Server Security Checklist

Introduction

There is absolutely no question that if you are running a server, you must ensure that it is locked up tight against security threats.

Hence why we here at Process Street came up with this server security checklist! Never again be afraid of missing a potential entry point or vulnerability when deploying a new server, or when auditing an existing one!

Let's get started with locking your servers down tightly.

Server identification and location:

Record basic details

Kicking off the server security checklist, you need to **identify and record the server and its location**. Do so by filling in the **form fields** below.

Note the date of completion

Next, make sure that you **take note of the date of completion**. Once again, we have a b to make sure that you'll always have this information handy.

Date of Completion

Obtain the signature of the server operator

Now you need to ensure that the **server operator's signature** is posted. **Record a copy** of this using the **form field** below.

Server Operator's Signature

Record the date of the next review schedule

Next, make sure that the **date of the upcoming review schedule** is recorded. Use the form field b

Upcoming Review Schedule

Get the manager’s signature

You're almost done with the server identification and location checks! Now you need to verify that the **manager** has **signed** the checklist. Do so by **recording** their **signature** with the **form field** below.

Manager's Signature

Note the date of the manager's signature

The final step in this section is to verify that the **date of signature** is recorded. Once again, we have a **form field** set up and ready to go for just this purpose.

Manager Signature Date

Secure Network and Physical Environment:

Ensure a restricted access area

The first true security server checklist measure is to **ensure that the**

server has restricted access.

This could be done by checking that the server is secured in a **locked file** or in an **area with restricted access**.

Check non-removable media configuration

Next, make sure that all **non-removable media** is **configured** with the file systems and the **access controls** are activated.

Set up a restricted network environment

Now you need to set up the server in an environment with **appropriately restricted network access**.

Note that this may have already been achieved, but if so you still need to **check** that this is the case.

Ensure the correct banner display

You also need to ensure that the **trespassing banner** is **displayed at login**.

Patching and Server Maintenance:

Check maintenance process documentation

Ongoing maintenance is a key aspect in any decent server security checklist, and so you must make sure that the **maintenance process** is **documented and followed**.

If you do not have a set maintenance process, don't worry! We've got you covered with our very own server maintenance checklist.

Check vendor-supported OS and application patches

Now it's time to check for **vendor-supported operating systems** and **application patches**.

These should always be available to RIT.

Check other operating systems or applications

Next, you should ensure that **all other operating systems or applications** have **exception requests or approval**.

Operating systems or applications that are **no longer supported by the vendor** (or an open source community) should have a pending exception request or be approved by the ISO.

Ensure patch application integration

The next step in the server security checklist is to **ensure smooth patch application integration**.

Check to verify that **vendor patches**, along with the patch application connected into a documented server maintenance process, **support the systems**.

Check the inventory process for current patches

Now you need to make sure that there is a **process to inventory the current level of patches specific to this server**.

Ensure a solid patch installation monitoring process

The final step to checking your patching and general server maintenance is to **check in on your patch installation process**.

Primarily, you should make sure that there is a process for **monitoring patch installation failures**, and that any such failures are securely documented (and dealt with).

Verify real time server configuration

Kicking off our logging section, you need to check to **verify that the server is configured**, with appropriate real-time OS/application logging turned on.

Document routine log monitoring

Although this should already be being carried out, make sure that there is a **documented process for routine log monitoring and analysis**.

Ensure a monthly logging process review

There's no point in **logging** various aspects of your server if you don't **review** them. Whilst you may not be reviewing them right now, you must at least **check that this is occurring frequently**.

Reviews should be undertaken frequently to ensure the effectiveness of the server logging process - we would recommend at least **once per month**.

Implement a log monitoring schedule

Once again, although this should already be taking place, you need to make sure that there is a **schedule for log monitoring of the server**.

OS/application information configuration

Ensure that **logging** has been configured to **include at least 2 weeks of related OS/application information**.

The logging elements include:

- 1

  All authentication

- 2

  Privilege escalation

- 3

  User additions and deletions

- 4

  Access control changes

- 5

  Job schedule start-up

- 6

  System integrity information

- 7

  Log entries must be time and date stamped

Disable private information logging

Now ensure that **all deliberate logging of private information**, such as passwords, **has been disabled**.

Check for real time logging on a secured server

Logging needs to be **reflected in real time and stored on another secure server**, and so this is what you must check is occurring.

System Integrity Controls:

Limit changes to start-up procedures

Onto the system integrity controls! Your system should be configured to **limit changes to start-up procedures**.

If this has not already been done, do so now.

Revise documentation of server control process

Next, make sure that there is a **documented change control process for system configurations**.

Disable unused services

This step is exactly what it says on the tin; you need to **disable all unused services**.

Check your anti-virus software

Next up, make sure that **anti-virus software and definitions are existing and updated**.

Enable host firewall

If you have not already, you need to **install and enable the server with a host firewall**.

Once again, although it is very likely that this step has already been completed, you need to **at least check** that everything is above board and running as expected.

Activate HIPS

Now you need to check whether **host-based intrusion prevention software (HIPS) is activated**. If not, activate it immediately.

Ensure that there is and authentication server

Next up in the server security checklist is to **identify that there is an authentication server**.

HIPS is needed for authentication servers, hence why the previous step was to activate the software.

Activate hardware-based system integrity control

Whilst this may not always be available, you need to **activate hardware-based system integrity control**. Use the **dropdown** below to record the status of this step.

