Table of Contents

Server 3

Server: Physical Access 3

Server: Servers Resource Access 3

Server: User Authentication 3

Server: External Devices and Removable Media 4

Server: Services and Functionality 4

Server: Logging and Monitoring Policy 4

Server: Server Implementation Plan 5

Server: Server Acquisition 5

Server: UPS 6

Server: Server Configuration 6

Server: Server Network Configuration 6

Server: Server Operational Documentation 7

Server: Server Accident Readiness 7

Server: Server Monitoring 7

Server: Server Regular Security Checks 8

Server: Server Decommissioning 8

Server: Server Data Storage Encryption 9

Server: Server Operation Documentation Management 9

Server: Server Boot Security 9

Server: Security Critical Software and OS Components Encapsulation 10

Server: One Service Per Server Principle 10

Linux and Unix Servers 10

Linux and Unix Servers: Identification Assignment 10

Linux and Unix Servers: Removable Media Mounting 10

Linux and Unix Servers: Application Security 11

Linux and Unix Servers: Secure Software Packages Installation 11

Linux and Unix Servers: Groups and Users Management 11

Linux and Unix Servers: SSH-encrypted Data Transfer 12

Linux and Unix Servers: Privilege Escalation Prevention 12

Virtualization 12

Virtualization: Virtualization Implementation 12
Virtualization: Virtualization Environment Security Configuration 12
Virtualization: Virtualization Management System Security 13
Virtualization: Virtualization System Logging 13
Virtualization: Virtualization System Time 13
Virtualization: Virtualization System Architecture Planning 14
Virtualization: Virtualization System Network Architecture Planning 14
Virtualization: Virtualization System Maintenance 14
Virtualization: Virtualization Infrastructure Maintenance Rights and Roles 15
Virtualization: Virtualization Compatible Hardware 15
Virtualization: Virtualization Infrastructure Unified Configuration Requirements 15
Virtualization: Isolation of Virtual Guest with Different Security Requirement 15
Virtualization: Virtual Machines Isolation 16
Virtualization: Virtualization Server Resource and Configuration Checks 16
Virtualization: Virtualization System Regular Checks 16

Server

Server: Physical Access

Purpose

To ensure physical access security, prevent unauthorized access, tampering, or damage by environmment.

Server or server rack location must be restricted. Restriction implies:

- Separate server room or locked server rack
- Server room is locked, door has a closer, lock is configured to lock the door when it is shut
- Outside tampering with power and internet connection is sufficiently prevented
- Server rack is protected against possible water damage (e.g. Sprinkler System, intentional water spillage)

Server rack or Server Room access is granted only to System Administrator or an employee who is designated to maintain and configure server equipment.

Server: Servers Resource Access

Purpose

To ensure servers are used only for their intendent function, restrict access to authorized personnel .only.

Policy

Server is not used as a workstation and workstation is not used as a Server.

Acces to servers is granted only to System Andministrator or an employee who is designated to maintain and configure server equipment.

Server: User Authentication

Purpose

To ensure secure user authentication, restrict access based on the least privilege requiremments, secure remmote maintenance and configuration.

Policy

User authentication is done via personalized account, account sharing is prohibited.

User authentication is done following the main authentication procedure.

Minimal Access Requirements principe is followed and routine tasks must be executed utilizing limited administative accounts.

SSH, HTTPS protocols are only allowed for remote maintenance and configuration.

SSH private keys on user workstation must be always protected by a strong password.

Server: External Devices and Removable Media

Purpose

To ensure restriction of external devices only for maintenance only, enchance security by disabling unnecessary boot options and interfaces.

Policy

External devices and data carriers of the server are used only for server maintenance.

Booting the server from CD/DVD and removable media devices is deactivated in BIOS.

All unnecessary interfaces in the server are deactivated.

Server: Services and Functionality

Purpose

To ensure only required services and functionality are installed on the server.

Policy

Only a minimal set of services and functionality is installed required by the server's purpose of use.

Usage of additional trusted-source applications/packages is permitted during troubleshooting.

Installed applications/packages during troubleshooting must be documented and removed from the server after the troubleshooting is done.

Configuration of server software, services, and accounts is documented.

Server: Logging and Monitoring Policy

Purpose

To ensure security and availability of server by logging and monitoring security events

Policy

Security events are logged and checked once a week.

Access to Security logs has Security Specialist or an employee who is designated to execute tasks related to Cyber Security.

The log data is stored on the Server and is also temporarily stored on the NAS.

Log data stored on the NAS must be encrypted using a strong password.

