New Zealand Diploma in Cybersecurity		
Course No: HTCS6703	**Network Security**	**Level: 6 Credits: 15**

Student Name: Gerard Doctora, Anna Masliaeva, Christopher Pahnke, Rosario Valle	**Student ID: 1596339, 1572067, 1577828, 1562804**
Assessment Type: Project Report	**Weighting:**
Due Date:	**Total marks:**

Student declaration

I confirm that:

- This is an original assessment and is entirely my own work.
- The work I am submitting for this assessment is free of plagiarism. I have read and understood the Academic Integrity Policy. I have also read and understood the Student Disciplinary Statue.
- Where I have used ideas, tables, diagrams etc. of other writers, I have acknowledged the source in every case.

Student Signature: Gerard Doctora, Anna Masliaeva, Christopher Pahnke, Rosario Valle	**Date: November 17, 2024**

Table of Contents

Introduction

This report has been made for Bill Jines, ABC Food company's Managing Director, to provide an overview of the company's current network, explore its security posture, and design a solution to improve the company's security. The report consists of two parts. The first one describes the company's network, provides a scenario of an attack that is possible due to existing vulnerabilities and deficiencies in security, breaks down data flow in accordance with the OSI model, and gives recommendations on improved security. The second part contains the proposed solution to improve ABC Foods' security posture with consideration of the customer's requirements regarding security measures and topology. It incorporates various aspects of the company's improved security infrastructure, including a firewall with configured rules, a logging and monitoring solution, host and network hardening, and role-based access control.

ABC Foods Network and Vulnerability Overview

1. Network Overview

The existing network consists of a router connected to our customer client through the internet, a web server and a switch that connects various devices and our DHCP/DNS server.

Router:

- Routes network traffic and allows communication from the internal network to the internet/customer client.

Web Server:

- The Web server is currently hosting ABC FOOD's online platform for selling food packages. This server is where the WordPress website is being hosted.

Switch:

- The switch connects devices from Finances, Management and Operations as well as the DHCP/DNS server.

DHCP/DNS server:

- The DHCP/DNS server facilitates the automatic assigning of IP addresses for devices connected to ABC FOOD's network and allows access to our website via www.abcfoods.co.nz.

2. Network Vulnerability

The vulnerable component within this network is the web server, hosting ABC FOOD's WordPress website. It is a critical component for the business as its main operation is to take in customer orders and details for the company to service.

As the web server is exposed to the internet it is at risk from attacks from threat actors considering a lack of security hardening and protection. As this component is hosting a WordPress website the vulnerabilities to be considered are unpatched plugins, weak authentication mechanisms, no Web Application Firewall (WAF), server misconfigurations and poor segmentation.

Threats relating to these vulnerabilities could be Web Application attacks that include SQL injections and Remote Code Execution (RCE).

3. Introducing a Vulnerability

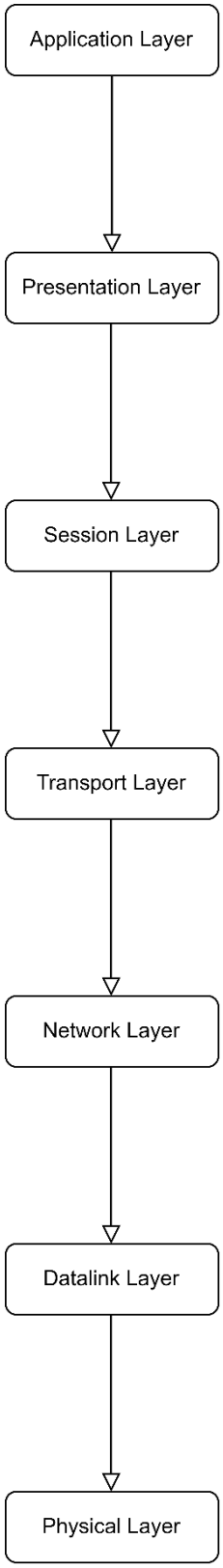
The vulnerability being introduced is a WordPress File Manager plugin (WPFM plugin) (Korhonen, 2020). This plugin is used to manage files from the WordPress dashboard and allows admins to upload, delete, and edit files directly within the web server's file system. In other words, the plugin allows comprehensive direct access to ABC FOOD's web server.

In this scenario, this plugin is running on an outdated version and does not carry out checks against authorisation or file types (Acunetix, n.d.). A known compromised script within the plugin can be freely accessed through a URL (https://abcfoods.co.nz/wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php) where no authorisation checks are carried out on the user or file being uploaded.

The exploit happens when an attacker executes a cURL request to the plugin link above. This POST request includes a malicious PHP file containing a code that creates a page/link (https://abcfoods.co.nz/wp-content/plugins/wp-file-manager/lib/files/payload3.php) within the web server that displays "Exploit successfull". This link can be distributed as the attacker wishes but it is important to note that codes with greater negative impact can be injected such as escalating privilege within the web server or creating a page from which credentials can be stolen.

