The DynaSis Education Series for C-Level Executives

Email Security

Threats to your IT network abound, many of them delivered through email. Fortunately, there are cost effective tools available to protect your hardware, software, data, and ultimately, your business.

Effective mail security used to rely on a "hard exterior – soft interior" model, meaning that if you made it tough for hackers to get in, everything from then on would be okay. But in today's world, maintaining a secure perimeter is becoming more and more difficult as every defense we erect is quickly challenged by the ever-advancing technologies of the cyber-criminal. This includes an ever-increasing ability of hackers to create what seem like legitimate safe emails, but are actually very sophisticated "phishing"[1] and "spear-phishing"[2] tools. Because of this, instead of the security model in which we trusted incoming emails from seemingly known sources, the adoption of a new "Zero Trust" model is critical. We also know that use of the cloud in business continues to grow and while the cloud offers greater speed, flexibility, availability, security and mobility, it is important to understand that this usage can also come with loss of the effectiveness of our on premises, office-based security solutions that were designed for the applications you were using five years ago. This includes web-based email. In other words, if you are using web-based email, the security you seek must protect web-based email.

Add to this the fact that our network perimeters are rapidly becoming fuzzy as our employees become more and more dependent on the cloud from both business-operational and personal perspectives. Your business probably has a significant number of employees – maybe even you – who use both personal and company-owned devices, both in and out of the office, so you can begin to see how the "hard exterior" in a mobile world can be riddled with holes by accomplished professional thieves.

When you think about the growing number of high-profile security breaches, many of which were initiated through email phishing[1] and spear-phishing[2] schemes, you begin to understand the need to pair current technology with current security. The need is so real that in addition to a CIO (Chief Information Officer), many large companies will also employ a CISO (Chief Information Security Officer) to oversee this implementation. When budgets to do not allow this position, CIOs will be tasked with the effort, and, unfortunately, in many typical small to midsized businesses (SMBs) this will fall into the laps of business owners or others already burdened with a wide variety of other duties.

To better understand how to thwart these attacks, one must first understand the attacks themselves, so let's take a look at the various threats currently out there.

> **Spam:** Although often just a nuisance and not a real danger, spam email can distract employees during work hours and affect productivity. Enterprise solutions these days generally have proper defenses set up against spam, so if this is a problem in your company, this is something that can and should be addressed.
>
> [1]**Phishing** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic environment. The word is an adaptation of "fishing" and derives from the fact that "bait" is put out there to lure the unsuspecting recipient into providing this information. Communications appear to be sent from common social web sites, auction sites, banks, online payment processors or IT administrators and may include links to websites that are infected with malware and/or ask the recipient to disclose personal information. An advanced level of this tactic is called "spear-phishing."
>
> [2]**Spear-Phishing:** This is probably the highest danger faced by today's IT security pros today. First, criminals need *some* inside information on their targets to convince them the e-mails are legitimate. They often obtain it by hacking into an organization's computer network or sometimes by combing through other websites, blogs, and social networking sites. Then they send e-mails that look like the real thing to targeted victims, offering all sorts of urgent and/or legitimate-sounding explanations as to why they need your personal data. Finally, the victims are asked to click on a link inside the e-mail that takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, user IDs, access codes, PINs, etc.
>
> **Viruses:** Like spam, most large company security programs are very effective against viruses, so the cyber-criminal finds more success against home-based PCs and small businesses. This is why attacks against small companies have sky-rocketed in recent years.

Malware: The goal of malware is to steal as much information as possible from the database of the company being hacked. Once they obtain the login credentials from financial sites, credit card companies, banks, etc., they use this to gain access to the accounts of their victims, and to set up new accounts, such as credit cards, in the victims' names and max out the account before the victim is even aware. A fairly new methodology that falls into the category of malware is ransomware.

Ransomware: This variation of malware drops a piece of code into the IT network that "phones home" to let the cyber-criminal know that it has been placed, then uses that link to encrypt the company's files. Once the files are encrypted, they are locked from use by the hacker who then sends a ransom note, ironically by email, demanding payment before the files will be unlocked. Once they are locked, the files are next to impossible to unlock without the hacker's key. Fortunately, advanced methodology now provides "crypto-containment" software that quickly identifies an encryption intrusion, isolates the infected files and prevents further encryption. (Note: encryption of an entire database is not instantaneous so a well-designed containment system can shut the infection down before it does serious damage.) Here at DynaSis we have seen instances where crypto-containment software detected and shut-down intrusions in large 10 terra-byte environments with as little as 5 gigabytes being compromised. This data was quickly deleted and restored from back-ups.

