DATA SHEET

Active Directory Hardening

Why is Active Directory Hardening so Important?

At the core of most organizations' infrastructure, Active Directory manages various aspects of the user and computer resources in an environment. If an attacker controls these keys to the kingdom, they can control an organization the same way its system administrators would, without the need to use any hacking tools.

Active Directory affects security at multiple levels. It defines the high-level security of trusts between global offices as well as the low-level, granular permissions that determine whether a specific program can run on a user's laptop. Hardening this core infrastructure is a critical first step in improving the security posture of an environment.

What to Expect

- MOXFIVE working closely with your infrastructure team to fully understand the environment and Active Directory architecture.
- A review of trust relationships.
- An audit of privileged groups for appropriate membership.
- An evaluation and enhancement of granular audit policies to improve security, efficiency, and incident response preparedness.
- Documentation to aid administrators and end-users.
- Regular status updates detailing accomplishments, next steps, and engagement economics.

©2021 MOXFIVE LLC. All rights reserved.

What Tactical Steps Should We Expect for Active Directory Hardening?

The below activities are a high-level roadmap of how a standard MOXFIVE Active Directory hardening engagement is performed.

Introduce us to the key stakeholders:

- Someone who can speak to the existing Active Directory architecture and configuration.
- Someone who can speak to the existing applications and services in the environment that require service accounts.

Provide MOXFIVE details about your environment to facilitate customization of a hardening plan for your Active Directory.

- An understanding of the organization, and implementation of your Active Directory.
- Expected requirements and trusts between forests and domains.
- Privileged user groups.
- Services and applications that require privileged accounts.
- Special considerations for your unique environment.

Provide MOXFIVE access to your environment to facilitate hands-on-keyboard support.
Establish a regular meeting cadence with MOXFIVE and agree on status update timing.
Once engaged, MOXFIVE engineers will deliver the following:

- Reducing the size of the privileged Domain, Enterprise, and Schema Admins groups.
- GPO Restricted Groups for Domain, Enterprise, and Schema Admins groups.
- Migration from Microsoft's File Replication Service (FRS) to Distributed File System Replication (DFRS), if applicable.
- Configure customized granular audit policies.
- Explore and test disabling insecure protocols: SMBv1, LLMNR & NetBIOS, WDigest
- Require SMB and LDAP signing, if possible, and perform testing.
- Ensure no passwords are stored within Group Policy/SYSVOL.
- Disable unsecure Kerberos delegation.
- Implement Microsoft Local Administrator Password Solution (LAPS) for servers and workstations, and restrict LAPS password access to authorized groups.
- Lockdown of service accounts:
    - Audit and review of servers and accounts
    - Principle of least privilege backed by strong passwords
    - Avoid local administrator and domain administrator access
    - Deny logon locally and as batch

Once the Active Directory hardening has been completed successfully, the MOXFIVE team will schedule a meeting with the engagement owner for a debrief discussion.

MOXFIVE is a specialized technical advisory firm founded to help minimize the business impact of cyber attacks. Over the last decade, our team of experts has helped thousands of businesses respond to major incidents and saw firsthand that there needed to be a better way for organizations to get the technical expertise they need when they need it most. With deep roots in incident response and corporate IT, MOXFIVE Technical Advisors strive to be the go-to technical resource for our clients - helping organizations of all types solve their most challenging technology-related problems and provide technical expertise at scale.

www.moxfive.com
(833) 568-6695
info@moxfive.com
MOXFIVE

©2021 MOXFIVE LLC. All rights reserved.