TRIANZ℠

System Hardening Procedure

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

1. Introduction

1.1 Purpose

This procedure has been developed to provide management support and direction for the information security of all Trianz' s information assets within the Trianz environment. The purpose of this procedure is to ensure management commitment towards Information Security.

1.2 Objective

The objective of this procedure is to ensure system hardening of end user computing devices or Servers connected within Trianz logical environment.

1.3 Scope

- This procedure applies to all users of information systems, vendors, business partners, contractor personnel and functions/business units. This procedure covers all Information System operated by Trianz.
- The procedure applies to all Trianz products and services.

2. Procedure for Linux System Hardening

2.1 Document the host information

Each time on a new Linux hardening job, create a new document that has all the checklist items listed, and check every item applied on the system. Furthermore, on the top of the document, include the Linux host information:

- Machine name
- IP address
- Mac address
- Name of the person who is doing the hardening (most likely you)

- Date
- Asset Number

Linux Hardening Checklist:

1) NTP
2) Linux user password complexity
   - Password length minimum 15 chars
   - Password is alphanumeric.

- Password expiry 30 days
- Password history remember last 4 passwords
- Password lock after 6 unsuccessful login attempts
- Lock account for 30 minutes and after that unlock automatically

3) Harden SSH

- Session idle timeout 15 minutes.
- Disable cbc ciphers.
- Disable md5 and sha2 MACS.

4) Antivirus installation and configuration
5) FIM installation
6) Audit trail to log all user commands.
7) Audit trail for administrative commands in db
8) Find and remove unwanted packages.
9) Find and stop unneeded services.
10) NGINX/Apache beast attack

NTP:

- Setup a centralized ntp server.
- Check whether all the servers have ntp client installed. If not install them

- Configure ntp to synchronize from the central ntp server.
- Put up a cron to synchronize 4 times a day.

Linux user password complexity:

- Configure pam for password complexity.
- Check whether pam-cracklib is installed, if not install/upgrade it. Now configure pam such that minimum password length is 7 characters long, with both numbers and alphabets. Password expiry of each user should be 90 days. Password expiry warning messages should be should start from 7 days before expiry.
- PAM should remember the last 4 used passwords and reject them if set.
- Account should be locked after 6 continuous unsuccessful logins and unlocked after 30 minutes.

2.2 Harden SSH:

- Set session idle timeout to 15 minutes.
- Configure SSH to use only the below ciphers - aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128
- Configure SSH to use only the below MACS - umac-64@openssh.com,hmac-sha2-256,hmac-sha2-256-96,hmac-sha2-512,hmac-sha2-512-96,hmac-ripemd160,hmripemd160@openssh.com

2.3 Antivirus installation and configuration:

- Install antivirus with a centralized setup such that each machine does not download the update files directly from the internet.

- The centralized update server is configured to download the update files every 4 hours and serves installed servers whenever needed.
- Antivirus is installed in all servers (Linux and Windows) and configure to get updates from the centralized update server. Full system scan is run every day at midnight and status mails are sent.

2.4 FIM (File Integrity Monitoring) installation:

- FIM server is installed in one of the servers and configured to send alerts through mails and displayed in web interface.
- FIM agents are installed in all servers and configured to send the logs/alerts to the central ossec server. The central server then parses them and generates alerts.
- Things like file integrity, administrative actions, logs , etc. .., are monitored through FIM

2.5 File integrity:

- File modification (with exact modified content)
- File size.
- File owner, group.
- File permissions.
- Md5 checksum
- SHA

2.6 Audit trail to log all user commands:

An audit trail mechanism should be enabled and should log all the commands executed by all users and sends them as warnings to the central syslog server.

2.7 Audit trail for administrative commands in db:

Postgres db servers should be configured to log all the commands executed by the administrative users as syslog messages, which in turn is sent to the central syslog server.

2.8 Find and remove unwanted packages:

All installed packages should have justification. Any package not having justification should be removed

2.9 Find and stop unneeded services:

All running process and services should have justification. Any service or process running without justification should be stopped.

Nginx/Apache beast attack: SSL ciphers were reconfigured in nginx/apache such that they cannot be hacked through beast attack.

2.10 Services and ports & scripts:

- All the services running must be secure and justified. No unwanted or unrequired port or services running on the system are allowed.
- If insecure services (such as ftp, telnet) are allowed, an extra control to mitigate the risk associated with the implementation of the insure protocol must be in place. For example, in case of telnet use Multi factor authentication and in case of ftp use either encrypted channel or the data itself must be encrypted before sending over ftp.