Social Engineering: This is the modern equivalent of the old "con game." It begins by gaining the trust of the victim by phone, email, or even in person. Often it is tied in with the human desire to help other people, hence false charitable requests. In this way, the bad actor obtains information about social media accounts, and then uses this information to gain access to these accounts to commit his crimes.

State Sponsored Hacking: While this won't affect most small businesses, your company may still be at risk if you are involved in defense contracting, multi-national deals, aerospace, or other areas that involve sensitive information, OR if you are a supplier to a larger company that fits this description. Remember that the infamous Target intrusion began with a small supplier who was hacked. The intruder then worked his way into the Target system through this supplier.

Remember this: all the above cyber-attacks can start with a single email.

Once upon a time combatting threats like these was fairly simple. A company would employ a secure email gateway (SEG), and everything would be okay. But as rule sets became more complex, and anti-virus required multiple deployments, and end user quarantines multiplied, these solutions became the points of failure. This has been further complicated by the fact that a company's own employees, as end-users, have become very skilled at circumventing the once hardened perimeter, and it is still further complicated by the potential of bad actors within the company itself. Today's IT professionals, and managed IT service providers, understand that the "hard exterior – soft interior" paradigm must be replaced by the Zero Trust Security Model.

The Zero Trust Security Model

While this might not sound too friendly, in light of the advanced quality of the threats facing us today, adopting a zero trust email model is critical. It is way too easy for business email users to be lulled into a false sense of security because of the high level of protection they understand is in place against traditional malware, etc., but the truth is, the bad guys never stop working on newer and "better" ways of hurting us so we can never assume that just because it "got through" your older security filters, an email is safe. It is exactly this sense of trust that the criminals exploit and it is up to each business and/or its IT service provider to treat every email that arrives as suspicious until a sophisticated email security solution has cleared it. To do this, we must add a new layer of IT security that checks your incoming emails for the malicious links that may be embedded in them, or in their attachments, so that no link is trusted until it has been cleared by a technology that is advanced enough for this detection.

With many companies that believe they are adequately protected, we are finding that in recent years they have inadvertently introduced new vulnerabilities into their IT networks through the use of what we call BYOD, or "bring your own device" into the picture. How many of your employees use their own smartphones, tablets or laptops for company work, and how many of these devices have access to your company email, not to mention other files?

Best Practices

Here at DynaSis, after evaluating the top tier email security products, we have chosen Mimecast for our clients, so for purposes of illustration, we will use their product, although there are other services available.

A properly designed Secure Email Gateway (SEG) will be delivered from the cloud and add a great deal of valuable functionality along with the security you need. These services should include[3]:

Allow-Auto Listing: Your "good contacts" are prioritized.

RFC Check Greylisting: Ensuring that incoming emails are RFC compliant for SMTP servers.

Global Reputation Checks: Employing the commonly used global reputation services to block email addresses with bad reps.

Recipient Validation & Active Directory: Verifying inbound addresses to thwart directory harvest attacks.

Anti-Spoofing: Locking out spoofed email to ensure it never reaches internal domains.

Email Firewall: Administrative lock out of email identified by sender, recipient, IP address, domain, etc.

Policy Control: Data leak control, large email distribution, encryption, and other enhanced security controls.

[3] The above terms are those used by Mimecast. Other services may use other terminology.

Another advanced technique that serves an important function is what some IT service providers call Targeted Threat Protection, designed to block spear-phishing and other targeted attacks. When a recipient clicks on a link in a received email, the link is actually rewritten, sent to the cloud where it is scanned for security. If cleared, the link can then be opened by the recipient. While the technical details of this are a bit above the scope of this paper, the process that Mimecast uses includes:

Delivery: When an email is received by Mimecast, all URLs contained in that email are rewritten, then delivered to the recipient.

