SAFEGUARDING CYBER LANDSCAPE OF A MANUFACUTURING INDUSTRY

PART I - EXECUTIVE SUMMARY

Overview

Implementing effective cyber security in a manufacturing industry organisation necessitates a comprehensive approach that includes developing a well-defined cyber security policy that is aligned with business goals, conducting thorough risk assessments, training employees on best practises, implementing strong access controls, deploying network and endpoint security measures, encrypting sensitive data, diligently managing patches, developing an incident response plan, conducting regular audits, and establishing a cyber security culture. This multimodal approach offers cyber threat protection while also building a security-conscious culture and adaptation to a shifting threat landscape.

Cyber security is a constant process, and it is critical to be cautious and adaptable. Threat environments change over time, thus updating and adjusting the cyber security strategy on a regular basis is critical to maintaining a robust defence against cyber threats. A comprehensive and proactive strategy to establishing cyber security within an organisation addresses a wide range of issues, from policy development to incident response. Each stage is broken down further below:

Develop a comprehensive cyber security policy and strategy

- Establish the cyber security goals and objectives for the organisation.
- Clearly define cyber security management roles and responsibilities.
- Align the cyber security plan with the company's goals and risk tolerance.

Conduct a Complete Risk Assessment

- Detect potential risks and vulnerabilities unique to the organisation.
- Sort risks according to their impact and likelihood.
- Create a risk management strategy to address any identified vulnerabilities.

Employee Education and Training

- Provide all personnel with cyber security awareness training.
- Train personnel on popular attack vectors including phishing and social engineering.
- Encourage the reporting of suspicious activities and foster a security-conscious culture.

Implement Strict Access Control Measures

- Require staff to have the least amount of access possible.
- For sensitive systems and data, use multi-factor authentication (MFA).
- Review and adjust access permissions on a regular basis.

Network Security

- Install firewalls, intrusion detection systems, and secure gateways.
- Control and monitor network traffic in order to detect and prevent unauthorised access.

Endpoint Protection

- On all devices, install antivirus software, endpoint protection technologies, and host-based firewalls.
- Update and patch endpoint security software on a regular basis.

Data Encryption

- Encrypt sensitive data at rest as well as in transit.
- Ensure that encryption keys are managed securely.

Patch Management

- Create a procedure for applying security fixes and updates as soon as possible.
- Update software, operating systems, and firmware on a regular basis to resolve vulnerabilities.

Incident Response Planning

- Create a detailed incident response plan (IRP).
- Include procedures for detecting, reporting, containing, eliminating, and recovering from events.
- Run regular drills and exercises to evaluate the IRP's effectiveness.

Security Audits and Assessments

- Conduct internal and external security audits on a regular basis.
- Assess the organization's security posture and identify any holes or flaws.
- Make use of audit findings to improve security measures..

Monitoring and Logging

- Implement centralized logging and real-time network and system monitoring.
- Configure alerts for suspicious activity and situations.

Communication and Reporting

- Establish explicit reporting mechanisms for security issues
  - Communicate with stakeholders like as employees, customers, partners, and regulatory authorities.

2. List of Vulnerable Parameter, Location discovered

Vulnerability Name	CWE Reference
A01:Injection	CWE-94: Improper Control of Generation of Code ('Code Injection')
A02:Broken Access Control	CWE-285: Improper Authorization
A03:Cryptographic Failures	CWE-326: Inadequate Encryption Strength
A04:Identification and Authentication Failures	CWE-287: Improper Authentication
A05:Insecure Design	CWE-657: Violation of Secure Design Principles
A06:Security Misconfiguration	CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File
A07:Vulnerable and Outdated Components	CWE-1104: Use of Unmaintained Third-Party Components
A08:Software and Data Integrity Failures	CWE-353: Missing Support for Integrity Check
A09:Security Logging and Monitoring Failures	CWE-532: Insertion of Sensitive Information into Log File
A10:Server-Side Request Forgery	CWE-918: Server-Side Request Forgery (SSRF)

1.1. Vulnerability Name: Improper Control of Generation of Code ('Code Injection')

CWE: 94

OWASP Category: Injection

Description: The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

Business Impact: The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

1.2 . Vulnerability Name: Improper Authorization

CWE: 285

OWASP Category: Broken Access Control

Description: The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action**.**

Business Impact: When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

1.3. Vulnerability Name: Improper Authentication

CWE: 287

OWASP Category: Identification and Authentication Failures

Description: When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.

Business Impact: Improper authentication can lead to violations of regulatory compliance requirements, such as data protection regulations. Reputation damage: A successful attack exploiting improper authentication can lead to loss of customer trust and reputational damage for the organization.

1.4. **Vulnerability Name**: Inadequate Encryption Strength

CWE: 326

OWASP Category: Cryptographic Failures

Description: The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required.

Business Impact: The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required. A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources**.**

1.5. **Vulneability Name**: Violation of Secure Design Principles

CWE: 657

OWASP Category: Insecure Design

Description: The product violates well-established principles for secure design

Business Impact: The product violates well-established principles for secure design. This can introduce resultant weaknesses or make it easier for developers to introduce related weaknesses during implementation. Because code is centered around design, it can be resource-intensive to fix design problems.

1.6. **Vulnerability Name**: J2EE Misconfiguration: Plaintext Password in Configuration File

CWE: 555

OWASP Category: Security Misconfiguration

Description: The J2EE application stores a plaintext password in a configuration file.

Business Impact: The J2EE application stores a plaintext password in a configuration file. Storing a plaintext password in a configuration file allows anyone who can read the file to access the password-protected resource, making it an easy target for attackers.

