Resetting Your
EMAIL SECURITY STRATEGY

mimecast®

RETHINKING YOUR STRATEGY

It's no secret that organizations find themselves the target of increasingly sinister and highly sophisticated phishing, spear-phishing, whaling and ransomware attacks –typically delivered through emails. While risks are clearly mounting, many organizations still aren't keeping up with the challenge. The list of companies recently in the news, includes: Seagate, Snapchat and Weight Watchers International, among others. Each one either suffered multi-million dollar financial losses or saw critical employee data compromised.

Addressing these threats requires different strategies, tactics and technologies than in the past. It's important to recognize that a "castle and moat" or hard network perimeter approach to cybersecurity is no longer viable. There are no perimeters in an era of clouds, mobility, computing and applications are easily accessed by even the most technically challenged employees, often without IT knowledge. Instead, organizations must focus on delivering maximum protection through a more systemic security framework that minimizes the risks of social engineering attacks, including impersonation attacks like whaling. Ultimately, an organization must focus on four critical areas: people, processes, technology and a solid foundation of leadership.

DID YOU KNOW?

91% of attacks start with email[1]

30% open the phish and click the link[2]

1 MINUTE and 40 SECONDS is the median time to first click[3]

70% of whaling attacks involve domain spoofing[4]

64% of IT security pros regard email as a major cybersecurity threat[5]

HOW SCAMS WORK

Virtually every organization, large and small, is vulnerable. Cybercriminals collect critical data and target organizations in a number of ways:

They scrape data from executive bio pages at a company website or they mine social media sites, such as LinkedIn or Facebook, to glean details about targets.

Cybercriminals also grab data from human resources pages, as well as résumé engines that include details about individuals.

They sift through corporate materials, such as annual reports and press releases, as well as outside news stories and trade-show programs.

Hackers are known to target mid-level managers and clerks that have the authority to initiate large financial transactions or data transfers, often without requiring a verification or approval.

Cybercriminals will impersonate executives, as well as use company stationery, signature lines and logos to trick the recipient into believing he or she is receiving a real request.

Requests for money typically revolve around wire transfers. Once a transfer has been completed, it's difficult to pull back the money, as it is quickly laundered through the international financial system.

WHY SCAMS WORK

There are clear warning signs that an assault is underway. It's important to pay attention to the details and subtleties of a phishing, spear-phishing or whaling attack. Some examples are below.

The request originates from a domain name and spoofed link that are misspelled but appear authentic. For instance, *testcompany* becomes "testconpany" or "testcornpany." Unless the recipient takes a few seconds to double check the link, he or she is duped.

The recipient is afraid of upsetting the boss or undermining a critical transaction – and perhaps losing his or her job.

The targeted employee is in a hurry and under pressure to complete all of his or her work. In the rush to finish a task, the target clicks the link.

The hackers have identified a loophole or gap in enterprise procedures and they exploit it. For example, an organization may lack a mandatory second sign-off for a transaction above X amount or for any data transfer involving social security numbers or other sensitive employee data. Even if it has rules, it may not have the technology in place to force compliance.

Requests for fund or data transfers often appear to be highly time-sensitive and an employee may fear that he or she is interfering with critical business processes, unless the transaction takes place immediately.

PEOPLE MATTER

Social engineering techniques spin a tight orbit around a very basic concept: it's possible to trick *people* into doing the dirty work for thieves. These methods are effective even when stringent procedures and state-of-the-art security technology is in place. In fact, it can be argued that people are the weakest link.

But this doesn't mean your organization has to serve as the next victim of gaps, glitches and breakdowns. When employees across the enterprise understand risks, threats and how attacks take place, they're in a position to avoid making common mistakes that lead to a breach. In fact, a human defense – essentially an invisible protection boundary comprised of your employees can serve as the best safeguard and last line of defense because it renders social engineering completely ineffective and payloads entirely benign.

The upshot? There's a need for greater education, awareness and, most importantly, an understanding of how attacks unfold and what methods cybercriminals use. A best-practice approach typically involves:

- direct training about attack methods and risks;
- newsletters and alerts that keep employees informed;
- simulations that expose weaknesses and mistakes;
- ongoing discussion of the problem; and
- technology that alerts and educates them.

When employees fully understand the issue – and the risks – they're in a position to serve as the barrier of protection, essentially the "human firewall" that protects the organization. While it's not possible to prevent every breakdown or breach with training, it stacks the odds in the organization's favor.

PROCESSES ARE CRITICAL

Successful social engineering attacks inevitably exploit another weakness within an organization: a gap or breakdown in processes. Too often, security leaders and others do not keep up with current and evolving threats. Unfortunately, some have never addressed fundamental problems and threats in the first place. Either way, the result is the same: the enterprise is at risk. The attack surface – even with security tools and solutions in place – expands exponentially.

HOW IT HAPPENS:

Attackers may target a mid-level manager who has the authority to make a multi-million dollar wire transfer.

By using LinkedIn, referencing a corporate bio page and creating a fake Facebook account to "friend" the target, cybercriminals gather the necessary details to launch an attack. That is, they create an email that appears to come from a high-ranking executive (e.g. CEO, CFO, etc.).

Yet, all the information would be rendered useless if the organization had a very simple process in place: a rule that requires the manager to verify any transfer above $10,000, and technology that forces compliance.

Without it, the manager initiates the wire with the belief he's aiding the CEO. Millions of dollars are lost and the organization's reputation potentially ruined.

