14.1. Standard Operating Environments

Objective

14.1.1. Standard Operating Environments (SOE) are hardened in order to minimise attacks and compromise through known vulnerabilities and attack vectors.

Context

Scope

14.1.2. This section covers information on the hardening of software used on workstations and servers on systems within agency control.

Characterisation

14.1.3. Characterisation is a technique used to analyse and record a system's configuration. It is important as it can be used as a baseline to verify the system's integrity at a later date. It is also important that the baseline has high levels of integrity and assurance to avoid reinfecting systems or reintroducing compromises when restoring from baselines.

14.1.4. In virtual environments a baseline is usually a "snapshot" or image take at a point in time. If the image or snapshot is infected, then restoring from that image can result in further compromise. See also Section 22.2 – Virtualisation and 22.3 – Virtual Local Area Networks.

14.1.5. Methods of characterising files and directories include:

- performing a cryptographic checksum on the files/directories when they are known to be virus/contaminant free;
- documenting the name, type, size and attributes of legitimate files and directories, along with any changes to this information expected under normal operating conditions; or
- for a Windows system, taking a system difference snapshot.

References

14.1.6. Further references can be found at:

Reference	Title	Publisher	Source
ISO/IEC 27001:2013	**A.12.4.1, Control of Operational Software**	ISO	https://www.iso.org/standard/54534.html
ISO/IEC 27001:2013	**A.12.6.1, Control of Technical Vulnerabilities**	ISO	https://www.iso.org/standard/54534.html
	Independent testing of different antivirus software and their effectiveness	AV Comparatives	https://www.av-comparatives.org/

PSR references

14.1.7. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Developing hardened SOEs

14.1.8.R.01. **Rationale**

Antivirus and anti-malware software, while an important defensive measure, can be defeated by malicious code that has yet to be identified by antivirus vendors. This can include targeted attacks, where a new virus is engineered or an existing one modified to defeat the signature-based detection schemes.

14.1.8.R.02. **Rationale**

The use of antivirus and anti-malware software, while adding value to the defence of workstations, cannot be relied solely upon to protect the workstation. As such agencies still need to deploy appropriately hardened SOEs to assist with the protection of workstations against a broader range of security risks.

14.1.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1149]

Agencies SHOULD develop a hardened SOE for workstations and servers, covering:

- removal of unneeded software and operating system components;
- removal or disabling of unneeded services, ports and BIOS settings;
- disabling of unused or undesired functionality in software and operating systems;
- implementation of access controls on relevant objects to limit system users and programs to the minimum access required;
- installation of antivirus and anti-malware software;
- installation of software-based firewalls limiting inbound and outbound network connections;
- configuration of either remote logging or the transfer of local event logs to a central server; and
- protection of audit and other logs through the use of a one way pipe to reduce likelihood of compromise key transaction records.

Maintaining hardened SOEs

14.1.9.R.01. **Rationale**

Whilst a SOE can be sufficiently hardened when it is deployed, its security will progressively degrade over time. Agencies can address the degradation of the security of a SOE by ensuring that patches are continually applied, system users are not able to disable or bypass security functionality and antivirus and other security software is appropriately maintained with the latest signatures and updates.

14.1.9.R.02. **Rationale**

End Point Agents monitor traffic and apply security policies on applications, storage interfaces and data in real-time. Administrators actively block or monitor and log policy breaches. The End Point Agent can also create forensic monitoring to facilitate incident investigation.

14.1.9.R.03. **Rationale**

End Point Agents can monitor user activity, such as the cut, copy, paste, print, print screen operations and copying data to external drives and other devices. The Agent can then apply policies to limit such activity.

14.1.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1158]

Agencies MUST ensure that for all servers and workstations:

- a technical specification is agreed for each platform with specified controls;
- a standard configuration created and updated for each operating system type and version;
- system users do not have the ability to install or disable software without approval; and

- installed software and operating system patching is up to date.

14.1.9.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1159]

Agencies SHOULD ensure that for all servers and workstations:

- malware detection heuristics are set to a high level;
- malware pattern signatures are checked for updates on at least a daily basis;
- malware pattern signatures are updated as soon as possible after vendors make them available;
- all disks and systems are regularly scanned for malicious code; and
- the use of End Point Agents is considered.

