Application security, Malware, Phishing, Ransomware

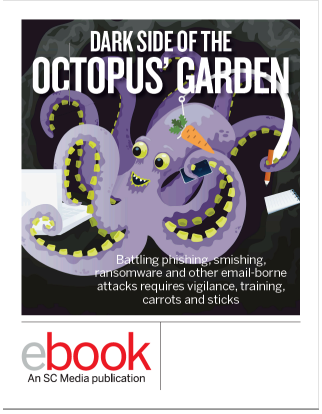
Forging an email security plan – The dark side of The Octopus' garden

December 28, 2018

Share

By Lee Sustar

Before the phish gets its way, it is essential to have email security down pat. Lee Sustar looks at how tech and face-to-face education improve your defenses.



Users in large organizations are firewalled, proxied, scanned, logged and analyzed, around the clock and worldwide. Companies find all kinds of ways to protect their email, but still, users click on phishing emails.

The sender might be a spray-and-pray spammer hoping to snare a gullible user looking for quick riches or a nation-state actor rolling out the latest advanced persistent threat (APT). But a poor security culture and a semi-plausible pitch from a bad actor can compromise an IT environment full of the latest cyber defenses.

The Ponemon Institute 2017 State of Endpoint Security Risk report opening includes the phrase, "endpoint security is breaking down." According to 665 information security professionals surveyed by Ponemon, some 69 percent agreed that "endpoint security risk to our organization has significantly increased."

from your organization. A clever phishing attack might try to entice a business partner into transferring funds to a fraudulent bank account.

"The question is: do they know the response process when someone pretends to be a Motorola employee," Rushing says. "We know that is phishing — it has Motorola spelled with a zero. It's not ours, but someone else's monetary loss."

File-less email attacks in general and phishing, in particular, allow hackers to do an endrun around cybersecurity defenses. Yet the regular review and upgrade of security tools for email cannot be neglected. Small and medium-size businesses can, like their enterprise-class counterparts, avail themselves of email security services for on-premises or cloud offerings.

What's more, various cloud-based vendors offer ways to corral inbound email for inspection for malware, knock down all or specified file types attachments and insert an unsubtle warning banner on every email that originates outside the organization.

When suspicious emails do get diverted to incident response teams, another set of tools can come into play. Containment, URL inspection, comparisons to previous attacks, and analysis are common elements of an incident response playbook.

"Thanks to logs, sandboxes, and web scrapers, the security operations center (SOC) has the ability to get most of the data needed to search if the user browsed to the site or if something contains malware," says Xena Olsen, a cyber threat intelligence analyst at a Chicago-based Fortune 500 financial services company.

"If the sandbox comes back with inconclusive results the threat intel team or another team that does reversing can find the indicators of compromise to search in the environment. Then DFIR (digital forensics and incident response) just has to review the base analysis and remove the email from the user or potentially reimage the machine, reset corporate credentials, and follow the rest of the DFIR process."

It does not always go quite as smoothly as that, Rushing points out. Auto-forwarding suspicious emails to incident response can sometimes lose header information that is critical to forensic specialists. And if the tools are not configured correctly, valid emails can be blocked due to their resemblance to their spoofed counterparts.

Is encryption the answer? (Story continues below)

design decision made early in the history of the Internet. The Simple Mail Transfer Protocol (SMTP), the Internet protocol for email, was designed to make it easy for computers to send and receive messages, even if information was incomplete or corrupt."

Encrypted emails are often seen as the best means to mitigate the inherent risks of SMTP. But the difficulties in training users to handle encryption and the technical overhead has led many organizations to conclude that the use cases for such technology is limited. "We've set up secure mail tunnels between our servers and those of our best trading partners, so those messages will not travel un-encrypted over the Internet," says Joe Rickard, CTO and CISO at Incapital, a Chicago-area bond-trading firm.

Anthony Scarola, security consulting senior manager with Accenture and a former financial services CISO and CIO from Virginia now based in Cincinnati, makes a similar point. "Recipients' email systems may not support [encryption] due to incompatibilities, or solutions may burden clients to the point of frustration," he says. "For organizations like financial, insurance and others with highly sensitive or regulated information to protect, this can be addressed by notifying clients of new messages via email or text and offering them options" for secure links using multi-factor authentication and encrypted Internet connections via SSL/TLS.

For Rushing, encrypted email has its place "in a certain portion of our supply chain that is deemed critical." But the training required for the use of encrypted email discourages the organization from a more generalized deployment of encrypted email. "I can train all or some of my users to do this, but it is a daunting task," he says.

In Olsen's view, widespread adoption of encrypted email will come only if and when web

and phishing remains the end user, whatever their level of cybersecurity awareness or technical proficiency, the experts agree. Despite the tens of billions of dollars spent on cyber tech over the past decade, user training remains at the core of cybersecurity in 2018.

Time to test

Cybersecurity awareness training is now standard at a growing number of large organizations today. Their effectiveness is another matter entirely. In some cases, there is no way to gauge whether end users skip through training as quickly as possible to comply with policy without internalizing basic points, nor is there any way to differentiate those who speed through the material because they are technically savvy from those who rush because they feel overwhelmed and intimidated. Online training, PowerPoint slides, memos and lengthy documents might contain all the key points highlighted in attractive formatting, but it is difficult to judge users' ability to retain that information when they confront a suspicious email.

To better focus employee attention on email security, some large organizations are increasingly resorting to penalties for employees who repeatedly click links on phishing training emails.

