ManageEngine
Log360

14- POWERFUL measures for fortifying your Active Directory

Hi,
My name is Ella. **Did you know that nearly 90%** of organizations use Active Directory in their IT infrastructures to manage user authentication and authorization? Therefore, it's not a surprise that cybercriminals view AD as a lucrative target. I'm here to give you a checklist of best practices to enhance your AD security.

1 UPDATE AND PATCH CONSISTENTLY

Make sure to patch your operating system, applications, and AD servers regularly. You can deploy vulnerability scanners and patch scanning to detect these vulnerabilities. It will help your organization stay ahead of vulnerabilities.

2 SECURE ADMINISTRATIVE PRIVILEGES

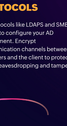
Ensure that you grant administrative privileges only to those who require them for their tasks. This will again reduce your organization's vulnerabilities.

3 UTILIZE INDESTRUCTIBLE PASSWORD POLICIES. ENSURE YOUR ORGANIZATION:

- Employs unique, strong passwords that combine capital and lowercase alphabets, digits, and unusual characters.
- Considers using passphrases instead of passwords.

4 IMPLEMENT MULTI-FACTOR AUTHENTICATION

Add an additional layer of security for your organization by implementing MFA.



5 MONITOR AND REVIEW YOUR AD CONTINUOUSLY

Closely track changes in your AD to detect possible breaches and threats. Enable appropriate auditing and detection rules.

6 IMPLEMENT NETWORK SEGMENTATION

Make sure to restrict lateral movement, by employing micro segmentation to isolate the vital AD infrastructure from other network resources.

7 USE SECURE PROTOCOLS

Use protocols like LDAPS and SMB signing to configure your AD environment. Encrypt communication channels between AD servers and the client to protect against eavesdropping and tampering.

8 APPLY STRONG FIREWALL RULES

Ensure that you employ effective firewall rules to permit just the essential network traffic to and from the AD servers.

9 UTILIZE WELL-ORGANIZED BACKUPS

Back up your AD data frequently, and verify that the restoration process is proceeding as intended.

10 APPLY SECURITY BASELINES AND BENCHMARKS:

Compare your AD configurations to established security standards and benchmarks.

11 HAVE A RECOVERY PLAN:

- Create an **incident response** policy and plan.
- Establish procedures for handling and **reporting incidents.**
- Cultivate procedures for communicating with **third-parties.**
- Set up **response teams and leaders.**

12 PROVIDE USER TRAINING TO INCREASE SECURITY AWARENESS

In order to remain conscious and prevent attacks, educate users about common security threats and the ways to prevent them.

13 DELETE UNNECESSARY ACCOUNTS

To prevent the attackers from using dormant accounts, make sure your IT team deactivates or deletes them as soon as possible.

14 STANDARDIZE GROUP NAMES

It's important to give standardized names for AD groups. This decreases confusion and also aids in preventing hackers from gaining unauthorized access.

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. Log360 provides holistic security visibility across on-premises, cloud, and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities. For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

GET IN TOUCH

WITH OUR PRODUCT
EXPERTS FOR FREE DEMO

SIGN UP FOR FREE DEMO