CYBER WARDEN

PRACTICAL CYBER RISK MANAGEMENT

The Dangers of Business Email Compromise (BEC)

Business Email Compromise (BEC) is a sophisticated scam targeting businesses and individuals who perform legitimate transfer-of-funds requests. It is a form of cybercrime that can have devastating financial and reputational consequences for businesses of all sizes. Understanding the dangers of BEC is crucial for protecting your organization.

What is Business Email Compromise?

BEC involves cybercriminals gaining access to a business email account and using it to deceive employees, customers, or partners into transferring money or sensitive information. These attacks often involve impersonating a high-ranking executive or a trusted vendor. The goal is to trick the recipient into believing the request is legitimate and urgent.

Financial Losses

The most immediate danger of BEC is financial loss. Cybercriminals often request large sums of money to be transferred to accounts they control. These transfers can be difficult to reverse once completed. According to the FBI, BEC scams have resulted in billions of dollars in losses globally. Even a single successful attack can have a significant impact on a company's finances.

Reputational Damage

In addition to financial losses, BEC can severely damage a company's reputation. Customers and partners may lose trust in a business that falls victim to such scams, and may also become targets of BEC due to the attacker being able to copy the writing style, email signatures, etc of the follow-on victim, as well as gaining significant insight into business relationships. This loss of trust can lead to a decline in business opportunities and long-term damage to the brand. Rebuilding a tarnished reputation can be a costly and time-consuming process.

Legal and Regulatory Consequences

Businesses that fall victim to BEC may also face legal and regulatory consequences. Depending on the nature of the compromised information, companies may be required to report the breach to regulatory bodies and affected individuals. Failure to comply with these requirements can result in fines and other penalties. Additionally, businesses may face lawsuits from customers or partners who suffer losses due to the breach.

Operational Disruption

BEC attacks can disrupt normal business operations. Employees may need to spend significant time and resources addressing the fallout from the scam. This can include

investigating the breach, communicating with affected parties, and implementing new security measures. The disruption can lead to decreased productivity and increased operational costs.

How to Protect Your Business

1. **Employee Training**: Educate employees about the risks of BEC and how to recognize suspicious emails. Regular training sessions can help keep security top of mind. Contact us for more information on how we can help at https://cyberwarden.io/contact/
2. **Email Authentication**: Implement email authentication protocols such as SPF, DKIM, and DMARC to help prevent email spoofing. See https://cyberwarden.io/services/aegis.php for how we can help with this.
3. **Implement Mail Filtering** to stop most email phishing and malware attacks. See https://cyberwarden.io/services/aegis.php for how we can help with this.
4. **Be Aware Of Supply Chain Vulnerabilities**. Although your business may have implemented technical controls such as DMARC and Strong Authentication, you may be attacked by someone in your supply chain. Contact us for more information on how we can help at https://cyberwarden.io/contact/. You can also check the DMARC, SPF, DKIM, and MTA-STS status of your supply chain at https://cyberwarden.io/tools/sc_recon.php
5. **Verification Procedures**: Related to the above point, establish procedures for verifying the authenticity of email requests for financial transactions. This can include requiring a second form of verification, such as a phone call. This should be implemented as part of a company wide set of procedures & policies that align with common frameworks such as NIST CSF 2.0 and ISO 27001. Contact us for more information on how we can help at https://cyberwarden.io/contact/
6. **Secure All Accounts**: Enable strong authentication for all user accounts, utilizing multi-factor authentication (MFA) or Phishing Resistant Authentication (when available) such as Passkeys to add an extra layer of security. See https://cyberwarden.io/docs/enable-entra-sec-defaults.pdf. Remember that ALL accounts need to be protected, especially those that provide access to customer systems or data.
7. **Monitor and Respond**: Regularly monitor email accounts for signs of suspicious activity and have a response plan in place in case of a breach.

Conclusion

Business Email Compromise is a serious threat that can have far-reaching consequences for businesses. By understanding the dangers and implementing robust security measures, companies can protect themselves from falling victim to these sophisticated scams. Staying vigilant and proactive is key to safeguarding your organization's financial health and reputation.