In other exploitation cases, the attacker may upload a PHP file with a reverse shell on it .

4. Vulnerability data flow – OSI Model



Application Layer: This is where the attacker communicates to the WPFM plugin through HTTP, sending a crafted post request to the server, uploading a malicious file as raw data. The application layer processes the HTTP request against the plugin, then the server provides an HTTP response.

Presentation Layer: The data is encoded and compressed by the browser and the WPFM plugin receives it within the web server.

Session Layer: The connection is established and maintained, going through a HTTP request and response cycle.

Transport Layer: The raw data (PHP file) is split into segments for delivery where TCP headers are attached. The communication established through a 3-way handshake ensures reliable delivery and no packets are lost.

Network Layer: The segments are encapsulated into packets and an IP header is added (containing source and destination IP addresses). The packet is routed across the network finally reaching the singular router.

Datalink Layer: As the router and the web server are on the same network, a header is added to the packet by the router which turns this into an ethernet frame (as they are directly connected). The router uses its own MAC address as the source and the web server MAC address as the destination.

Physical Layer: The frame is converted into bits and transmitted across a physical medium, in this case an ethernet cable as the router and web server are directly connected.

5. Recommendations

5.1 Network Segmentation

Segmenting the network into VLANs helps to isolate different departments and critical infrastructure, reducing the potential attack surface. This limits the effects of a security breach, preventing attackers from easily traversing the network if one segment is compromised.

5.2 Firewalls and ACLs

Firewalls and strict access controls are essential for filtering incoming and outgoing traffic, helping to ensure that only legitimate communication is allowed (CISCO, n.d.). This helps to block unauthorised access to the network and protects against viruses, phishing emails, malware, and DDoS attacks.

5.3 Web Server Hardening

The web server which hosts the company's online platform, is a business-critical resource for ABC FOOD. It must be protected from attacks such as RCEs, SQL injections and DDoS attacks. Hardening the server ensures the confidentiality and integrity of customer data while maintaining the availability of the platform.

5.4 DHCP/DNS Server Security

Securing the DHCP and DNS servers is essential to prevent unauthorised devices from gaining network access and to protect against DNS spoofing. Securing servers helps ensure that devices are properly authenticated and that users are directed to legitimate websites.

5.5 Access Controls and Authentication

Strong access controls and authentication mechanisms, such as multi-factor authentication (MFA) and role-based access, safeguard sensitive data and systems. These measures ensure that only authorised individuals can access critical resources, reducing the risk of internal and external breaches.

5.6 Network Monitoring and Logging

Continuous monitoring and logging of network activities allow the detection of suspicious behavior and potential security breaches (Kidd, 2023). By implementing a SIEM and

centralizing logs, the network can be proactively protected, and incidents can be addressed as they arise in real time.

Improving ABC Foods Security Posture

1. Overview

1.1. Requirements

These requirements have been gathered from the Customer (ABC Foods).

Requirement	Details	How met
Requirement one	Firewall solution with configured rules	Paragraphs 2.2.1, 2.4.1
Requirement two	System hardening: a) Host hardening b) Network device hardening	Paragraph 2.2.2, 2.3.1, 2.4.2
Requirement three	Monitoring and logging solution	Paragraph 2.4.3
Requirement four	Role-based access control	Paragraph 2.3.2, 2.4.4

1.2. Constraints

There have been no identified constraints to document for the solution design.

2. Design

The design is shown using the following views:

Conceptual View: presents an overall high-level diagram and enlists its components.

Network View: Specifies firewall and router rules.

Security View: Specifies security policies for authentication (password policy) and breaks down roles with permissions/restrictions within the Role-Based Access Control Model to be implemented for user accounts in ABC Foods.

Solution Design View: Describes security controls recommended as ABC Foods Secure Solution.

2.1. Conceptual View

The below diagram demonstrates the concept solution for ABC Foods.

