Email Security – Best Practices to Consider

WHAT YOUR SECURITY TEAM IS FACING

- Adlware aimed at businesses – up 6,000% in 2019
- Web threats - dominated by online credit card skimmers, exploit kits, malvertising and malicious redirection
- Mobile malware – up 50% thus far in 2020
- Phishing – 65% of businesses experienced a successful phishing attack in 2019
- Malware – contained in 1 in every 645 emails
- Ransomware – variants increased by 72% during COVID-19 pandemic

TARGETED ATTACKS ARE DIFFERENT

Unlike a traditional phishing attack, a targeted attack is designed to bypass an organization's security defenses using sophisticated malware and social engineering to gain access to endpoints or other resources. Fundamentally, the goal is to locate, exfiltrate, and monetize stolen data and intellectual property before the victim becomes aware of the breach.

- UNDERSTAND THE RISKS
- CONDUCT A THOROUGH AUDIT OF THE CURRENT SECURITY INFRASTRUCTURE, TRAINING PRACTICES AND CORPORATE AND COMPLIANCE POLICIES
- CONSIDER A MULTI-LAYER APPROACH.
- VIEW SECURITY HOLISTICALLY
- ESTABLISH DETAILED AND THOROUGH POLICIES
- IMPLEMENT AND REVISE COMPANY PROCEDURES
- TRAIN ALL USERS, INCLUDING SENIOR EXECUTIVES
- CONSIDER THE GDPR AS A SECURITY ISSUE
- DEPLOY ALTERNATIVES TO "SHADOW IT"
- CONSIDER ALL OTHER ISSUES

Security teams and the organizations they support live in difficult times: they increasingly are the targets of sophisticated threats developed by a shadowy and well-financed cybercrime industry that has demonstrated it can often outsmart even the most robust security defenses. Cybercriminals are aided by the fact that security teams often lack the human and financial resources necessary to keep pace, and so often cannot defend against the latest threats that are directed at them. Add to this the fact that security teams often support users who unwittingly aid cybercriminals (or occasionally become them) through mistakes or intentional acts that can result in the loss of sensitive data or corporate funds.

One of the many reasons cybercriminals are achieving success is because many organizations are not exercising adequate due diligence in addressing the problems of phishing, spear phishing, CEO fraud/business email compromise (BEC) and ransomware.

Another reason for the success of cybercrime is that criminal organizations are generally well funded and have the technical resources to create new and more capable attack methods. Their highly collaborative nature also contributes to their success.

To more efficiently generate revenue, cybercriminals are changing their focus from more traditional data (such as stolen credit card numbers, login credentials, passport information, etc.) to ransomware and activities like CEO Fraud/BEC that enable them to steal directly from victims rather than stealing something of value that then has to be sold to someone else.

It's important to understand cybercrime is an industry, and like any industry that wants to thrive over the long term, adapts its methods to changing market conditions and human behaviors.

webservio

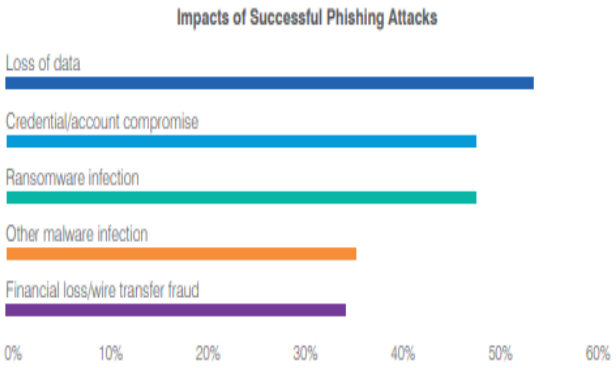
TODAY'S CYBER ATTACKS TARGET PEOPLE, NOT INFRASTRUCTURE

- Cybercriminals trick your employees into opening unsafe attachments or clicking on a questionable web link.
- Cybercriminals persuade your customers into downloading a fake mobile app or sharing login credentials to a social media account they believe is yours.
- Cybercriminals impersonate your executives and partners, duping people in your organization into wiring money and sending sensitive data.

NATIVE SECURITY IS NOT ADEQUATE

Many organizations rely on the native security that is included with their email system or other applications. However, these security capabilities often do not provide the same level of protection as third-party solutions that are more specifically focused on threat detection and remediation.

Conduct Thorough Audits



STATE OF THE PHISH 2020

SOURCE: *Proofpoint, Inc*

Decision makers must understand the risks that their organizations face and address them as a high priority. That seems obvious, but many give intellectual assent to the risks they face without taking them to heart. For example, in mid-2017 a developer with Tata Consultancy Services uploaded an enormous volume of internal reports, web banking code development plans, telephone records and other sensitive information for 10 financial services customers - including six Canadian banks and two U.S. institutions – to a public GitHub repository. Tata's management clearly knew about the technologies and processes that could have been put in place to prevent this occurrence, but did not implement the appropriate controls necessary to ensure this was caught before it happened.

Understand the Risks

Decision makers should conduct a complete audit of their organization's current security awareness training programs, the security solutions they have in place, and the processes they have implemented to remediate security incidents. This is a key element in identifying the deficiencies that may exist. These audits may then be used to prioritize spending to resolve any problems.

Consider a Multi-Layer Approach for Email Security

It is important to note the need for advanced threat protection features because email security is no longer simply about spam and phishing campaigns. Threats like ransomware, crypto-jacking, zero-day, CEO Fraud/BEC, etc. are sophisticated, and require advanced defense capabilities. These capabilities include attachment sandboxing and time-of-click URL analysis to complement the incumbent anti-spam and anti-malware engines.

