about cyber attackers, it’s that they’re always trying new ways to catch their victims out,” they said.

While a shift away from email to communications tools such as Slack might be tempting in the short term, the researchers said it may not be an effective tactic in the longer term because attackers are likely to change tactics in response to that shift.

“In the longer term, the right combination of technology and security awareness training is the key to email attack protection,” they said.

Next Article

In this e-guide

In this e-guide

UK government organisations' email security lagging

Warwick Ashford, security editor

Only 28% of gov.uk domains have been proactive in implementing the Domain-based Message Authentication, Reporting and Conformance (Dmarc) protocol, a study has revealed.

This finding is in sharp contrast to central government departments, where the majority have implemented Dmarc, according to the National Cyber Security Centre (NCSC).

Dmarc is a key component of the NCSC's Active Cyber Defence (ACD) initiative, which aims to protect the UK from high-volume commodity attacks.

Once enabled, Dmarc provides an email validation system designed to detect and prevent email spoofing, ensuring that email senders and recipients can better determine whether or not a given message is from a legitimate sender. If an email is from an untrusted source, and Dmarc is fully enabled, administrators can decide whether the email should be placed in quarantine or rejected.

Attackers sending fake emails purporting to be from the government has been one of the biggest problems in UK cyber security, according to the NCSC. But

much of it is preventable by adopting the Dmarc protocol because it helps authenticate an organisation's communications as genuine by blocking emails pretending to be from government.

Dmarc is also an effective tool for preventing domain impersonation attacks, which are the most common and most harmful kind of phishing attacks.

Lack of preparation leaves door open for phishing attacks

The UK Government Digital Service (GDS) issued guidance advising government organisations to implement the Dmarc email authentication and reporting protocol in preparation for the retirement of the Government Secure Intranet (GSI) platform in March 2019.

The GSI has enabled government organisations to communicate securely at low protective levels since 1996, but just weeks before its retirement less than a third of gov.uk domains have enabled Dmarc themselves ahead of the deadline, according to analysis of more than 2,000 email domains by data security company Egress.

This means that nearly three-quarters are not following the minimum standard requirements suggested by GDS to authenticate email messages.

This highlights a lack of preparation by the majority of email administrators at government organisations in readying themselves for the domain migration, which, in effect, leaves domain users open to phishing attacks.

The number of public sector organisations that have not yet set up Dmarc to assure their email network's ability to withstand phishing attacks is "quite startling" according to Neil Larkins, chief technology officer at Egress.

"With only weeks left before the GSI framework is retired, it's critical that organisations heed the advice laid out by GDS," he said.

Further analysis by Egress revealed that of the 28% of government organisations that have set up Dmarc, 53% have the policy set to "do nothing". This means email buffering and business email compromise (BEC) cannot be prevented for these domains, and spam and phishing messages go straight into the recipient's inbox, regardless of whether the message has been sent from a trusted sender or not.

Any organisation using a default gov.uk Dmarc setting will also not be taking advantage of the "reject email" policy, said Egress. This means less than 14% of organisations are using Dmarc effectively if they want to stop phishing attacks, according to Egress.

Central government shores up email defences effectively

In central government, however, Dmarc has been implemented by the majority of departments, according to the NCSC.

"Our world-leading ACD programme was launched two years ago, but 89% of central government departments have already implemented Dmarc and 95%

are using the NCSC's Mail Check service," an NCSC spokesperson told Computer Weekly.

The NCSC's approach has been to focus on the primary domains of central government departments which are the most valuable to phishers, the spokesperson said, adding that gov.uk domains using Mail Check were much more likely to reach a Dmarc policy of "reject" or "quarantine" (blocking) to protect recipients from spoofed email from domains.

The Mail Check service, which is also part of the ACD programme, works by assessing an email server's configuration and providing guidance on the implementation of various email security protocols, most notably Dmarc.

Government departments with Dmarc that are using Mail Check are blocking 35% more spoofed emails than those not using Mail Check to achieve a more secure Dmarc configuration, according to an NCSC blog post.

"The ACD programme intends to increase our cyber adversaries' risk and reduces their return on investment, and it is for organisations to understand their own risk and act accordingly," said the NCSC spokesperson.

"We are proud that Dmarc is available to organisations and believe our unique bold and interventionalist approach is making the UK an unattractive target to criminals or nation states."

A quarter of phishing emails bypass Office 365 security

Warwick Ashford, security editor

A quarter of phishing emails bypass default Office 365 security, an analysis of more than 52 million emails across nine industry sectors by enterprise cloud-native security firm Avanan reveals.

