Cybersecurity Threat Intelligence Assessment Report

Client Information

- **Client Name:** Bay Area Hospice Care
- **Assessment Date:** July 30, 2024
- **Assessor Name:** K.M. Stewart, B.S., A.S. Cybersecurity
- **Client:** Bay Area Hospice Care (assignment)

Executive Summary

This assessment evaluates Bay Area Hospice Care's cybersecurity posture and identifies areas for improvement. Key findings include the need to strengthen network security, enhance incident response capabilities, and improve employee security awareness. Recommendations include implementing advanced threat detection tools, conducting regular security audits, and providing comprehensive security training.

Introduction

1.1 Purpose of the Assessment

The purpose of this assessment is to evaluate Bay Area Hospice Care's cybersecurity posture, identify vulnerabilities, and provide recommendations for improvement.

1.2 Scope of the Assessment

This assessment covers the organization's network infrastructure, systems, applications, and data.

Methodology

The assessment methodology included:

- **Network vulnerability scanning:** Using Nessus and OpenVAS to identify vulnerabilities in the network infrastructure.
- **Application vulnerability scanning:** Using OWASP ZAP and Burp Suite to assess vulnerabilities in web applications.
- **Endpoint vulnerability scanning:** Using Microsoft Baseline Security Analyzer and Qualys to identify vulnerabilities on endpoints.
- **Interviewing key stakeholders** to understand the organization's security posture and requirements.
- Reviewing existing security policies and procedures.

Organizational Overview

2.1 Business Profile

Bay Area Hospice Care is a non-profit organization providing palliative care services to patients with life-limiting illnesses.

2.2 IT Infrastructure Overview

The organization operates a hybrid cloud environment with a mix of on-premises and cloud-based resources.

Key Assets and Data

Critical assets include patient health records, financial data, and confidential communications.

Threat Landscape

3.1 Current Threat Environment

The healthcare industry is a prime target for cyberattacks. Common threats include ransomware, phishing, and data breaches.

3.2 Historical Incidents

The organization has not reported any major security incidents in the past year.

Risk Assessment

4.1 Risk Identification

Identified risks include:

- Unauthorized access to sensitive data
- Malware infections
- Phishing attacks
- Insider threats
- Supply chain attacks

Risk Analysis

The likelihood and impact of each risk were assessed based on the organization's current security controls and the potential consequences of a successful attack.

Risk Mitigation Strategies

Recommended strategies include:

- Implementing stronger access controls
- Enhancing endpoint security
- Conducting regular security awareness training
- Implementing a robust incident response plan

Vulnerability Assessment

5.1 Network Vulnerability Assessment

Findings:

- Multiple vulnerabilities identified in network devices and applications.
- Recommendations: Apply patches and updates, implement intrusion detection systems, and segment the network.

5.2 Application Vulnerability Assessment

Findings:

- Several vulnerabilities identified in web applications.
- Recommendations: Conduct regular penetration testing, implement web application firewalls, and enforce secure coding practices.

5.3 Endpoint Vulnerability Assessment

Findings:

- Outdated operating systems and software on endpoints.
- Recommendations: Enforce regular patching and update policies, implement endpoint protection solutions.

Incident Response and Recovery

6.1 Incident Detection and Reporting

Tools and techniques:

- SIEM systems
- IDS/IPS
- Security monitoring tools

6.2 Incident Analysis

Methods for analyzing and understanding incidents:

- Forensic analysis
- Threat intelligence
- Incident response frameworks

6.3 Incident Containment and Eradication

Steps to contain and eliminate threats:

- Isolate affected systems
- Remove malware
- Patch vulnerabilities

6.4 Recovery

Procedures to restore affected systems and data:

- Utilize backups
- Follow incident response plan

6.5 Post-Incident Review

Conduct a thorough review of the incident to identify lessons learned and improve future responses.

Security Policies and Compliance

7.1 Current Policies Review

Review existing security policies and recommend improvements to ensure alignment with industry best practices and regulatory requirements.

7.2 Compliance Requirements

Assess compliance with relevant regulations such as HIPAA and HITRUST.

Training and Awareness

8.1 Security Awareness Training

Implement a comprehensive security awareness training program to educate employees about best practices and common threats.

8.2 Phishing Simulation Exercises

Conduct regular phishing simulations to assess employee awareness and identify training gaps.

Threat Intelligence Integration

9.1 Threat Intelligence Sources

Utilize internal and external sources of threat intelligence to stay informed about emerging threats.

9.2 Threat Intelligence Analysis

Analyze threat intelligence data to identify potential risks and inform security decisions.

9.3 Proactive Threat Hunting

Employ proactive threat hunting techniques to identify and mitigate threats before they cause harm.

Recommendations

10.1 Short-Term Recommendations

- Implement a robust incident response plan.
- Enhance network and endpoint security controls.
- Conduct regular security audits and assessments.

10.2 Long-Term Recommendations

- Invest in advanced threat detection tools.
- Consider implementing a security operations center (SOC).
- Continuously update security policies and procedures.

10.3 Continuous Improvement

- Regularly review and update the security program to address emerging threats and best practices.

Conclusion

This assessment has identified several areas for improvement in Bay Area Hospice Care's cybersecurity posture. By implementing the recommended strategies, the organization can enhance its security and protect sensitive patient data.

Appendices

Network Vulnerability Assessment

Vulnerability #1: Remote code execution (RCE) vulnerability in Apache Struts framework

Location: IP (for privacy purposes)

Recommendation: Apply the latest security patches to the Apache Struts framework to address the vulnerability.

Vulnerability #2: Weak password policies for network devices

Location: Multiple network devices (devices omitted for privacy purposes)

Recommendation: Enforce strong password policies, including minimum password length, complexity requirements, and regular password changes.

Vulnerability#3: Unpatched vulnerabilities in network devices

Location: Multiple network devices

Recommendation: Apply the latest security updates and patches to all network devices.

Application Vulnerability Assessment

Vulnerability #1: SQL injection vulnerability in a custom web application

Location: Web application URL omitted for privacy purposes

Recommendation: Sanitize user input to prevent SQL injection attacks, update the application framework to the latest version, and conduct regular penetration testing.

Vulnerability #2: Cross-site scripting (XSS) vulnerability in a web application

Location: Web application URL omitted for privacy purposes

Recommendation: Implement input validation and output encoding to prevent XSS attacks, update the application framework, and conduct regular penetration testing.

Endpoint Vulnerability Assessment

Vulnerability #1: Outdated operating systems on multiple endpoints

Location: Omitted

Recommendation: Enforce regular patching and update policies for operating systems and applications.

Vulnerability #2: Missing security updates for third-party software

Location: Multiple endpoints

Recommendation: Implement a patch management process to ensure all third-party software is up to date.

Tools

- **Nessus**
- **OpenVAS**
- **OWASP ZAP**
- **Burp Suite**
- **Microsoft Baseline Security Analyzer (MBSA)**
- **Qualys**

Additional Resources and References

NIST Cybersecurity Framework: https://NIST.gov

OWASP Top 10: https://owasp.org/www-project-top-ten/

SANS Institute: https://www.sans.org/

SANS DFIR blog: https://www.sans.org/digital-forensics-incident-response/

Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/

Sign off here:

K. Stewart

K. Stewart (Cybersecurity Consultant)

T. Anderson

T. Anderson (Bay Area Hospice Care Representative)