SecOps® Solution

Server security policy

Free Use Disclaimer: *This policy may be utilized entirely or in part by your organization without restriction. There is no need for prior authorization. Please email hello@secopsolution.com if you would like to contribute a new or updated version of this one.*

1. Overview

Server security includes the procedures and equipment required to safeguard the priceless information and assets stored on a company's servers and if these servers are vulnerable can lead to a key point for malicious threat actors. So, it is crucial to ensure that there is a consistent server installation policies, ownership, and configuration management.

2. Purpose

This policy's objective is to specify the guidelines for the base configuration of the servers owned and operated by **<Company Name>.** It aims to ensure that servers maintain a security posture that will reduce the chances of unauthorized access to the information.

3. Scope

All employees, including permanent, temporary, consultants, and contractors of **<Company Name>** must follow this policy.

It ensures that all server security assessment is done by the employee or professional appointed by the **<Company Name>**. And the results obtained after assessments are kept confidential and distribution of results outside the company is prohibited unless approved by the Company.

This policy is specifically for equipment on the internal network. For secure configuration of equipment external to the DMZ, refer to the Internet DMZ Equipment Policy.

4. Policy

4.1 Ownership and Responsibilities

All internal servers deployed must be owned by an operational group that is responsible for system administration. Approved server configuration guides

must be established and maintained by each operational group, based on business needs, and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

4.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved InfoSec guidelines.
- Services and applications that will not be used must be disabled where practical. Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when the immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trusting relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.

- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security-related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

4.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within.
- Audits will be managed by the internal audit group or InfoSec, in accordance with the Audit Policy. InfoSec will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.5 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Related Standards, Policies, and Processes

- Audit Policy
- DMZ Equipment Policy

6. Definitions and Terms

DMZ: De-militarized Zone. A network segment external to the corporate production network.

7. Revision History

Version	Date	Description
1.0	15-10-2022	Initial Policy