**Project Phase 1 Report**

Group 4: Gevorges Chenmala, Masrura Tasnim, Richard Beiswanger, Uju Anachebe

Department of Information Systems and Security, Kennesaw State University

CYBR 7910: Capstone in Cybersecurity Practicum

Dr. Zhigang Li

March 27, 2024

**Status Update**

Last Wednesday our team kicked off this capstone project by submitting a project plan and accompanying Gantt chart. In the project plan, we completed the milestones of the first deliverable, including establishing roles and responsibilities for each team member and agreeing on a communication and collaboration strategy to follow as we complete the project together. As CyberGuardian Solutions, we have begun securing Akwaaba’s online data and infrastructure by following the timetable we created in the Gantt chart for the second deliverable. This included creating a 2-part security policy along with a risk assessment and technical plan, which we will follow in future deliverables as a guide to secure Akwaaba’s e-commerce infrastructure from potential cyberattacks.

While working on the Phase 1 milestones, our team has conducted daily meetings, helping each other keep tabs on our progress, and ensuring we all stay on the same page, creating a cohesive product. We’ve had several minor adjustments with variance in research time especially when learning about and considering what tools we can and/or might want to use for each stage in the project. Despite these challenges, our updated Gantt chart timeline shows we are still on target to meet the official deadlines for our future deliverables ahead of schedule. Each team member has taken on the responsibility for a significant part of this project, which has helped us keep the ball rolling toward success in our mission to secure Akwaaba’s digital assets and gain real practical experience in the process.**General Security Policy**

1. **Purpose**

The primary objective of the general security policy is to:

1. Define the principles for protecting Akwaaba's information assets.
2. Protect the digital assets of Akwaaba.
3. Mitigate the risks linked with breach of confidentiality, unauthorized access, and the compromise of sensitive information.
4. **Policies**
   1. **Internet Access & Usage Policy**
      1. Internet access is provided for business purposes.
      2. Internet usage is for supporting business activities necessary to carry out job functions. Employees should not visit unauthorized websites or take part in cyber activities that can compromise the security of Akwaaba's network.
      3. The use of virtual private networks (VPNs) to bypass the network’s security measures put in place is prohibited.
      4. To ensure compliance, internet activity will be regularly monitored.
   2. **Email Policy**
      1. Akwaaba's email system is for the use of business communication only.
      2. Users are prohibited from automatically forwarding business emails to third parties. Employees should not make use of the email system for personal use. Employees should not send confidential information without the use of encryption.
      3. Use caution when opening email attachments and when accessing links from suspicious sources to reduce the chances of malware attacks.
   3. **Bring Your Own Device (BYOD) Policy**
      1. BYOD is permitted for employees authorized by management and the devices used must meet Akwaaba's security standards.
      2. Employees are responsible for ensuring the security of their BYOD devices.
      3. Employees should encrypt their devices to protect data in the event of loss or theft.
      4. If needed, Akwaaba has permission to remotely wipe data from BYOD devices in case of loss or theft.
   4. **Software Installation Policy**
      1. Only software approved by the system administrator may be installed on Akwaaba's IT assets.
      2. All software installations should be used for conducting business activities.
      3. Employees should ensure that software installations do not compromise the confidentiality and integrity of the company’s or customer’s data.

**Access Management Policy**

Purpose – To create an Authority and Access Control Policy (AACP) for the Akwaaba e-commerce web server infrastructure. This policy will safeguard all sensitive data, stipulate appropriate access levels for all employee roles, and help maintain security for all server infrastructure including systems integrity by complying with relevant regulations.

**Policy Details**

User Access - Employees should be granted access to systems relevant to their specific roles. Wait staff should have access to order and payment systems, while managers and HR should have broader access to administrative tasks. Assign a designated system administrator to maintain a list of authorized users and their assigned access levels.

Authority Levels – Establish two authority levels for system access. Only restaurant managers and IT personnel should hold administrative privileges. Administrator access is used to manage user accounts, access permissions and security configurations within their designated areas such as restaurant location and IT infrastructure. Other employees should be granted User access based on their job function. Users should have limited access only to specific systems and data necessary for their daily tasks.

Access Control Measures - All users require unique User IDs and strong passwords with a minimum length of nine characters including a mix of uppercase and lowercase letters, numbers, and special characters. Passwords must be changed every 90 days or immediately if a security breach is suspected. User accounts should be locked after five consecutive failed login attempts, requiring administrative intervention for reset. Remote access to the server should be limited to the web developer and authorized cybersecurity team members using VPN.

Maintenance and Configuration - Server configurations and any changes to the e-commerce site, should only be performed by authorized IT personnel or the cybersecurity team.

Access Control Principles - Users are granted the minimum level of access required to perform their duties effectively. This minimizes potential damage from unauthorized access or human error. Access to sensitive information is restricted to personnel with a legitimate business need. This protects confidential data from unauthorized disclosure. Critical tasks involving access control or financial transactions are divided among users to reduce the risk of fraud or misuse of authority.