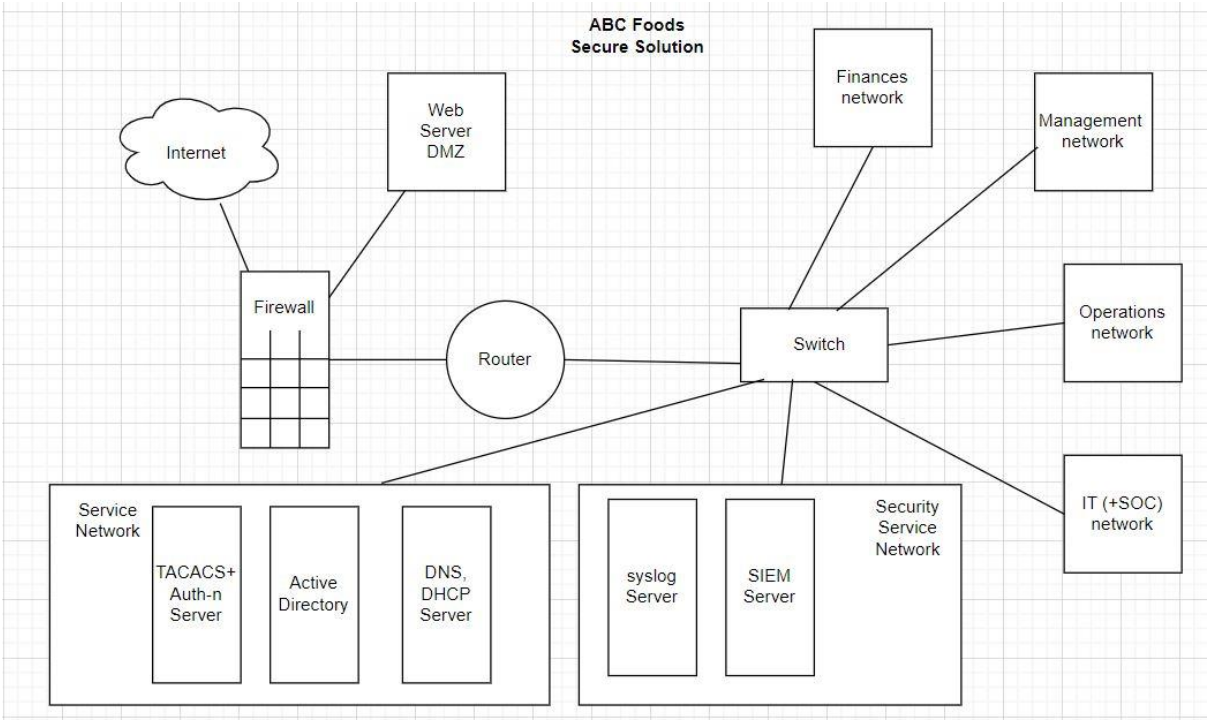


Figure 1: Conceptual View

The conceptual design includes establishing a demilitarised zone with a firewall as part of ABC network infrastructure. The existing server subnet with DHCP/DNS server is complemented with a domain controller with Active Directory and TACACS+ authentication server to manage role-based access within the company. Secure Service subnet is introduced to host a SIEM server and a syslog server.

Key	Component	Description
1	Firewall	Protects the company's internal network and the Web Server
2	Web Server	Hosts ABC Foods website
3	Router	Manages traffic forwarding based on in-bound and out-bound rules
4	Switch	Segments internal interwork into VLANs
5	Workstations	Support internal operations
6	SIEM Server	Aggregates logs

7	Syslog Server	Aggregates logs from network devices
8	Active Directory Server	Manages identities and access based on roles within the company
9	DNS/DHCP Server	Assigns internal IP addresses and performs domain name resolution into IP addresses

2.2. Network View

2.2.1. Firewall Rules

Name	Description	Source Zone	Destination Zone	ServiceID (port)	Actions	Log	Rule Type
Allow-HTTPS-Web-Server	Allows secure access (HTTPS) to the Web Server in the DMZ.	Internet	DMZ	TCP 443	Allow	Yes	Permanent
Allow-Internal-to-DMZ	Allows access (HTTPS) from the Internal Network to the Web Server	Internal Network	DMZ	TCP 443	Allow	Yes	Permanent
Allow-DNS-from-Internal-Network	Allow DNS queries from Internal Network to DNS servers, allowing users to resolve domain names.	Internal Network	Internet	UDP 53	Allow	Yes	Permanent
Allow-HTTPS-outbound	Allow secure access (HTTPS) from the DMZ and Internal Network to the internet.	DMZ/Internal Network	Internet	TCP 443	Allow	Yes	Permanent
Block-DMZ-Inbound-to-Internal-Network	Blocks all inbound traffic from the DMZ to the Internal Network, except for specifically allowed services.	DMZ	Internal Network	TCP 443	Deny	Yes	Permanent
Block-All-Inbound-Untrust-to-Trust	Blocks all inbound traffic from the internet to Internal Network, except for specifically allowed services	Internet	Internal Network	Any	Deny	Yes	Permanent
*DDoS-Protection	Helps mitigate DDoS attempts by setting maximum connection and packet limits, dropping traffic or rate-limiting it if these thresholds are exceeded.	Internet	DMZ/Internal Network	Any	Deny or Rate-limit	Yes	Permanent
Block-Access-Malicious-Websites	Uses URL Filtering to block access to inappropriate or suspicious/malicious content. Any traffic attempting to access such websites over HTTPS will be blocked.	Internal Network	Internet	TCP 443	Deny	Yes	Permanent
Block-inbound-Malicious-URL	Blocks phishing sites, malicious domains or known command and control servers.	Internet	DMZ/Internal Network	Any	Deny	Yes	Permanent
Block-Remote-Shell-and-Code Execution	Blocks attempts to upload or execute web shells and RCE payloads (e.g. cmd.exe, PowerShell, sh.exe)	Internet	DMZ/Internal Network	TCP 443	Deny	Yes	Permanent

