VIRGINIA BANKERS ASSOCIATION

2024 Security Assessment Management Response

Key Details

- Updated On: 6/4/2024
- Updated By: Todd Hancock

Introduction and Purpose

This is a management response and follow-up to the IT security assessment conducted by SBS CyberSecurity (SBS) (3/25/2024 - 3/29/2024).

The IT security assessment consisted of the following components:

- Social engineering testing, including phishing emails and impersonation telephone calls
- Internal vulnerability assessment

Response and Remediation

Social Engineering Testing

Phishing email (High)
Findings: Twenty-eight phishing emails were sent by SBS mimicking an email coming from an IT administrator email, resulting in 2 employees clicking on links and entering usernames and passwords.

SBS Recommendation: The Virginia Bankers Association should continue security awareness, training, education, and testing of employees to remediate current and emerging attack threats found in phishing email and websites.

VBA Remediation: The director of IT spoke with the two individuals about the phishing email and possible consequences of clicking on links and entering credentials. The Virginia Bankers Association has also added a checklist note to inform new users that VBA email will not be sent from generic email addresses. The Virginia Bankers Association will continue to perform quarterly training with monthly testing.

Telephone impersonation calls (Low)
Findings: Out of two attempts made by a social engineer to retrieve internal network information, the employees denied releasing internal network information to the social engineer due to proper verification methods and employee training.

SBS Recommendation: Virginia Bankers Association should continue to train employees on the proper procedures when verifying a vendor over the phone. Also, Virginia Bankers Association should continue to educate employees on current social engineering attacks that impersonate vendors over the phone.

VBA Remediation: No remediation steps were necessary related to the telephone impersonation findings.

Internal Vulnerability Assessment

Findings: SBS considers the Virginia Bankers Association's internal network as patched in a manner which delivers timely remediation of newly identified vulnerabilities. Similarly, to our 2023 findings, servers were noted with higher levels of unpatched vulnerabilities compared to workstations. SBS also noted that the Virginia Bankers Association patching levels are significantly better than peers for the 5 most commonly unpatched software applications. None of the vulnerabilities identified have a known ability to be exploited remotely.

SBS Recommendations: Continuing to run weekly internal vulnerability scans helps the organization keep up with internal vulnerabilities.

VBA Remediation: Continue to stay vigilant on the correction of any items noted in the weekly internal vulnerability scans. The most observed vulnerabilities include vulnerabilities that were less than 30 days old remediated/mitigated by the VBA's patching cycle and historically known risks that have proper mitigations in place to prevent exploitation.

Recommendations

- Continue to conduct annual IT audits with social engineering and vulnerability assessments.
- Continue using KnowBe4 phishing and training campaigns to keep a good email security posture.
- Continue with weekly internal vulnerability scans as a method of ensuring updates and configurations are being applied when possible and as needed.