That proportion is expected to increase as attackers design new obfuscation methods that take advantage of zero-day vulnerabilities on the Office 365 and other cloud-based office software platforms, according to the *Global phish report*.

The report notes that phishing attacks have become the most widespread email threat to organisations around the world, with attacks keeping pace with security controls, evolving to evade detection.

"For most organisations, phishing is the number one email security threat, outranking both malware and ransomware," the report said, highlighting the finding that one in every 99 emails is a phishing attack.

"Cloud-based email, despite all of its benefits, has unfortunately launched a new era of phishing attacks," said Yoav Nathaniel, lead security analyst at Avanan.

"The nature of the cloud provides more vectors for hackers and gives them broader access to critical data when a phishing attack is successful.

"Organisations are in desperate need for more information on phishing attacks and how to combat these attacks. We conducted this research to help inform organisations and shed light on how to keep sophisticated attacks out of their environment," he said.

In their analysis of emails sent to Office 365, Avanan researchers scanned every email after the default security, enabling them to see the phishing attacks that were caught as well as those that were missed.

Whitelisting emails

The analysis shows that while 49% of phishing emails were marked as spam by Office 365 Exchange Online Protection (EOP) and 20.7% were identified correctly as phishing emails, 25% were marked as clean and 5.3% were not blocked due to admin configurations set up by the organisation that inadvertently whitelist emails that would otherwise get blocked, meaning that 30.3% of phishing emails were delivered.

According to the researchers, obfuscation methods are the most advanced phishing attacks, leveraging specific vulnerabilities in Office 365 security layers.

"Hackers obfuscate the URL [uniform resource locator], making it unrecognisable to Office 365 security, which fails to blacklist the malicious

content," the report said, which means attackers can use URLs that are even known to be malicious.

"And because EOP and Advanced Threat Protection (ATP) use the same first layer of email body parsing (though ATP has a unique attachment parser), all email body obfuscation methods we tested effectively bypassed both security layers of Office 365," the report said.

Obfuscation methods have been used in some of the most notable attacks in the past year, the reports said, with researchers uncovering several high-profile obfuscation methods. Most notably, the BaseStriker attack, which used <base> tags in the html of the email to split links into multiple parts, making them unrecognisable to Microsoft Safe Links.

Most recently, the report said the NoRelationship attack bypassed Proofpoint and EOP by removing malicious links from the relationship file to confuse link parsers, which scan Office documents like PowerPoint ,Word, and Excel.

An analysis of 55.5 million emails, including 3.1 million sent to organisations using G-suite revealed that attackers use four main approaches.

The top objective is to lure recipients into launching malware on their systems (50.7%), followed by credential harvesting (40.9%), extortion (8%) and spear phishing (0.4%).

In this e-guide

Malicious content

Malware attacks often bypass traditional malware scans because the email itself is not malicious, but contains a link that triggers a download of malicious content or has a malicious attachment.

Credential harvesting attacks are typically designed to lure the victim into divulging personal information that grants access to corporate and online accounts or personal finances.

Usually, credential harvesting attacks impersonate trusted brands to trick the recipient into entering their username and password in a spoofed login page. With these credentials, hackers take over the victim's account or sell the information on the black market.

Although spear phishing is far less common than the other three vectors, the report said it often has the largest impact because these attacks typically target high-level employees who have access to either company finances or other sensitive information.

The report notes that these phishing attacks can also be the most difficult to detect, given the lack of attachments or links that can be flagged by anti-phishing tools.

"They rely on social engineering, rather than technical bypass methods, to deceive targets into surrendering a wealth of information," the report said.

Approached for comment, a Microsoft spokesperson said: "Contrary to Avanan's marketing claims, Office 365 uses a multi-layered filtering solution to detect and combat phishing attacks."

In a September 2018 blog post, company representative Debraj Ghosh said that since launching Office 365 Exchange Online Protection (EOP) and Advanced Threat Protection (ATP), Microsoft has continuously made significant enhancements across anti-phish capabilities, reporting, and effectiveness in malware and phish catch.

"To this end, we have reported a >99.9% average malware catch rate, and the lowest miss rate of phish emails reported amongst other security vendors for Office 365."

The blog post also notes that often third-party testing is incomplete in its assessment of the full end to end service.

"These tests at times can provide guidance on the performance of a particular service and how it compares with peers. However, there are often gaps in the testing that can misconstrue results," the blog post reads.