*Block-Executable-Files	Blocks the download or upload of executable files that are commonly used in malware attacks.	Internet	DMZ/Internal Network	Any	Deny	Yes	Permanent
Block-HTTP-Traffic	Block inbound and outbound HTTP traffic.	Any	Any	HTTP 80	Deny	Yes	Permanent
Block-FTP	Block inbound and outbound FTP traffic – used for sending data in plaintext like usernames and passwords.	Any	Any	TCP 21	Deny	Yes	Permanent
Block-Telnet	Block inbound and outbound Telnet traffic – used for sending data in plaintext like usernames and passwords.	Any	Any	TCP 23	Deny	Yes	Permanent

***DDoS-Protection – Global DDoS Rate Limiting Profile Configuration:**

- Maximum New Connections per Second: 500
- Maximum Packets per Second: 10,000
- Action: Drop or Rate Limit based on thresholds

***Block-Executable-Files – Block File types:**

- Block files with extensions: .php, .exe, .bat, .msi, .vbs, .scr, .cmd, .pif, .js, .jar

2.2.2. Router Rules

1. Finances
    a. Allow outbound access for the Finances to the Service Network (AD, DNS/DHCP).
    b. Allow outbound access for the Finances to the Security Service Network (SIEM, Syslog).
    c. Allow outbound access for the Finances to the Internet.
    d. Allow inbound access to the Finances from the Service Network.
    e. Allow inbound access to the Finances from the IT.
    f. Block other outbound access for the Finances.
    g. Block all inbound access for the Finances.
2. Management
    a. Allow outbound access for the Management to the Service Network (AD, DNS/DHCP).
    b. Allow outbound access for the Management to the Security Service Network (SIEM, Syslog).
    c. Allow outbound access for the Management to the Internet.
    d. Allow inbound access to the Management from the Service Network.
    e. Allow inbound access to the Management from the IT.
    f. Block other outbound access for the Management.
    g. Block all inbound access for the Management.
3. Operations
    a. Allow outbound access for the Operations to the Service Network (AD, DNS/DHCP).
    b. Allow outbound access for the Operations to the Security Service Network (SIEM, Syslog).
    c. Allow outbound access for the Operations to the Internet.
    d. Allow outbound access for the Operations to the Web Server.
    e. Allow inbound access to the Operations from the Service Network.
    f. Allow inbound access to the Operations from the IT.
    g. Block other outbound access for the Operations.
    h. Block other inbound access for the Operations.

4. IT
    a. Allow outbound access for the IT to the Service Network (AD, DNS/DHCP).
    b. Allow outbound access for the IT to the Security Service Network (SIEM, Syslog).
    c. Allow outbound access for the IT to the Internet.
    d. Allow outbound access for the IT to the Web Server.
    e. Allow outbound access for the IT to the Finances.
    f. Allow outbound access for the IT to the Management.
    g. Allow outbound access for the IT to the Operations.
    h. Allow inbound access to the IT from the Service Network.
    i. Block other outbound access for the IT.
    j. Block other inbound access for the IT.
5. Service Network
    a. Allow outbound access for the Service Network to the Finances.
    b. Allow outbound access for the Service Network to the Management.
    c. Allow outbound access for the Service Network to the Operations.
    d. Allow outbound access for the Service Network to the IT.
    e. Allow outbound access for the Service Network to the Security Service Network (SIEM, Syslog).
    f. Allow outbound access for the DNS Server to Web Server.
    g. Allow inbound access to the Service Network from the Finances.
    h. Allow inbound access to the Service Network from the Management.
    i. Allow inbound access to the Service Network from the Operations.
    j. Allow inbound access to the Service Network from the IT.
    k. Block other outbound access for the Service Network.
    l. Block other inbound access for the Service Network.
6. Security Service Network
    a. Allow inbound access to the Service Network from all internal networks.
    b. Block all inbound access for the Security Service Network.
    c. Block all outbound access for the Security Service Network.
7. Web Server
    a. Allow inbound access to the Web Server from the IT.
    b. Allow inbound access to the Web Server from the Operations.

c. Allow inbound access to the Web Server from the Internet.
d. Allow outbound access for the Web Server to the Security Service Network.
e. Block all other outbound access for the Web Server.

Security View

2.2.3. User Account Password Policy

It is proposed that ABC Foods company is guided with the following principles for its password policy (White, 2024), (Vicente, 2024):

1. The use of password managers should be enforced.
2. Passwords should be at least 8 characters long (64 characters maximum).
3. Automatic monitoring of existing passwords should be performed to detect compromised passwords.
4. Password hints should be avoided.
5. "Copy-and-paste" and "show password" options for password input should be available.
6. Frequent password changes (short expiration periods) should be avoided.
7. Hashing and "salting" for password storage should be implemented.
8. Password lockout should be enforced after a series of unsuccessful authentication attempts (and CAPTCHAs for a lower threshold of failures to authenticate).
9. MFA should be implemented for critical applications.

