14.2. Application Allow listing

Objective

14.2.1. Only approved applications are used on agency controlled systems.

Context

Scope

14.2.2. This section covers information on the use of technical controls to restrict the specific applications that can be accessed by a user or group of users.

References

14.2.3. Further information on software restriction policies as implemented by Microsoft can be found at:

Reference	Title	Publisher	Source
	Using Software Restriction Policies to Protect Against Unauthorized Software	Microsoft	https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457006(v=technet.10)?redirectedfrom=MSDN
	APPLOCKER	Microsoft	https://docs.microsoft.com/en-nz/windows/security/threat-protection/applocker/applocker-overview
SP 800-167	**NIST Special Publication 800-167 - Guide to Application Whitelisting**	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf [PDF, 622 KB]

Rationale & Controls

Application allow listing

14.2.4.R.01. **Rationale**

Application access control can be an effective mechanism to prevent the successful compromise of an agency system resulting from the exploitation of a vulnerability in an application or the execution of malicious code.

14.2.4.R.02. **Rationale**

Defining a list of trusted executables, an allow list, is a practical and secure method of securing a system rather than relying on a list of bad executables, a deny list, to be prevented from running.

14.2.4.R.03. **Rationale**

Application allow listing is considered only one part of a defence-in-depth strategy in order to prevent a successful attack, or to help mitigate consequences arising from an attack.

14.2.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1234]

Agencies SHOULD implement application allow listing as part of the SOE for workstations, servers and any other network device.

System user permissions

14.2.5.R.01. **Rationale**

An average system user requires access to only a few applications, or groups of applications, in order to conduct their work. Restricting the system user's permissions to execute code to this limited set of applications reduces the attack surface of the system.

14.2.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1242]

Agencies MUST ensure that a system user cannot disable the application allow listing mechanism.

14.2.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1246]

Agencies SHOULD prevent a system user from running arbitrary executables.

14.2.5.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:896]

Agencies SHOULD restrict a system user's rights in order to permit them to only execute a specific set of predefined executables as required for them to complete their duties.

14.2.5.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:898]

Agencies SHOULD ensure that application allow listing does not replace the antivirus and anti-malware software within a system.

System administrator permissions

14.2.6.R.01. **Rationale**

Since the consequences of running malicious code as a privileged user are much more severe than an unprivileged user, an application allow list implementation should be strictly enforced for system administrators.

14.2.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:907]

Agencies SHOULD ensure that system administrators are not automatically exempt from application allow list policy.

Application allow listing configuration

14.2.7.R.01. **Rationale**

A decision to execute a routine, application, or other programme should be made based on a validated cryptographic hash as it is more secure than a decision based on the executable's signature, path or parent folder.

14.2.7.R.02. **Rationale**

In order for application allow listing to be effective an agency MUST initially gather information on necessary executables and applications in order to ensure that the implementation is fully effective.

14.2.7.R.03. **Rationale**

Different application allow listing controls, such as restricting execution based on cryptographic hash, filename, pathname or folder, have various advantages and disadvantages. Agencies need to be aware of this when implementing application allow listing.

14.2.7.R.04. **Rationale**

Application allow listing based on parent folder or executable path is futile if access control list permissions allow a system user to write to the folders or overwrite permitted executables.

14.2.7.R.05. **Rationale**

Executables may create multiple processes in the course of execution. These may be identified through examination of programme specifications, testing in a "sand-boxed" environment before development, and logs of any processes spawned or created.

14.2.7.R.06. **Rationale**

Spawned processes may behave in ways that can compromise system security, change security settings and modify access permissions. Clearly this can be undesirable behaviour.

14.2.7.R.07. **Rationale**

Adequate logging information can allow system administrators to further refine the application allow listing implementation and detect a pattern of deny decisions for a system user.

14.2.7.R.08. **Rationale**

An example of relevant information that could be included in logs for application allow listing implementations would be decisions to deny execution incorporating information that would present a reviewer with evidence of misuse.

14.2.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:934]

Agencies SHOULD ensure that the default policy is to deny the execution of software.

14.2.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:936]

Agencies SHOULD ensure that application allow listing is used in addition to a strong access control list model and the use of limited privilege accounts.

14.2.7.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:940]

Agencies SHOULD plan and test application allow listing mechanisms and processes thoroughly prior to implementation.

14.2.7.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:942]

Agencies SHOULD restrict the decision whether to run an executable based on the following, in the order of preference shown:

1. validates cryptographic hash;
2. executable absolute path;
3. digital signature; and
4. parent folder.

14.2.7.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:945]

Agencies SHOULD restrict the process creation permissions of any executables which are permitted to run by the application allow listing controls.

14.2.7.C.06. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:5529]

Agencies SHOULD validate executable behaviour, in particular process creation, permission changes and access control modifications through examination, testing, monitoring and restriction of the permissions.

14.2.7.C.07. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:947]

Logs from the application allow listing implementation SHOULD include all relevant information.