3 Email Security Threats and How to Safeguard Your Business in 2020

Email security threats play a major role in the cyber battleground. In fact, most companies report they encountered email-based attacks in the past year. In addition, CSO Online reports that 92 percent of malware finds its way into the network via email.

To protect their business and their customers, organizations need to anticipate email security threats and develop corresponding strategies. Experts predict that for 2020, major threats to email cyber security will include spear phishing, cloud-targeting ransomware and insufficient password measures.

Spear Phishing

Phishing attacks remain the primary cause of data breaches. In these attacks, criminals pose as legitimate business entities in order to trick users into sharing sensitive information. Spear phishing takes this a step further by introducing a high degree of personalization to target specific users.

For example, American company Ubiquiti Networks, Inc. lost millions in a successful spear phishing scheme. An attacker impersonating an employee submitted fraudulent requests to the company's finance department using addresses and domains that appeared legitimate. As a result, Ubiquiti employees transferred $46.7 million to an outside entity.

Ransomware Focused on the Cloud

While cyber criminals have used ransomware for several years, they have evolved their approach over time. Attacks have become more targeted, focusing on businesses that depend on constant access. In addition, experts believe that cyber attacks will move to the cloud in 2020.

If attackers gain access to a cloud services provider, the fallout can affect multiple customers. And unless the organizations involved store backups completely offline, the attack may affect the backups necessary for the recovery process.

Unfortunately, many businesses have not adjusted their security practices to fully address the cloud environment. Organizations erroneously assume that the cloud services provider will handle all cyber security, not understanding the shared responsibility model for cloud security.

Poor Password Hygiene

For years, security experts have warned users to employ strong passwords. And yet, we continue to re-use the same passwords over and over again. A recent survey suggests that the average user operates nearly 30 different online accounts, though my own count reaches closer to 100. No wonder we pale at the task of remembering unique passwords for each account!

Cyber criminals know this, and they exploit that dilemma. With lists of compromised credentials from previous attacks, attackers gain access to other sites. For instance, a hacker may breach the security of a small business, gaining access to passwords that they can then use on other accounts, such as Amazon.

Strategies to Counter Email Security Threats

Sophisticated email security threats require a multi-faceted cyber security strategy. To guard against prevalent threats, include measures like the following in your overall plan of attack:

- **Update email filters** – Use a high-quality spam filter. In addition, since a majority of phishing emails originate from a small block of countries, consider blocking emails with an IP address from those countries.
- **Multi-factor authentication** – Add an extra layer of security by implementing multi-factor authentication (MFA) throughout the organization. With MFA, an attacker cannot access an account with just a password. The system will also require another form of identification, such as a code or a biometric sign-on.
- **Implement cloud-native security** – Migrating to the cloud introduces new challenges to security that traditional strategies do not adequately cover. From firewalls to anti-malware, choose security solutions built for the cloud.
- **Employ artificial intelligence and machine learning** – Advanced threat detection solutions that employ machine learning work by analyzing communication patterns within the organization. When the system detects an anomaly, it sends an alert and automatically implements safety measures.
- **Cyber security training** – Any security strategy must include regular cyber security awareness training for employees. As users learn to recognize and report suspicious activity, they can avoid costly mistakes.

Take Control of Email Security Now

The aftermath of an attack is no time to start thinking about security. Take control of email security now to both protect your business and achieve regulatory compliance. The email security experts at Messaging Architects will guide you through the process of incorporating the tools and the policies that you need.