EMAIL SECURITY THAT MATTERS AT THE MACRO-SECURITY LEVEL

EXECUTIVE SUMMARY

Organizations are rapidly moving to digital business models that facilitate greater agility and efficiency and build new revenue streams. These changes also bring new security challenges. As organizations add digital services and processes, the attack surface expands. At the same time, the number, variation, and sophistication of threats are increasing. As a result, organizations are often uncertain what risk to address first, especially when much of their technology investments are allocated to business innovation and growth.

One area cybersecurity leaders too often overlook is email security, where traditional security approaches are no longer sufficient in the face of new cyber-criminal techniques. In 2017, bad actors successfully installed more malware through email than any other method, which also serves as the first attack vector in multistage attacks. Traditional email security approaches, especially those segregated from the broader security infrastructure, fall short. As a result, organizations quickly find themselves in a constant reactive mode, unable to keep pace with the threat landscape and the new challenges of digital transformation.

EMAIL SECURITY IS OFTEN OVERLOOKED

With email being the target of over 90% of malware attacks,[1] information sharing from email to other security elements is pivotal. But the majority of organizations run email security within silos segregated from the broader security architecture.

Here, traditional email security approaches work in isolation from other security components. But in the face of digital transformation, which dramatically expands the attack surface, and an evolving and increasingly more advanced threat landscape, security must transform. This includes email security. Following are critical reasons why enterprises need to reevaluate their email security approaches.

DIGITAL TRANSFORMATION EXPANDS THE ATTACK SURFACE

71% of enterprises see business and digital transformation as mission critical.[2] 86% of decision-makers say they have two years to make inroads with digital transformation before they suffer from financial or competitive threats. 59% worry they might be too late.[3]

However, an organization's attack surface is the sum of the points (attack vectors) where an attacker can try to enter an environment. Things like multi-cloud networks, shadow IT, Internet of Things (IoT), OT and IT convergence, big data, mobile devices and users, and hyperconnected networks dramatically expand the attack surface and put businesses, people, and data at greater risk.[4] In the past, organizations tried to minimize the attack surface to protect their organization. Today, digital transformation is causing the attack surface to grow exponentially, and organizations must look for ways to protect themselves against the additional risks.

SECURITY IN THE HEADWINDS OF THE ADVANCED THREAT LANDSCAPE

The velocity, volume, and sophistication of threats are increasing in leaps and bounds. Malware and attack exploits that were available only to nation-state bad actors and a very few number of cyber-criminals a couple years ago can be easily and quickly accessed by "everyday" hacktivists. Criminals can purchase Malware-as-a-Service models that employ polymorphic characteristics to evade detection and leverage artificial intelligence (AI) and machine learning to identify new vulnerabilities.[5]

Further, the polymorphic nature of malware makes it increasingly more difficult to identify and detect malicious intrusions. In 97% of infection instances, the malware is polymorphic.[6] Polymorphic techniques involve frequently changing identifiable characteristics like filenames, file types, or encryption keys that make the malware unrecognizable to numerous detection techniques.[7] The number of malicious attack vectors continues to balloon. For example, in Q1 2018, FortiGuard Labs recorded 15,071 new malware variants, which equates to an average of 167 new pieces of malicious code every day.[8]

86% of organizations say they have two years to make inroads with digital transformation (55% say a year or less).

59% worry they might be too late already.

The time it takes bad actors to exploit a vulnerability, penetrate a network or data center, and enact a data breach or destructive operation is quickly decreasing as a result of the availability of Malware-as-a-Service and AI and machine learning technologies.[9]

EMAIL SECURITY: MORE CRITICAL THAN EVER—AND OFTEN OVERLOOKED

Established security controls like email security can be easily overlooked in the new digital world and in the midst of the advanced threat landscape. While much prognostication about the death of email exists, it remains a critical part of virtually every business today. The average number of business-related emails sent and received by employees every day exceeds 120.[10]

EMAIL AS A PRIMARY MALWARE DELIVERY CHANNEL

In January 2017, only one out of every 12 users (8.6%) had a malicious email sent to them. Four months later (May), this number had nearly doubled to one in seven (15%).[11] It should be no surprise that a recent report found that 49% of malware is installed via email, and that phishing is in the top three cyber-criminal actions that led to breaches.[12]

FIRST STAGE FOR A BIGGER ATTACK CAMPAIGN

When it comes to data breaches, email ranks even higher. 91% of data breaches begin with an email.[13] And while some attacks start and end with email—too often successfully—others simply use email as the initial front in a multistage attack. For example, malicious code and URLs contained in email can be used to communicate with a supporting cyber-crime infrastructure or to download additional payloads employed to gain entry via other attack surface areas such as cloud services.

