Top Strategies to Harden Your Active Directory Infrastructure

blog.netwrix.com/2023/04/28/harden-active-directory

Microsoft Active Directory (AD) is the central credential store for 90% of organizations worldwide. As the gatekeeper to business applications and data, it's not just everywhere, it's everything! Managing AD is a never-ending task, and securing it is even harder. At Netwrix, we talk to a lot of customers who are using our tools to manage and secure AD, and over the years, key strategies for tightening security and hardening AD to resist attacks have emerged. Here are 10 Active Directory security hardening tips that you can use in your environment:

Handpicked related content:

Active Directory Group Management Best Practices

Tip #1: Clean up stale objects.

Active Directory includes thousands of items and many moving elements to safeguard. A core method for increasing security is to decrease clutter by removing unused users, groups and machines. Stale AD objects may be abused by attackers, so deleting them reduces your attack surface.

You may also find seldom-used items. Use HR data and work with business stakeholders to determine their status; for example, for user accounts, determine the user's manager. While this takes time, you'll appreciate having it done during your next audit or compliance review.

Tip #2: Make it easy for users to choose secure passwords.

To prevent adversaries from compromising user credentials to enter your network and move laterally, passwords need to be hard to crack. But users simply cannot remember and manage multiple complex passwords on their own, so they resort to practices that weaken security, such as writing their passwords on sticky notes or simply incrementing a number at the end when they need to change them. That led security experts to weaken their recommendations concerning password complexity and resets.

However, with an enterprise password management solution, you can make it easy for users to create unique and highly secure passwords and manage them effectively, so you do not have to compromise on strong password requirements. A user needs to memorize just one strong password, and the tool manages all the others for them.

Tip #3: Don't let employees have admin privileges on their workstations.

If an attacker gains control of a user account (which we all know happens quite a bit), their next step is often to install hacking software on the user's workstation to help them move laterally and take over other accounts. If the compromised account has local admin rights, that task is easy.

But most business users do not actually need to install software or change settings very often, so you can reduce your risk by not giving them admin permissions. If they do need an additional application, they can ask the helpdesk to install it. Don't forget to use Microsoft LAPS ensure all remaining local admin accounts have strong passwords and change them on a regular schedule.

Tip #4: Lock down service accounts.

Service accounts are used by applications to authenticate to AD. They are frequently targeted by attackers because they are rarely monitored, have elevated privileges and typically have passwords with no expirations. Accordingly, take a good look at your service accounts and restrict their permissions as much as possible. Sometimes service accounts are members of the Domain Admin's group, but typically don't need all of that access to function — you may need to check with the application vendor to find out the exact privileges needed.

It's also important to change service account passwords periodically to make it even more difficult for attackers to exploit them. Doing this manually is difficult, so consider using the group managed service account (gMSA) feature, introduced in Windows Server 2016. When you use gMSAs, the operating system will automatically handle the password management of service accounts for you.

Tip #5: Eliminate permanent membership in security groups.

The Enterprise Admin, Schema Admin and Domain Admin security groups are the crown jewels of Active Directory, and attackers will do everything they can to get membership in them. If your admins have permanent membership in these groups, an attacker who compromises one of their accounts will have permanent elevated access in your domain.

To reduce this risk, strictly limit membership in all of these highly privileged group and, furthermore, make membership temporary. The Enterprise Admin and Schema Admin groups are not frequently used, so for these, this won't be an issue. Domain Admin is needed much more, so a system for granting temporary membership will have to be set up.

Tip #6: Eliminate elevated permissions wherever possible.

There are three fairly common permissions that attackers need to execute attacks against AD: Reset Password, Change Group Membership and Replication. These permissions are harder to secure since they are so frequently used in daily operations.

Accordingly, you should monitor all changes to security group permissions or membership that would grant these rights to additional users. Even better, implement a privileged access management (PAM) solution that enables just-in-time temporary provisioning of these privileges.

Tip #7: Implement multifactor authentication (MFA)

MFA adds an extra layer of security by requiring users to verify their identity by providing at least two of the following types of authentication factors:

- Something they know, such as a password, PIN or answer to a security question
- Something they have, such as a code from a physical token or a smart card
- Something they are, which means biometrics like a fingerprint, iris or face scan

Tip #8: Closely audit your Active Directory.

It is important to audit Active Directory for both non-secure settings and suspicious activity. In particular, you should perform regular risk assessment to mitigate security gaps, monitor for anomalous user activity, and promptly identify configuration drift in critical system files. It's ideal to invest in tools that will automatically alert you to suspicious events and even respond automatically to block threats.

Tip #9: Secure DNS.

Securing DNS can help you to block a variety of attacks, including as domain hijacking and DNS spoofing. Steps to take include implementing DNSSEC, using a secure DNS server and regularly reviewing DNS settings.

Tip #10: Regularly back up Active Directory.

Having a recent backup of your Active Directory is crucial for recovery from cyber incidents, including ransomware attacks and natural disasters. Backups should be stored securely, tested regularly and be readily accessible to ensure your critical AD settings are recoverable in the event of a disaster.

Conclusion

Active Directory is an amazing system for controlling access. However, it's only secure when it's clean, understood, properly configured, closely monitored and tightly controlled. These tips are practical ways that you can tighten security and harden your Active Directory.

Frequently Asked Questions

What is hardening in Active Directory?

Hardening in Active Directory is the process of securing and strengthening the directory service to reduce the risk of data breaches and downtime. It involves controlling access to sensitive data, removing unnecessary objects, enforcing password policies and monitoring for suspicious activity.

What is domain controller hardening?

Domain controller hardening is the process of strengthening the servers that run Active Directory to reduce the risk of unauthorized access, data breaches and service disruption. It includes deactivating superfluous services, deploying security patches and updates, establishing firewall rules, and enforcing strong password practices.

What happens if a domain controller is compromised?

An adversary who compromises a domain controller can do significant damage, from accessing sensitive data to creating, modifying and deleting user accounts and other critical AD objects.

How do I secure Active Directory?

Securing Active Directory is an ongoing process that involves multiple layers of security controls. In particular, organizations need to implement strong password policies, limit user access, monitor for suspicious activity, keep machines patched and updated, secure domain controllers, use multifactor authentication (MFA) to add extra security, and educate employees on cybersecurity best practices and potential threats.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.