Business Email Compromise

Email scams targeting companies who conduct wire transfers and have suppliers and partners abroad

In 2019, more than US$26 billion was lost globally due to Business Email Compromise (BEC).

BEC is a type of phishing that attempts to fraudulently obtain passwords, credentials, credit cards, or even money. It usually comes in the form of a URL or link that when clicked leads to a fake page where unsuspecting victims enter their details which are then used by the attackers to perpetrate the crime.

Hacked Sydney hedge fund part of $170m cyber crime spree

***Taken from Australian Financial Review, Nov 24th 2020.**

Victims are tricked into handing over sensitive information to attackers who then use this information to compromise accounts, or gain unauthorised access to your network. However this type of cyber crime is not instant. Attackers can spend months gathering information and collect intelligence on their victims right up to and during the exploitation. Once the email is compromised, the attacker may impersonate the individual, attempt to defraud or even steal sensitive information and data.

Other types of BEC attacks include:

- **CEO/Chairman Fraud**: The criminal impersonates a high level employee at the company by compromising their email accounts or spoofing their email from another domain. They then request a funds transfer from CEO or Chairman to the CFO or another staff member with funds authority.
- **Invoice Fraud**: A business is contacted by criminals impersonating their supplier. They request to wire funds payment to an alternative fraudulent bank account. The request may be made from post, telephone, email or facsimile.
- **Account Compromise**: This can be used against targets other than internal employees. Criminals can send requests for invoice payments to multiple vendors in the victim's address book. The funds are then requested to be paid to a fraudulent account.
- **Attorney or Government Official Impersonation**: Criminals impersonate lawyers and/or government officials and state they are handling time sensitive matters requesting urgent payment. This typically happens at the end of day or week. Victims are persuaded to make the payment in haste and often in secret or suffer consequences.
- **Data Theft**: A compromised internal executive's email account is used to request sensitive payment or personally identifiable information (PII). Criminals will target the CEO, HR or even Audit functions.

Signs to be aware of:

- 30% of BEC emails use the word "payment" in the email subject
- Many require an urgent task of some kind
- Always required to circumvent standard procedures

In a particular case, the inbox of both the CEO and their personal assistant was compromised where all emails received by these individuals was automatically forwarded to an attacker for six months. The reputation damage alone can be significant. The loss due to confidential information being released is undefined.

At Tannhauser, we can assist with the following to reduce your attack surface and reduce the likelihood of an incident occurring:

- Perform a risk assessment to determine how susceptible you are to a BEC attack
- Arm your staff through awareness training to know what to look for
- Conduct a phishing exercise to test your people, process and technology controls
- Confirm open corporate culture allows suspect events to be reported immediately
- Train staff to use "out-of-band" confirmation (phone call, text message)
- Review your email system security configuration (including forwarding and redirection rules)
- Implement technical controls (multi-factor authentication, strong passwords, automatic updates and patches, set-up and regular back-ups are configured)
- Configure Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC) for added protection against spoofing and phishing.
- Table top crisis exercises to train staff how to respond to a cyber incident. Help prepare a cyber security emergency plan and training so that your staff know exactly what to do in the event of an attack.

Further guidance to defend against a BEC attack is available from the Australian Cyber Security Centre (ACSC): Protecting Against Business Email Compromise
https://www.cyber.gov.au/acsc/view-all-content/publications/protecting-against-business-email-compromise