The blog cited the main gaps from third-party testing as: how to count a "miss", misconfiguring the solution, and the fact that third-party testing does not measure many aspects of the email security stack.

In this e-guide

How to beef up Office 365 email security features

Kevin Tolly, guest contributor

Microsoft Office 365, the company's subscription-based services product suite, is king of the hill in the cloud-based email systems market. And while Office 365's full-service product line includes security components, there is no such thing as too much security. That's an important consideration because some security functions, such as advanced persistent threat (APT) protection, are only provided in more expensive subscription tiers. The fact that some security features are extra-cost options opens the door to other vendors' offerings engineered to augment Office 365 email security.

Core Office 365 services span the gamut

While many people think of Office 365 as email, it offers much more than that. Microsoft's Outlook Web Access was once considered only a browser-based email access tool but now it is a feature-rich, collaborative environment that has been extended to provide access to Microsoft Office applications.

In this e-guide

The Office 365 services you use will necessarily influence the security features you need -- whether from Microsoft or from a third-party vendor -- so a brief overview of the services is in order.

In addition to email, Office 365 includes SharePoint, OneDrive and Skype for Business. SharePoint is a content management system and collaborative web application launched more than 18 years ago. It can be used for simple, team-based web applications and documents as well as for more complex, custom-developed applications. OneDrive is a file hosting and syncing service similar to Google Drive, Dropbox and others. Skype for Business, formerly known as Lync, provides instant messaging, as well as VoIP gateway features and functions. Each one has its own security requirements. Let's examine security options for email. A future article will address protection alternatives for SharePoint, OneDrive and Skype for Business.

Office 365 email protection options

Email security is a given. For years, that largely meant reducing junk mail and keeping out viruses -- both spam and malware. While both issues remain important, features designed to combat phishing are arguably the most important elements of Office 365 email security today.

Microsoft bundles its anti-phishing and zero-day malware support as part of its Office 365 Advanced Threat Protection add-on. While it might seem simplest to

license Microsoft's anti-threat protection, it's fairly easy to implement alternative, third-party anti-phishing options.

For example, to use a third-party secure email gateway instead of -- or in addition to -- Microsoft's offering, configure email domain name system entries to point email at the third-party gateway. That gateway, in turn, is configured to forward acceptable email to the Microsoft Office 365 system for delivery to the user's inbox.

Many options exist for Office 365 email security. Along with long-time security vendors such as Symantec and McAfee, newer entrants such as Proofpoint and Mimecast market products with similar capabilities.

Choosing the right gateway

Email gateways differ from each other much more than other types of network infrastructure. Where one LAN switch will do the same job as another -- maybe faster, maybe cheaper -- that's not the case with email gateways.

Spot-checks conducted by The Tolly Group have revealed gateways so porous that they have allowed basic viruses and days-old phishing attacks to pass through unrecognized.

Complicating the situation is that it's difficult to pin down the features offered by various gateway vendors. If they want your business and you are a big enough

customer, they should be willing to provide details revealing how they deliver the accuracy they claim to have.

With email gateways, take nothing for granted. Make sure your vendor knows you will monitor advancements in the art of threat protection, and they should not assume you will remain a customer forever.

Data loss protection

While users generally focus on what's coming into the inbox, let's not forget security threats related to outbound mail. Malware isn't the only way to compromise your data. A disgruntled sales rep planning to leave the company might use email to send a confidential customer list from his corporate account to a private account, for example.

Data loss protection (or prevention, a term favored by some vendors) is an important email security consideration. Assess gateway security products that have the capability to apply company policies to external emails to ensure they don't have any customer or personally identifiable information. This will help ensure your corporate system isn't a conduit for unauthorized or confidential information.

The bottom line on Office 365 email security: Once you decide on your security product, don't just cross it off of your to-do list. Attackers are forever busy and you need to be ever vigilant.

In this e-guide

What are the most important email security protocols?

Peter Loshin, guest contributor

Not long after the first internet email protocols were developed, computer scientist Andrew S. Tanenbaum wrote, "The nice thing about standards is that you have so many to choose from."

He wasn't wrong. Although the original internet application protocols rarely addressed security, there are now many choices for email security protocols.

Basic, unsecure email depends on just a handful of protocols:

- The Simple Mail Transfer Protocol (SMTP) specifies how messages are transmitted.
- The Internet Message Format, or Request For Comments 5322, and Multipurpose Internet Mail Extension (MIME) specifications determine how messages are to be formatted.
- The Internet Message Access Protocol, or IMAP4, and the Post Office Protocol, or POP3, specify how email clients retrieve messages from SMTP servers.