Physical Access Control - Measures should be implemented to control physical access to restaurants and server locations. Laptops, desktops, and other devices should be secured with password protection and encryption to prevent unauthorized access in case of theft or loss.

**Risk Assessment**

March 27, 2024

Purpose: To conduct an initial vulnerability assessment of Akwaaba’s server infrastructure relating to its e-commerce website to assess which threats are most likely and decide what security measures can be taken to mitigate them.

Scope: Akwaaba’s Webserver infrastructure located in their headquarters, accessed remotely by a secure Virtual Private Network (VPN).

Security Category: Moderate (3). Contains sensitive customer information in the database and business-critical operations i.e. Akwaaba’s entire online presence.

Authorization Boundary: Software, hardware and personnel of the e-commerce infrastructure.

Overall Level of Risk: Moderate (3).

Specific Risks Identified in this Assessment:

* Level 1 (Very Low): Unencrypted data theft, zero-day attacks, physical breaches
* Level 2 (Low): Outdated vulnerabilities, SQL injections, unpatched OS, insider threats
* Level 3 (Moderate): Misconfigurations, privilege escalation, outdated WordPress themes & plugins, bad admin passwords, man-in-the-middle attacks, unsecured endpoints
* Level 4 (High): Cross-site scripting (XSS) / Cross-site request forgery (CSRF) attack, social engineering / phishing attack

This initial assessment identifies the potential vulnerabilities of Akwaaba’s web server infrastructure to determine the threat level of these risks based on the likelihood and negative impact they could cause on critical business operations. This assessment will help determine the best security tools and practices to patch up the greatest vulnerabilities to the company.

Constraints include an inability to access the hardware directly, no budget, the website must be online before security measures are taken, and certain software is restricted from being uninstalled or replaced. Due to the lack of direct access, assumptions must be made about current security methods. Also, probable threats must be based on publicly available insights into similar e-commerce infrastructures.

Risk Tolerance Inputs: Damages range from simple disruptions of the e-commerce site to greater financial and reputation loss to any litigation due to a data breach involving customers’ sensitive information.

This assessment uses a qualitative approach which factors the predicted likelihood of an attack with its residual impact on critical business operations. This is done by comparing the asset's value with the vulnerability's severity and the threat's capability.

Reasons/Rationale for decisions: All assessments were guided by known best practices, adherence to National Institute of Standards and Technology (NIST) guidelines, and the unique needs of Akwaaba. The major uncertainties in this assessment include the accuracy of asset values and the unknown aspect of new threats.

Relation to business functions: The e-commerce website is a direct income stream for Akwaaba, and a platform for customer interaction. Disruptions and other attacks would negatively impact customer relations and key business operations as well.

|  |  |  |  |
| --- | --- | --- | --- |
| Assets | Threats/Risks | Possibilities of Compromise | Damage if Asset Compromised |
| WebServer (Apache) | Misconfigurations  Outdated  DoS attacks | Moderate(3)  Low (2)  Moderate(3) | Data Loss / Errors  Data Access / Loss  Service Disruption |
| Database Server (MariaDB) | SQL injection  Unencrypted data theft  Privilege escalations | Low (2)  Very Low (1)  Moderate (3) | Data Loss  Sensitive Data Theft  Manipulation |
| Operating System (Red Hat OS) | Unpatched  Misconfiguration  Novel attacks | Low (2)  Moderate (3)  Very Low (1) | Compromised System  Malware Infection  Wrongful Root Access |
| WordPress | Oudated plugins  Bad admin PW  XSS/CSRF attack | Moderate (3)  Moderate (3)  High (4) | Website Defaced  Hijacked Admin  Data Loss |
| Network Infrastructure | Man-in-the-middle  Unsecured endpoints  Phishing attacks | Moderate (3)  Moderate (3)  High (4) | Intercepted Data  Network Intrusion  Compromised Account |
| Employees  (HR, Web Developer, Managers) | Social Engineering  Insider threats  Physical Breach | High (4)  Low (2)  Very Low (1) | Sensitive Info Theft  Unauthorized access  Data Loss |

**Technical Plan**

Akwaaba’s server infrastructure for their e-commerce website includes Red Hat Enterprise Linux (RHEL), Apache web server, MariaDB (RDBMS) to manage the database, and WordPress for the webpage development. This infrastructure is integral to their business operations, as it hosts their e-commerce website which processes online orders and manages online customer data.

Four major strategies to enhance security of this infrastructure:

1. Uphold tight privilege guidelines. Eliminate root access and general admin privileges. Each user-level and component needs to be updated with the minimal level of access required to function properly. This includes login access for every system, the web server, the database, the operating system, and admin access to WordPress.
2. Schedule regular patches and updates. Not only the four main systems need updating, but any themes and plugins inside WordPress that are used for the website need to be updated regularly as well.
3. Encrypt sensitive data in transit. Any data sent between the server and clients during login must be encrypted with SSL/TLS. The webpage should be https, not http.
4. Recommend a recovery strategy. Critical data must be backed up regularly to smooth the process of recovery operations. An off-site location and/or a secure cloud platform would work.

