Akwaaba Cybersecurity Phase 1 Report

W02-12777 Project 11 Group 2

February 20th, 2022

Team Lead:	Brandon Turner
Technical Specialist:	Kowou Agbavon
Technical Specialist:	Andres Morales
Technical Specialist:	Felton Strickland
Technical Writer:	Aleksandar Punos

Project Status Update

Many things have been accomplished since the project plan submission. As a team we have had at least three meetings a week to ensure that the project stays on track. The team worked together to create an information security policy by dividing the policy into sections and equally distributing the work. Around the time we had our information security policy written we got the login information for the VM which allowed us to see where the server infrastructure was most vulnerable and assess the risks for the business. It also allowed us to make our ecommerce site alive, A k w a a b a – Where Authenticity Meets Deliciousness. The team used this information to construct a risk assessment document evaluating infrastructure, important assets to protect, threats to such assets, possibilities of a successful compromise, and the damage if said assets were to be compromised. Finally, from the risk assessment and vulnerabilities found a technical plan was created with how we plan to monitor and make the Apache server, MariaDB, and VM more secure.

The team keeps weekly logs of our work and records every meeting. With an information security policy, risk assessment, and technical plan created we were able to piece them together to make a phase 1 report. So far, the team has been able to stay on track with the project plan and has not had any deviations. With set meeting times three times a week we were also able to stave off any significant issues with project management. We plan to stay on track as we progress on to phase two of the project which is implementing the security program on our server and prepare strategies to exploit vulnerabilities on the opposing team's server.

Information Security Policy

Purpose

The purpose for creating an information security policy (ISP), is to create a framework that outlines the overall approach to information security. The policy is to allow the company to think ahead and pinpoint vulnerabilities that may lead to security breaches and stop them before they become an issue. It also gives all employees a clear guideline of what is allowed when dealing with company servers, even limiting some access based on classifications and roles. It is our duty to respect customers' rights and uphold ethical and legal responsibilities.

Audience

The audience that the ISP focuses on is all workers at Akwaaba, from the restaurants to the corporate office, contractors, vendors, and even the owner. We need to ensure that security is of the utmost priority and that does not just stop with management and IT. One of the most vulnerable aspects of security is people/users.

Information Security Objective

The security objective protects the privacy of Akwaaba's information content that prevents unauthorized individuals from accessing business information and systems. It restrains the employees' and customers' errors or malicious entries in the data that can compromise their confidentiality. To maintain the accuracy of the business information and the business' system, restriction permission is delegated to the staff member for editing or modifying them without disrupting the data integrity. As a result, an authorized person can access the information, back up the data, and ensure that they are always available for business operation.

Data Classification

All corporate databases that process, stores, and transmit customers' and employees' PII (personal identifiable information) are considered "High Security Systems" and should be clearly marked as such. The data stored on these systems is considered confidential.

Authority and Access Control Policy

This policy applies to Akwaaba staff, contractors, and vendors that connect to servers, applications, or network devices belonging to the company. Access to these devices is role-based therefore, access will be granted based on the role of each employee. IT (Information Technology) administrators and members of the security consulting firm hired by the company will have remote access to all servers and databases. The company web developer will only have access to WordPress with permission to access and make changes to the eCommerce website. "High Security Systems" must only be accessed for security and/or maintenance purposes. All other employees not mentioned above will not have access to any of the company's servers or databases. Server rooms storing network devices will require badge access, which will be accessible to the network administrators only. Access logs will be kept and maintained for these server rooms as well.

Data support and operation

This policy applies to all Akwaaba systems that contain sensitive information. These systems must be protected according to the organization's standards, best practices, industry compliance standards and regulations. Data should be encrypted and protected by a firewall and anti-malware protection. Backup media should be safely and securely stored if physical or moved to cloud. Any data movement should only be transferred via secure protocols. All data copied to portable devices or transmitted on a public network should be encrypted.