Minimal set of logs that must be stored for security purposes:

- system startups and booting

- operating system and application logins and login attempts
- attempts to exceed privileges
- attempts to violate access lists or firewall rules
- creation or modification of users, user groups, and rights
- security-related error messages (e.g., power outages, hardware failures, exceeding size limits)
- security mechanism warning messages (e.g., alerts from antivirus applications)

Server: Server Implementation Plan

Purpose

To ensure a clear and documented server implementation

Policy

Server implementation Plan must at least contain:

- hardware platform, operating system, and application software
- suitability of hardware parameters (performance, memory capacity, throughput, etc.)
- space requirements and construction type
- server power consumption and heat dissipation
- types and number of communication interfaces
- user access rights
- logging
- monitoring
- integration with existing network management, data backup, and information security (e.g., antivirus software, intrusion detection system) solutions

Decisions made when planning the server implementation are documented

Server: Server Acquisition

Purpose

To ensure a structured and documented approach to server acquisition.

Policy

A specification of requirements has been prepared for the acquisition of the server and criteria have been established for the comparison of products:

- physical parameters (dimensions, fit in server rack)
- functionality requirements (required hardware interfaces, compatibility)
- reliability and user-friendliness (reliable information from an independent source)
- administration (manufacturer support and maintenance contract)
- total cost (acquisition and ongoing costs). b. From the perspective of information security, the following requirements have been set
- sufficient availability and data integrity

- secure protocols for data management
- compatibility with rights management and organization-wide security concept

Decisions made when planning the server acquisition are documented.

Server: UPS

Purpose

To ensure all servers are protected by a sufficicently powerful and maintained UPS system.

Policy

All Servers must be connected with the power-grid through UPS.

UPS maximum output power must be more than demand power by not less than 15%.

UPS is operated in manufacturer specifed temperature and humidity range.

Maintanance and capacity controls are made in manufacturer specified time intervals.

Maintanance and capacity controls are made according to the manual provided by the manufacturer.

All maintenance and controls must be documented and signed.

Server: Server Configuration

Purpose

To ensure consistent server configuration, following trusted sources and manufacturer guidelines.

Policy

Server system and application software are obtained only from authentic and reliable sources.

Server configuration follows manufacturer recommendations and recommended configuration, provided it is sufficiently secure and not conflicting with organizational needs and requirements.

Server baseline configuration is documented, even if default settings provided by the manufacturer are used.

Server baseline configuration complies with security guidelines. Security settings are checked before putting the server into operation and after any changes are made to the server.

Only necessary services for fulfilling the server's purpose are installed.

Servers must only be connected to the internet after installation and configuration are fully completed.

Installation and configuration steps of services and utilities must be documented.

Server: Server Network Configuration

Purpose

To ensure that server's network configuration is secure, maintaining control over firewall settings

Policy

The servers must have OS provided basic firewall active.

Any modifications to firewall rules must be documented, including rule names, affected ports, date, purpose of the changes.

Communication only with predefined hosts is permitted, while unnecessary protocols and ports must be blocked.

ICMP protocol must be disabled, with exceptions made during troubleshooting.

Review of the firewall rules must be done at least once annually.

Server: Server Operational Documentation

Purpose

To ensure that actions done on the server are traceable

Policy

Server operational documentation must be maintained to ensure traceability of all actions done on the server.

Configuration changes must be documented.

Documentation must contain and provide clear purpose of changes and result of actions done on the server.

Server: Server Accident Readiness

- Backup and Recovery plan are composed and implemented
- Backups must be always encrypted using strong encryption algorithms
- 3-2-1-1-0 backup strategy must be implemented
- Backup frequency is based on server purpose, but the period must be not less than once monthly
- Detailed Recovery Plan must be composed
- Recovery Plan must contain at least:
    - Introduction
    - Recovery Team
    - Pre-Recovery Checklist
    - Recovery Procedures
    - Backup Validation Procedure
    - Communication Plan in case of production environments
    - Post-Recovery Review

Server: Server Monitoring

Purpose

To ensure that server performance and health are constantly monitored, with clear and understandable data, notifications of issues.

Policy

Continuous monitoring of server performance and health must be implemented.

Monitoring must provide comprehensive observability through metrics visualization.

Monitoring solution must monitor crucial server metrics.

Alert rules must be configured to notify administrators of metric thresholds exceeding.

Server: Server Regular Security Checks

Purpose

To ensure that servers' security is tested regularly, and non-compliances are addressed immediately.

Policy

Regular Security Check must be done to public network exposed servers at least once a month.

Security compliance with password policies, user account activity, permissions, system configuration and network settings must be controlled.

Automated tools must be used when possible.

Results from security checks must be documented and non-compliance immediately eliminated.

Server: Server Decommissioning

Purpose

To ensure that servers are decommissioned securely, critical data is backed up and new servers are tested.

Policy

Servers decommissioning must follow a structured plan, preventing critical data loss and downtime.

Relevant stakeholders must be informed of the servers' decommissioning.

The check list must be composed and followed during decommissioning planning.

New production servers must be tested and approved before the decommissioning of the previous one.