2.2.4. Roles (Permissions and Restrictions)

Administrator:

- **Responsibilities**: Full access to all systems, network settings, and user permissions.
- **Permissions**: Manage all servers, configure firewalls, set up user roles, and access all business applications.

Manager:

- **Responsibilities**: Management of daily operations, including sales, inventory control, and customer order processing.
- **Permissions**: Access to sales data, inventory management, order processing systems, and employee scheduling.
- **Restrictions**: Cannot manage network security or configurations.

Operations:

- **Responsibilities**: Handle customer orders, process payments, and assist with order inquiries.
- **Permissions**: Access to the order management system and customer-facing sales platform.

- **Restrictions:** Cannot view financial data or change system settings.

IT Support:

- **Responsibilities**: Provide technical support for employees, troubleshoot network issues, and support system upgrades.
- **Permissions**: Limited access to IT infrastructure (e.g., servers, network devices)
- **Restrictions:** Cannot modify sensitive company data or user roles.

Casual Workers:

- **Responsibilities**: Temporary users (e.g., contractors, auditors) who need access to the guest Wi-Fi network.
- **Permissions**: Internet access only.
- **Restrictions:** No access to any business systems.

Finance: Roles within the finance team are carefully established according to specific job functions. These roles are intended to enforce segregation of duties, minimizing the risk of fraud, errors, or improper handling of financial data. Important roles may include:

- **Chief Financial Officer (CFO)**
- **Financial Controller**
- **Financial Analyst**
- **Accounts Payable (AP) Clerk**
- **Accounts Receivable (AR) Clerk**
- **Payroll Manager**
- **Internal Auditor**
- **Treasury Manager**

Each of these roles will have different access rights and responsibilities within the financial systems. (AFP , n.d.)

Access can include **viewing, editing, creating, deleting**, or **approving** financial data, among other tasks.

For Example:

- **CFO**: Full access to all financial data, reporting, and decision-making tools.
    - Permissions: **View/Modify** financial reports, approve budgets, manage high-level financial transactions, make strategic financial decisions, and oversee all financial operations.

- **Financial Controller**: Full access to accounting and financial reporting systems but limited approval authority compared to the CFO.
    - Permissions: **View/Modify** general ledger, **create/edit** financial statements, and **approve** certain accounting entries but cannot make high-level investment decisions.
- **Accounts Payable (AP) Clerk**: Limited access to AP systems and vendor payment records.
    - Permissions: **View/Edit** vendor invoices and **create transactions** for payments, but **cannot approve** payments or initiate large transfers.
- **Accounts Receivable (AR) Clerk**: Access to customer payment data and invoice generation.
    - Permissions: **View/Edit** customer invoices and payment records and **create transactions** for incoming payments, but **cannot approve** discounts, credits, or large write-offs.
- **Internal Auditor**: Access to audit logs and financial records to ensure compliance and accuracy.
    - Permissions: **View only** financial reports, audit logs, and transaction data for compliance checks but cannot modify or approve financial transactions.

2.3. Solution Design

2.3.1. Firewall

A firewall is the first line of defence that monitors incoming and outgoing traffic and decides to allow or block specific traffic based on a defined set of security rules (CISCO, n.d.) .

Implementing a Palo Alto firewall for ABC FOOD's network, addresses both internal and external threats while ensuring secure traffic flow between different network segments. The firewall functionalities include intrusion prevention and URL filtering, and the company can enforce granular security policies tailored to specific departments, users, and applications. This solution allows for monitoring, access control, fortification between network segments, and scalability.

Network Segmentation and Access Control

The firewall is configured to protect different parts of the network, such as Finance, Management, Operations, and Web Servers. These zones help isolate critical systems and control traffic flow between them. The firewall uses security policies or access control lists (ACLs) to define rules that govern which devices or users can communicate across zones.

An example is a policy that may be configured to allow traffic from the Finance VLAN to access the financial database server but block traffic to the Operations VLAN to prevent unauthorised access to sensitive financial information.

The purpose of network segmentation is to minimise the attack surface through the isolation of segments. By separating different, ABC FOOD can ensure that a breach in one area doesn't automatically lead to a compromise in another. Network segmentation is a fundamental security practice that prevents lateral movement.

Intrusion Prevention and Threat Detection

The Intrusion Prevention System (IPS) is enabled to detect and block malicious activity, including attempts to exploit vulnerabilities in internal systems like the WPFM plugin within the web server. The firewall's WildFire threat prevention engine is used to detect zero-day threats, advanced persistent threats (APT), and malware (Palo Alto, n.d.).

