Active Directory Security Checklist

Top-10 Active Directory Security Measures

At the very foundation of your organization’s cyber security infrastructure, lies your mission-critical Active Directory deployment.

As the very foundation of your organization’s security, your Active Directory is an extremely high-value organizational IT asset. Its adequate protection and security are thus paramount to business and merit being your organization’s #1 cyber security priority.

Active Directory Security Checklist

The following checklist is provided to help organizations assess and maintain the security of their Active Directory deployments:

- Ensure that the logical (forest, domain and trust-relationship) structure of your Active Directory is conceptually secure
- Ensure that all Active Directory configuration (e.g. Schema, Replication, FSMOs, Backups) data is sound and secure
- Ensure that adequate Active Directory management, security and disaster-recovery plans are in place and implemented
- Ensure that adequate physical, system and network security is provided for all Domain Controllers and admin workstations
- Ensure that the number of IT personnel who possess unrestricted administrative access in Active Directory is minimal
- Ensure that all non-critical administrative tasks (e.g. password resets) are delegated based on the principle of least privilege
- Ensure that IT personnel can audit all administrative delegations (i.e. assess and verify effective access) in Active Directory
- Ensure that auditing mechanisms are in place to capture the enactment of all admin/delegated tasks in Active Directory
- Ensure that all applications and tools used by IT personnel are trustworthy (i.e. verifiably safe, reputable and secure)
- Ensure that security and effective access audits are performed on a regular basis to consistently ensure security