

ACTIVE DIRECTORY SECURITY HARDENING

Improve the security level of your
Windows enterprise environment



Improsec's Active Directory Security Hardening will remediate misconfigurations and implement missing defensive measures which will withstand, or reduce, the impact of a cyber security intrusion in your Windows enterprise environment.

Value

The Active Directory Security Hardening will mitigate various attack techniques within privilege escalation, obtaining remote access, lateral movement, and data exfiltration within your Active Directory environment. If hackers compromise a single user or computer, the risk of hackers being able to further compromise large sections - or the entire Windows enterprise environment - will be significantly reduced with the security hardening implemented.

Product

The deliverable of the engagement is:

- Remediation of (mis)configurations of privileges and permissions on computers, users, files, etc. which form a security risk
- Disabling of features not utilized within your environment, which may be exploited by hackers
- Phase-out of insecure, legacy software and protocols as NTLMv1, SMBv1, etc.
- Implementation of best practice features as LAPS, Group Managed Service Accounts, Resource-Based Constrained Delegation, Protected Users, etc.
- Security improvement of administration and support methods utilised by your IT department

- Implementation of the Tier Model. The purpose of this Tier Model is to protect identity systems using a set of buffer zones between full control of the environment (Tier 0) and the high-risk workstation assets that attackers frequently compromise. Should a cyber intrusion occur, it will be limited to a compromise only to that specific tier (or part of it) and should not expose the rest of the infrastructure from Active Directory perspective
- Documentation for each improvement made in the environment, reason behind the improvement, and description of maintenance

Method

For all parts of the delivery, Improsec will assess the current security state of the entity and initialize a discussion with the responsible employees from your IT operation on potential security improvements, what issues there might be in your environment, and together create a plan for remediation. Improsec A/S can perform both the actual implementation and enforcement in your environment, depending on your preferences.

Involvement

The delivery requires on-going involvement of your technical staff.