Hardening Guidelines

Santos Bevilaqua Advogados

Summary

1. Introduction

Hardening is the process of enhancing the security of an infrastructure to withstand attacks. It encompasses everything from identifying vulnerabilities and mapping threats to implementing actions that mitigate or minimize risks, as well as executing corrective activities.

This security procedure includes various practices, such as:

- ⇒ User authentication and access authorization control.
- ⇒ Maintenance of logs for future audits.
- ⇒ Clock synchronization to ensure data consistency.
- ⇒ Application of secure access techniques to the infrastructure.

In addition to these measures, hardening also involves keeping records of operations, ensuring system characteristics are maintained (such as constant software updates), guaranteeing that only essential resources are active, and meeting configuration requirements, including regular backups.

It is essential to emphasize that non-compliance with these guidelines can significantly impact on the firm's efficiency. Therefore, all staff members—regardless of their hierarchical position—are obligated to follow the guidance presented in this document.

Santos Bevilaqua Advogados formalizes the organization's commitment to the protection of its information assets, whether owned by the firm or under its custody.

The primary objective of these guidelines is to establish strategies for maintaining Information and Communications Security. The aim is to ensure the confidentiality, integrity, availability, and authenticity of data and information. This includes all data and information that are produced, acquired, stored, in transit, discarded, owned by, or under the control or operation of Santos Bevilaqua Advogados' systems.

2. Scope

Compliance with this policy is mandatory across all physical premises of Santos Bevilaqua Advogados, including:

⇒ Headquarters

⇒ Regional units

⇒ Processing centers

⇒ Any other locations owned by or under the custody of Santos Bevilaqua Advogados.

2.1. Covered Computing Assets and Environments

The hardening guidelines also apply to all computing environments and information assets owned by or under the custody of Santos Bevilaqua Advogados. This includes, but is not limited to:

⇒ Computers

⇒ Routers and switches

⇒ Servers

⇒ Databases

⇒ Storage systems

⇒ Communication networks

⇒ Applications and software in general.

2.2.Staff Responsibilities

All employees and associates of Santos Bevilaqua Advogados, regardless of their role, must fully understand and comply with the established guidelines. Adherence to these standards is crucial for the company's information security.

2.3.System and Application Changes

Any changes or modifications to the systems and applications of Santos Bevilaqua Advogados must strictly follow the internal standards and procedures established for change management, ensuring the integrity and security of the environments.

3. Regulatory References

Technical Standards of the Brazilian Association of Technical Standards (*Associação Brasileira de Normas Técnic*as- ABNT) A set of standards that establish guidelines and requirements for various aspects of information security, such as NBR ISO/IEC 27002:2022, which addresses the information security management system.

https://www.abntcatalogo.com.br/pnm.aspx?Q=T2JVQ1FZQkZsejNJL1QvVEhmcXlZTUdITWczYm9IZGhGOFNhcnc0WlVDbz0=

4. Hardening Procedures

4.1.Authentication

Authentication is the process of verifying a user's identity when attempting to access systems. According to the ABNT NBR ISO/IEC 27000 standard, it is the assurance that the identity of an entity is genuine.

At Santos Bevilaqua Advogados, the basic user authentication requirements include:

⇒ Creating an individual user account for each active operator and deactivating old accounts.

⇒ Avoiding the use of a single default administrative account shared among different users.

⇒ Requiring the use of strong passwords.

⇒ Prohibiting the storage of passwords in plain (unencrypted) text.

⇒ Using multi-factor authentication (MFA) for an additional layer of security.

4.2.Authorization

Authorization defines the access privileges granted to users who have already been authenticated in the systems It follows the principles of "least privilege" and "need to know" — that is, each user has access only to what is strictly necessary to perform their duties.

The authorization procedures at Santos Bevilaqua Advogados are:

- All users of the Santos Bevilaqua Advogados System must have permission to access equipment according to their job responsibilities.
- The administrator password must not be shared with all users, in order to prevent accidents, malicious actions, or use by individuals without the proper training to handle such resources.
- External devices to be connected to the Santos Bevilaqua Advogados network must first be authorized by the Information Security Committee.
- Users are classified into privilege groups, a common feature in many systems, to efficiently manage their permissions.

4.3.Audit

Auditing involves accessing information about how users utilize infrastructure resources.

The basic audit procedures are:

⇒ Maintain a detailed record of each user and their respective permissions.

⇒ Log all user actions within the systems.

⇒ Classify logs by criticality level: Informational, Warning, and Critical.

⇒ Classify logs by type: Documents, Logs, and Configuration Backup.

⇒ Ensure that all logs have the correct date and time.

4.4. Access

Access to network equipment must be performed securely, following these basic procedures:

- ⇒ All equipment must be encrypted.
- ⇒ All equipment must have an automatic lock rule based on inactivity.
- ⇒ Access permissions are granted according to the permission policies defined by managers.
- ⇒ Permissions vary according to each employee's role.

4.5. Logs

All logs generated by network operation and configuration must follow these basic procedures:

- ⇒ Logs must be configured with different levels of criticality.
- ⇒ The date and time of the logs are synchronized with https://ntp.br/.

4.6. Server Time Management

We understand that time synchronization is essential because all network management, protection, planning, and troubleshooting activities depend on accurately determining when events occur. Time is the only common reference across all devices in the network. Without synchronization, it is difficult — or even impossible — to correlate and analyze events properly.

Additionally:

- ⇒ Tracking security breaches, network usage, or issues affecting multiple components can be nearly impossible if the timestamps in the logs are inaccurate. Time is often the critical factor that allows mapping an event on one network node to a corresponding event on another.

⇒ To avoid confusion in shared file systems, it is important that modification timestamps remain consistent, regardless of the machine where the files are stored.

4.7. Patching

Operating systems and many software programs have built-in components that may contain security vulnerabilities. To mitigate this, vendors regularly release security patches that must be applied.

Ignoring these updates can allow a hacker to compromise a computer, threatening the integrity of the Santos Bevilaqua Advogados network and all connected devices.

Santos Bevilaqua Advogados uses the Microsoft Windows operating system. Security and critical patches related to this system must be installed as quickly as possible.

To manage and prioritize the application of updates and fixes, security patches are classified according to Microsoft's severity rating system, detailed in the following tables:

Classification	Description
Critical	Machines with vulnerabilities may become vectors for the automatic spread of viruses, without requiring any user interaction.
Important	Vulnerabilities that may lead to loss of confidentiality, integrity, or availability of user data, and may also affect the performance or reliability of processing resources.
Moderate	Security fixes for vulnerabilities that become significantly less exploitable through default configurations, regular audits, or mechanisms that hinder their activation.
Low	Vulnerabilities that are extremely difficult to exploit or that, even when exploited, result in minimal impact.

4.8.System

All new systems must follow these recommendations:

⇒ Install according to the vendor's guidelines.

⇒ Disable unused interfaces.

⇒ Disable unused or insecure services, recursive DNS, and NTP Server.

⇒ Remove or disable unused extra feature packages.

⇒ Keep the system always updated with the latest stable version.

⇒ Perform vulnerability scans and remediate all detected vulnerabilities.

5. Implementation and Update

The Encryption Policy of Santos Bevilaqua Advogados shall be updated whenever necessary.