If an attacker attempts to exploit a vulnerability in the WPFM plugin by uploading a malicious PHP file, the IPS and App-ID feature detects and prevents this from happening. App-ID recognises that the plugin should only accept certain file types, so if it is one other than what is allowed, it is blocked.

The IPS provides proactive protection against known attack signatures, while WildFire enhances this by detecting zero-day malware and advanced threats that signature-

based defences may miss. Together, these features help prevent malware infections and exploits from compromising the network.

Application Control and Filtering

The firewall uses App-ID to identify, classify, and control applications running on the network. It is configured to allow business essential applications and block non-business related or risky applications, such as social media. Additionally, URL filtering can be applied to block access to malicious or inappropriate websites.

ABC FOOD may configure the firewall to block applications like Facebook or YouTube on employee devices, ensuring that network bandwidth is used for legitimate business purposes and preventing exposure to potential risks like phishing attacks or malware.

This gives organisations granular visibility and control over network traffic, especially the applications that generate it. By controlling which applications are allowed on the network, ABC FOOD can reduce the likelihood of introducing risks from non-business applications or potentially harmful websites.

Blocking non-essential and risky applications reduces the attack surface of the network. Many applications have vulnerabilities or can be used to bypass traditional security measures, making them attractive targets for attackers. By blocking access to unnecessary applications, ABC FOOD limits the potential for a security breach.

The Palo Alto firewall is a critical component of ABC FOOD's network security, which offers traffic inspection, application control, and fortification of network segments. By utilising its capabilities, ABC FOOD can secure their internal and external communications and prevent malicious activity. The firewall’s ability to scale with the organisation’s needs while providing granular control over network traffic ensures that ABC FOOD can continue to protect its infrastructure from evolving cyber threats.

2.3.2. System Hardening

2.3.2.1. Host Hardening

To apply a comprehensive approach to ABC Foods' cyber security, no host or communication channel should be left unattended, and security controls should be implemented for every device and their connection to one another. Host hardening comprises a set of measures aimed at making a device more resistant to threats from both the outside and the inside. From the operating system perspective, patch management policy is essential to make sure all critical updates are in place. All unnecessary applications, services, ports, and device drivers must be disabled, and only the ones that are required for operation should be turned on. Another security aspect involves identity access management and authentication policies. ABC Foods staff member should be grouped according to their corporate roles (finances, management, operations, IT team) and access to resources should be based on this

division. The principle of least privilege plays a key role here. Existing accounts and associated permissions are to be reviewed on a regular basis (Greco, n.d.). Strong password requirements must also be implemented.

Having an EDR that monitors hosts for threat-related activities and performs timely mitigation is another essential practice for companies like ABC Foods. EDR ensures continuous logging of suspicious behaviours (providing for enhanced visibility), alerting, and automated containment of attacks and acts an antivirus and an IPS at the same time (Microsoft, n.d.).

For additional protection of data on the machines, disk encryption can be used. There are options for Windows (BitLocker) and for Linux (LUKS). BitLocker security tool protects information from unauthorised access by encrypting the drive of a Windows computer. Its work is based on AES-128 or AES-256 algorithms (Gillis, 2022). With LUKS, a symmetric-key encryption is used to encrypt the entire hard drive or just a part of it (Anirudhadak, 2024).

On the physical side of securing data on the host, users can be assigned “Deny” permissions to Usbstor.pnf and Usbstor.inf system files to disable the possibility of installing a USB device on the computer and prevent data theft (Microsoft, n.d.).

2.3.2.2. Network Device Hardening

Network hardening is intended to protect a company’s network from attacks by applying relevant network security controls, appropriate device configurations, and removing functionalities that are not required (Agrawal, 2023).

One of the key concepts of secure network design is segmentation. By segmenting the network into smaller subnets physically or logically (using VLANs) for the purpose of only allowing access to the resources required to perform certain functions, a company can reduce the impact of infected devices spreading the malware across the network (CERT NZ, n.d.). This principle is already implemented by ABC Foods: each department is placed in its own network, and critical servers are separated from the rest of the network.

Firewalls, as mentioned previously, are primary network security devices. They can be used to create a DMZ and separate internet-facing subnets from the company’s internal infrastructure. Next-generation firewalls equipped with IDS/IPS functionalities, URL filtering, sandboxing, and other security features and operating at OSI Levels 2-7 perform a deeper packet inspection, looking into its content and more efficiently protecting the network from sophisticated attacks (Check Point, n.d.). To harden the firewall, policies must be configured following the identification of the most critical applications and in accordance with the principle of least privilege (Microserve, n.d.) and IPS feature implemented to block suspicious activity.

For additional security, ABC Foods can implement vulnerability scanning to its website to identify potential security flaws and take necessary action.