It goes without saying that stopping the initial email attack is critical, but it is just one action in a larger set of coordinated security activities. Stopping this initial attack is just the first step in email security, and security leaders will remain in a defensive mode waiting for the next attack to strike unless they adopt a different approach. Instead, they need to look holistically at the intended attack life cycle to gather valuable insights and to build a proactive security posture. Further, they can harvest threat intelligence and distribute it across each security area. This enables organizations to update threat protections proactively against attacks that have not been launched across other attack vectors. But this is difficult, if not impossible, to do when email security resides within a siloed network and isn't integrated with other security components.

THE COST—IMPACT—OF EMAIL ATTACKS

While it can be difficult to demonstrate the financial impact of cybersecurity investments in certain areas, email security is not one of them. For example, the U.S. Federal Bureau of Investigation found that email compromises cost U.S. businesses $5.3 billion between October 2013 and 2016.[14] Further, 15,690 incidents were reported in 2017, with an average cost of $52,000 per incident.[15]

But the impact of email security compromises is more than the financial cost. Theft of intellectual property, where email serves as a primary infiltration channel as well as exfiltration channel, is a serious issue. In just one example, more than 30 terabytes of data from more than 300 universities and 47 private-sector enterprises were stolen by an international terrorist organization and sold to fund terrorism activities. The attack targeted 8,000 email accounts of professors.[16] This is just one of countless examples where email served as the gateway for intellectual capital theft.

In 2017, 49% of malware was installed via email.

91% of cyberattacks and the resulting data breach begin with an email.

Each business email compromise, on average, costs $52,000.

The top data type compromised by social attacks (viz., phishing) is personal information, followed by organizational secrets and internal data.[17]

CONCLUSION

Digital transformation expands the attack surface, increasing an already complex security infrastructure and adding to the heavy burden on security teams. Coupled with a threat landscape that is increasing in velocity and sophistication, cybersecurity teams are reaching a breaking point in many instances.

Traditional email security approaches are inadequate and unable to meet these new security challenges. With malware attacks targeting email more often than any other attack vector, security organizations need to take serious heed. Specifically, a next-generation approach to email security that breaks down silos between email security and other security areas is critical. This model not only addresses threats to email, but also enables organizations to share threat intelligence gathered at the email vector with other security areas before attacks occur. This integrated email security model uses automation to turn workflows and information sharing into a proactive risk management strategy.

[1] "2018 Breach Data Investigations Report," Verizon, March 2018.

[2] "Forrester Technology Adoption Profile—Cisco," Forrester, 2016.

[3] "Are Businesses Really Digitally Transforming or Living in Digital Denial?," Progress, May 2016.

[4] Jonathan Nguyen-Duy, "Securing the Next Generation of Digital Transformation," CSO Online, February 13, 2018.

[5] GoldSparrow, "'Malware-as-a-service' Market Booms as Prices for Malware and Botnet Creation Tools Decline," Enigma Software Group USA, accessed May 5, 2018.

[6] Milena Dimitrova, "97% of Malware Infections Are Polymorphic, Researchers Say," Sensors Tech Forum, March 8, 2016.

[7] Nate Lord, "What Is Polymorphic Malware? A Definition And Best Practices For Defending Against Polymorphic Malware," Digital Guardian, March 20, 2017.

[8] "Fortinet Threat Landscape Report Q1 2018," Fortinet, May 2018.

[9] GoldSparrow, "'Malware-as-a-service' Market Booms as Prices for Malware and Botnet Creation Tools Decline," Enigma Software Group USA, accessed May 5, 2018.

[10] Ben Nahorney, "Internet Security Threat Report (ISTR)," Symantec, October 2017.

[11] Ben Nahorney, "Internet Security Threat Report (ISTR)," Symantec, October 2017.

[12] "2018 Data Breach Investigations Report," Verizon, March 2018.

[13] "Phishing and Spear Phishing Remain the No.1 Attack Vector," Cofense, 2016.

[14] "FBI: Business Email Compromise is a $5 Billion Industry," The Security Ledger, May 8, 2017.

[15] "2017 Internet Crime Report," U.S. Federal Bureau of Investigation, 2017.

[16] Yojana Sharma, "Hundreds of universities targeted in global data steal," University World News, March 27, 2018.

[17] "2018 Data Breach Investigations Report," Verizon, March 2018.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

208268-A-0-EN

May 24, 2018 3:05 PM

wp-email-security-at-the-macro-level