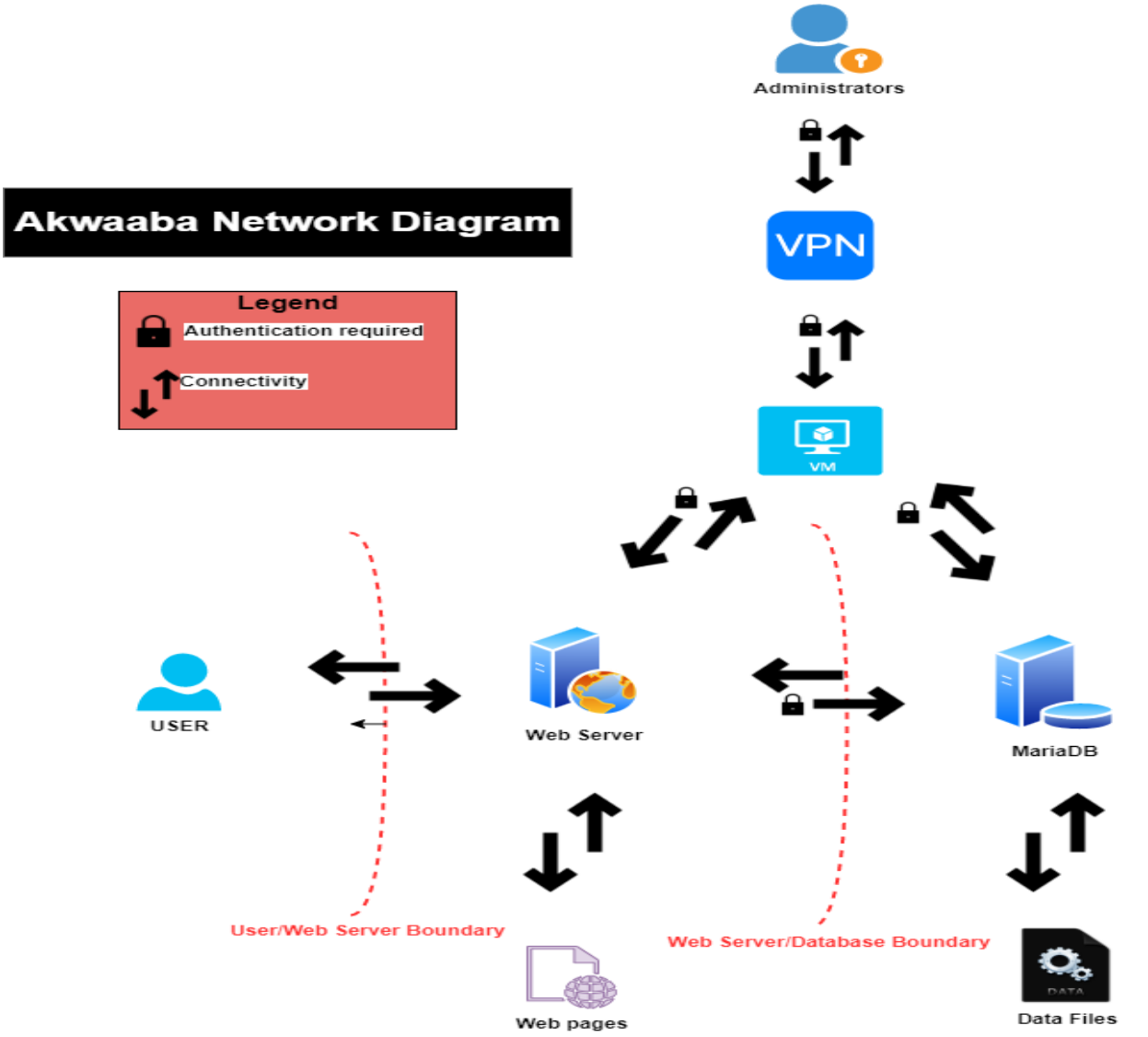
Security awareness and behavior

Akwaaba's employees could access the company IT security policy online and they also have the option to have a paper copy of the policy in the IT security office. Every new employee would have training and a quiz about security policy. Every six months every single employee should finish a 30-minute security policy training course. Employees are responsible for noticing, preventing and reporting any social engineering attacks (for example phishing emails). The company needs to practice a clear desk policy- all laptops need to be secure with cable locks. Shred all documents that are no longer needed. Internet usage should be restricted, especially YouTube and other social media websites (Facebook, Instagram etc.) and these actions would be determined by IT security team. All unwanted websites should be blocked using a proxy system.

Responsibilities, rights, and duties of personnel.

Responsibilities are divided between the regular team members, the IT team and members of the management team. All rights and duties of personnel are more specified in their rights and duties book for each department and the implementation of these activities should be monitored by the special management team. IT security team is responsible for periodically updating ISP and informing other parts of the Akwaaba's company about these updates.

Risk Assessment



Infrastructure Evaluation

- The public-facing Apache web server and database are located on the same network/subnet. These two entities should be separated to prevent attacks from external threats.
- Password to web server and database is too weak; therefore, a strong password policy should be implemented.
- Web server can be potentially exploited from user/web server boundary.
- Servers, particularly the web server, are susceptible to denial-of-service (DoS) attacks.
- Data stored in the database is unencrypted.
- There are vulnerabilities associated with servers and VM (Virtual Machine) operating systems that need to be addressed.
- Unsecure ports such as HTTP and telnet along with other ports are open.

Important digital assets to protect

- Administrator account – Admin has access to all data in the Akwaaba infrastructure.
- Apache Web Server - Important asset that hosts the Akwaaba ecommerce website.
- Ecommerce website – Asset that brings revenue from customer purchases.
- MariaDB database – Contains important data from customers and employees of Akwaaba.
- Data stores on database – contains PSI of both customers and employees of Akwaaba.

