Security Standard: Servers, Server-based Applications and Databases

Scope

This standard applies to all servers (including production, training, test, and development servers) and the operating system, applications, and databases (unless explicitly excluded) defined by this standard that provide services to the RIT community.

This standard applies to administrators and information trustees of all servers that are connected to the Institute network.

Requirements

The following security controls should be applied to, enabled, and running on all servers that connect to (or access) the Institute network no later than August 1, 2009, and all times thereafter. If products are not available from reputable commercial or reliable open source communities for a specific requirement, then the specific requirement is waived until an appropriate solution is available. When the term "appropriate" is used, systems administrators are expected to use their professional judgment in managing risks to the information and systems they support.

1. **Secure Network and Physical Environment**
   - 1.1. Servers should be secured in locked racks or areas with restricted access.
   - 1.2. All non-removable media should be configured with file systems with access control enabled.
   - 1.3. Servers should be set up in an environment with appropriately restricted network access.
   - 1.4. Whenever possible, the server shall display a trespassing banner at login. Sample banner language may be found at http://www.rit.edu/security/content/server-security-standard

2. **Patching/ Server Maintenance**
   - 2.1. A documented maintenance process should be established to keep applications and operating systems at the latest practical patch levels.
   - 2.2. Vendor-supported patches should be available to RIT for operating systems and applications. Use of operating systems or applications that are no longer supported by the vendor or an open source community requires filing an exception request with the ISO.
   - 2.3. The maintenance process should include a reasonable timetable for routine application of patches and patch clusters (service packs and patch rollups).
   - 2.4. In order to maximize protection of servers from the exploitation of vulnerabilities, for systems supported by vendor patches, patch application should be integrated into an overall server maintenance process.
   - 2.5. In order to support effective incident response, there should be a means to inventory the current level of patches specific to the server.

2.6. In order to reduce the exposure of unpatched servers and to reduce the efforts required to manage servers in a dynamic update environment, there should be a process for monitoring patch installation failures.

3. Logging

3.1. In order to support the creation of an operational baseline for system, and service activities, and to detect and document access control violations, servers should be configured with appropriate real-time OS/application logging turned on.
3.2. There should be a documented process for routine log monitoring and analysis.
3.3. The systems administrator should review the logging process for effectiveness on a semi-annual basis or at a more frequent interval appropriate for the system.
3.4. A log monitoring process should be done on an appropriate schedule.
3.5. Where capabilities exist, logging should include at least 2 weeks of relevant OS/application information. Typically, logging should include the following elements:
- All authentication
- Privilege escalation
- User additions and deletions
- Access control changes
- Job schedule start-up
- System integrity information
- Log entries should be time and date stamped

3.6. Intentional logging of private information, such as passwords, etc., is prohibited.
3.7. Logging should be mirrored in real time and stored on another secure server.

4. System Integrity Controls

4.1. To prevent and detect unauthorized programs from running, systems should be configured to restrict changes to start-up procedures.
4.2. There should be a documented change control process for systems configuration.
4.3. Risks should be mitigated by disabling all unused services.
4.4. Up-to-date anti-virus software and definitions should be used where available.
4.5. Servers should use a host firewall.
4.6. Where available, host-based intrusion prevention system software should be enabled.
- Host-based intrusion prevention (HIPS) software should be employed on authentication servers
- A list of recommended host-based intrusion prevention software may be found at https://www.rit.edu/security/content/technical-resources

4.7. Hardware-based system integrity control should be enabled where available

5. Vulnerability Assessment

5.1. A pre-production configuration or vulnerability assessment should be performed on all servers or services prior to moving them to production.

5.2. Servers should be scanned using an ISO-approved vulnerability scanner before being moved to production, after being moved to production, and ISO-specified periods thereafter.

- Acceptable vulnerability scanners are listed at http://www.rit.edu/security/content/server-security-standard

5.3. ITS is authorized to perform vulnerability scanning on any server on the network

- Explicit blacklisting or permanent whitelisting of the ITS vulnerability scanner is prohibited.