Default passwords and accounts

14.1.10.R.01. **Rationale**

Default passwords and accounts for operating systems are often exploited by attackers as they are well documented in product manuals and can be easily checked in an automated manner with little effort required.

14.1.10.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:1162]

Agencies MUST reduce potential vulnerabilities in their SOEs by:

- removing unused accounts;
- renaming or deleting default accounts; and
- replacing default passwords before or during the installation process.

14.1.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1163]

Agencies SHOULD reduce potential vulnerabilities in their SOEs by:

- removing unused accounts;
- renaming or deleting default accounts; and
- replacing default passwords, before or during the installation process.

Server separation

14.1.11.R.01. **Rationale**

Servers with a high security risk can include Web, email, file, Internet Protocol Telephony (IPT) servers, Mobile Device Manager (MDM) servers and gateway components. It is important to clearly identify all services and connections to design a complete and secure server separation architecture. Refer also to Chapter 19 – Gateway Security.

14.1.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1169]

Where servers with a high security risk have connectivity to unsecure public networks, agencies SHOULD:

- use appropriately designed and configured gateways;
- consider the use of cross-domain solutions;
- segment networks;
- maintain effective functional segregation between servers allowing them to operate independently;
- minimise communications between servers at both the network and file system level as appropriate; and
- limit system users and programs to the minimum access needed to perform their duties.

Characterisation

14.1.12.R.01. **Rationale**

There are known techniques for defeating basic characterisations, therefore other methods of intrusion detection are also needed, particularly in situations where it is impractical to use a trusted environment for the generation of the characterisation data. Characterisation is very useful in post-intrusion forensic investigations where an infected disk can be compared to stored characterisation data in order to determine what files have been changed or introduced.

14.1.12.R.02. **Rationale**

Characterisation is also directly related to business continuity and disaster recovery and is influenced by Business Impact Analyses and Risk Assessments. Grouping elements by business applications and setting priority and criticality of the elements to the business may assist in determining the most appropriate and useful characterisations.

14.1.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1185]

Agencies SHOULD:

- characterise all servers whose functions are critical to the agency, and those identified as being at a high security risk of compromise;
- store the characterisation information securely off the server in a manner that maintains integrity;
- update the characterisation information after every legitimate change to a system as part of the change control process;
- as part of the agency's ongoing audit schedule, compare the stored characterisation information against current characterisation information to determine whether a compromise, or a legitimate but incorrectly completed system modification, has occurred;
- perform the characterisation from a trusted environment rather than the standard operating system wherever possible; and
- resolve any detected changes in accordance with the agency's information security incident management procedures.

14.1.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1189]

Agencies SHOULD use an Approved Cryptographic Algorithm to perform cryptographic checksums for characterisation purposes.

14.1.12.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1190]

Agencies SHOULD consider characterisations in the context of a BCP or DRP and any related Business Impact Analyses and Risk Assessments.

Automated outbound connections by software

14.1.13.R.01. **Rationale**

Applications that include beaconing functionality include those that initiate a connection to the vendor site over the Internet and inbound remote management.

14.1.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1193]

Agencies SHOULD review all software applications to determine whether they attempt to establish any unauthorised or unplanned external connections.

14.1.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1194]

If automated outbound connection functionality is included, agencies SHOULD make a business decision to determine whether to permit or deny these connections, including an assessment of the security risks involved in doing so.

14.1.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1195]

If automated outbound connection functionality is included, agencies SHOULD consider the implementation of Data Loss Prevention (DLP) technologies.

Knowledge of software used on systems

14.1.14.R.01. **Rationale**

Information about installed software, that could be disclosed outside the agency, can include:

- user agent on Web requests disclosing the Web browser type;
- network and email client information in email headers; and
- email server software headers.

This information could provide a malicious entity with knowledge of how to tailor attacks to exploit vulnerabilities in the agency's systems.

14.1.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1198]

Agencies SHOULD limit information that could be disclosed outside the agency about what software, and software versions are installed on their systems.