BIZCOMMUNITY

Why IT security experts feel unprepared for email attacks

By Simeon Tassev

11 May 2016

IT security experts are feeling increasingly unprepared and too out-of-date to reasonably defend against email-based threats, with a late 2015 finding that only 35% of its respondents were confident of their preparedness to deal with email attacks.

The global study, created by Mimecast and March Communications, surveyed 600 IT security decision makers - 200 from the United States of America, 200 from the UK, 100 from Australia and 100 from South Africa. The focused on companies' level of email security, IT preparedness and confidence in defending against cyber threats, as well as past experiences with data breaches and email hacks.

It found that of the 65% of respondents who felt unprepared against email attacks, almost half had experienced such attacks in the past. Yet, despite their history dealing with the issue, they felt no more protected after an attack than they did before.

These findings are disconcerting in view of the fact that email is a vital tool in business and yet, while we might appreciate the danger it poses, many companies are still not taking strong enough measures to defend against email-based threats. One-third of the respondents of the Mimecast study also believe email is more vulnerable today than it was five years ago.

Popular attacks

Phishing, whaling and ransom are the three most popular attack methods. In phishing, the attacker sources confidential information such as user names, passwords and credit card information by means of mass electronic communications to potential targets. The mass mailing appears to be from a trustworthy source, such as a financial institution.

A whaling attack is where specific individuals who perform strategic tasks within in a company are targeted in a more structured way for maximum financial gain. A whaling target may receive an instruction from what seems to be a trusted source, like the chief executive officer or a known customer, urging them to make a payment to a fabricated invoice. The attacker counts of the target doing what seems to be their job and fulfilling the request. Targets may include prominent and wealthy personalities, senior executives in global enterprises, and commonly, financial institutions.

Ransom is where attackers infect the target's network with a virus and then threaten to destroy the company's data or to publicly release confidential client data unless the company pays a specified amount or do a certain task. The recent spate of data leak stories in the media to show how well this tactic is working for attackers.

Why email remains vulnerable

Most companies have email security controls in place. However, the lightning-fast evolution of email attacks, the ubiquitous need for email in business and human factors mean that traditional IT security protections are not nearly enough to protect them.

Fast evolution of attacks: The ransomware development trend is a good indicator of how fast malware is being developed. To illustrate, the popular Cryptowall ransomware was first seen in March 2014. The next version was released six months later, with the third version released three months later and the fourth version released after only months. Clearly the time between updates has been getting shorter, indicating that companies must adapt more quickly to deal with current threats and prepare to deal with threats they don't even know about yet.

Bring-your-own-device policy bites: The popular policy for employees to use their own devices, such as smartphones, for portions of their work poses a great risk to email security. While the policy reduces the employer's investment in hardware, the traditional way of controlling employees' email fails, as it becomes harder for the employer to control what employees can do on their own devices.

Employees a big security threat: Employees are also prone to click on unknown email links and attachments on their devices, providing a gateway for viruses into the network. Unfortunately, it's difficult for companies to quash this practice, as the Basic Conditions of Employment Amendment Act of 2011 provides that an employer needs to take certain remedial measures before firing an employee.

To counter this vulnerability, companies need to not only put clear email security measures in place, but to ensure that employees are fully aware of what they can and they can't do with their emails, the consequences of risky behavior on the company's data and any punitive measures the company may take. This acts as a deterrent for employees who willfully disregard the company's IT security measures by claiming ignorance.

Key strategies

Email security should be customised to fit the way email is used within the company's operations. However, there are some basic principles that apply across board:

C-suite involvement critical: Email attacks are not just an IT problem; they can harm the entire business. And while email security was traditionally the province of the IT department, the growing risk it represents to the business means that the company's CEO, COO and CIO need to be strongly engaged with security initiatives and to collaborate to ensure that the business is adequately protected. The Mimecast research supports this view. It found that the top 20% of organisations that

felt the most secure against email attacks were also 250% more likely to see email as their biggest vulnerability. It also found that confident IT security managers were 270% more likely to be from companies whose top executives very engaged in email security.

Adopt zero-day approach: IT professionals need to start talking more about zero-day (0day) approach to email attacks, where IT security prepares not just for threats they have previously come across but for unknown attacks. The 0day refers to the amount of time the company has to respond to a newly discovered and/ disclosed threat.

Install filtering and end-point tools: Filtering solutions are the first level of defense against email attacks. This involves the installation of a program that scans all email for threats, spam and viruses, filtering email in the cloud or, if the email server is on the premises, via a firewall gateway. These systems now also scan attachments for malware and validate web links to prevent phishing attacks.

End-point protection must also be installed on all employee devices, including personal devices that have some overlap with business functions. Email protection also includes protection against human error. Such errors include sending a confidential email to a group rather than an individual. This ensures that confidential emails are sent targeted to recipients who hold a qualifying security level.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa
- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...