- All the start-up and shutdown scripts must be reviewed and justified on a system.

2.11 User account procedure

- All guest must be disabled
- Default user ID must be either removed or disabled.
- If account cannot be remove or disabled then it should be renamed
- All custom accounts must be justified and defied based on need to know basis.
- All custom accounts must be approved before addition and deletion and a proper change management procedure must be followed.

3. Procedure for Window System Hardening

- Install the latest Service Pack from http://windowsupdate.microsoft.com.
- Each Service Pack for Windows includes all security fixes from previous Service Packs. Keep up to date on Service Pack releases and install the correct Service Pack for your servers as soon as operational circumstances allow.
- Install the appropriate post-Service Pack security hot fixes from http://windowsupdate.microsoft.com.
- Microsoft issues security bulletins through its Security Notification Service. When these bulletins recommend installation of a security hot fix, you should immediately download and test the hot fix, then install it on your member servers as soon as operational circumstances allow.
- Configure local accounts.

- Make sure the local Guest account is disabled. This is the default in Windows Servers.
- Enable account lockout on the local administrator account (this still needs to be done using passprop on Windows Servers)
- Rename the local Administrator account to something other than Administrator.
- Ensure that the local Administrator password meets the following criteria:
- It contains at least sixteen alphanumeric characters.
- It contains both upper and lower case characters.
- It has digits and punctuation characters as well as letters.
- It is not a word in any language, slang, dialect, jargon, etc.
- It is not based on personal information.
- Make sure that Domain Admins are members of the Local Administrators group.
- Disable or delete unnecessary accounts quarterly.
- Review the list of active accounts (for both users and applications) on the system in the Computer Management snap-in, disabling any non-active accounts, and deleting accounts that are no longer required, including duplicate user accounts, test accounts, shared accounts, and general departmental accounts.
- Use group policies to assign permissions as needed.
- Disable unnecessary services.
- After installing Windows Server, disable any network services not required for the server role. In particular, consider whether the server should be running the Server service for file and print sharing.
- This list could include web services or ftp services if those are not needed.

- Also, avoid installing applications on the server unless they are necessary to the server's function. For example, do not install e-mail clients, office productivity tools, or utilities that are not strictly required for the server to do its job.
- If SNMP is enabled, there must be no R/W community string, and the RO community string must be set to something other than "public." When choosing an SNMP community string, follow the same guidelines as choosing a complex password.
- Set stronger password policies, as per password policy.
- Use the Domain Security Policy (or Local Security Policy) snap-in to strengthen the system policies for password acceptance, including:
  - Set the minimum password length to at least eight characters.
  - Set a minimum password age.
  - Set a maximum password age.
  - Set a password history maintenance.
  - Enable password complexity.

- Local Security Policy -> Security Settings -> Account Policies ->Password Policy:

Password Setting	**Recommended Settings**
Enforce password history	4
Maximum password age	30
Minimum password age	2
Minimum password length	8
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Note: Increase the log size from the 16384 mb default to at least 81920 mb.

Prevent the last logged-in username from being displayed.

The login dialog box makes it easier to discover a username that can later be employed in a password- guessing attack. Disable this feature using the security templates provided on the installation CD, or via Group Policy snap-in. Local Security Policy… Security Settings… Local Policies… Security Options… Domain Member: Do not display last username.

- Configure a strong audit policy. Successful and failed logins, as well as privilege use, should be logged and monitored to detect any unauthorized activity. Applied Trust suggests the following Auditing settings:

Audit Policy	**Recommended Settings**
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing.
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing.
Audit system events	No auditing.

- Install antivirus software and updates. Make sure file scanning is enabled and automatic definition updates are configured.
- Configure appropriate settings for access control on file shares, given that permissions are set through NTFS security.
- All folders and files should be secured with standard NTFS settings. Minimum access rules should apply such that groups are created that allow the minimum number of users to have write access.
- Where possible, the “Everyone” setting should be removed and replaced with user groups.
- Once NTFS settings have been applied, then the most efficient share setting is to give all Authenticated Users full control access. (Please confirm with your application guidelines)
- Disable the autorun feature on the CD-ROM drive

Boot from the **Hard Drive Only**

Disable the F12 key
Enable a BIOS password.
Run the Registry Editor (REGEDIT.EXE).
Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom

Double-click the Autorun value, and type 0 for its value. (If it is not there, create it by selecting Edit -> New -> DWORD Value, and typing "Autorun" for its name.)

