span

Business E-mail Compromise

E-BOOK

MIHAELA
Trbojević
MEMBER OF THE MANAGEMENT BOARD AND CPO

NEVEN
Zitek
CYBER SECURITY BUSINESS SOLUTIONS DIRECTOR

September 2024

Business E-mail Compromise (BEC)

Business E-mail Compromise (BEC) is a sophisticated type of cybercrime that targets companies and individuals who conduct wire transfers and have access to sensitive financial information. Unlike traditional phishing attacks, BEC involves using social engineering tactics to trick victims into revealing confidential information or making unauthorized financial transactions.

How BEC Works

BEC attacks typically follow a series of steps:

Research: Cybercriminals identify a target organization and gather information about its employees, particularly those in finance or executives with the authority to approve payments.

Identity Theft: The attackers use various techniques to impersonate a trusted individual within the company. This could involve hacking E-mail accounts, creating look-alike domains, or using spoofed E-mail addresses.

Exploitation: Using the stolen or spoofed identity, the criminals send convincing E-mails to employees, instructing them to transfer funds, reveal sensitive information, or change payment details.

Monetization: Once the victim complies, the stolen funds are quickly transferred to bank accounts controlled by the attackers and often moved through a series of transactions to obscure the money trail.

Consequences of Business E-mail Compromise

Business E-mail Compromise (BEC) can have severe and far-reaching consequences for organizations. The financial impact is often the most immediate and obvious, with companies losing substantial amounts of money through fraudulent transactions. However, the damage extends beyond mere monetary loss.

Financial Loss:
Organizations can face significant financial damages, often amounting to millions of dollars, which can disrupt operations and jeopardize financial stability.

Reputational Damage:
The breach of trust that results from a successful BEC attack can tarnish an organization's reputation. Clients, partners, and stakeholders may question the organization's ability to protect sensitive information, potentially leading to lost business opportunities and damaged relationships.

Legal and Regulatory Consequences:
Depending on the jurisdiction and the nature of the compromised data, organizations may face legal actions and regulatory fines. Non-compliance with data protection laws can result in penalties and increased scrutiny from regulatory bodies.

Technical Measures to Prevent BEC

Given the sophisticated nature of BEC attacks, implementing robust technical measures is crucial in safeguarding organizations against such threats.

Here are recommended effective strategies where Span can help in the prevention of BEC:

Multi-Factor Authentication (MFA):
MFA is a powerful security measure that requires users to provide two or more verification factors to gain access to their accounts. This could include something they know (password), something they have (security token), or something they are (fingerprint). By adding an extra layer of security, MFA significantly reduces the risk of unauthorized access to E-mail accounts.

Risk-based reactions:
Taking proactive measures to mitigate suspicious login patterns and increased sign-in risks such as impossible travel, password leaks, and similar by disabling accounts, requiring password resets, or blocking access to sensitive resources.

E-mail Monitoring and Anti-Phishing Tools:
Implementing advanced E-mail monitoring solutions can help detect and block phishing E-mails before they reach employees' inboxes. Anti-phishing tools use machine learning algorithms to identify and quarantine potentially malicious E-mails, reducing the likelihood of successful BEC attacks.

Domain-Based Message Authentication, Reporting, and Conformance (DMARC):
DMARC is an E-mail authentication protocol that helps prevent E-mail spoofing by verifying the sender's domain. Implementing DMARC can help organizations monitor and block unauthenticated E-mails, ensuring that only legitimate E-mails reach their intended recipients.

Endpoint Protection:
Ensuring that all devices within the organization are equipped with up-to-date antivirus and anti-malware software can help detect and prevent malicious activities. Endpoint protection solutions provide an additional layer of defense against BEC attacks by safeguarding devices from being compromised.

Data Loss Prevention (DLP):
Implementing DLP solutions can help organizations monitor and control the transfer of sensitive data. DLP technologies can detect and prevent the unauthorized sharing of confidential information, ensuring that data does not leave the organization without proper authorization.

Encryption of Confidential E-mails:
Encrypting sensitive E-mails adds a robust layer of security by ensuring that only intended recipients can access the content. This measure is particularly important for preventing unauthorized access during E-mail transmission, thereby protecting sensitive information from interception by malicious actors.

Span Security Operations Center (SOC):
SOC can help continuously monitor, detect, and respond to security incidents. A SOC team utilizes advanced tools and technologies to identify suspicious activities and cyber threats in real time, enabling quick mitigation of potential BEC attacks.

Span Cyber Security Center Education and Training:
Cybersecurity awareness programs are vital in educating employees about the risks of BEC and the best practices to prevent them. Regular training sessions should cover recognizing phishing E-mails, verifying unusual requests, and following procedures for reporting suspicious activities.

Regular Security Audits:
Conducting routine security audits can help identify vulnerabilities and ensure that cybersecurity measures are up to date. Audits should include reviewing access controls, assessing E-mail security protocols, and testing the effectiveness of implemented security measures.

How to start?

Span comprehensive cybersecurity assessment will help identify the organization's current security posture and areas of vulnerability. This assessment involves several key components:

Evaluation of Existing Security Measures:
Review the current security protocols and tools in place, such as general sharing settings, antivirus software, and encryption methods. Assessing effectiveness and identifying any gaps in current configuration compared to vendor security recommendations and agnostic security frameworks.

Detection of Potential Vulnerabilities:
Conducting vulnerability scans and penetration testing to detect weaknesses in the system that could be exploited by attackers. This includes evaluating the security of E-mail systems, network infrastructure, and endpoints.

Review of Access Controls:
Ensuring that access controls are properly configured to limit the ability of unauthorized users to access sensitive information. This includes verifying the use of strong passwords, multi-factor authentication, and role-based access controls.

Employee Training and Awareness:
Assessing the current level of employee awareness regarding cybersecurity threats and best practices. Determining the need for additional training programs to educate employees about recognizing and responding to BEC attempts.

Policy and Procedure Review:
Reviewing and updating the organization's cybersecurity policies and procedures to ensure they are aligned with industry best practices and regulatory requirements. This includes incident response plans, data protection policies, and E-mail security protocols.

Technology Assessment:
Evaluating the effectiveness of current security technologies, such as E-mail filtering and anti-phishing tools.

By conducting a thorough cybersecurity assessment as a first step, organizations can identify and address potential vulnerabilities, strengthen their defenses against BEC, and develop a robust strategy for ongoing security management.

Contact us at
info@span.security

to schedule your comprehensive cybersecurity assessment and take the first step in preventing Business E-mail Compromise.