Mailbox Compromised to Intercept Bank Account Payments

networkdoctor
IT SOLUTIONS & SERVICES

The Breach

We received an alert generated by our Microsoft 365 monitoring agent regarding a suspicious sign-in to a client's account from an unauthorized country. It appears the attackers gained access to the employee's account through a phishing attack and obtained the user's password.

Malicious emails were sent from the account to vendors and customers attempting to persuade them to send payments to the attacker's bank account. The hackers created mailbox rules to reroute and delete inbound messages in order to control responses from the user's contacts.

The Response

Upon receiving a notification from the Security Operations Center (SOC), our engineers jumped on it right away to sever unauthorized connections to the mailbox and safely restore access for the client. The user's password was reset, and the client approved a previously made recommendation to enable MFA (multi-factor authentication) for all employees to mitigate these types of exposures.

Mailbox rules created by the attackers were disabled. The phishing email was analyzed and any related addresses or links were blocked from the network. Finally, we scanned the employee's device to ensure no malicious software was running or suspicious files were installed.

The Silver Lining?

Unscathed, the client learned an important lesson and now their environment is significantly more secure. This incident gave the client the motivation to finally enable MFA and take the implementation of a strong password policy more seriously. They reviewed their insurance policies to better understand their coverage in the event of a cybersecurity breach. The incident was also shared with their staff to strike home the importance of verifying sources before sharing sensitive information.

How can you make your environment more secure?

If you're interested in what **Network Doctor** can offer and recommend to make your network and users more secure, please contact us at info@networkdr.com or 201-735-0140. We'll share how our expertise on the latest technology and partnerships with the right companies can help alleviate your security concerns and enable your staff to stay productive.

PROBLEM

A mistake by an employee who clicked on a link in a phishing email and unknowingly granted access to an attacker resulted in a sensitive breach.

SOLUTION

The employee's email account was immediately disabled, password changed, and all active sessions logged out, thereby preventing any imminent damage.

BENEFITS

- Improved cybersecurity
- Increased user education
- Decreased risk from phishing-related malware attacks
- Alleviated stress, boosted confidence, and increased employee productivity