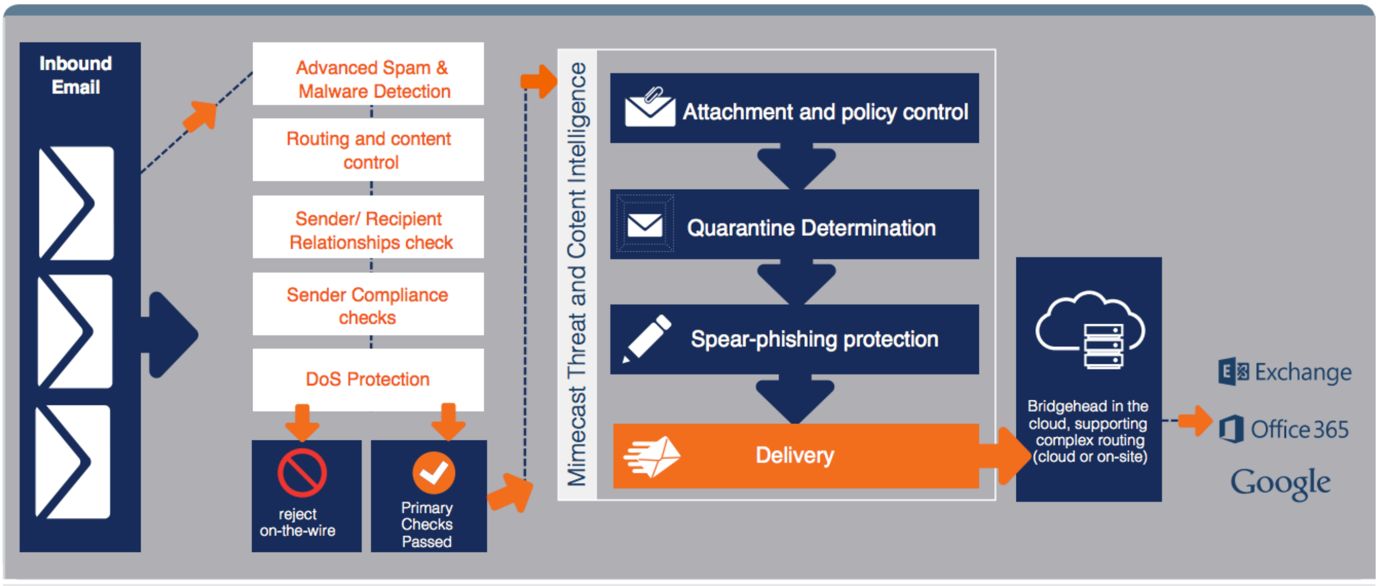
User Receipt: If the user clicks on a URL, the URL is checked against allow and block lists, and if the URL is not found on any of these lists it is sent to the scanner.

URL Scanning: The link is scanned though several layers of detection and any questionable emails are blocked.

Link, Domain, and Phishing Reputation: The link is verified by running it through internal and third party intelligence engines and other security checks.

Webpage Deep Analysis: The website from which the link originated is scanned for spear-phishing and other potentially malicious content that may be launched through that site.

Block or Allow Decision: If all pages related to the email are deemed clean, the email is passed on to the recipient. If there is anything deemed questionable, both the administrator and the recipient are notified and given the opportunity to receive or block.


Inbound Email
Advanced Spam & Malware Detection
Routing and content control
Sender/ Recipient Relationships check
Sender Compliance checks
DoS Protection
reject on-the-wire
Primary Checks Passed
Mimecast Threat and Cotent Intelligence
Attachment and policy control
Quarantine Determination
Spear-phishing protection
Delivery
Bridgehead in the cloud, supporting complex routing (cloud or on-site)
Exchange
Office 365
Google

Best Practice Defense in Depth at a Micro Level – © Mimecast

When you signed up for an AOL email account 25 years ago, the tech world was a much simpler place. If you used the word "phishing", it would be assumed you simply did not know how to spell. But times have truly changed and along with all the good things technology brings us, it also brings as an ever-growing variety of cyber threats and bad actors who spend countless hours devising their own technology to rob, cheat and steal. Vigilance must become a way of life and employing tools that work for you and that are continuously updated are vital. As an Atlanta managed IT services provider, we have seen it all and understand the complexities. If you have any questions about email security or IT support, please feel free to contact us.

http://www.computerweekly.com/feature/Email-security-Essential-Guide

https://www.mimecast.com/products/email-security/

http://www.digitaltrends.com/computing/can-email-ever-be-secure/

http://www.darkreading.com/operations/how-many-layers-does-your-email-security-need/d/d-id/1325791

http://www.inc.com/larry-alton/email-security-in-2016-what-you-need-to-know.html

https://www.techopedia.com/definition/29704/email-security

[1, 2] www.Wikipedia.com