CANADIAN CENTRE FOR CYBER SECURITY

Managing and controlling administrative privileges

June 2024 **ITSAP.10.094**

A user with administrative privileges has more control than a regular user to modify, customize or erase data over a computer system or network. Often, organizations assign these elevated privileges to general user accounts. This practice gives outside threat actors, as well as unintentional and malicious insiders, another way to compromise an organization's networks. When your organization better manages and controls its administrative privileges, it can reduce its exposure to common cyber threats.

Why threat actors target administrative privileges

If threat actors gain access to an administrative account, they can:

- use the elevated privileges to affect your organization's operating environment
- degrade or disrupt network traffic
- access sensitive information

Attackers can also learn which detection and recovery activities are in place on your systems, helping them avoid discovery and preventing you from stopping further attacks.

Techniques used to access administrative privileges

Cyber threat actors use different techniques to acquire user account credentials that they then use to gain entry to networks and systems. Initial compromises often result from normal user activity, such as opening a malicious email attachment or visiting unsecure websites. Threat actors may also take advantage of known vulnerabilities to escalate their privileges or use stolen credentials to access administrative accounts.

Here are some common attack methods leading to administrative account compromise.

Malware and phishing: Threat actors can gain access to local or domain administrative accounts by sending an email with malicious attachments or links to malicious sites. When a user who has administrative privileges or is signed in as an administrator opens the email or visits the site, the threat actor can then leverage the administrator's credentials to deploy malware onto your system.

Password cracking: Threat actors can attempt to access accounts directly by conducting password cracking attacks such as:

- **brute force**, where a threat actor uses automated tools to randomly guess common password combinations
- **dictionary-based attacks**, where a threat actor uses a list of commonly used passwords to guess the correct password

Privilege escalation: Threat actors can exploit vulnerabilities in your system or network, by taking advantage of devices or applications that haven't been updated with the latest security patches, to acquire elevated privileges within your information systems.

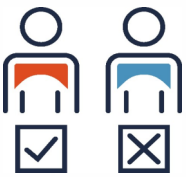
Pass the hash: Threat actors can replay user's hashed authentication credentials, such as a password, from a compromised workstation. These hashed credentials allow the threat actor to move laterally throughout the network. When credentials have been hashed they are changed from readable data into scrambled characters using an algorithm. However, without proper mitigation a replayed hashed credential can be used to create a new login session.

AWARENESS SERIES

Cat. No. D97-1/10-094-2024E-PDF
ISBN 978-0-660-69994-3

Considerations for securing administrative accounts

When assigning administrator accounts or privileged access to users, your organization should take the following measures:



- Apply the principle of least privilege by giving the minimum amount of access required for a user to complete their tasks
- Create administrative accounts that are separate from users' normal access login, which can not access the Internet or email
  - Ensure that administrative tasks are performed on dedicated administrative consoles
  - Ensure remote access to privileged accounts occurs on dedicated consoles
- Use strong authentication methods
  - Use multi-factor authentication for all administrative accounts
  - Use a unique password or passphrase for each privileged account
  - Change default passwords for applications and devices
  - Authenticate users before they are granted access to applications or devices

- Implement two-person integrity (TPI) and dual authentication
  - Require at least two authorized individuals to access or perform a critical task at the same time for TPI
  - Seek mandatory approval from at least two authorized individuals before system changes are applied for dual authentication

- Ensure that unique, identifiable accounts are attributed to individual users
- Log and monitor actions on privileged accounts
- Provide training on expected behaviours for privileged account users
- Delete and remove special access privileges when users no longer need them

Managing non-administrative accounts

Threat actors are not only interested in gaining access to administrative accounts. They will leverage any user account in attempt to gain as much access as possible.

When your organization manages and controls administrative accounts and privileges, it creates an operating environment that is stable, reliable, and easier to support. Proper access control and account management means that fewer users can make significant changes to the operating environment.

When users only have access to the systems and the information required to perform their job functions, your organization is better protected from outside threat actors. Managed user permissions and access will also limit the impact of unintentional and malicious insider threats.

Learn more

For more information, read our other publications:

- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.189)
- Top 10 IT security actions: No.3 managing and controlling administrative privileges (ITSM.10.094)
- Best practices for passphrases and passwords (ITSAP.30.032)
- How to protect your organization from insider threats (ITSAP.10.003)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)
- Steps for effectively deploying multi-factor authentication (ITSAP.00.105)
- Offer tailored cyber security training to your employees (ITSAP.10.093)