Office 365

LAYER BY LAYER: PROTECTING EMAIL FROM ATTACK IN OFFICE 365

Office 365 is the world's most popular office productivity suite, with numbers already soaring well past 100 million users. Yet with the vast amount of data shared via email in the Office 365 Suite, a critical question IT admins should be asking is: How secure is it?

The sophistication and instances of phishing and spear phishing attacks continue to rise, and it's clear that organizations need to be ready to prevent infiltrations from every angle. No single solution can keep you as safe as you need to be. And if you're in a regulated industry, like healthcare or finance, the stakes to maintain data security are even higher.

appriver.com/layer-by-layer

appriver®
a zix company

Office 365

When you buy into the idea of replacing a number of productivity solutions with a single suite –such as Office 365 – there is a clear reduction of cost and increase in efficiency. However, the suite doesn't offer the layered security protection businesses need to safeguard data. While Office 365 comes equipped with native security features that protect data in a number of ways, customers need to look beyond what comes in the box.

This white paper will detail how companies reduce the risk associated with email-based malware attacks in an Office 365 environment by implementing a layered security approach that includes policies and training, filtering and encryption services and security software.

Layer I: Policies & Training

As we know, phishing and spear phishing attackers use a mix of social engineering and spoofed email addresses to obtain information they shouldn't have access to. When these attacks are aimed at a company, hackers could access sensitive data belonging to both employees and customers. As well-known as these types of attacks are, there's a reason they still exist: People fall for them.

A hacker only needs one person to click on their fraudulent link to access credit card, debit card and Social Security numbers, names, addresses, proprietary information and other sensitive data. One of the best defenses against hacks is to implement consistent end user training and implement and enforce policies regarding the handling of email.

Policies

Email policies should be created in a manner that reduces risk of an attack, while addressing your organization's specific challenges and goals. Consider the following basic policies for internal emails:

- Don't send e-mail in HTML format
- Don't send unrequested attachments or hyperlinks
- Don't include or ask for personal information
- Use the full name of the user

One way companies can help users minimize the risk of attack is to require a specific format for how each message is written. This provides an identifying element for users to verify each internal correspondence. If an internal email doesn't follow that format and includes a link, it could serve as a red flag for something suspicious. While it's possible the sender accidentally failed to follow the format, the recipient can quickly call or IM the sender via phone to authenticate and prevent a potential infiltration.

Training

A good place to begin to determine potential vulnerability is to establish a baseline of end user security practices. You can't accurately fix a problem if you can't quantify it. This seems like a no-brainer, however nearly 80% of organizations don't conduct any sort of security testing.

Here are some things to consider when implementing testing and training:

- **Penetration testing:** Sending end users suspicious—yet harmless—emails to gauge whether or not they open them, respond to them or click on imbedded links. Whether conducted by your IT department or through a solution provider, penetration testing is a good way to see how susceptible your organization may be to attacks.
- **Follow-up:** Should an employee improperly interact with an email during penetration testing, it's critical to discuss the exercise as soon as possible and further emphasize best practices.
- **Quizzing:** At random intervals throughout the year, implement mandatory quizzes to test staffers' knowledge of data management best practices. This can help determine how well policies are being followed and guide areas of training improvement.
- **Don't forget phones:** Many hackers are now turning to the phone to lay the groundwork for an attack. They'll often pose as someone within the organization, a customer or outside vendor and convince the employee on the line to open an email they've sent. A phone conversation can build trust that couldn't otherwise be gained by an email alone.

Security policies and training should be reviewed continuously to keep up with the changing threatscape. Consider both to be living documents in constant need of refinement to ensure vulnerability is minimized.

Layer II: Filtering and Encryption Services

The second layer of securing email in an Office 365 environment is implementing cloud-based filtering and encryption services. Policies and training can reduce the possibility of a phishing or spear phishing attack, but the risk is never eliminated. Humans make mistakes and hackers are devising more sophisticated and unexpected ways to gain access to networks. Here's what you should know about selecting point-to-point encryption and spam and web filtering solutions.

