2022 Security Assessment Management Response

Key Details

- Updated On: 5/17/2022
- 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) (2/14/2022 - 2/21/2022).

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 (High)

Phishing email
Findings: Twenty-five phishing emails were sent by SBS mimicking the IT administrator's email, resulting in four employees clicking on a link. One of these employees entered username and password into a fake website after clicking the link.

SBS Recommendation: The Virginia Bankers Association should continue to promote training and awareness to employees on how to identify and report suspicious email activity.

VBA Remediation: A conversation was initiated with the employee that had entered their username and password into the fake website. The VBA will continue to implement security awareness training for all employees to ensure they understand and exhibit the necessary behaviors and skills to increase the security of the organization. Virginia Bankers Association has training programs for new hires as well as ongoing phishing email testing for current employees. The VBA has begun semiannual training for all employees.

Telephone impersonation calls
Findings: Two attempts lead to one employee attempting to visit a website that was blocked by technical controls. The remote employee visited another site and disclosed their home office IP address.

SBS Recommendation: The VBA employees should verify the identity of the caller by contacting their ISO or IT department before releasing any information or performing any actions at the instructions of the caller. Also, continue educating employees on related social engineering attacks that impersonate vendors over the phone.

VBA Remediation: The one employee realized what had happened after the call and contacted the IT administrator. VBA will be emphasizing to all employees the procedures to be followed prior to releasing any information over the phone.

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. 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. The number of identified vulnerabilities are considerably less than the previous scan in 2015.

SBS Recommendations: Continue running 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. Most of the observations were updates that were less than 30 days old and remediated/mitigated by the VBA patching cycle's expected timeframe. One of the remaining observations were from previously utilized software which was found to be no longer needed and has been removed from the system to remediate the vulnerability. The remaining observations are 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.