Security Policy

Security Policy

Security Design

System Examination

System Configuration

Firewalls and Filters

Hardening Software

Backups and Change Management

Access Control and Authentication

Virtual Private Networking

Logging and Monitoring

Security Policy and Management Support

SELinux

Linux Systems Security

Introduction to Digital Security Policies

Definition

- Digital security policies define rules and procedures to protect digital assets, including information and systems.

Importance

- Essential for safeguarding data, ensuring system reliability, and complying with regulations.

Scope

- Applies to all organizational digital assets, particularly Linux systems in this context.

CIA: Confidentiality, Integrity, Availability

Confidentiality

- Ensures that information is only accessible to those authorized.

Integrity

- Guarantees that information is accurate and unaltered.

Availability

- Ensures that information and resources are accessible when needed.

Applying the CIA Triad in Security Policies

Confidentiality in Policies

- Role-based access controls, encryption, secure communication channels.

Integrity in Policies

- Version control, audit trails, digital signatures.

Availability in Policies

- Redundancy, backup strategies, disaster recovery plans.

Sources for Formulating Digital Security Policies

Regulatory Requirements

- GDPR, HIPAA, and other compliance standards.

Industry Best Practices

- NIST guidelines, ISO/IEC standards, industry groups such as CIS.

Internal Audits and Assessments

- Identifying risks and vulnerabilities.

Creating a Digital Security Policy for Linux Systems

Step-by-Step Approach

- Identify assets, assess risks, define policies, implement, monitor, and review.

Policy Components

- Access controls, data protection, network security, logging and monitoring.

Tools

- SELinux, AppArmor, `iptables`, `auditd`.

Incorporating Authentication and Non-Repudiation

Authentication

- Verifying identity using passwords, SSH keys, biometrics.

Non-Repudiation

- Ensuring that actions cannot be denied, using digital signatures and logging.

Policy Integration

- Include authentication and non-repudiation measures in security policies.