Sponsored by ITPro Today

Active Directory Vulnerabilities and Mitigation Tactics

That Active Directory you're saddled with? Chances are you **didn't design or implement it**. So how can you be sure it will hold up to today's threats? **It helps to understand security vulnerabilities and ways to mitigate risk.**

1 Security vulnerabilities

Is my Active Directory secure?

AD is a rich attack surface

95% of Fortune 1000 companies **use AD**[1]

With common security issues

- AD Forests are **14 years old** on average[2]
- Passwords set to never expire
- Inactive **user accounts**
- Unnecessary elevated **permissions**
- Lack of **governance**
- Lack of **AD disaster recovery planning**

Are you prepared?

51%

of IT pros are "**not very well**" or "**not at all**" prepared for threats[3]

2 Attack vectors and methods

How am I most vulnerable?

80%

Over **80% of breaches involve brute force**, or the use of **lost or stolen credentials**[4]

The problem could be your AD management...

Read access
A good idea in 1999; **not so much anymore**

GPOs
Unused or neglected GPOs are **susceptible to attacks**

Bad passwords
26% of users have **weak or commonly used passwords**

Groups
Watch out for empty, **forgotten or unmanaged groups**

...or your AD access

User accounts
- Too many rights
- Poor group management
- Unconstrained delegation

Forgotten test user accounts
- Password set to never change
- Easily guessable password
- Password set using outdated password policy

Service account dangers
- Old passwords no longer used
- Over permissioned
- Unconstrained delegation

3 Quick tips on mitigation and remediation

How can I reduce my risk?

Monitor your Active Directory
- Audit changes such as logons, group membership, and any object modification

Manage service accounts
- Perform yearly audits
- Use limited access rights
- Rotate passwords

Follow sound user account management
- Use a password manager with complex passwords
- Never use dictionary words or old passwords
- Educate users on best practices

Work with HR on role-based security practices
- Automate rights based on HR system
- Only grant permissions you need

Set up a fortified administration management system
- Use an enhanced security admin environment
- Limited rights reduce the damage of compromise accounts

Guard computers with most access to secure system
- Use privileged access workstations (PAWs) on hardened computers
- Never connect PAWs to the internet

Actively manage AD Groups
- Understand who's in a group and audit regularly
- Remove old, underused or unused groups
- Understand groups across AD

4 Disaster recovery

How do I recover from an attack?

Mistakes happen.
When a disaster like a cyber attack or ransomware strikes your AD, every second counts.

Restore quickly.
You need a way to quickly restore your AD at the object and attribute level, the directory level and the operating system level across the entire forest.

Plan for disaster.
Before an attack occurs, create a virtual lab to demonstrate and execute a complete disaster recovery plan so you're prepared when disaster strikes.

5 Quest for AD management and security

184 million AD accounts managed

166 million AD accounts audited

Whether you're running AD, Azure AD or a hybrid AD environment, **Quest is your go-to vendor for everything Active Directory**. With Quest, you have one partner and one set of tools to address all of your **AD migration, management and cybersecurity resilience needs**.

Visit www.quest.com/solutions/active-directory to get started.

Quest

Sources:

[1] **Offensive Active Directory 101**
https://swasp.org/www-pdf-archive/OWASP_FFM_41_OffensiveActiveDirectory_101_MichaelRitter.pdf

[2] **Quest Active Directory Security Assessments Reveal Top 4 Issues: #1 Service Accounts (Part 1 of 3)**
https://www.quest.com/community/blogs/b/microsoft-platform-management/posts/top-4-issues-in-active-directory-service-accounts

[3] **Who is responsible for Active Directory security within your organization?**
https://www.help-netsecurity.com/2019/11/06/active-directory-security

[4] **Verizon 2020 Data Breach Investigations Report**
https://enterprise.verizon.com/resources/reports/dbir

[5] **Western Australian Auditor General's Report**
https://audit.wa.gov.au/wp-content/uploads/2018/05/report2018_14-IS-GCC-App-Pass.pdf