National Cyber Security Centre

General Security Advisory

GSA-010-17

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

Application Whitelisting

Application whitelisting is one of the top four strategies to mitigate targeted cyber intrusions. This document provides high-level guidance on what application whitelisting is, is not, and how IT Security Advisers can implement it effectively in a Windows-based environment.

What is application whitelisting?

Application whitelisting is a security approach designed to protect against unauthorised and malicious programs executing on a system. It aims to ensure only authorised applications (such as programs and software libraries) can be executed.

While primarily designed to prevent the execution and spread of malicious code, it can also prevent the installation or use of unauthorised applications.

Implementing application whitelisting across an entire organisation can be a daunting undertaking, however implementation on systems used by high-value or oft-targeted employees such as executive officers and their assistants can be a valuable first step.

What application whitelisting is not:

While the below approaches are valuable for defence-in-depth they are not considered application whitelisting:

- Providing a portal or other means of installation for authorised applications.
- Using web or email content filters to prevent users from downloading applications from the internet.
- Checking the reputation of an application in a cloud-based database before it is executed.
- Using a next-generation firewall in an attempt to identify whether network traffic is generated by an approved application.

How to implement application whitelisting:

Implementing application whitelisting comprises the following high-level steps:

- Identify applications which should be permitted to execute on a given system;
- Develop whitelisting rules to ensure only those authorised applications can execute on that system;
- Restrict users to a subset of the authorised applications required to undertake their specific duties;
- Prevent users from being able to bypass the application whitelisting solution or change associated whitelisting rules;
- Maintain the application whitelisting solution and associated whitelisting rules using a change management program.

When determining the method used by an application whitelisting solution to specify whitelisting rules, the use of cryptographic hashes, publisher certificates, absolute paths and parent folders are considered suitable if implemented correctly. However if whitelisting rules based on absolute paths or parents folders are used, particular care should be taken with the implementation of file system permissions to ensure users do not have the ability to write or execute content in any path that has been whitelisted as this would enable them to bypass the whitelisting solution.

To ensure an application whitelisting solution has been appropriately implemented, testing should be undertaken on a regular basis to check for misconfigurations of file system permissions and other ways of bypassing application whitelisting rules or executing unauthorised content on a system.

In addition to preventing the execution of unauthorised applications, an application whitelisting solution can contribute to the identification of attempts by an adversary to execute malicious code on a system. This can be achieved by configuring the application whitelisting solution to generate event logs for failed execution attempts. Such event logs should ideally include information such as the name of the blocked file, the date/time stamp and the username of the user attempting to execute the file.

Finally, it is important that an application whitelisting solution does not replace antivirus and other internet safety software already in place on systems. Using multiple security solutions together is an effective defence-in-depth approach to preventing the compromise of systems.

Reference:
Australian Signals Directorate (ASD):
http://asd.gov.au/publications/protect/application_whitelisting.htm

For further information:
NSA publication: "Application Whitelisting Using Microsoft AppLocker"
For the full list of mitigation strategies see:
http://www.asd.gov.au/infosec/top35mitigationstrategies.htm.

The NCSC can be contacted by email via ***incidents@ncsc.govt.nz*** *or by phone on:* ***04 498 7654****. We encourage you to contact us at any time if you require any further assistance or advice.*