Critical data must be backed up and migrated to a new server before decommissioning of the previous one.

Server: Server Data Storage Encryption

Purpose

To ensure that servers data storage is encrypted and encrypted keys safely stored.

Policy

All server data storage must be encrypted.

Data storage containing virtual machines must be encrypted.

Strong encryption must be used for data encryption.

Trusted Platform Module must be enabled in BIOS for encryption key management.

Recovery keys must be stored securely and encrypted.

Server: Server Operation Documentation Management

Purpose

To ensure server operation documentation is properly managed, documented and complies with legislation.

Policy

The server operation documentation is prepared based on the server main purpouse and type.

The Information Security must be at least covering the requirments stated in local legislation.

Access to Operation Documentation is restricted only to personnel that is designated to manage servers (e.g. System Administrator or a designated employee).

The server operation documentation is versioned and updated at least annualy.

Server: Server Boot Security

Purpose

To ensure server boot security, restrict access and provide integrity check for bootloader, kernel.

Policy

Access to boot settings management is restricted only to designated employees (e.g. System Administrator or designated employee).

Firmware configuration interface is secured by at least a password.

Operation Systems are used that support UEFI SB (Secure Boot).

UEFI Secure Boot is enabled at all times.

Bootloader, system kerneal are signed.

Unnecessary signing keys have been removed from the server.

Server: Security Critical Software and OS Components Encapsulation

Purpose

To ensure sensitive data security by isolating software and OS components.

Policy

Security-critical data of applications and operating system (e.g., authentication and certificate data) are encapsulated or isolated in a separate execution environment from other application and operating system components.

Applications processing data from untrusted sources (e.g., web browsers) are run in a separated execution environment from the operating system.

Server: One Service Per Server Principle

Purpose

To ensure that server is dedicated to a single service.

Policy

Each physical or virtual server provides only one server service.

Any exceptions are documented with justification.

Other services are not run on the virtualization server besides virtualization software and related services (such as virtualization management service, etc.).

Linux and Unix Servers

Linux and Unix Servers: Identification Assignment

Purpose

To ensure user and group identification management.

Policy

No username, User Identifier (UID), or Group Identifier (GID) are repeated.

Exception of repeated Group Indentifier are groups that are created by services to give acces to cli commands without sudo (e.g. docker group).

Each user belongs to at least one group.

All group identifiers listed in the file "/etc/passwd" are defined in the file "/etc/group".

Each group contains only necessary users.

Linux and Unix Servers: Removable Media Mounting

Purpose

To ensure that removable media is not automatically mounted when plugged in.

Policy

Automatic mounting of removable media (e.g. CD/DVD, USB flash drives) must be disabled at all times.

Linux and Unix Servers: Application Security

Purpose

To ensure components that enchance protection against exploits are enabled and configured.

Policy

Applications use kernel-activated mechanisms ASLR and DEP/NX to make exploiting application vulnerabilities more complex.

Kernel and user-space security features are enabled at all times.

Linux and Unix Servers: Secure Software Packages Installation

Purpose

To ensure that packages are securely and repeatebly installed.

Policy

Prior to installation, the integrity and authenticity of the software packages to be installed are checked by comparing the source and package hash.

When compiling software from source code, it is unpacked, configured, and compiled with non-privileged account rights.

When compiling software from source code, all choices made are documented so that the compilation process can be repeated with the same parameters.

Software is not installed in the server's root file system.

All installation steps are documented so that the configuration can be quickly restored if necessary.

Linux and Unix Servers: Groups and Users Management

Purpose

To ensure that configuration files are configured without mistakes and prevent unauthorized access.

Policy

Configuration files "/etc/passwd", "/etc/shadow", "/etc/group", and "/etc/sudoers" are never edited with a regular text editor.

Linux and Unix Servers: SSH-encrypted Data Transfer

Puprose

To ensure that data exchange is made only secure SSH protocol.

Policy

Data exchange is made only with SSH protocol.

All insecure data exchange protocols are deactivated.

User generated keys must be used for authentication .

SSH password authentication must be disabled on server first configuration.

Linux and Unix Servers: Privilege Escalation Prevention

- Services and applications are protected with kernel security module (for example AppArmor or SELinux)
- LXC and Docker container must be reviewed for vulnerabilities prior to installation

Virtualization

Virtualization: Virtualization Implementation

Purpose

To ensure that virtualization systemm are implemented securely, resource managed, monitoring established.

Policy

System administrators understand virtualization affects running IT systems and applications.

Access to virtualization system is using Least Privilege Principle.

Before implementing the virtualization system, it has been verified that:

- Virtualization host system has sufficient resources to facilitate virtualized solutions and maintain stable functioning
- Separation and Encapsulating of the applications running in the virtualization environment are met
- The virtualization system meets the availability and data transmission performance requirements

Continuous Monitoring of the Virtualization host system is established.

