REMEDIATION PLAN

Overview

The assessment of DevEngineers' information security posture identified several critical vulnerabilities across key assets. This plan provides a structured approach to mitigate these vulnerabilities, ensuring improved security, compliance with standards such as ISO 27001, and the protection of sensitive data..

Purpose

The purpose of this remediation plan is to address identified vulnerabilities with a prioritized and actionable approach. It aims to enhance the organization's security posture, protect client information, and maintain stakeholder trust through systematic remediation and continuous improvement.

Asset	Vulnerability	Remediation Action	Timeline	Responsible Party	Verification/ Testing
Email Server	Email Spoofing (CVE-2023-5679)	Implement SPF, DKIM, and DMARC; conduct user awareness training	3 weeks	IT Security/HR Teams	Verify SPF/DKIM/ DMARC setup, phishing simulations
Web Application Server	XSS (CVE-2023-1234)	Implement input validation, update WAF rules	2 weeks	IT Security Team	Penetration testing to ensure XSS is mitigated
Database Server	IDOR (CVE-2023-	Apply patches,	1 week	Database Admin Team	Conduct access

	2345)	review and enforce access controls			control review and testing
Employee Workstations	Outdated OS (CVE-2023-3456)	Upgrade operating systems, apply patches	4 weeks	IT Support Team	Run vulnerability scans on updated workstations
Source Code Repository	Unauthorized Access (CVE-2023-6780)	Enhance authentication, review access logs	2 weeks	Development/IT Security	Test authentication mechanisms, review access logs
Network Infrastructure	Misconfiguration (CVE-2023-7890)	Review and update network configurations, enforce segmentation	2 weeks	Network Admin Team	Network security audit, penetration testing
Backup System	No vulnerabilities	Regular security reviews, ensure encryption and access controls	Ongoing	IT Security Team	Periodic reviews and tests
Remote Access	Weak VPN (CVE-2023-	Strengthen VPN	1 week		Test VPN security,

System	9012)	configuration, enforce multi-factor authentication		IT Security Team	review access logs
Customer Portal	CSRF (CVE-2023-0123)	Implement and validate CSRF tokens	2 weeks	Development Team	Conduct application security testing
Corporate Website	No vulnerabilities	Continuous monitoring, regular security updates	Ongoing	Web Development/IT Teams	Regular monitoring, periodic security assessments

Documenting and Reporting

1. Email Server

- **CVSS Score**: 7.0
- **Action Initiation and Completion Dates**: Initiation Date: August 10, 2024, Completion Date: August 20, 2024
- **Specific Steps Taken**:
    - Implemented SPF, DKIM, and DMARC.
    - Conducted user training on phishing awareness.
- **Challenges and Resolutions**:
    - *Challenge*: Conflicting DNS records.
    - *Resolution*: Collaborated with the DNS management team.
- **Verification and Testing Results**:
    - SPF, DKIM, and DMARC were tested and verified.
    - Phishing simulation showed a 90% reduction in successful phishing attempts.

- **Sign-Offs**: IT Security Team: August 21, 2024
- **Version Control**: Version 1.1, August 22, 2024

2. Source Code Repository

- **CVSS Score**: 7.5
- **Action Initiation and Completion Dates**: Initiation Date: August 12, 2024, Completion Date: August 22, 2024
- **Specific Steps Taken**:
    - Implemented MFA and updated access permissions.
- **Challenges and Resolutions**:
    - *Challenge*: Resistance from development teams.
    - *Resolution*: Provided training and communicated the importance of MFA.
- **Verification and Testing Results**:
    - MFA and access controls verified.
- **Sign-Offs**: Development Team Lead: August 23, 2024
- **Version Control**: Version 1.2, August 24, 2024

3. Network Infrastructure

- **CVSS Score**: 6.8
- **Action Initiation and Completion Dates**: Initiation Date: August 14, 2024, Completion Date: August 24, 2024
- **Specific Steps Taken**:
    - Audited and corrected network configurations.
    - Enhanced firewall rules and segmentation.
- **Challenges and Resolutions**:
    - *Challenge*: Legacy systems.
    - *Resolution*: Planned and executed configuration changes carefully.
- **Verification and Testing Results**:
    - Configuration and penetration testing completed.
- **Sign-Offs**: Network Engineering Team: August 25, 2024
- **Version Control**: Version 1.3, August 26, 2024

4. Backup System

- **No vulnerabilities were identified.**
- **Action Initiation and Completion Dates**: August 15, 2024 - August 18, 2024
- **Specific Steps Taken**:
    - Security review, encryption, and access controls were ensured.
- **Verification and Testing Results**:
    - Successful test restoration and access audit.

- **Sign-Offs**: Data Security Team: August 19, 2024
- **Version Control**: Version 1.4, August 20, 2024

5. Customer Portal

- **CVSS Score**: 6.5
- **Action Initiation and Completion Dates**: Initiation Date: August 17, 2024, Completion Date: August 25, 2024
- **Specific Steps Taken**:
    - Implemented CSRF tokens and strengthened access controls.
- **Challenges and Resolutions**:
    - *Challenge*: User experience with CSRF tokens.
    - *Resolution*: Usability testing conducted.
- **Verification and Testing Results**:
    - CSRF tokens and security testing completed.
- **Sign-Offs**: Security Team Lead: August 26, 2024
- **Version Control**: Version 1.6, August 27, 2024

6. Corporate Website

- **No vulnerabilities were identified.**
- **Action Initiation and Completion Dates**: August 20, 2024 - August 24, 2024
- **Specific Steps Taken**:
    - Configured WAF and enforced HTTPS.
- **Verification and Testing Results**:
    - Verified WAF and HTTPS configurations.
- **Sign-Offs**: IT Security Team: August 25, 2024
- **Version Control**: Version 1.7, August 26, 2024

References

ISO/IEC 27001:2013

- **Title:** Information Security Management Systems — Requirements
- **Description:** International standard for information security management systems (ISMS) which provides a framework for managing and protecting sensitive information.

Common Vulnerabilities and Exposures (CVE)

- **Title:** CVE List
- **Description:** A publicly available list of vulnerabilities and exposures. Each CVE entry includes a description of the vulnerability and its impact.

Vendor Documentation and Tools

- **Title:** Documentation for Specific Security Tools
- **Description:** Documentation and best practices for security tools used in the remediation process (e.g., WAF, antivirus software, VPN configurations).

Internal Documentation

- **Title:** DevEngineers Internal Security Policies
- **Description:** Internal documents and policies related to security practices within DevEngineers.