National Cyber Security Centre

Restricting Administrative Privileges Explained

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

Restricting administrative privileges is considered one of the Top 4 strategies to Mitigate Targeted Cyber Intrusions

This document supports the implementation of the Strategies to Mitigate Targeted Cyber Intrusions by providing high-level guidance on how to restrict administrative privileges and examples of approaches that do not meet the intent of this strategy.

Why should administrative privileges be restricted?

Users with administrative privileges for operating systems and applications are able to make significant changes to their configuration and operation, modify critical security settings and access sensitive information. Domain administrators have similar abilities over an entire network domain, which usually includes all of the workstations and servers on the network.

Adversaries often use malicious code to attempt to exploit vulnerabilities in workstations and servers. Restricting administrative privileges makes it more difficult for an adversary's malicious code to elevate its privileges, spread to other hosts, hide its existence, persist after reboot, obtain sensitive information or resist removal efforts.

An environment where administrative privileges are restricted is more stable, predictable, and easier to administer and support, as fewer users can make significant changes to their operating environment, either intentionally or unintentionally.

How to restrict administrative privileges

Simply minimising the total number of privileged accounts does not meet the intent of the restricting administrative privileges strategy. The correct approach to restricting administrative privileges is to:

a. Identify tasks that require administrative privileges to be performed.
b. Validate which staff members are required and authorised to carry out those tasks as part of their duties.
c. Create separate attributable accounts for staff members with administrative privileges, ensuring that their accounts have the least amount of privileges needed to undertake their duties.
d. Revalidate staff members' requirements to have a privileged account on a frequent and regular basis, or when they change duties, leave the organisation, or are involved in a security incident.

To reduce the risks of using privileged accounts, organisations should ensure that:

a. Staff members elevate from a standard user account to a privileged account to perform administrative tasks.
b. Privileged accounts do not have the ability to access the internet or read email.
c. Administrative activities are performed on a separate physical workstation to that used for day-to-day non-administrative tasks.
d. Multi-factor authentication is implemented for privileged accounts.
e. Administrative activities are performed on hardened workstations.

All actions taken with privileged accounts should be logged and archived to provide an auditable history. This can assist in both real-time analysis of unusual behaviour patterns, as well as in any investigations following a cyber security incident.

Logging and auditing can also assist in identifying the number of active privileged accounts, the staff members who have access to them, and the tasks for which the privileged accounts are being used. This information will provide a clear understanding of the state of privileged account use in an organisation, and help ensure that a robust secure enterprise administration strategy is implemented.

Approaches which do not restrict administrative privileges

There are a number of approaches which, while they may appear to provide many of the benefits of restricting administrative privileges, do not meet the intent of this strategy, and in some cases may actually increase the risk to an organisation's network. These approaches include:

a. Implementing shared non-attributable privileged accounts.
b. Temporarily allocating administrative privileges to regular users.
c. Placing standard user accounts in user groups with administrative privileges.

Further information:
The full list of strategies and their relative security effectiveness rating is available at
http://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm

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

The NCSC can be contacted by email via ***info@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.