Virtualization: Virtualization Environment Security Configuration

Purpose

To ensure that virtualization environment is securely configured.

Policy

Access from guest systems to the virtualization server or host system is restricted.

Persistent data storage volume creation is allowed.

Guest Systems in rare cases allow to acces timezone configuration files in read-only mode for time zone configuration.

The configuration and security of virtual guest systems and the IT systems comply with the organization's security policy.

Virtualization: Virtualization Management System Security

Purpose

To ensure that management system is acces only using secure connection protocols and access is restricted.

Policy

Andiminstrative acces is restricted and only granted to System Administrators or a designated employee who executes System Administrators tasks.

Administrative interfaces can not be accessed from untrusted networks.

Secure protocols are used for data exchange such as SSH, HTTPS.

Virtualization: Virtualization System Logging

Purpose

To ensure that virtualization host system is constantly monitored and log data reviewed.

Policy

Virtualization host system state must be moniterod at all times.

In case of exhausting the resource of virtualization host system by the virtual server or virtual server resource depletion, the resource limits must be increased or the virtualized guest system relocated.

Log data of Virtualization host system is reviewed once per week.

Virtualization: Virtualization System Time

Purpose

To ensure that all virtualized systems time is synchronized.

Policy

All virtualized IT systems time are always synchronized.

Virtualization: Virtualization System Architecture Planning

Purpose

To ensure that virtualization system architecture is designed compliying with companys' policies, security requirements.

Policy

The architecture of the virtualization host system muste be desinged.

Policies and rules applicable to IT systems, applications, networks (including storage networks) are considered when designing the virtualization host system.

If a virtualization host system has more than one guest system, their security must be unified and allign.

Virtualization host system components are covered by administrative activities (e.g. configuration, upgrades).

Virtualization: Virtualization System Network Architecture Planning

Purpose

To ensure that network architecture for virtualization system is segmented and isolated.

Policy

The network architecture of the virtualization system must be designed.

If applicable the created network segments (e.g., management network, storage network) and processes how network segments are isolated and secured.

If applicable the management network is separated from the operation network. If necessary, a separate network segment is created for certain virtualization functions (e.g., live migration).

The network architecture must ensure the required availability of virtualized IT systems.

Virtualization: Virtualization System Maintenance

Purpose

To ensure that proper maintanance, operation and deecommissioning of virtualized systems.

Policy

At least following procedures must be established and implemented:

- Accounting of virtual servers and virtualized IT systems
- Operation of virtual servers and virtualized IT systems
- Decommisioning of virtual servers and virtualized IT systems

The administration rule of the virtualization system is updated as required, but not less than once annualy.

Testing and development environments are prohibited to operate on same virtualization host system as the production environment.

Virtualization: Virtualization Infrastructure Maintenance Rights and Roles

Purpose

To ensure that role based acces for maintanance is established.

Policy

Required rights and roles for managing the virtualization server are established.

Virtualization: Virtualization Compatible Hardware

Purpose

To ensure that hardere used is compatible with virtualization solution requirements.

Policy

The hardware used meets the requirements of virtualization solution.

Product support is guaranteed for the intended period of use on the hardware.

Virtualization: Virtualization Infrastructure Unified Configuration Requirements

Purpose

To ensure that configuration are standardized and consistent.

Policy

Unified type of configuration is defined for the virtualization infrastructure (including guest systems).

Guest systems are configured following the standard configuration.

Configuration rules are checked and adjusted if necessary but not less than once annualy.

Virtualization: Isolation of Virtual Guest with Different Security Requirement

Purpose

To ensure that virtual guest systems with diffrent security requirements are isolated.

Policy

Virtual guest systems running on the same host must be isolated at all times.

Any exceptions must be documented and justified.

Network connections of virtual guest systems are seperated in the virtualization host system.

Virtualization: Virtual Machines Isolation

Purpose

To ensure that unauthorized data transfer between virtualized guest systems is prevented.

Policy

Transfer of data between virtualized guest systems is prohibited and must be disabled.

Virtualization: Virtualization Server Resource and Configuration Checks

Purpose

To ensure that virtualization server has enough resources for operation and detect any unauthorized changes in configuration.

Policy

Monitoring metrics that must be considered during checks:

- resource sufficiency of the virtualization host system
- absence of conflicts in shared resources virtualization host system
- unauthorized changes in configuration files
- virtual networks are associated with the correct virtual IT systems

Configuration changes of the virtualization server are tested before implementation in production environments

Virtualization: Virtualization System Regular Checks

Purpose

To ensure that virtualization system operates in the intended state.

Policy

Regular reviews must include:

- Anomalies in the intended state of the virtualization host system
- Configuration matches the predefined standard configuration

Results of the reviews are documented, and any discrepancies identified are addressed at the earliest opportunity.