Hardware-Based System Integrity Control An option will be selected here ⇕

If this **service is unavailable**, you need to **record** that this is the case to prevent confusion down the line, hence why this feature necessitates a dropdown whereas previous features do not; it is not always possible, but you need to record it if that is the case.

Vulnerability Assessment:

Check for the presence of pre-production assessments

No server should move to production without either a **pre-production configuration or vulnerability assessment**, and so here is where you must check for its existence.

Remember that both the **server and its services** must have these pre-production checks, so be sure not to forget either in your checks.

Ensure the server has been scanned

Much like the pre-production checks, your server needs to have been **scanned using an ISO-approved vulnerability scanner** - here is where you must **check for past and upcoming scans**. If your server is due a scan, carry this out now.

Next Vulnerability Scan

The server needs to have been scanned with this **before and after being transferred to production**, **along with regular scans** according to an ISO-specified schedule afterwards.

Even if a scan is not due, **record the date of the next scan** in the date form field above.

File the configuration reports

Next up in our list is to check that the **configuration reports** (or vulnerability assessment report) have been **copied and filed**. This is primarily to ensure ease of access for any **possible future reference by the ISO**.

The copy of the configuration and/or vulnerability assessment report accomplished at initial server configuration should be well documented - ideally by using the **form field above**.

Update the system configuration

Now you need to **update the system's configuration**!

After vulnerabilities with the CVSS score results of 7 or greater are announced, the corresponding patches and/or configurations are updated within one working day, so **even if you're sure that you're up to date, it's worth a check**.

Review system configuration vulnerability

If **no CVSS applies** to a **detected vulnerability** then you need to make sure that is it **reviewed for remote exploitation**.

Authorize ISO vulnerability scanners

The **ISO must always be authorized to conduct vulnerability scanning for this server**, and so now you must double check that this is the case.

Authentication and Access Control:

Review documentation on trust relationships

Kicking off the authentication and access control section of our server security checklist is a **review** of all **trust relationships**.

You need to identify and review all trust relationships, especially concerning the **documentation** of them. If something isn't up to scratch or documented well, rectify this and carry on.

Modify all default passwords

Although this is another step which should have been done immediately following the server's setup, **all manufacturer and default passwords** need to have been **modified** and you need to ensure this.

One of the worst things you can do when attempting to lock down a server's security is to leave the default passwords - everyone and their grandmother will be able to guess them! Make sure that all passwords are also **recorded** somewhere (even if it's pen and paper, though this is far from advisable).

Configure strong user authentication

Now you need to configure **strong authentication** for all **users** with **root** or **administrator** system **privileges**. Again, this should be done immediately upon setup, but you should always **check** - better safe than sorry.

Refer to the ISO website for a list of strong authentication practices.

Configure Data Access Control

Configure your Access Control to **allow only authorized, authenticated access** to the system and its applications and data.

Document the access authorization process

Next on our list is to make sure that there is a **documented process for granting and removing authorized access**.

This will not only ensure that there are **no mistakes in the process**, but it will also provide invaluable records should a problem occur.

Activate Generic or persistent guest accounts

The final step in this authentication segment is to ensure that **generic or persistent guest accounts allowing user interactive logins have been activated**.

Backup, Restore, and Business Continuity:

Back up all critical data

We can't say it enough; ensure that there is a **backup** of **all Operationally Critical data**!

Document backup files

Next, make sure that **all servers with Operationally Critical data** have **documented back-ups**, **system and application restoration** (including configurations) and **data restoration procedures** to support business continuity and disaster recovery planning.

Verify backup procedures

Make sure that **backup procedures are verified at least monthly** through automated verification, customer restores, or through trial restores. Store the date of the next scheduled back in the **form field** below to avoid losing track!

Next Backup Procedure Verification

Verify offsite backups

Check to verify that **backups** are **not being stored solely in the same building** where the **Operationally Critical data** is located. That way, in the event of an emergency you'll always have an offsite backup ready to go to help you get back on your feet.

Check backup media

Make sure that **backups have been made readily accessible** and that **backup media is compliant with the Portable Media Security Standard**.

Check to verify that the application administrator is responsible for application-specific aspects, ensuring that the **application is in compliance with the server standard** where applicable.

Applications Administration:

Secure documentation of applications/modules

Check to verify that the **applications/module administrator is responsible for ensuring the security of applications/modules**.

Check there is an application admin systems administrator

Make sure, for **each application**, the application owner identifies an **application administrator systems administrator**. These administrators must be approved by their management.

Risk Management System:

Ensure server registration

Make sure that the **server has network access** and has been **registered in an ISO-approved registration system**.

Check for hardware replacement and retirement

Check to verify if any **server storage media** and/or **devices containing RIT Confidential** have been **removed or replaced**. Record these changes in the **form fields** below.

Replaced Server Hardware Something will be typed here...

Retired Server Hardware Something will be typed here...

Check server administration

Make sure that all computers used to administer servers **conform to the requirements for RIT-owned** or computers as stated in the Desktop and Portable Computer Security Standard.

High Performance and Distributed Computing server

participation

Finally, check to verify that the server **participates in High Performance/Distributed Computing/Grid computing**.

Congratulations! You've completed the server security checklist and can sit safe in the knowledge that your server's as safe as safe can be.

Sources:

Taylor Armerding - The 15 worst data security breaches of the 21st Century

Relevant Checklists:

Inventory Management Process

Network Security Management

Client Data Backup Best Practices

Computer Maintenance Guide

Server Setup Process

Virtual Private Server Setup

IT Support Process

Helpdesk Management

Server Maintenance Checklist

Information Security Incident Response

SQL Server Audit Checklist