With the dominance of webmail, however, email exchanges between servers and users are now almost universally accomplished using web browsers. Most

of those exchanges can be encrypted while they are in transit using the HTTPS protocol.

Securing email requires more than just encrypting data in motion, however. Protocols for encrypting email messages are just the beginning. Email security encompasses the exchange of messages and other data between email servers, as well as providing mechanisms for preventing email domain spoofing, authenticating that messages have been sent from valid domains and encrypting transactions between email servers that are forwarding email for delivery.

Message encryption

Encrypting transmissions between clients and servers provides some degree of privacy as the message is in transit. However, the only way to be sure that the body of an email message remains private until it is decrypted by its intended recipient is to encrypt it. Encryption protocols include the following:

- HTTPS uses Transport Layer Security (TLS) to encrypt streams of network traffic between clients and servers. It is not invoked directly in email, but is used for web traffic and thus is used to encrypt webmail messages. SMTP Secure (SMTPS) works like HTTPS for SMTP, and uses TLS to encrypt message exchanges between clients and servers. However, encrypted TLS traffic is decrypted at its destination, so cleartext messages may be accessible on email servers as messages are routed unless some other encryption protocol like STARTTLS is in use.

- STARTTLS is a service extension for SMTP that supports opportunistic encryption between mail servers and clients. When the STARTTLS extension is in use, communicating mail systems negotiate the use of encryption and authentication algorithms to protect exchanges. All message content, as well as message metadata, can be encrypted. However, once the transmissions are received, the data will be decrypted.
- S/MIME (Secure/MIME) is the standard that defines how to encrypt and authenticate MIME-formatted data. While S/MIME content can be encrypted, the email headers are not, so an attacker would be able to see who is sending the message and who the intended recipient is.
- OpenPGP is a standard for encryption and authentication of data, including email messages, based on the Pretty Good Privacy framework. OpenPGP is interoperable with S/MIME, and while data can be protected, the metadata around encrypted messages is not.

The primary use of these email security protocols is to encrypt messages and prevent attackers from gaining access to the information in the messages, but there is more to email security than encryption.

Email infrastructure security protocols

One of the most important email security challenges is keeping spam, phishing attempts and other malicious email out of users' inboxes. These email security protocols support efforts to reduce spam by using domain authentication:

- The SMTP Mail Transfer Agent Strict Transport Security protocol helps secure the email environment by enabling SMTP servers to add

encryption via TLS. It also gives enterprises a mechanism to enable servers to refuse to connect with other servers that do not offer TLS connections with a trusted certificate. By requiring a trusted certificate and rejecting connections from unauthenticated servers, email providers can prevent attackers from using fraudulent domains to send phishing or spam email.

- The Sender Policy Framework (SPF) provides a protocol that enables domain owners to identify which hosts are authorized to use their domain names when sending email and defines how that authorization can be verified. It provides a way for domain owners to announce which IP addresses are authorized to send email on behalf of the domain. It also reduces the likelihood that spam or phishing emails can be sent with that domain spoofed as the source of the messages, though SPF is usually enabled with additional email security protocols that provide stronger assurances that email originated from the proper domain.
- DomainKeys Identified Mail (DKIM) builds on the SPF and enables the entity that owns the signing domain to link itself with a digital signature that authenticates that entity.
- Domain-Based Message Authentication, Reporting & Conformance (DMARC) provides mechanisms for notification and mandating actions when messages fail authentication under SPF and DKIM. While SPF and DKIM can flag messages as being spoofed, DMARC enables domain owners to advertise what actions should be taken when spoofed addresses are detected and for recipients to determine the appropriate response action.

There have been many other email security protocols proposed over the years. For example, the DNS-Based Authentication of Named Entities (DANE) protocol was intended to enable authentication of domains by applications like email.

In this e-guide

However, the internet at large has been very slow to deploy DANE, along with the DNS Security Extensions -- a protocol for signing DNS records -- that DANE relies on.

Commercial or proprietary approaches may address some email security challenges. In fact, much of the DKIM protocol originated at Yahoo Mail as DomainKeys just as TLS is based on the proprietary SSL protocol developed by Netscape to enable encrypted e-commerce. History shows that when a good proprietary security protocol gains traction in the market, it will soon become an open standard.

In this e-guide

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com