Case Study: Business Email Compromise

Our client became aware of fraudulent activity when following up with their customer regarding a sum they had yet to receive.

The Challenge

A health service provider engaged Avalon to conduct a cyber incident investigation related to an alleged business email compromise (BEC) that resulted in an unauthorized transfer of funds of approximately $300,000.

Our client became aware of fraudulent activity when following up with their customer regarding a sum they had yet to receive. The customer indicated that payment had been made to the updated bank account, which had been recently provided by an employee of our client. Our client immediately realized that fraudulent communication must have occurred.

The Strategy

Avalon was engaged to perform an analysis to determine:

- The anomalous or suspicious activity occurring within our client's employee's M365 account
- The extent of compromise in the client's M365 tenant
- Whether an unauthorized third party may still be present within the client's M365 tenant

Based on the review of the available and collected data, Avalon identified artifacts indicating that an unauthorized third-party was indeed able to gain access to the employee's M365 account.

Our client's employee had received a phishing email containing a malicious attachment, had clicked on the attachment, and ultimately divulged their credentials. The unauthorized third-party was then able to successfully gain access to the employee's M365 account, perform reconnaissance on the mailbox, craft fraudulent email communications with the customer, and create mailbox rules to obfuscate this communication from the employee which ultimately resulted in the fraudulent transfer of funds.

The Results

Our investigation, which ultimately confirmed that the inappropriate access occurred from our client's end, was needed for our client to continue doing business with this customer and likely needed for insurance purposes as well.

Case Study: Business Email Compromise

Don't miss out on more free content from Team Avalon!

Join the Avalon mailing list to receive useful case studies, industry insights, handy tips, and more delivered straight to your inbox.

Sign up to receive exclusive content!

Avalon: Your Battle-Tested, Full Service MSSP

Arm your organization in the fight against cyberattacks by partnering with the experts at Avalon. Our expertise in digital forensics and incident response (DFIR) stems from years of experience performing some of the most complex cyber investigations across the globe.

Through our proactive and reactive cyber services, we help businesses identify and manage cyber risk and assist them in prioritizing their response to prevent cyber incidents from occurring. Whether we're conducting a vulnerability assessment, providing security advisory services, or initiating incident response, we provide a five-star experience and unwavering support throughout the engagement.

QUESTIONS?

For more information on any of our services, please contact:

Rebecca Rudell, Marketing Manager
rebecca.rudell@teamavalon.com