T2025_03 Secure Your Active Directory Service Accounts by Following the Principle of Least Privilege (27th February 2025)

AD service accounts should only have the minimum permissions required to perform their tasks. Avoid assigning excessive privileges, such as making a service account a domain or enterprise administrator, as this can create significant security risks. Restricting permissions helps reduce the attack surface and prevents malicious actors from exploiting over-privileged accounts to move laterally within the network. Regularly audit and refine permissions to ensure accounts are properly restricted.

References

- Iainfoulds. (2023, October 11). Best Practices for Securing Active Directory. Retrieved from Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
- Specops Software. (2025, February 25). Five best practices for securing Active Directory service accounts. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/five-best-practices-for-securing-active-directory-service-accounts/