View Security Holistically

Security should be viewed as a holistic exercise, from the cloud services that are utilized to detect and remediate threats all the way down to every endpoint solution. This doesn't mean single sourcing of security infrastructure, but it does require that appropriate reporting and monitoring mechanisms be in place so that security teams can have a full understanding of their organization's security posture in as close to real time as possible.

webservio

KEY PREVENTION TIPS

Advanced malware-based threats (ie. ransomware):

- Keep malware away from the endpoint by isolating personal internet activity
- Identify high-risk users and train them to change their behavior

Non-malware threats (ie. email fraud):

- Block all domain spoofing to end users, partners and customers by deploying DMARC & DKIM
- Provide visibility into all senders who use your domain.
- Consider requesting ARC implementation from partners acting as an email intermediary.
- Find and block lookalike domains before they're used in attacks

Credential phishing:

- Use phishing simulation to see what users are most susceptible and raise awareness
- Find and block lookalike domains before they're used in attacks

Establish Detailed and Thorough Policies

It is essential to develop policies for all of the email, websites, collaboration, social media, mobile, and other tools that IT departments have deployed or that they permit employees to use. An important step should be the establishment of detailed and thorough policies focused on the tools that are or will be used in the future. These policies should focus on the regulatory, legal, industry and company standards to encrypt emails if they contain sensitive or confidential data; monitor all communication that is sent to social media, blogs and other venues for malware; and control the use of personally owned devices that access corporate systems housing any kind of business content.

Implement and Revise Company Procedures

All organizations should implement and regularly update company procedures regarding the protection and accessibility of sensitive and confidential data assets, as well as business-critical systems. For example, all organizations need an effective set of backup, restoration and testing procedures for sensitive data so they can recover quickly from a ransomware or other malware infection. Dual-control procedures should be implemented for access to critical data, especially those focused on financial transactions. This can prevent a single, rouge employee from creating a data breach.

Implement Best Practices for User Behavior

There are a number of best practices to address the cybersecurity gaps that may exist in organizations:

- All employees, but especially senior executives who are more likely to be the target of a CEO Fraud/BEC attack, should be reminded regularly about the risks associated with oversharing information on social media. For example, sharing one's travel itinerary and business-class upgrades might impress a senior executive's friends, but it also provides cybercriminals with an opportunity to target employees with a convincing email fraud/BEC campaign. An employee who deals with finances or sensitive data should have pre-established backchannels or communication methods provided to them for verifying sensitive requests.
- Employees should be required to use passwords that match the sensitivity and risk associated with the corporate assets they are accessing, and these passwords should be changed on a regular schedule enforced by IT. Two-factor authentication should also be deployed.
- Software and operating systems should be kept up to date to reduce the potential for a known exploit to infect a system with malware. IT can help by implementing automated management and policy enforcement.
- Ensure all employees maintain good endpoint defenses on their personal devices if there is any chance these devices will be used to access corporate resources like email or databases.

webservio

INCIDENT RESPONSE IS ESSENTIAL

A growing proportion of IT and security decision makers would like to adopt automated capabilities as part of the incident response process to shorten the resolution and escalation time required to manage security incidents and to handle more routine alarms.

Here's why:

- A typical security incident takes 10 hours to resolve, but for a large portion of the organization, the process takes 16+ hours to resolve
- When a typical security incident requires escalation to the next level of incident response, it takes 45 minutes on average for security analysts to process the incident

OTHER BEST PRACTICES

- Keep systems up to date
- Keep recent backups and verify them
- Deploy good endpoint solutions
- Consider the risks inherent in the Internet of Things (IoT)
- Use adequate threat intelligence
- Protect all high-value data
- Encrypt sensitive and confidential email communications
- Consider using behavior analytics

Train All Users, Including Senior Executives

Every organization should have a robust security awareness training program that enables users to make better decisions about the emails they receive, how they surf the web and how they use social media, etc. The goal of any security awareness training program is to help users to be more conscientious and skeptical about what they receive in email, what they view on social media, and what they consider to be safe to access.

Consider the GDPR as a Security Issue

The European Union's General Data Protection Regulation (GDPR) has two tiers of administrative fines for non-compliance (Article 83), which can be levied by a supervisory authority based on the type of infringement, rather than on a first, second, or subsequent infraction:

- The fine for lower level offenses is up to €10 million or up to two percent of the total worldwide annual turnover from the preceding financial year, whichever is higher. Infringements at this level include failing to enact data protection by design and by default (Article 25), failing to keep adequate records of processing activities (Article 30), and not ensuring appropriate security of processing (Article 32), among others.
- The higher level of fines is up to €20 million or four percent of total worldwide annual turnover, whichever is higher, and is for offenses such as failing to comply with the basic principles for processing, including conditions for consent (Article 5-7, and 9), not providing data subjects with their rights (Articles 12-22), and unauthorized or inappropriate transfers outside of the EU (Articles 44-49), among others.

Because data protection in the GDPR must be by "design and default," security should be prominent in any organizations' approach to protecting data.

Deploy Alternatives to Shadow IT

Most organizations permit employees to use their own smartphones, tablets, file-sharing accounts and cloud storage services. While this alleviates the burden on IT from having to provide all these tools to users, it can create enormous security holes. As a result, it's important for IT to offer robust alternatives to the solutions that employees might want to deploy. This includes options for file-sync-and-share, VOIP, VPN, cloud storage, real-time communication and other capabilities that employees use. Employees often utilize these solutions because they do not have an equivalent capability provided by their IT department, or because IT-provided solutions are not as good as the free solution they are familiar with. Providing an IT-approved solution that is as capable and user-friendly as the solutions that employees have deployed on their own can enhance cybersecurity and give IT more control over corporate content.

webservio