cOURSEWORK 1: Security assesment analysis

**Introduction**

Organizations must prepare for unplanned attacks, especially from hacktivist groups, which may aim to disrupt operations, expose sensitive information, or damage reputations. This assessment focuses on evaluating current vulnerabilities, potential risks, and developing strategies to enhance the organization's security posture in response to such threats.

**Why cyber security matters to organizations?**

**Cybersecurity is critical for organizations in today's digital world as it protects sensitive data, ensures availability, and safeguards trust.**

A diagram of a firewall

Description automatically generated

TOpology

Router:

responsible for directing data packets between different networks. It serves as the gateway that connects the internal network of an organization to external networks

WAF (Web Application Firewall):

It acts as a barrier between the web application and external users, filtering, monitoring, and blocking malicious traffic based on predefined security rules

Switch:

Responsible for managing the internal traffic

Vulnerability categorization

1. **High-Severity Vulnerabilities**

* Weaknesses in websites, APIs, or other externally accessible systems that could allow unauthorized access, defacement, or data breaches.
* Examples: Unpatched software, SQL injection vulnerabilities, or weak authentication mechanisms.

1. **Medium-Severity Vulnerabilities**

* poor Threat Intelligence lead to Limited or no monitoring of external signals, such as hacktivist group communications or malicious indicators targeting the organization.
* Employees not trained to recognize or respond to phishing campaigns or social engineering attacks that could be initiated as part of the hacktivist's efforts.

**III. Low-Severity Vulnerabilities**

* Legacy or peripheral systems not directly critical to operations but still exploitable as entry points for further attacks.
* Insecure management of official social media accounts, allowing attackers to hijack accounts for spreading misinformation or defamation.

# How to Prevent Web Application Vulnerabilities?

# Secure Authentication and Authorization

## **Strong Password Policies:** Enforce strong passwords and implement multi-factor authentication (MFA).

## **Role-Based Access Control (RBAC):** Limit access to resources based on user roles and least privilege principles.

# Data Security

## **Encryption:** Encrypt sensitive data both at rest and in transit using strong protocols (e.g., TLS/SSL).

# Proper Error Handling

## **Avoid Information Leakage:** Do not expose detailed error messages to users, as this can provide attackers with useful information.

## **Log Securely:** Ensure error logs are stored securely and do not include sensitive data.

# Update and Patch Regularly

##  **Monitor Vulnerabilities:** Stay informed about vulnerabilities in frameworks and tools.

##  **Apply Security Patches:** Regularly update all components of the application to address known vulnerabilities.

# Perform Regular Security Testing

##  **Penetration Testing:** Simulate attacks to identify vulnerabilities.

##  **Automated Scanning:** Use tools like OWASP ZAP or Burp Suite to test for common web vulnerabilities.

|  |  |
| --- | --- |
| **Policy** | **Description** |
| Password Management Policy | This policy ensures that passwords used within the organization meet security standards. It enforces strong password requirements, and periodic changes, and discourages reuse of old passwords. Passwords must be stored securely using hashing algorithms, and tools like password managers are recommended. |
| Acceptable Use Policy | This policy defines acceptable behaviors and usage of organizational IT resources. It prohibits activities like accessing unauthorized systems, sharing credentials, or installing unapproved software. Employees are educated about their responsibilities to maintain a secure and ethical work environment. |
| Continuous Monitoring Policy | This policy ensures the ongoing detection of threats and vulnerabilities within the organization's IT infrastructure. It involves using tools like intrusion detection systems (IDS0 and Security Information and Event Management (SIEM) solutions. The policy focuses on real-time visibility and prompt response. |
| Access Control Policy | This policy specifies rules for granting and constraining user access to systems, networks, and data. It includes role-based access control (RBAC) to ensure users only access information relevant to their responsibilities. The policy also includes authentication mechanisms like passwords and multi-factor authentication (MFA) to secure entry points. |
| Backup and Recovery Policy | This policy ensures data is regularly backed up and can be restored quickly in case of an incident. Backups are encrypted and stored in a secure cloud environment. The policy also enforce periodic testing of recovery procedures to ensure availability during disasters. |
| Patch Management Policy | This policy establishes a systematic mechanism for identifying, testing, and deploying updates or patches to software, hardware, and firmware to address vulnerabilities and improve system performance. The policy ensures that all systems remain secure and available by applying necessary updates promptly |

# Security Policies:

# Recommendation for mitigation

|  |  |
| --- | --- |
| Appliance | Cost |
| Web Application Firewall (WAF) | x |
| 1. Endpoint Protection and Malware Detection | xx |
| 1. Regular Patch Management | x |
| 1. Intrusion Detection and Prevention Systems (IDS/IPS) | x |
|  |  |
|  |  |
| Total Cost |  |