1.7. **Vulnerability Name**: Use of Unmaintained Third-Party Components

CWE: 1104

OWASP Category: Vulnerable and Outdated Components

Description: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

Business Impact: Reliance on components that are no longer maintained can make it difficult or impossible to fix significant bugs, vulnerabilities, or quality issues. In effect, unmaintained code can become obsolete.This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities.

1.8. Vulnerability Name: Missing Support for Integrity Check

CWE: 353

OWASP Category: Software and Data Integrity Failures

Description: The product uses a transmission protocol that does not include a mechanism for verifying the integrity of the data during transmission, such as a checksum.

Business Impact: If integrity check values or "checksums" are omitted from a protocol, there is no way of determining if data has been corrupted in transmission. The lack of checksum functionality in a protocol removes the first application-level check of data that can be used.

1.9. Vulnerability Name: Insertion of Sensitive Information into Log File

CWE: 532

OWASP Category: Security Logging and Monitoring Failures

Description: Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.

Business Impact: Because this can be used to exploit other threats related to CWE-284: Improper Access Control I rank it with a Moderate severity. An insider with knowledge of this could do many mischievous things and get away with them for a long time without victims knowing about it.

1.10. Vulnerability Name: Server-Side Request Forgery (SSRF)

CWE: 918

OWASP Category: Server-Side Request Forgery

Description: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

Business Impact: A successful SSRF attack can often result in unauthorized actions or access to data within the organization, either in the vulnerable application itself or on other back-end systems that the application can communicate with.

Stage: 2 Report

NESSUS Vulnerability Report

Overview

Using the Nessus tool, a vulnerability assessment report for the college website is created . This report summarises the findings of a vulnerability assessment performed on the college website using Nessus, a popular vulnerability scanning tool. The goal of this audit was to find potential flaws that could expose the website to security dangers.

The evaluation concentrated on the public-facing components of the college website, such as web servers, apps, and supporting infrastructure. The scanning tool Nessus was used to look for known vulnerabilities in the target assets. The evaluation was conducted utilising a combination of active and passive scanning. The following significant vulnerabilities were discovered during the assessment:

1. Outdated Software Versions

On web servers and backend systems, several instances of outdated software versions were discovered. Attackers targeting known flaws in older software could potentially exploit these vulnerabilities.

2. Weak SSL Configuration

The SSL setting on the website's login page was discovered to be insecure, possibly exposing sensitive user data to eavesdropping or man-in-the-middle attacks.

3. Missing Security Patches

Several systems needed important security fixes, raising the likelihood of exploitation by attackers looking for known vulnerabilities.

4. Cross-Site Scripting (XSS) Vulnerabilities:

Cross-Site Scripting attacks were discovered to be possible on a few online application pages. Because of these flaws, attackers may be able to inject malicious scripts into the website, potentially compromising user data or spreading malware.

5. Directory Traversal Attack Possibility

On the website, a directory traversal vulnerability was discovered, which might allow attackers to access files outside of the intended directory structure and obtain unauthorised access to sensitive information.

Based on the findings, the following recommendations are made to mitigate the detected vulnerabilities and improve the college website's security posture:

- Regular Software Updates - Keep all web servers and backend systems up to date in order to limit the chance of known vulnerabilities being exploited..
- SSL/TLS Enhancement - Improve SSL setups to ensure the encryption and integrity of critical user data. Make use of robust encryption protocols and cyphers.
- Patch Management - Implement a routine patch management strategy to apply security updates to all systems and software components as soon as possible.
- Web Application Security - Implement input validation procedures to prevent Cross-Site Scripting vulnerabilities in web applications. Test and secure web applications on a regular basis against common attack vectors.
- Directory Access Restrictions - Use proper access controls to avoid directory traversal attacks. Before using user input in file operations, ensure that it has been sanitised and validated.

This vulnerability assessment using Nessus revealed multiple flaws that, if not resolved, could expose the college website to security hazards. The college can improve its cyber security posture and lower the chance of successful attacks by implementing the recommended procedures. It is crucial to note that vulnerability assessments provide information about potential security flaws but do not guarantee the absence of other flaws. The results and suggestions in this report are based on an assessment completed at a given moment in time and may not reflect subsequent changes or revisions.

S.No	Vulnerability name	Severity	Plugin	Description	Solution	Business Impact	Port
1	HTTP Server Type and Version	Low	10107	This plugin attempts to determine the type and the version of the remote web server.	n/a		8880
2	Nessus SYN scanner	Low	11219	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled	Protect your target with an IP filter.		443

				target.			
3	Service Detection		22964	Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.			80
4	HyperText Transfer Protocol (HTTP) Information		24260	This test gives some information about the remote HTTP protocol – the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled,etc... This test is informational only and does not denote any security problem.			443
5	Common Platform Enumeration (CPE)		45590	By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.	n/a		0

Stage: 3

Report generated by Nessus™

vvsrec

Fri, 04 Aug 2023 20:05:31 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Expand All | Collapse All

35.213.138.163

Severity	CVSS v3.0	VPR Score	Plugin	Name
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
LOW	2.6*	-	54582	SMTP Service Cleartext Login Permitted
INFO	N/A	-	46180	Additional DNS Hostnames
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	10092	FTP Server Detection

INFO	N/A	-	42149	FTP Service AUTH TLS Command Support
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	11414	IMAP Service Banner Retrieval
INFO	N/A	-	42085	IMAP Service STARTTLS Command Support
INFO	N/A	-	10719	MySQL Server Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10185	POP Server Detection
INFO	N/A	-	42087	POP3 Service STLS Command Support
INFO	N/A	-	26024	PostgreSQL Server Detection
INFO	N/A	-	54580	SMTP Authentication Methods
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support

INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	-	42981	SSL Certificate Expiry - Future Expiry
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection

INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Hide