



Minimising Administrative Privileges Explained

SUMMARY

1. Minimising administrative privileges is one of the top four strategies in DSD's list of *Strategies to Mitigate Targeted Cyber Intrusions*. This document provides high-level guidance on what minimising administrative privilege is, what it isn't, and how to apply it effectively.

DETAILS

Why Minimise Administrative Privileges

2. Accounts with local administrative privileges to a computer are able to make significant changes to the configuration and operation of that computer, as well as access sensitive information such as password hashes. Domain administrators similarly have the ability to impact an entire network domain, which usually includes all of the computers on a network.

3. Malicious software (malware) often seeks to gain administrative privileges to compromise computers. Minimising administrative privileges makes it more difficult for malware to spread, hide its existence, persist, obtain sensitive information and resist efforts to remove it.

4. Minimising administrative privileges provides an environment that 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.

What Minimising Administrative Privileges is

5. Minimising administrative privileges involves the following steps:
- identify tasks which absolutely require administrative privileges to be performed;
 - identify staff who are required, and are authorised, to carry out such tasks;
 - create separate administrative accounts for those staff, ensuring that those credentials have the least privilege required for their specific task;
 - ensure administrative accounts do not have the ability to access the Internet or read email; and,

SECRET

- e. where possible, ensure administrative access is performed on a separate computer to that used for day-to-day tasks.

What Minimising Administrative Privileges is not

6. There are a number of techniques which, while they may appear to provide many of the benefits of administrative privilege minimisation, do not significantly improve the security of a network. Some of these techniques may actually increase the risk to a network. These include:

- a. temporarily allocating administrative privileges to regular users;
- b. allocating administrative privileges to standard accounts; and,
- c. giving administrative accounts the ability to access the Internet or read email.

7. Standard accounts should not have administrative privileges. Most compromises occur as part of a user's normal activity, such as opening email or visiting a website. A separate account should be created for system administration, ensuring administrators make an explicit decision to use administrative privileges.

How to Implement Minimisation of Administrative Privileges

8. It is important that the principle of least privilege is applied to administrative accounts.

9. All actions taken as an administrative user should be logged and monitored to provide the agency with a clear picture of the number of administrative accounts that exist, whether they are active or disabled, and which users have access to administrative accounts. This information should be used to ensure that administrative privileges are limited to those that require them and are being used appropriately.

More information on restricting administrative privileges can be found in DSD's *Information Security Manual*.

CONTACT DETAILS:

Australian government agencies seeking clarification about this document can contact DSD via assist@dsd.gov.au.