Point-to-Point Encryption

Encryption is critical to a layered security approach because emails may contain sensitive data like Social Security numbers, credit card numbers and proprietary information about the company. Microsoft's offering encrypts emails once it reaches the server, leaving it readable while in transit. To best protect emails, point-to-point encryption—which encrypts the message immediately—is necessary to protect the email throughout the entirety of its lifecycle.

But point-to-point's benefits don't end just with encryption. By clicking on a "send secure" button, the encrypted message will remain in the server, and the recipient will receive a message allowing them to access the email via a secure portal. In short, infected emails are never sent or received.

Advanced point-to-point encryption solutions offer secure recipient experiences in both mobile and desktop offerings, include client

branding on emails to assist recipients in determining the validity/source of the email, and provide true message recall, which allows the sender to "un-send" an email when needed.

Spam and Web Filtering

Office 365 features some spam filtering offerings, but they're often not comprehensive enough to address most organization's needs. The default filtering settings provide potential holes for spam, malware and phishing leaks and increased administrative burdens.

While the settings can be customized, doing so can be time consuming, especially when certain tasks have to be performed by end-users, which disrupts productivity – not good for a suite selling customers on productivity. For many companies, finding a spam filtering service outside of Office 365 is a necessity. Here's what you should be looking for in a spam filtering service:

- Longer spam filter retention (Office 365's spam filtering retention can be expanded to as many as 15 days)
- Greater admin control over group and individual access restrictions
- Easy rule implementation to catch more spam
- Reduction of clutter from known spam sources

Should an email get through with a corrupted link, web filtering, which isn't offered by Office 365, can provide another layer of defense to block malware from infecting your network. When considering a web filter, ensure it performs each of the following tasks:

- Shields your network from a wide range of malware, adware and viruses via email, web download and java script download.
- Continuously monitors outbound traffic and sends real-time notifications if a malicious program is detected.
- Maintains fast browsing experience to maintain productivity.
- Updates thousands of times per day.

When web and spam filtering are both employed in a layered approach, sophisticated attacks can be stopped. Consider the following scenario:

- An email with an embedded link is sent to someone in your organization late at night – when they're not checking email.
- The link points to a clean Dropbox file, which has never been used in a previous attack.
- Because it hasn't been reported by any network monitoring programs your organization uses, the spam filter recognizes it as safe and lets the email through to the intended user.
- At some point between the email being sent and passing through the network's filter, the malware provider changes the endpoint of the link, which leads the business user to malware when clicked.
- The end user gets up in the morning and the now-malicious email is waiting for them in their inbox.

This issue is common and can be combatted with the right web filtering solution. While the spam filter did what it was supposed to do, the hackers "tricked" the system by changing the link. Web filters with downstream monitoring will immediately notice when the link has been changed and redirect the email out of the user's inbox. A layered approach will position your organization to reduce the risk of email-related security issues to its absolute minimum.

Layer III: Security Software

While cloud-based filtering and encryption services can drastically reduce the risk associated with email security, it's important to have the right locally-installed security software to complement your filter – and in some cases serve as a final line of defense. Layered security is important because attacks come in all different forms and no one solution can block them all. For example: An anti-virus solution can block and quarantine infected files brought in via local media, whereas a network firewall cannot. A network firewall is instead intended to block attacks from outside the network. Layered security is the best way to protect businesses from attacks and their own users.

Here are other things you should look for in a locally-installed security software solution:

- Anti-virus protection: This is the most common need. While cloud-based web and spam filters can keep most corrupted emails out, security software adds another layer of defense.
- Content and image control: This can prevent potentially offensive material, which may also contain viruses, from getting through.
- Scalability: As your security needs grow, your software solution should be able to adapt to avoid lapses in security.

Conclusion

Hackers continue to find new ways to infiltrate networks and gain sensitive data via email, so it's more important than ever to have the most comprehensive security platform possible.

Within an Office 365 environment, a layered approach consisting of comprehensive policies and training, cloud-based filtering and encryption services and locally-installed security software – and hardware, depending on your organization's size – will dramatically reduce the risk of an attack. Learn how AppRiver can strengthen your layered security approach.

appriver.com
sales@appriver.com
(866) 223-4645