FORESITE

CASE STUDY: Emergency Services agencies have become a target for cyber attacks and need to proactively assess and mitigate their risks.

BACKGROUND

The FBI's Criminal Justice information Services Division (CJIS) provides resources to law enforcement, national security and intelligence community partners the information they need to protect the public. CJIS v5.5 is the Information Services Security Policy that provides a framework and guidance for protection of data.

Foresite was contacted by an Association of emergency services agencies who wanted to proactively educate their members on the risks by assessing one of their member agencies who had agreed to share their results with the other members during the association's annual meeting.

OBJECTIVES

- Assess member agency against the CJIS/NIST 800-53 framework to establish a baseline for all members;
- Educate members on the key risks and steps to remediate by presenting our findings during their annual conference;
- Provide ongoing support and resources to members on an "as needed" basis to assist them in assessing their own risks and remediation steps.

The subject organization had approximately 200 connected network devices and about the same number of staff. In addition to assessing the organization's policy, process and procedures against the cybersecurity framework, Foresite also performed internal vulnerability scans and penetration testing against the agency's technical controls.

As many breaches are caused by human error, we also conducted and email phishing campaign targeting a sampling of the agency staff to see how susceptible they were to common phishing tactics that can install malware, ransomware, or trick them into providing their credentials and allow a hacker to gain network access.

We first presented our findings to the member who had agreed to be the subject agency for this assessment. We found that their external posture from a technical perspective was good, there were no serious vulnerabilities found. Internal scans exposed a number of high and critical vulnerabilities that could be compromised, and this highlighted the importance of ongoing vulnerability scans and remediation to protect against common exploits.

The staff's security awareness was very good overall. Only about 10% of the staff opened our phishing emails and only one staff member provided us with their credentials, but it only takes one set of credentials to access the network and the data that user has privileges to see and edit.

The agency's overall compliance with the cyber framework was 73%, which was not bad considering they had never been through an outside assessment before, but showed that there was work to be done to prepare for an audit.

Emergency services

BUSINESS CHALLENGES

- Need to comply with CJIS 5.5 cyber guidelines
- Lack of assessment to confirm level of compliance for member agencies
- Individual agencies don't have budget to hire full-time cyber security experts

FORESITE SOLUTION

- Cybersecurity Assessment with functional testing

OPPORTUNITIES

- Determine current state of sample member agency and share results with all members to educate them on common risks and how to proactively remediate them
- Provide ongoing access to cybersecurity and compliance resources on an "as needed" basis

INDUSTRY