Potential known threats and vulnerabilities to each asset

- In today's world we are experiencing so many possible risks to our system in general. This is the majority part of threats and vulnerabilities to Akwaaba company.
- Physical security violation and intrusion
- Social engineering attacks
- DoS- denial of service attacks
- Attack from insider threat

Probability of Major Attacks per Asset

- Administrator account - Moderate probability. If the admin is properly educated and keeps all passwords secure, then they can reduce that probability. However, people are normally the weakest link in security, mistakes happen, and the account can be taken by means of physicality. This account is highly targeted because it can access the highest levels of security.
- Apache Web Server - Moderate probability. Web server is currently vulnerable to attacks from users and can lead to access to the ecommerce website. This would be valuable to attackers and should be looked at as a point of interest for security.
- Ecommerce website – Moderate probability. If attackers can get into the web server there would be nothing stopping them from attacking the ecommerce website which grabs valuable customer data and payments.
- MariaDB database – High probability. Weak passwords make it simpler for hackers to break into and with data in the database not being encrypted it would make a great target.
- Data stored in Database – High probability, data is valuable especially with customer information and payments. Having this data unencrypted makes it very vulnerable to attack and theft if the attackers can get access to the database.

Damage to each asset when attacked

The risks identified have a significant impact on the direction of the business and cause operation disruption, monetary loss, reputation loss, and safety. The amount of damage to the digital asset determines the exposure factor (EF), which is the percentage of loss the business Akwaaba will allow as a single loss expectancy (SLE); therefore, we quantify the damage posed on each asset of the business monetary each time the attack occurred.
SLE = EF * AV (Asset Value)
Then, we will determine the business annual loss expectancy based on the attack rate occurrence (ARO) each year.
ALE = SLE * ARO

Assets	Threats/Risks	Possibilities of Successful Compromise	Damage if Asset Compromised
Administrator Account	Social engineering	Moderate	Access to web server and database
Apache Web Server	Dos attacks	Moderate	Information theft Access to website
Ecommerce Website	XSS, SQL Injection	Moderate	Vandalism Downtime
MariaDB database	Software exploits, malware	High	Access to data stored on database
Data stored on database	Hackers, social engineering	High	Data can be leaked/stolen

Technical Plan

The technical infrastructure of the Akwaaba network consists of 3 core systems: MariaDB, Apache Server, and VM. The Apache server is a front-end public facing web server accessed by Akwaaba customers. It is also the most vulnerable and susceptible to external attacks. The backend database, MariaDB, is connected to the Apache server in which both the MariaDB and Apache server can be accessed by administrators via a virtual machine. Overall, the network consists of a lack of security controls and weak authentication methods. These security faults will be addressed with the security controls listed below.

Apache Server

- **Disable the server-info directive-** displays information about the server's configuration
- **Disable the server-status directive-** displays information about server performance, such as server uptime, server load, current HTTP requests, and clients' IP addresses.
- **Disable the server-signature directive-** displays information about server configuration such as version of Apache and the operating system.
- **Disable the directory listing-** allows users to view complete directory contents.
- **Establish accountability via logging**
- **Install ModSecurity WAF-** This is used to prevent SQL injection/XSS attacks that are common
- **Redirect HTTP requests to HTTPS-** Because HTTP is unsecure the web server will be configured to redirect users' requests to the more secure protocol, HTTPS.

MariaDB

- **Establish accountability-** Implement logging via the MariaDB Audit plugin.
- **Stronger password on the database-** administrators' passwords must have at least eight characters containing one uppercase letter, number, and unique personality. This will decrease the likelihood of a successful brute force attack on the network. The password will **NOT** be the same as the password for the root account.
- **Encrypt data-** Provides data confidentiality using Advanced Encryption Standard (AES) to encrypt data via the File Key Management plugin on MariaDB.
- **Establish user accounts with strong passwords and permissions-** based on principle of least privilege to enforce access control policy.

VM

- **Implement a stronger password for root account-** The administrator's password must have at least eight characters containing at least one uppercase letter, number, and special character. This will decrease the likelihood of a successful brute force attack on the network. Addition layer of two- factor authentication enforces the security of the account by sending the PIN text through SMS
- **Establish user accounts with strong passwords and permissions based on the principle of least privilege-** Require creating at least eight-length characters including at least one uppercase letter, number, and special character. Revocable access after one year of non-activities will decrease the likelihood of an insider attack or a breach of security using a compromised user account.
- **Disable unused ports-** Closing unused/unsecure ports such as port 631 will help prevent exploitation of the servers.
- **Activate port 443 (HTTPS)-** Allows the web server to successfully redirect users' requests to HTTPS.
- **Install OSSEC HIDS (Host Intrusion Detection System)-** Provides log-based intrusion detection, malware detection, and file integrity monitoring.

References

Acunetix. (2021, March 12). *10 tips for Apache Security*. Acunetix. Retrieved February 19, 2022, from https://www.acunetix.com/blog/articles/10-tips-secure-apache-installation/

Clouder , A. (2019, July 15). *How to secure connections to mariadb with SSL encryption*. Alibaba Cloud Community. Retrieved February 19, 2022, from https://www.alibabacloud.com/blog/how-to-secure-connections-to-mariadb-with-ssl-encryption_595079

Managing User Via Command-Line Tools . Red Hat Customer Portal . (n.d.). Retrieved February 19, 2022, from https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/s2-users-cl-tools

Sen, K. (2021, October 17). *Tripwire Open Source vs OSSEC: Is This Tripwire Alternative Right for You?* UpGuard . Retrieved February 19, 2022, from https://www.upguard.com/blog/tripwire-open-source-vs-ossec-which-is-right-for-you