GALVESTON ISLAND Park Board of Trustees

Agenda Item Overview

Agenda Item: Discuss And Review IT Security Audit Results

Background: On June 15, 2021, staff presented a technology assessment to the Finance and Operations Committee. The presentation included a recommendation to perform an IT security risk assessment. On December 14, 2021, the board approved a proposal to have the assessment performed by AltiusIT.

AltiusIT was contracted to perform three risk assessments. The assessments were completed in February 2022:

1. NETWORK SECURITY AUDIT PENETRATION TEST
    a. Active analysis of our pubic network entry points for any potential vulnerabilities that result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses.

2. WEB APPLICATION SECURITY AUDIT PENETRATION TEST
    a. Our web sites/applications are vulnerable to wide range of attacks. Auditors emulated the approach used by hackers and perform a controlled real-life attack on our web sites/applications.
    b. The three websites tested were galvestonparkboard.org, galvestonbeachpatrol.com, and visitgalveston.com

3. SOCIAL ENGINEERING SECURITY ASSESSMENT
    a. Social engineering assessment evaluates the effectiveness of our security education and awareness training. Auditors sent a fake (phishing) e-mail to selected members of our staff. Auditors tracked to see how many responded to the message.

The results are as follows:

1. NETWORK SECURITY AUDIT PENETRATION TEST
    a. There were some high-risk, medium-risk, and low-risk vulnerabilities detected. The auditors provided recommendations on how to resolve these risks including software updates. Galveston Computer Solutions manages our network. Staff will work with GCS to determine the appropriate measures to be taken to mitigate or eliminate the risks prioritizing high-risk vulnerabilities. The measures taken will be based on the auditors' recommendations.

2. WEB APPLICATION SECURITY AUDIT PENETRATION TEST
    a. There were some high-risk, medium-risk, and low-risk vulnerabilities detected for two websites. The third was clean with no vulnerabilities detected. The auditors provided recommendations on how to resolve these risks including protocol updates. Different web developers/hosts manage

our websites. Staff will work with the developers to determine the appropriate measures to be taken to mitigate or eliminate the risks prioritizing high-risk vulnerabilities. The measures taken will be based on the auditors' recommendations.

3. SOCIAL ENGINEERING SECURITY ASSESSMENT
    a. 10 staff members were sent fake phishing emails and auditors tracked who responded. Three different emails were sent. One was benign and intended to see if the receiver would respond so the attacker would know the email was active and the person responded to phishing e-mails. The other two were a bit more malicious and required the receiver do more than respond. Of the three types of emails, only two staff members responded to the benign email. No staff members responded to the more malicious emails. We will have the two staff members take IT security training and will make the IT security training a part of the onboarding process for new employees and an annual requirement for existing employees.

Staff Recommendation: N/A