April 2016

Implementing Application Whitelisting

Introduction

1. Application whitelisting is the most effective strategy in the Australian Signals Directorate's (ASD) *Strategies to Mitigate Targeted Cyber Intrusions*.
2. This document has been developed by ASD to provide high-level guidance on what application whitelisting is, what application whitelisting is not and how to implement an application whitelisting solution.

What application whitelisting is

3. Application whitelisting is a security approach designed to protect against unauthorised or malicious code executing on a system. It aims to ensure that only authorised applications (e.g. programs, software libraries, scripts and installers) can be executed.
4. While application whitelisting is primarily designed to prevent the execution and spread of malicious code, it can also prevent the installation or use of unauthorised applications.
5. Implementing application whitelisting across an entire organisation can be a daunting undertaking; however, implementation on systems used by high-value or often targeted staff members such as executive officers and their assistants, human resources staff members, FOI staff members or public relations staff members can be a valuable first step.

What application whitelisting is not

6. The following approaches, whilst still valuable for defence-in-depth, are not considered to be application whitelisting:
    a. providing a portal or other means of installation for authorised applications
    b. using web or email content filters to prevent users from downloading applications from the Internet
    c. checking the reputation of an application in a cloud-based database before it is executed
    d. using a next-generation firewall in an attempt to identify whether network traffic is generated by an approved application.

How to implement an application whitelisting solution

7. Implementing an application whitelisting solution comprises the following high-level steps:
    a. identify applications which should be permitted to execute on a given system
    b. develop whitelisting rules to ensure only those authorised applications can execute on that system

c. restrict users to a subset of authorised applications required to undertake their specific duties
d. prevent users from being able to bypass the application whitelisting solution or change associated whitelisting rules
e. maintain the application whitelisting solution and associated whitelisting rules using a change management program.

8. When determining the method used by an application whitelisting solution to specify whitelisting rules, the use of cryptographic hashes, publisher certificates (combining both publisher names and product names), absolute paths and parent folders are considered suitable if implemented correctly. However, if whitelisting rules based on absolute paths or parent 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 and execute content in any path that has been whitelisted, as doing so would enable them to bypass the application whitelisting solution.

9. 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 gaining execution of unauthorised content on a system.

10. 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 an 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.

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

Further information

12. The *Australian Government Information Security Manual* (ISM) assists in the protection of official government information that is processed, stored or communicated by Australian Government systems. It can be found at: http://www.asd.gov.au/infosec/ism/.

13. ASD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at: http://www.asd.gov.au/infosec/mitigationstrategies.htm.

Contact details

14. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

15. Australian businesses or other private sector organisations with questions regarding this advice should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.