RSM

Corporate account take over in cybercrime

My company frequently received strange emails from unknown sender; do any of those pose threat to my organization? Should there be any risk management or control measures need to be considered?

Nadiem, Jakarta

Strange email from unknown sender could be simply junk or it could be malicious. If its malicious, then it pose risk to the organization.

Cyber criminals are targeting the financial accounts of owners and employees of small and medium sized businesses, resulting in significant business disruption and losses. This is a fraud scheme known as "corporate account take over". A guideline on corporate account takeover issued by US Secret Service, Federal Bureau of Investigation, the IC-3 and FS-ISAC addressed this problem.

To obtain access to financial accounts, cyber criminals target employees – often senior executives or accounting and HR personnel and business partners and cause the targeted individual to spread malicious software (or "malware") which in turn steals their personal information and log-in credentials. Once the account is compromised, the cyber criminal is able to electronically steal money from business accounts.

Cyber criminals also use various attack methods to exploit check archiving and verification services that enable them to issue counterfeit checks, impersonate the customer over the phone to arrange funds transfers, mimic legitimate communication from the financial institution to verify transactions, create unauthorized wire transfers and payments, or initiate other changes to the account. In addition to targeting account information, cyber criminals also seek to gain customer lists and/or proprietary information that can also cause indirect losses and reputational damage.

How it is done?

Cyber criminals employ various technological and non-technological methods to manipulate or trick victims into divulging personal or account information. Such techniques may include performing an action such as opening an email attachment, accepting a fake friend request on a social networking site, or visiting a legitimate, yet compromised, website that installs malware on their computer.

How to manage it?

There are 3 steps to take: Protect, Detect, Respond.

Protect. Educate everyone on this type of fraud scheme. Don't respond to or open attachments or click on links in unsolicited e-mails. Be wary of pop-up messages claiming your machine is infected and offering software to scan and fix the problem. Enhance the security of your computer and networks and enhance the security of your corporate banking processes and protocols.

Detect. Monitor and reconcile accounts regularly and note any changes in the performance of your computer such as dramatic loss of speed, unexpected rebooting, new toolbar or icon. Pay attention to warnings on potential viruses and check your outbox folder to look for email that you did not send. Run regular virus and malware scans on your computer hard drive.

Respond. If you detect suspicious activity, cease all online activity and disconnect your network connections to isolate your computer from jeopardizing the entire corporate network. Assign a function within your company that is responsible to manage this issue and make sure that your employees know how and to whom to report on this. It is also advisable that your organization have a contingency plan that cover resolutions for a system infected by malware, data corruption, and catastrophic system/hardware failure.

KEY POINTS

- Cyber criminals target employees to spread malware which in turn steals their personal information and log-in credentials.
- Protect your organization by designing and executing appropriate internal controls to manage your network security. Socialize the procedures to all employees and monitor it periodically.
- Have a contingency plan to recover systems suspected of compromise.

Angela Simatupang
Partner
Governance Risk Control
angela.simatupang@rsmindonesia.id

RSM Indonesia
Audit | Tax | Consulting

THE POWER OF BEING UNDERSTOOD