Isobar Server Security Policy

1.0 Overview

Unsecured and vulnerable servers remain a major point of entry for malicious threat actors. Consistent installation policies for servers, ownership management, and configuration are all about doing the basics well.

2.0 Purpose

The purpose of this policy is to establish the standards for the base configuration of Isobar's internal server equipment. The policy will minimize unauthorized access to Isobar's proprietary information and technology.

3.0 Scope

This policy applies to server equipment owned and/or operated by Isobar, and to servers registered under any Isobar-owned internal network domain. This policy is specifically for equipment on the internal Isobar network.

4.0 Policy

4.1 Ownership and Responsibilities

4.1.1 All internal servers deployed at Isobar must be owned by an operational group that is responsible for system administration. Approved server configuration guidelines must be established and maintained by the Webmaster(s) of Isobar, based on business needs and approved by the General Management of Isobar. A Webmaster should monitor configuration compliance and implement an exception policy adapted to the Isobar environment. The Webmasters must establish a process for changing the configuration guidelines, which must be reviewed by the General Manager. The following requirements must be met:

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

4.1.2 The Webmaster(s) may monitor and audit equipment, systems, processes, and network traffic for security, compliance, and maintenance purposes.

4.2 Configuration Requirements

4.2.1 The Web Server used should be compatible with the Operating System of the local machine.

4.2.2 Applications that will not be used must be disabled where practical.

4.2.3 Trusted Antivirus software must be installed and updated on all applicable Isobar devices.

4.2.4 Servers should be physically located in an access-controlled environment.

4.2.5 All web applications including PHP and MySQL should be updated every six months, if and only if doing so will not interfere with the smooth running of Isobar business activities.

4.2.6 All updated web applications must be adequately documented.

4.2.7 The virtual host that hosts the Isobar website must have an SSL certification signed by a trusted Certificate Authority to comply with Google's website security requirement.

4.2.8 The server logs must be authenticated in order to be accessed online.

4.2.9 Databases should be backed-up every weekend.

4.3 Monitoring

4.3.1 Approved log analyzer should be used for analyzing and reporting server logs.

4.3.2 All security-related events on sensitive systems must be logged and kept online for a minimum of 6 months.

4.4 Emails & Passwords

4.4.1 Employees can only use work email addresses to send work-related emails.

4.4.2 All emails must be encrypted.

4.4.3 Passwords must be used to restrict access to all sensitive data.

4.4.4 Work-related passwords of employees must be different from that of their personal accounts.

4.4.5 All passwords should be changed at least, once a year.

4.4.6 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords must be treated as sensitive, Confidential Isobar information.

4.4.7 Passwords may be stored only in "password managers" authorized by Isobar.

4.3.8 Any user suspecting that their password may have been compromised must report the incident and as soon as possible and change the password.

4.5 Countermeasures to Common Threats

4.5.1 Isobar will never ask its members for sensitive information such as the member's username and password combination. Only work emails (e.g. "*****@isobar.org") will be used to send emails to members to avoid phishing.

4.5.2 Member logins will also require CAPTCHA answer verification in order to avoid brute-force attack.

4.5.3 Various countermeasures will be employed including Intrusion Protection Systems and reverse DNS lookup in order to prevent or fight Denial-of-Service attacks.

5.0 Compliance

5.1 Compliance Measurement

The BadaCorp team will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the BadaCorp team in advance.

6.0 Enforcement

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

7.0 Definition and Terms

Term	***Definition***
BadaCorp	The parent company of Isobar.
Denial of Service	A cyber-attack in which the perpetrator seeks to make a network resource unavailable to its intended users by indefinitely disrupting services of a host connected to the internet.
Brute force attack	When an attacking submits many passwords with the hope of eventually guessing correctly.
Phishing	A fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity.

References

Avolio, F. M., Pinzon, S. D., & Fallin, S. (2007). *Producing Your Network Security Policy*. Retrieved from Watchguard: http://www.watchguard.com/docs/whitepaper/securitypolicy_wp.pdf

SANS [a]. (2017). *Password Protection Policy*. Retrieved from Consensus Policy Resource Community: https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

SANS [b]. (2014). *Server Security Policy*. Retrieved from Consensu Policy Resource Community: https://www.sans.org/security-resources/policies/server-security/pdf/server-security-policy

Wikipedia, the free encyclopedia [a]. (2020). *Brute-force attack: Counter measures*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Brute-force_attack

Wikipedia, the free encyclopedia [b]. (2020). *Denial-of-service attack: Defense techniques*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Denial-of-service_attack

Wikipedia, the free encyclopedia [c]. (2020). *Phishing: Anti-Phishing*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Phishing