To ensure network device hardening, several steps need to be taken on each of the planes as proposed by the vendors, e. g. Cisco. On the management plane, only secure protocols need to be enabled (SSHv2, HTTPS), and insecure ones disabled (Telnet, HTTP). Access lists need to be configured to restrict access from networks and IP addresses other than the authorised ones. On the switch, unnecessary ports need to be disabled; for the enabled ones, the number of MAC addresses accessing them needs to be limited. All devices must support logging for the logs to be sent to a syslog server, and then further to a SIEM server. NTP configuration is essential for accurate correlation of timestamps in the logs. To implement RBAC model for accessing network devices, AAA authentication can be set up using TACACS+ protocol. Password policy must include a requirement for strong, complex passwords and a password retry lockout functionality.

On the control plane, an update policy must be implemented to patch vulnerabilities. The router must support rate limiting for DoS protection. It must have a CoPP feature enabled for the same purpose.

On the data plane, it is essential to configure ACLs on the router and the firewall to restrict unauthorised traffic and enable anti-spoofing protections. On the switch, networks must be segmented using VLANs (Cisco, 2024).

2.3.3. Monitoring and Logging Solution

2.3.3.1. Security Information and Event Management (SIEM)

Network monitoring tool provides companies with a clear structure of their network performance and helps to identify unusual network activity. Security Information Event Management is a software solution to help companies to analyse, detect and respond to potential security threats in real time with the help of Artificial Intelligence (AI) and Machine Learning (ML). SIEM is a security management system that combines two important factors to defend potential threats, Security information management (SIM) and security event management (SEM). SIEM aggregates data from all network devices and endpoints within the network, such as routers, servers, software, and firewalls. It runs under pre-defined rules to pick up patterns, suspicious activity, or threats in real time and alerts administrators for action and investigations against potential cybersecurity threats (Kidd, 2023). It operates as a tower and combines the network traffic centralized in one place. To visualise and understand data, tools like Splunk can be used for proper insight into the incidents to investigate responses.

2.3.3.2. Syslog Server

The Syslog Server is a supporting pier for logging and monitoring the network's infrastructure. It's a protocol that allows network devices like firewalls, switches, and servers to communicate with a logging server. The syslog server receives, categorizes and stores log messages in real time. Those log messages include a timestamp, device ID, IP address, and information required for the event. The log messages get sent via User Datagram Protocol (UDP) and the log file is classified depending on urgency, from 0 (emergency) to 7 (debug). The syslog server sends the information to the SIEM system, a centralized place for data to get efficiently checked.

2.3.3.3. Wireshark

Wireshark captures packets from any device within a network in real time and saves data offline to analyse. It can capture network traffic through Ethernet, Wireless, and Bluetooth. A packet represents a message between two devices and allows detailed tracking for incoming, outgoing, and internal communication. When a malicious activity is detected, Wireshark provides important information about a potential security incident.

When a malicious incident happened:

- Shows the number of malicious packets
- When did the attack happen (timestamps)
- Identifies IP address of the sender and receiver
- How big the packets are (in Bytes)
- How the packages have been sent for example TCP, DNS
- What kind of malicious content has been used

Companies need to stay ahead to protect their data from criminals who try to steal their most valued part, information. To do so, it is crucial to monitor all activities within a network. SIEM is a great solution, used together with tools like Syslog and Wireshark to centralize data communication of the network devices and network traffic in one place. Thanks to Artificial Intelligence and Machine Learning the tools can identify malicious activities in real time. With the prioritization of importance, administrators can prioritize important alarms to protect the company and not get overwhelmed by all unimportant activities.

2.3.4. Role-Based Access Control

One of the key security controls that ABC Foods should prioritize is Role-based Access Control (RBAC). ABC Foods faces unique security challenges as a global organization with a franchise in Auckland. To mitigate potential risks and safeguard against cybersecurity threats, we have determined that implementing RBAC is the most effective and appropriate security measure.

Role-based access control (RBAC) is a system for managing user permissions based on their organizational role rather than assigning access individually to each user. Instead of configuring specific access for every user, RBAC allows IT administrators to define the required access level for all individuals in each role and assign the corresponding permissions.

This approach enables IT teams to efficiently manage access by making bulk changes to user permissions within a role or adjusting the access level of a single user by modifying their assigned role. (Red Hat, n.d.)

Furthermore, RBAC has several benefits that can be implemented at this ABC Foods franchise. **RBAC Configuration** will be essential in reducing risk, securing sensitive data, and ensuring employees only have the necessary access. We have defined how the RBAC could be implemented and updated from their original plan.

Roles and Responsibilities

The first step is defining roles based on the Auckland franchise's job functions. In addition, different roles may be created, such as Administrator, Manager, Finance, Operations, IT team and any temporary or casual workers. For a detailed description of roles, responsibilities, permissions, and restrictions, refer to Paragraph 2.3.2.

