CSS 3XX Winter 2021
February 4, 2021

Secure Email Gateway Analysis

One of the most enduring issues faced by modern day businesses is email security. Email is the most common method of relaying information both internally and externally for companies, and while it is a powerful communication tool, it is inherently insecure with numerous vulnerabilities. These vulnerabilities take a variety of forms, the foremost being malware and phishing attacks. Additionally, problems like spam which are not directly harmful can also waste crucial man-hours and resources. The most critical objective for businesses is to mitigate harmful messages and clutter in order to communicate with customers, protect their systems, and streamline their operations to be as efficient as possible. Traditionally, these first two goals have been achieved through strict administrative guidelines on how to handle emails with simple rules such as not opening suspicious links or only opening attachments in sandboxed environments. However, this has led to inefficiency where businesses spend thousands of man-hours following such protocols manually.

To compensate for these security deficits whilst also maintaining efficiency, the practice of instituting Secure Email Gateways (SEGs) has emerged within the industry. Instead of stringently following manual protocols, an SEG operates automatically on a cloud backend. In effect, traditional safe email practices are contracted out to a company which runs a detection software through each item, ensuring it's validity and safety. By routing all email traffic through this control, potentially harmful emails are filtered, blocked, or discarded while valid ones are allowed through. This provides protection for the company's systems against malware and phishing attacks as well as saving time better spent on customer relations or company communications.

However, SEGs are primarily geared toward counteracting only the most common email vulnerabilities (VadeSecure, 2019); sophisticated threat actors can easily identify when an SEG is in use through discovering the mail exchanger record (MX record) that a company's email routes through. The MX record is tied to a particular SEG provider, giving phishers a heads-up to alter their email attack in order to bypass the automated filters. This opens up another issue in that SEGs are oriented toward external

emails; messages sent internally are not filtered through these same protocols. If a machine on-site is compromised, SEG offers no protections against malicious email spread in such a scenario. This spread could result in sensitive data being stolen, ransomware locking down all devices on a network, and damage to brand reputation if a breach is publicized. A new window of vulnerability also exists with the current trend of working from home. This has resulted in compliance problems among employees. Difficulty in expanding the protections afforded by an SEG to internal cloud architecture has brought trouble to users, as email is pressed into services like G Suite and Office365 which share vulnerabilities traditional SEGs do not address.

To compensate for these shortfalls, some businesses may choose to institute a second control in the form of a Cloud Email Security Supplement (CESS). This is a form of 'post-delivery protection' for email, which unlike standard SEG, can fine-tune itself through machine learning, natural language processing, and network anomaly detection to flag fewer false-positives, while also invalidating more sophisticated attacks. The use of a CESS, due to it's post-delivery nature, means it does not share the MX record issue observed with SEGs (AVANAN, 2019); an attacker cannot be made easily aware whether or not CESS is in use on the target's end. To address wider cloud architecture, an Integrated Email Security Solution (IESS) is often utilized, which employs many of the same tactics as CESSs but plug themselves directly into the API of non-email exclusive cloud services.

SEGs are regarded as a general solution while CESS and IESS are more particular and exacting with their detection. All operate behind-the-scenes to reduce the amount of emails that need to be treated as suspect in the first place, but do not offer complete protection. Even when adopted, reliance on these services should not entail loosening traditional safe-email handling practices. Using the controls defined above can, however, result in considerable productivity gains and lead to a more efficient workforce through automated protection. These services are a step forward for businesses hoping to save man-hours through multilayering digital security, allowing employees to use more of their time on missions more pertinent to the organization.

REFERENCES

VadeSecure (2019) 4 Ways Hackers Break Through Fingerprint and Reputation-based Email Security. Retrieved from https://www.vadesecure.com/en/blog/4-ways-hackers-break-through-fingerprint-and-reputation-based-email-security

AVANAN (2019) What Is a Secure Email Gateway and Are They Still Viable in 2020? Retrieved from https://www.avanan.com/blog/what-is-a-secure-email-gateway