National Cyber Security Centre
a part of GCHQ

Guidance (/)

10 Steps: Managing User Privileges

Created: 29 Sep 2015
Updated: 08 Aug 2016
Part of: 10 Steps to Cyber Security (/guidance/10-steps-cyber-security)

This section from within the NCSC's '10 Steps To Cyber Security' concerns Managing User Privileges.

Summary

If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

What is the risk?

Organisations should understand what level of access employees need to information, services and resources in order to do their job otherwise it won't be possible to manage rights appropriately. Failure to effectively manage user privileges could result in the following risks being realised:

- **Misuse of privileges:** Users could either accidentally or deliberately misuse the privileges assigned to them. This may result in unauthorised access to information to either the user or a third party or to unauthorised system changes having a direct security or operational impact.
- **Increased attacker capability:** Attackers may use redundant or compromised user accounts to carry out attacks and, if able, they may return to reuse the compromised account or possibly sell access to others. The system privileges provided to the original user of the compromised account will be available to the attacker to use which is why they particularly seek to gain access to highly privileged or administrative accounts.
- **Negating established security controls:** Where attackers have privileged system access they may make changes to security controls to enable further or future attack or might attempt to cover their tracks by making changing or audit logs.

How can the risk be managed?

Organisations should determine what rights and privileges users need to effectively perform their duties and implement a policy of 'least privilege'.

Establish effective account management processes: Manage user accounts from creation, through-life and eventually revocation when a member of staff leaves or changes role. Redundant accounts, perhaps provided for temporary staff or for testing, should be removed or suspended when no longer required.

Establish policies and standards for user authentication and access control: A corporate password policy should be developed that seeks an effective balance between security and usability as set out in our password guidance(/guidance/helping-end-users-manage-their-passwords). For some accounts an additional authentication factor (such as a token) may be appropriate.

Limit user privileges: Users should be provided with the reasonable minimum rights and permissions to systems, services and information that they need to fulfil their business role.

Limit the number and use of privileged accounts: Strictly control the granting of highly privileged system rights, reviewing the ongoing need regularly. Highly privileged administrative accounts should not be used for high risk or day to day user activities, for example web browsing and email. Administrators should use normal accounts for standard business use.

Monitor: Monitor user activity, particularly access to sensitive information and the use of privileged account actions. Respond where activities are outside of normal, expected bounds (such as access to large amounts of sensitive information outside of standard working hours).

Limit access to the audit system and the system activity logs: Activity logs from network devices should be sent to a dedicated accounting and audit system that is separated from the core network. Access to the audit system and the logs should be strictly controlled to preserve the integrity of the content and all privileged user access recorded.

Educate users and maintain their awareness: All users should be aware of the policy regarding acceptable account usage and their personal responsibility to adhere to corporate security policies.

Learn more

Read our End User Device Security Guidance (/guidance/end-user-devices-security-guidance-introduction)for help with how you might configure user devices appropriately.

Further reading

End User Devices Security Guidance: Introduction(/guidance/end-user-devices-security-guidance-introduction-0)

Topics

Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No