THAT'S IT SERVER SECURITY

Mark Boyle

THAT'S GROUP LTD 7 Merryfields, Ashby Road, Watford, WD245HT

Contents

Server Security Policy (Brief Version)

Overview

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

Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by . Effective implementation of this policy will minimize unauthorized access to proprietary information and technology.

Scope

All employees, contractors, consultants, temporary and other workers at and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by or registered under a -owned internal network domain.

Policy

General Requirements

OS / Best Practice

All servers regardless of operating system are configures with OS manufacturers best practice guideline and where applicable BPA (best practice analyser) will be run on a bi annual basis to insure compliance with this policy.

Patch Management

All That's Group Server patching is handled via a combination of the Kaseya Management Suite and Plesk Control Panel. All servers are set to receive critical security patches on release and optional patches are installed on each second Tuesday. Vulnerability scans for critical items are run on a weekly basis handled by the Kaspersky security suite and dealt with accordingly.

Antivirus

All servers regardless of Operating system are installed with Kaspersky security suite. This provides effective security for data at rest on the platform. All virus incidents are remediated within 4 hours of detection.

Antimalware

All servers regardless of operating system are installed with Malware Bytes anti-malware, detections are remediated within 4 hours of detection.

User Management / Password Management

All server administration accounts are handled via secure keys. These keys are generated and stored via Kaseya Auth Anvil meaning only authorised personnel can access the root level of any given server.

Where applicable server technologies will have 2FA enabled for access as a requirement for any administrative or super user level.

Directory Level Security

All servers will have appropriate user segregation to insure that data is not accessible between accounts.

Logging

Where applicable all server traffic and functionality is logged to a third party cloud logging service. Log are examined by machine learning to find failed login attempts and other suspicions traffic which is then investigated on a monthly basis.

All logs are retained indefinitely to allow investigation in the event of any breach of security.

Data in Transit

All data in transit to and from servers will (optionally client level configuration) be encrypted by SSL / TLS with appropriate high level ciphers. All weak and vulnerable ciphers are removed from servers to conform to present industry best practice.

Change Management

All BAU activities are subject to change management passed through appropriate server administration layers to insure that no activity taken in maintenance will result in any server vulnerability.

All changes are pushed to staging servers before being used in a production environment.

All work / changes on any production environment are documented and recorded.

Server Registration

Servers must be registered within the corporate enterprise management system (Kaseya). At a minimum, the following information is required to positively identify the point of

contact:

- Server contact(s) and location.
- 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

- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the Audit Policy.

Configuration Requirements

- 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 a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when 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 trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will be sufficient.
- 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.

Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

1. All security related logs will be kept online for a minimum of 1 week.
2. Daily incremental tape backups will be retained for at least 1 month.
3. Weekly full tape backups of logs will be retained for at least 1 month.
4. Monthly full backups will be retained for a minimum of 2 years.
5. Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management.
6. 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.

Policy Compliance

Compliance Measurement The InfoSec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

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

Non-Compliance An employee found to have violated this policy may be subject to disciplinary action, up to and including dismissal.