MSP

united technology imaging services

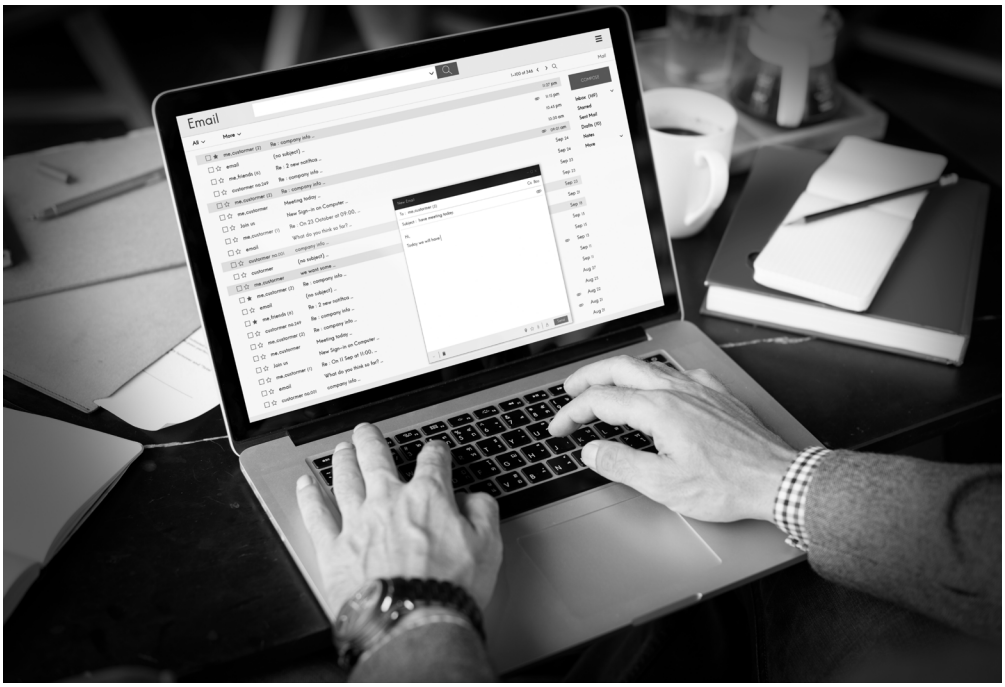
eBOOK

Why Email Security Matters

EMAIL: THE MOST VULNERABLE COMMUNICATION CHANNEL

Email is "the" critical business service, showing strong growth worldwide. According to Radicati's 2017 – 2021 Email Statistics Report, there were 6.3 billion email accounts in 2017, and it is forecasted to grow to over 7.7 billion accounts by the end of 2021. Business is the biggest source of email traffic, said the report, accounting for 269 billion emails per day, in combination with consumer emails in 2017—and the number will increase to 319.6 billion daily by 2021. Email is the lifeblood of business.

Unfortunately, email is also a channel for attackers to strike at any organization. Spam is a frequent problem for business users, who may be sent harmful attachments that could infect computers on their network. Our SolarWinds® Mail Assure™ solution data supports the worldwide statistics claiming that almost 70% of email traffic worldwide is spam or malicious.



COMMON METHODS TO ATTACK EMAIL SYSTEMS

- **Buffer overflows**—This will happen if an on-premises email server is hit with large quantities of data.
- **Phishing**—A relative of spam, this is a common email attack that can be used to fool employees into granting access to systems. In a typical phishing attack, a criminal may pretend to be from a trusted third party, such as an IT department, and will send an email asking employees to log into a web portal. The portal is fraudulent, and will gather their login data, enabling the attacker to infiltrate corporate systems and gain a foothold.
- **Mail flooding outbound and inbound**—Large volumes of inbound email are processed and filtered before being passed on to the on-premises email server; this saves the bandwidth and processing capability of the email server for legitimate email traffic.
- **Denial of Service (DoS)**—The arrival of large volumes of email over a limited bandwidth DSL or cable modem connection will degrade all externally hosted services and render other internet services, such as VPN or Remote Desktop, unusable.

In October 2013, 153 million Adobe accounts were breached, each containing clear text email addresses for their customers.

CASE IN POINT: SPAM AND PHISHING

In October 2013, 153 million Adobe® accounts were breached*, with each containing clear text email addresses for their customers. The password cryptography was poorly done and many passwords were easily decrypted as well. Since the activation and licensing of Adobe's suite of products requires a valid account on Adobe's servers; cybercriminals quickly identified these as valid email addresses and a plethora of phishing emails and spam soon followed. In light of incidences like this and the availability of large databases of valid email addresses, there is an urgent requirement to protect legitimate email accounts from the virus-infected and malicious link phishing emails cybercriminals send out by the millions.

* Source: Latest research report from Adobe, 2016, pg. 12

THE DIRECT CONNECTION ISSUE

One of the ways cybercriminals break into companies is by connecting to their email server directly. The value of IP address restrictions limiting the allowed list of connectors to an on-premises mail server is clear. This network reconnaissance technique of direct connection is almost completely thwarted by a defense-in-depth strategy.

One of the ways cybercriminals break into companies is by connecting to their email server directly.

"Since cybercriminals are unable to connect directly, it will be impossible for them to know which email server software is run. That makes it very difficult to find vulnerabilities to exploit. This issue is important if older versions of Microsoft Exchange are being run on older hardware with limited capacity." — Leading MSP, MSP Company.

THE ADVANTAGES OF HOSTED EMAIL PROTECTION

A LAYERED APPROACH TO EMAIL SECURITY

One of the key advantages of a hosted email protection service is that it sits in front of the existing mail infrastructure restricting the IP addresses of the connecting email servers. Configuring mail exchange (MX) records to send mail via the hosted email protection service for filtering of spam, viruses, ransomware, phishing attacks, malware and all email borne threats, and then configuring the email server and firewall to only accept connections from the hosted protection service provides robust protection against email threats. This configuration ensures that only legitimate email that passes through the filtering system is sent to the on-premises email server. This configuration also allows the hosted email protection service to monitor the volume of messages originating from the on-premises email server.

A sudden spike in the number of sent messages could indicate a major problem inside the host network. A mature email security system also features protection mechanisms such as blacklisting to lock down malicious senders, and thereby protect networks from IP blacklisting and ultimately IP reputation.

DEFENSE-IN-DEPTH OFFERS MAXIMUM PROTECTION

MULTIPLE LAYERS OFFER INCREASED PROTECTION

The best defense-in-depth solutions work together, complementing each other. Combined with other defense mechanisms, such as anti-malware scanners and web protection, email protection should play a crucial role in protecting clients' organizations.

Defense-in-depth is layered so that even if an attack makes it past one layer of defense, it will be stopped by another. Anti-malware scanners will check any attachments that an email blacklist and spam filter fail to stop, for example. Web protection can help to stop employees visiting bogus phishing or malware sites. Together, they create an armored web of protection that can shield a company from harm.