- Protect the registry from anonymous access
- Rename the guest account even though it may be disabled.
- Make sure that the server firewall is turned on is blocking unneeded ports such as 21 for FTP and 80 for web services. Please contact an IT security person if questions or assistance is needed.
- In the registry sub key

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsNT\RPC, select one of the following values:

  - This default setting permits access to interfaces only by using authenticated connections, unless those connections specifically request to be exempt from this requirement. (Note: This exemption is required for some DCOM scenarios.)

- This setting permits remote access to interfaces only by using authenticated connections. This setting does not permit exceptions to the authentication requirement.
- Ensure users have the correct level of debugging access. This can be done through:

  The control panel of each machine
  The platform SDK (SeDebugPrivilege)

Set up the event logs.

- GPO_name\Computer Configuration\Windows Settings\Security Settings\Event Log\
- Maximum application log size: 16384 mb
- Maximum security log size: 16384 mb
- Maximum system log size: 16384 mb
- Prevent local guests group from accessing application log: enabled
- Prevent local guests group from accessing security log: enabled
- Prevent local guests group from accessing system log: enabled
- Retain application log: Not defined
- Retain security log: Not defined
- Retain system log: Not defined
- Retention method for application log: Overwrite as needed
- Retention method for security log: Overwrite as needed
- Retention method for system log: Overwrite as needed
- Set logfiles for rollover
- Dump the system registry quarterly

- Once the server has been built, create a Level 0/Full backup of all drives and the System State. This backup should be stored for the life of the machine as a forensic baseline in case of a security incident. Additional Level 0 backups should be created and stored for the machine’s lifetime upon major system upgrades.

4. Procedure for other System Hardening

CIS (Centre for Internet Security) has released Bench Marks for many of the well-known industry systems such as Operating Systems, Network and Server Infrastructure, Cloud Systems, Applications etc. Please use the below link to access the bench marks and harden the systems as per the best practice:

https://www.cisecurity.org/cis-benchmarks/

For the remaining systems, please refer to the security best practice provided by the respective manufacturers/developers.

5. Review of the Procedure

The Information Security team is responsible for ensuring that this procedure document is reviewed at least annually or if there is any major change in the requirements of this procedure.

6. Exception(s)

Exceptions require a documented business justification. Exceptions are subject to the approval of higher management.

7. ISO Control Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological Controls	8.20 Networks Security 8.9 Configuration management	System Hardening Procedure
Technological	8.4 Access to source code	

Document Control

Owner:	CISO	**Release ID:**	SERVHARD_PROC_0133

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	02-July-20	Rajesh Benakannavar	Balu Nair	Phani Krishna	Initial Draft	None
1.0	02-July-20	Rajesh Benakannavar	Balu Nair	Phani Krishna	Reviewed and Approved	Added Reference to the CIS benchmark in the System Hardening Procedure section. Baselined.
1.1	03-May-21	Divya G	Vijaya	Phani	For Review	Updated with new Information classification
2.0	03-May-21	Divya G	Vijaya	Phani	For Approval	Approved and Baselined.
2.0	3-Jan-22	Karthik N			For Review	No changes
2.1	24-Feb-22	Kruti	Karthik N		For Review	• The scope has been extended to products and services

3.0	18-Mar-22	Kruti	Siva N	Siva N	For Approval	Approved and Baselined
3.0	02-May-23	Kruti	Pranesh K	Srikanth M	For Approval	Reviewed with no changes.
3.1	12-May-23	Asha Veeramallu	Vijaya		For Review	Migrated to New Template
4.0	12-May-23	Asha Veeramallu	Vijaya	Srikanth M		Approved and Baselined
4.1	4-Feb-24	Vijaya	Balu	Srikanth M	For Review	Updated the section ISO Control Mapping aligning to ISO 27001:2022
5.0	23-Feb-24	Vijaya	Vijaya and Bala	Srikanth M	For Approval	Approved and Baselined .
5.1	25-Apr-25	Vijaya	Balu			Migrated to new Template
6.0	14-May-25	Vijaya	Balu	Srikanth M	For Approval	Approved and Baselined .

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com