Cyberattack Study

Business E-Mail Compromise Scams Top Threat

BUSINESS E-MAIL compromise scams are now the most common type of cyberattack businesses face, and all types of these attacks are showing no signs of letting up, according to a new report.

Nearly three out of every four businesses were targets of these attacks and 29% of those firms became victims of successful attacks, according to the report by Arctic Wolf, a cyber-security firm..

While this has become the most common type of attack, a number of other schemes like ransomware attacks and data breaches continue growing in number.

Any of these attacks can drain a company's finances and result in tricky legal and possibly reputational issues that take time and money time to resolve.

The trends

The main threats businesses face, according to the report, are:

Business e-mail compromise (BEC) – Seven in 10 organizations surveyed said they had been targeted by these types of scams.

Some examples of BEC attacks include impersonating company executives to request wire transfers, falsifying invoice payment details, and tricking employees into revealing sensitive information. These scams can result in significant financial losses for businesses.

CAUTION: For businesses that use cloud-based e-mail services like Office365, these attacks are hard to detect since they don't reside on company servers.

With many organizations moving to cloud-based e-mail services, these types of attacks can be difficult to identify with traditional security tools and may go undetected until they have successfully executed their objectives.

Data breaches – Nearly half (48%) of organizations surveyed reported that they'd found evidence of a breach in their systems. The authors said that does not mean that the other 52% didn't suffer a breach; it means they failed to find evidence of one.

Ransomware – Some 45% of organizations surveyed admitted to being the victim of a ransomware attack within the last 12 months. These attacks usually involve criminals gaining access to a company's systems by getting an employee to click on a malicious link, after which they lock down the system and demand a ransom to unlock it.

Increasingly, perpetrators are also stealing data and demanding a second ransom to give it back and not release the data to others.

What you can do

How to Protect Against BECs

- Register all domain names that are similar to the business's legitimate website and can be used for spoofing attacks.
- Create rules that flag e-mails received from unknown domains.
- Monitor and/or restrict the creation of new e-mail rules on your servers.
- Enable multi-factor authentication.
- Conduct BEC drills, similar to anti-phishing exercises.
- Companies that use Office 365 or other cloud-based e-mail services, should employ detection tools or services specifically designed to monitor for threats related to BEC scams.

To combat ransomware:

Regularly back up system. Verify your backups regularly. This way you can restore functions if hit by ransomware.

Store backups separately. In particular, store backups on a separate device that cannot be accessed from a network, such as on an external hard drive.

Training your staff. Train your staff in how to spot possible phishing e-mails that are designed to convince an employee to click on a malicious link that will release the ransomware. ❖