Security Policy & Risk Management Plan

- Identity Management | Encryption | Network Segmentation | Risk Management
- By: Rohinish Sharma
- 2023a7r050
- CSE-CyberSecurity

Project Objective

- To develop a comprehensive security policy and risk management strategy.

- Key Elements:
- - IAM (Identity Access Management)
- - Encryption
- - Network Segmentation
- - Risk Identification
- - Compliance (OWASP ASVS)

Security Policy Scope

- Covers:
- - Internal Users
- - Third-Party Vendors
- - Systems & Applications
- - Data Storage & Transmission
- - Remote Access & Mobile Devices

Identity and Access Management (IAM)

- Includes:
- - Password Policies
- - Multi-Factor Authentication (MFA)
- - Role-Based Access Control (RBAC)
- - User Provisioning & De-provisioning

Encryption Standards

- Data Protection:
- - Data at Rest: AES-256, BitLocker
- - Data in Transit: TLS 1.3, HTTPS
- - Email Encryption: S/MIME, PGP
- - Key Management: AWS KMS

Network Segmentation

- Network Segmentation Strategy:
- - VLANs for Separation
- - DMZ for Public Servers
- - Access Control via Firewalls

Risk Assessment Matrix

- Example:
- Asset: HR Database | Threat: Data Breach | Risk: High | Mitigation: Encryption + IAM
- Asset: Laptops | Threat: Theft | Risk: High | Mitigation: Full Disk Encryption

Compliance Mapping

- Mapped to OWASP ASVS, ISO 27001:
- - TLS Enforcement
- - Strong Authentication
- - Secure Sessions
- - Logging and Monitoring
- - GDPR Compliance

Incident Response & AUP

- Incident Response Steps:
- 1. Detection
- 2. Containment
- 3. Eradication
- 4. Recovery

- Acceptable Use:
- - Safe Device Usage
- - No External USBs
- - Restricted Personal Email Use

Conclusion & Recommendations

- Recommendations:
- - Regular Audits
- - Employee Training
- - IAM Automation
- - Secure Development