RBAC Configuration Steps

1. **Assign Roles to all current users**: All employees are assigned their respective roles (Admin, Manager, Operations, Finance, IT Support) based on job function.
2. **Define Permissions for Each Role**:
    - For each role, define a set of permissions based on the principle of least privilege (i.e., users only get the minimum access necessary to perform their duties).
    - Admins can modify permissions, while non-admin roles (Managers, Operations) can only access the specific business systems they need.
3. **Implement Role-Based Access in Network Devices**:
    - Configure network devices (routers, switches, and firewalls) to enforce role-based access at the network level. For example, Managers and Admins can access sensitive internal applications, while Operations are restricted to customer-facing systems.
    - Implement centralised authentication management for accessing network devices (TACACS+ Server).
4. **Enforce Multi-Factor Authentication (MFA)**:

- Require MFA for all roles, particularly for users with higher levels of access, such as Admin and Manager roles, to prevent unauthorized access through compromised credentials.

5. **Audit and Review Access**:
    - Regularly audit role assignments and permissions, ensuring employees only have the access they need based on their current responsibilities.

(Microsoft , n.d.)

Conclusion

Cybersecurity is a crucial part of ABC Foods company to stay safe from potential cyber-attacks. In the proposed security solution, multiple security layers have been implemented within the companies' network. These layers include a firewall to ensure Intrusion Prevention and Threat Detection and network segmentation to minimise the impact of potential breaches, host and network hardening practices (including encryption to protect sensitive data, Multi-Factor Authentication with strong password policies), and Role-Based Access Control to restrict access to the company's network. To monitor the network and detect unusual behaviours, a Syslog Server is used to collect data from all devices within the network, and Wireshark tracks the network traffic in real time. These security mechanisms are used together with the Security Information and Event Management system to help ABC Food keep track of potential threats.

References

Acunetix. (n.d.). *WordPress Plugin File Manager Arbitrary File Upload (6.8)*. Retrieved from https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-file-manager-arbitrary-file-upload-6-8/

AFP . (n.d.). Retrieved from https://www.afponline.org/training-resources/resources/articles/Details/corporate-finance-job-descriptions

Agrawal, N. (2023). *Network Device Hardening (Try Hack Me)*. Retrieved from medium.com: https://medium.com/@technical_nitish/network-device-hardening-try-hack-me-8c2ef4ad156b

Anirudhadak. (2024). *LUKS: Linux Unified Key Setup Encryption on Disk Partitions of linux*. Retrieved from medium.com: https://medium.com/@anirudhadak25/luks-linux-unified-key-setup-encryption-on-disk-partitions-of-linux-71d41e4f8d53

CERT NZ. (n.d.). *Network segmentation and separation*. Retrieved from www.cert.govt.nz: https://www.cert.govt.nz/information-and-advice/critical-controls/network-segmentation-and-separation/

Check Point. (n.d.). *Next-Generation Firewall vs. Traditional Firewall*. Retrieved from www.checkpoint.com: https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/next-generation-firewall-vs-traditional-firewall/

Cisco. (2024). *Harden IOS Devices*. Retrieved from www.cisco.com: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#toc-hId--492986098

CISCO. (n.d.). *What is a firewall?* Retrieved from https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html

Gillis, A. S. (2022). *What is BitLocker?* Retrieved from www.techtarget.com: https://www.techtarget.com/searchenterprisedesktop/definition/BitLocker

Greco, T. (n.d.). *OS hardening checklist for cybersecurity*. Retrieved from www.connectwise.com: https://www.connectwise.com/blog/cybersecurity/os-hardening-checklist-for-cybersecurity

Kidd, C. (2023, october). *SIEM: Security Information & Event Management Explained*. Retrieved from Splunk: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html

Korhonen, V. (2020, September). *Severe 0-Day Security Vulnerability Found by Seravo in WP File Manager*. Retrieved from Seravo: https://seravo.com/en/0-day-vulnerability-in-wp-file-manager/

Microserve. (n.d.). *How to Harden Your Firewall and Fortify Firewall Security*. Retrieved from www.microserve.ca: https://www.microserve.ca/blog/firewall-hardening/

Microsoft . (n.d.). Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps

Microsoft. (n.d.). *How can I prevent users from connecting to a USB storage device?* Retrieved from support.microsoft.com: https://support.microsoft.com/en-us/topic/how-can-i-prevent-users-from-connecting-to-a-usb-storage-device-460ef516-8ac8-07af-e90b-0d9ac55bcd4d

Microsoft. (n.d.). *What is endpoint detection and response (EDR)?* Retrieved from www.microsoft.com: https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response

Red Hat. (n.d.). Retrieved from https://www.redhat.com/en/topics/security/what-is-role-based-access-control

Vicente, V. (2024). *NIST Password Guidelines 2024*. Retrieved from www.auditboard.com: https://www.auditboard.com/blog/nist-password-guidelines/

White, M. (2024). *NIST password guidelines: Full guide to NIST password compliance*. Retrieved from specopssoft.com: https://specopssoft.com/blog/nist-password-guidelines/