Tools:

ModSecurity: Web application firewall (WAF) designed to use with Apache, can block several common threats.  
<https://github.com/owasp-modsecurity/ModSecurity>

Fail2Ban: Log scanner that monitors brute-force attacks and other suspicious activity. Can also create an IP blacklist as malicious sources are discovered. WordPress has a Fail2Ban plugin.  
<https://github.com/fail2ban/fail2ban>

Let’s Encrypt: Gets SSL/TLS certificates, allowing HTTPS to be enabled.  
<https://letsencrypt.org/>

Trusona: Authentication Tool for WordPress. A passwordless authentication for WordPress admins that enhances security & usability.  
<https://wordpress.org/plugins/trusona/#description>

ClamAV: Open-source (general public license [GPL]) antivirus engine used in a variety of situations, including email, web scanning, and endpoint security. It provides utilities including a flexible and scalable multi-threaded demon, a command-line scanner, and automatic database updates.  
<https://www.clamav.net/>

UpdraftPlus: WordPress plugin that provides the ability to backup and store in the cloud.  
<https://wordpress.org/plugins/updraftplus/>

Nmap: Scans networks and servers for services hosted on the server, operating system, open ports, etc. It is available for Linux, Windows, and Mac OS.  
<https://github.com/nmap/nmap>

WPScan: Scans WordPress sites to identify vulnerable plugins, themes, weak passwords etc. No longer a free service, but security researchers are welcome to use the CLI scanner and API for non‑commercial purposes, with 25 API calls per day after registration.  
gem install wpscan (to install)  
<https://wpscan.com/wordpress-cli-scanner/>

OpenVAS: Vulnerability scanning and management tool. It can detect and assess security vulnerabilities on servers, applications and networks.  
<https://www.openvas.org/>

Wordfence: Security plugin for WordPress, it provides firewall protection, malware scanning, and security monitoring.  
<https://wordpress.org/plugins/wordfence/>

Vega: Web application vulnerability scanner and testing platform to identify and assess security vulnerabilities in web applications.  
<https://subgraph.com/vega/>

Hydra: Password-cracking tool to crack passwords by performing brute-force attacks.  
<https://github.com/vanhauser-thc/thc-hydra>

SQLMap: Penetration testing tool for detecting and exploiting SQL injection vulnerabilities in web applications.  
<https://sqlmap.org/>

Commix: Detects web application security vulnerabilities, focusing on command injection vulnerabilities.  
<https://commixproject.com/>

Gobuster: Directory and file brute-forcing in web applications, used to discover hidden or unauthorized content.  
<https://github.com/OJ/gobuster>

CUPP: stands for Common User Passwords Profiler, it is a script to generate custom wordlists for password cracking.  
<https://github.com/Mebus/cupp>

Metasploit: Penetration testing framework to develop and execute exploits against target systems.  
<https://www.rapid7.com/products/metasploit/>

Burp Suite: Tests web application security, it can intercept requests to server from browser.  
<https://portswigger.net/burp/>

XSSer: Detects and exploits Cross-Site Scripting (XSS) vulnerabilities in web applications.  
<https://xsser.03c8.net/>

Hashcat: Powerful open-source password recovery tool used for cracking hashes to recover passwords from hashed data.  
<https://hashcat.net/hashcat/>

Wazuh: Platform for real-time threat detection, log analysis, and compliance monitoring.  
<https://github.com/wazuh/wazuh>

Legion Framework: Hacking tool for penetration testing and security assessments. It is used for conducting reconnaissance, scanning, exploitation, and post-exploitation activities in network environments. It provides interface to access other security tools like Nikto, NMAP, THC Hydra, whataweb, sslyzer, Vulners, dirbuster, SMBenum, and webslayer.  
<https://www.geeksforgeeks.org/legion-tool-in-kali-linux/>

Nikto: Web vulnerability scanner. It can scan for common vulnerabilities such as outdated software, misconfigurations, and known vulnerabilities in web servers, including HTTP servers, CMS platforms, and web applications.   
<https://cirt.net/Nikto2>

Atomic Red Team™: PowerShell-based execution framework with defense tests that can be automated.  
<https://github.com/redcanaryco/atomic-red-team>

UTMStack: Open-source Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) solution powered by real-time correlation and threat intelligence. UTMStack specializes in threat detection and response with compliance reporting for regulations.  
<https://utmstack.com/>

Alien Labs Open Threat Exchange (OTX) Endpoint Security: Threat scanning service using Alien Labs OTX data to identify compromised endpoints.  
<https://otx.alienvault.com/endpoint-security/welcome>

Justifications for tool choices - Akwaaba is a small business, and our security team has no budget. Open-source tools were chosen in part because they are free to use. Open source also means that there is a huge community of developers working together online on the product, so there is documentation and a forum available for assistance. These chosen tools are designed to be used with Akwaaba’s infrastructure software, and are selected and used widely in the industry, which means they have a track record of success.