10. Windows Active Directory Audit

Criticality: **Info**
CVSS-Score: **0.0** | n/a
Affects: Active Directory User Objects

Overview

As part of the penetration test, the user and computer objects stored in Active Directory were analysed and various metrics were evaluated.

Description

Active Directory objects were analysed and metrics evaluated as part of the penetration test. This assessed the current situation within the Active Directory domain.

User statistics

Description	Number	Percent
Active Users	1102	97%
Inactive Users	32	3%
Password changed more than 1 year ago	402	35%
Password changed more than 5 years ago	281	24%
Password never expires	103	9%
Active users who have never logged in	97	9%
User delegation allowed	1097	96%
Password not required	0	0%
Passwords stored with reversible encryption	0	0%
Users with Kerberos Pre-Authentication disabled	0	0%

There are many active users in the Active Directory domain that are no longer used. These should be deactivated. Furthermore, the delegation of almost all user accounts - including highly privileged users - was allowed. This should be deactivated at least for highly privileged users. Almost 700 users have not changed their password for more than a year. It could be considered to reset the passwords of all users after adjusting the password policy to enforce complex passwords.

Privileged group statistics

Group name	Number of group members
ADMINISTRATORS@LAB.LOCAL	27

Group name	Number of group members
DOMÄNEN-ADMINS@LAB.LOCAL	16
ORGANISATIONS-ADMINS@LAB.LOCAL	4
SCHEMA-ADMINS@LAB.LOCAL	4
SERVER OPERATORS@LAB.LOCAL	12
ACCOUNT OPERATORS@LAB.LOCAL	6
BACKUP OPERATORS@LAB.LOCAL	16
PRINT OPERATORS@LAB.LOCAL	33
CERT PUBLISHERS@LAB.LOCAL	15
DNS ADMINS@LAB.LOCAL	1

27 Users were in the "Administrators" group at the time of the audit. Through this authorisation, the users are also local administrators on the domain controllers. There, these users could add themselves to the group of domain administrators and extend their rights. These users are therefore to be considered equivalent to domain administrators and should be reduced to a minimum. At the time of the audit there were 16 domain administrators. This is considered high given the size of the infrastructure. The number of domain administrators should be reduced as much as possible.

Computer statistics

At the time of the audit, there were 871 machine accounts registered in the Active Directory domain. The following table shows the operating systems used and their versions.

Operating System	Number
Microsoft Windows Server 2003 Service Pack 2	1
Windows XP for Embedded Systems	5
Microsoft Windows Server 2008 R2 Standard Service Pack 1	3
Microsoft Windows Server 2008 R2 Foundation Service Pack 1	1
Microsoft Windows Server 2016 Standard	7
Microsoft Windows 7 Professional	23
Microsoft Windows 10 Pro	831

17 Computers and servers were no longer using supported operating systems at the time of the audit.

Recommendation

- The number of domain administrators and other highly privileged accounts should be kept to a minimum.

- Users who have not logged in for a long time should be set to "inactive".
- After implementing a stricter password policy, we recommend resetting the passwords of all users once.
- Computers with unsupported operating system versions should be deprovisioned or upgraded.