"A quick way to increase user awareness is by instituting a companywide policy for employees that click on phishing campaigns generated by the company, up to and including losing their job, because they clicked on too many phishing emails," says Olsen. "If the employee has direct ramifications for clicking they tend to be more careful about what they do. Cultivating a vigilant culture in the workplace can ultimately result in fewer phished corporate credentials and compromised machines."

levels were brown and black belts; those who earned such designations were expected to forge relationships and mentor others.

While the technology skill level at Cisco might well be far above the average for non-technical organizations, the methodology can be adopted by smaller organizations without the Cisco's staff technical expertise. For example, cybersecurity awareness training can gain buy-in from users by including issues that they must cover in their personal lives, such as secure practices on social media, managing passwords and securing home internet access.

The more employees internalize sound cybersecurity practices throughout their lives, the easier it can become to convey the must-dos for email security and other information management issues.

Yet even if users can be drawn into a discussion of email security based on their personal concerns, there remains the challenge of focusing on such issues as they carry out their daily tasks. That is why it helps to make email security training as outlandish as possible, says Accenture's Scarola.

"I have seen and even participated in both very active, and very passive campaigns over the years," he says. "One of the best I've seen was from a small insurance organization whose CISO, a very passionate leader, would dress up like a fish on occasion and walk around the office, reminding employees of the best-practices for detecting socially-engineered emails and how to best handle them."

Of course, a CISO at a multinational organization might not carry the same gravitas in a

attacks. "The bad guys know our schedule. It is between 6:30 am and 8 am when most [phishing attempts] come in, based on time zone. That is where people are in a hurry," and most vulnerable to an email attack, such as an invitation to take action on a fake UPS delivery, he says.

Once assembled, the elements of email security in a medium or large organization look something like this: a set of policies and procedures developed by information security professionals and backed by C-level authority; a systematic and ongoing cybersecurity awareness training program with email security at center stage; a set of tools to detect and block threats and an incident response team poised to parse threatening emails; and — most important — users who are increasingly confident in their ability to spot suspicious emails, from scam personal offers, fake invoices or embedded links to ransomware.

There is a long way to go. Humans are the low-tech, weak link in the long chain of cybersecurity complexity. Yet unless and until we are better able to detect email-based threats and take appropriate actions, phishing will remain an ominous threat. Email security, once considered yesterday's problem, remains a critical cyber challenge of today.

Can email security culture go too far?

Cybersecurity awareness trainers seek to maximize email security awareness. But sometimes their very success cause problems downstream as incident response teams grapple not just with phishing, but legitimate emails mistakenly deemed suspicious.

Sometimes innocuous emails end up in automated phishing-flagging tools as users trained to be skeptical of good-news messages click to forward messages from company HR or executives straight to cybersecurity incident response team, kicking off an often time-intensive investigation of an email about an employee incentive program.

A key issue, says Motorola Mobility CISO Richard Rushing, is that "there is a difference between phishing, spam, and a third party email compromise. Each has its own security channels, but it all goes into the same phishing" category, he continues.

A typical DFIR (digital forensics and incidence response) team would almost certainly prefer to wade through false positive phishing emails then take up battle stations to contain ransomware or overcome a DDoS (distributed denial of service) attack. But systematic phishing attempts and a flow of legitimate email from overly vigilant users combine to create a "time sink" for incident response staff, Rushing says.

If users do shift from laxity to overkill to their attempts to spot phishing, it is because humans are inherently unreliable in detecting phishing, says, Abhishek Vyas, security solutions architect at the Coventry Building Society in Coventry, England.

"The social engineering spectrum — phishing, vishing, smishing — is based on an emotional response," Vyas says. "It calls out, 'this is urgent.' As a result, trying to drive an outcome based on user training alone is nonsensical." Phishing, he says, must be discredited by technical means.

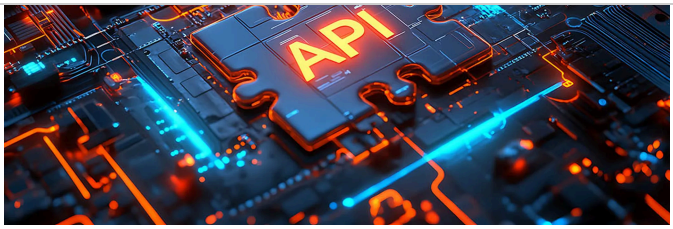
But even sophisticated cyber pros with all their tools cannot assume that with phishing, they always know 'em when they see 'em. The best resource for incident response teams

buy/lease and too expensive to implement," he says.

For that class of users, there is no such thing as overactive email vigilance, he says. "Companies need to have a strong internal or external partner evangelist to convince, prod, poke, and just push them into making it a priority." —LS

Lee Sustar

Related



detailed

SC Staff January 3, 2025

Power Platform's OData Web API Filter was impacted by two of the discovered security issues, the first of which stemmed from inadequate access control that enabled access to sensitive data and potential exploitation to obtain complete hashes while the other bug arose from orderby clause utilization in the same API to gather needed database information.

CRITICAL INFRASTRUCTURE SECURITY

Treasury's sanctions office reportedly subjected to Chinese hack

SC Staff January 3, 2025

Officials revealed that the department's Office of Financial Research had also been infiltrated as part of the incident, which was noted to have stemmed from an attack against the agency's implementation of the BeyondTrust remote support software-as-a-service platform in a disclosure to Congress earlier this week.

APPLICATION SECURITY

Apple to settle claims Siri collected user data without permission

Shaun Nichols January 2, 2025

Tech giant will be paying out a $95 million settlement

Related Terms

Adware

Banner

Browser

Cache Cramming

Common Gateway Interface (CGI)

Client

Cookie

DLL Injection