5.4. A systems/server administrator is authorized to perform scans when approved by the system owner or ITS.

- The systems/server administrator will inform ITS of upcoming scans.

5.5. In order to facilitate effective investigations, a copy of the configuration and/or vulnerability assessment reports done at configuration time should be retained and provided to the Information Security Office on request.

5.6. Vulnerability criticality measurements will use CVSS scores as measures of the severity of the vulnerability.

- Announced vulnerabilities with a CVSS ≥7 should be evaluated for risk within one business day and patches or configuration changes applied appropriately after being announced and made available by the vendor.
- If the patch would disable a production application or environment, then other steps should be taken to manage the risk of an unpatched vulnerability. The Information Security Officer and the Information Security Coordinator should be made aware of the risk within one business day of identifying the patch conflict.
- If no CVSS applies to the vulnerability then the vulnerability should be evaluated for remote exploitation

5.7. Only ISO-approved security assessment tools shall be used for scanning.

- Acceptable security assessment tools are listed at https://www.rit.edu/security/content/technical-resources

6. Authentication and Access Control

6.1. All trust relationships will be identified and reviewed at appropriate intervals.

6.2. All manufacturer and default passwords should be changed.

6.3. Strong authentication is required for all users with root/administrator or system privileges.

- Strong authentication practices are defined on the ISO web site.

6.4. Access Control should be configured to allow only authorized, authenticated access to the system, application and data.

- There should be a process for granting and removing authorized access.
- Generic or persistent guest accounts allowing users interactive logins should be disabled.
- Service accounts are excluded from this requirement.

7. Backup, Restore, and Business Continuity

7.1. Operationally Critical data should be backed up.

- All servers with Operationally Critical data should have documented back-up, system and application restoration (including configurations) and data restoration procedures to support business continuity and disaster recovery planning.
- Back-up procedures should be verified at least monthly, through automated verification, customer restores, or through trial restores.
- Backups shall not be stored solely in the same building where the Operationally Critical data is located.
- Backups should be readily accessible.
- Server backups shall be transmitted securely
- Back-up media should be handled according to the Portable Media Security Standard.

8. Applications Administration

8.1. The applications/module administrator is responsible for ensuring the security of their applications/modules.

- For each application, the application owner should identify an application administrator and systems administrator. These administrators should be approved by their management.

8.2. The application administrator is responsible for application-specific aspects including ensuring the application is in compliance with the server standard where applicable.

9. Security Review and Risk Management

9.1. When major modifications are made to services or servers, e.g., new installations, major software upgrade, hardware replacement, server replacement/retirement, the systems administrators and applications administrators should complete a security review/risk assessment.

9.2. The security review shall typically include an architectural diagram, technical and process security controls, and a security checklist.

9.3. The application owner is responsible for ensuring ITS acceptance of the security review.

9.4. The Information Security Office may also conduct security reviews.

9.5. Vendor Services

- Any system or application administration contracts should be reviewed by purchasing for appropriate risk management clauses.

10. Server Registration

10.1. All servers with network access should be registered in the ITS centralized registration system.

11. Server Hardware Replacement and Retirement

11.1. All server storage media and devices that contain RIT Confidential Information should be degaussed or the data otherwise rendered unrecoverable.

12. Server Administration

12.1. All computers used to administer servers should conform to all requirements for RIT-owned or leased computers as stated in the Desktop and Portable Computer Security Standard.

12.2. Protocols Related to Server Administration

- Only secure protocols may be used for administrative functions and/or the transmission of login credentials. A list of approved protocols may be found at https://www.rit.edu/security/content/technical-resources
- NTP and DNS require authoritative sources

13. High Performance/Distributed Computing (WCG, CONDOR, PLANET LAB, or other grids)

13.1. Servers participating in High Performance/Distributed Computing/ grid computing should employ appropriate and documented safeguards to protect RIT Confidential information and access to RIT internal networks.

Effective Date: August 1, 2009

Standard History:
August 16, 2005
May 15, 2009
November 11, 2013
October 19, 2015