PROCESSES ARE CRITICAL

It's critical to get a handle around policies, practices and procedures to ensure that they address social engineering threats – as well as other cybersecurity risks. This ripples into a wide range of areas, including how sign-ons, approvals for financial and wire transfers, W-2 data transfers and other events take place. Too often, line-of-business leaders in departments such as HR or finance complain that they cannot change policies because they are "hard-coded" into IT systems. This represents a disaster waiting to happen. No system, policy, practice or workflow should be exempt from review and change.

It's critical to get a handle around policies, practices and procedures to ensure that they address social engineering threats – as well as other cybersecurity risks.

TECHNOLOGY COUNTS

When organizations address cybersecurity threats, technology inevitably enters the picture. Yet, as the target and threat landscape move, so must technology tools and solutions. Old and antiquated security methods represent a very real danger. They put an organization at greater risk. Today, there's a need to evolve beyond a perimeter-centric approach, but also avoid draining a security budget – and increasing IT complexity by spending money on new solutions as an overreaction. For most organizations, it's important to spend strategically – about 10 to 12 percent of the overall IT budget.

The right security technology can aid in detection and automate crucial processes, such as detecting suspicious URLs, identifying suspicious keywords and matching known sources of scams and threats to a blacklist. Simply put, it adds another layer of protection – think of it as a safety net – for best practices revolving around people and processes. That way, when someone inevitably makes a mistake, the technology steps in and protects them and the organization. The technology sandboxes or blocks the malware, just as an inoculation blocks a real-world or virtual virus. Staying current with technology, software and systems that provide real-time targeted threat protection is paramount.

The right security technology can aid in detection and automate crucial processes, such as detecting suspicious URLs and identifying suspicious keywords.

LEADERSHIP LOOMS LARGE

A lack of leadership undermines all of the other pillars. People, processes and technology are built on a foundation of security leadership and investment. This requires a serious focus on cybersecurity – and an ability to learn from past mistakes and breakdowns. There are some important issues that an organization must address in order to slide the dial from risky business to a sense of security.

For example, it's critical to have a CSO or CISO who spearheads security and builds a strategic framework for the organization. Otherwise, with no one taking the reins or the business pulling the strings on decisions and solutions, gaps, breakdowns and oversights are likely, and inconsistent practices are inevitable. This represents the ideal environment for cyberthieves. At the end of the day, it's not just about information and technology, it's about risk.

But the task doesn't stop here: The board and C-suite must be fully invested in security in order to secure the 10 to 12 percent budget threshold that typically affords excellent protection, but also provides the foundation and buy-in for enterprise initiatives, including training and development. In fact, the holy trinity of people, processes and technology falter without solid leadership and board sponsorship. In the end, the majority of security breaches, hacks and problems can be traced back to a lack of leadership, rather than deficient people, process and technology.

The holy trinity of people, processes and technology falter without solid leadership and board sponsorship.

HOW TO PREVENT AN ATTACK

There are several ways to prevent and detect suspicious and dangerous emails:

Focus on ongoing education and training, and provide the budget and support to make these initiatives a priority.

Use technology that spots potential phishing, spear-phishing, whaling and malware through language analysis, blacklists and other means.

Use email stationery and other unique identifiers that make it more difficult to fake or counterfeit an email.

Use testing and simulations to determine who's going for the bait.

Train users to check the sender's domain to make sure it isn't misspelled and it matches the real domain name. Also, employees should know to hover their mouse above a URL to identify an alias site or fraudulent hyperlink.

Rethink policies and authorizations such as requiring a second signature on lower dollar transactions or written sign-off for a data transfer involving employee records or other sensitive data.

BUILDING A MORE SECURE CYBERSECURITY FRAMEWORK

Here are five best practices to ensure your success:

1 **Appoint a Security Leader:** There must be someone in place, such as a CSO, CISO or CIO, who leads the security initiative. It's critical to manage and integrate technology, processes, the business and its people.

2 **Secure Executive Buy-In:** The C-suite must fully support an initiative in order to secure the required budget support and organizational buy-in. It's important to build a security-centric framework and culture. What's more, senior executives must recognize that their jobs are increasingly at risk when a breach occurs. Over the last few years, several CEOs have lost their jobs due to security lapses.

3 **Measure Success:** The organization must have metrics or KPIs in place to gauge success and identify weak points. It must also use tools, such as simulations, to gauge how things are working.

BUILDING A MORE SECURE CYBERSECURITY FRAMEWORK

4 **Cybersecurity Tool Integration:** Email protections must complement other cybersecurity tools and processes, including password policies/authentication, encryption and authorizations for transactions.

5 **Ongoing Training and Education:** Training can't be limited to hiring and orientation. It also can't be limited to a once-a-month PDF or video link to test responses; it's vital to think out-of-the-box and attempt to emulate the way thieves think. It's also critical to provide ongoing training about threats and risks, so that it becomes second nature to approach any email, phone call or other event that requests money or any sensitive data with a suspicious mind.

PROTECTION IS PARAMOUNT

Phishing, spear-phishing, whaling and other cybersecurity methods aren't going away anytime soon. However, an organization that focuses on people, processes, technology and leadership builds a security foundation that supports the organization and allows it to weather the challenges of today's threat environment.

Mimecast can aid your organization in avoiding email breaches and achieving a best- practice approach to cybersecurity. For more information, visit www.mimecast.com.

Sources:

1. WIRED
2. 2015 Verizon Data Breach Investigations Report
3. Ibid.
4. Mimecast, "A Whale of a Tale: How to Stop the Rising Tide of Impersonation Attacks," 2016.
5. Ibid.

mimecast®

To learn more, visit www.mimecast.com.

Mimecast (NASDAQ:MIME) makes business email and data safer for thousands of customers and millions of employees worldwide. Founded in 2003, the Company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.