ACTIVE DIRECTORY PROTECTION CHECKLIST

Attivo NETWORKS

The Active Directory (AD) environment is a primary target for attackers. However, protecting AD is a daunting task, made more difficult because AD administrators must balance operational requirements with restrictive security measures. Many solutions exist that can secure the AD infrastructure, but identifying the right solution that meets the risk profile for a particular organization can be challenging. Use this checklist to evaluate current AD security procedures to identify risks and gaps. Compare them against solution capabilities to address specific requirements.

QUESTIONS TO ASK IN LOOKING TO SECURE ACTIVE DIRECTORY

ACTIVE DIRECTORY CYBER HYGIENE

- ☐ Is there an inventory of all user or device accounts?
- ☐ Is there an inventory of all privileges & entitlements for every account?
- ☐ Is there an implemented least privilege policy for all accounts?
- ☐ Are AD security settings regularly reviewed & reassessed?
- ☐ Are kerberos vulnerabilities regularly assessed in AD?
- ☐ Are AD servers hardened against the latest CVEs & other vulnerabilities?
- ☐ Are trusts relationships across forests regularly audited?

ATTACK DETECTION FROM THE DOMAIN CONTROLLERS

- ☐ Are attempts to harvest AD data detected or stopped?
- ☐ Are audit policies enabled?
- ☐ Are audit logs periodically analyzed?
- ☐ Is there visibility into Domain directory replication?
- ☐ Is there visibility into attempts to discover user & group permissions?
- ☐ Is there real-time visibility into mass changes to AD?
- ☐ Is there real-time detection for attacks like password spraying & DCShadow?

ACCOUNT ISSUES

- ☐ Are account privileges regularly audited & reassessed for each account?
- ☐ Are service or privileged accounts regularly audited & reassessed?
- ☐ Is there a limit to the scope & number of privileged accounts?
- ☐ Are delegations regularly audited & reassessed?
- ☐ Are password policies sufficient & regularly reassessed?
- ☐ Is there real-time detection for built-in AD "Administrator" account usage?

ATTACK DETECTION FROM ENDPOINT

- ☐ Is there detection for intelligence-gathering & discovery attempts from the endpoints targeting AD?
- ☐ Are there security controls to misdirect AD discovery queries originating from endpoints?
- ☐ Are AD credentials stored on endpoints? If so, should they be removed?
- ☐ Is there visibility to stored privileged or high-risk AD credentials at the endpoints that attackers can leverage for lateral movement?
- ☐ Is there visibility into attempts to discover delegated accounts with special privileges?

Security teams can also choose to use a weighted score for their answers and trend these scores over time for ongoing health analysis and management reporting. Attivo Networks offers several solutions that address these and many other Active Directory-related problems.

DEFINITIONS

ACTIVE DIRECTORY CYBER HYGIENE

The items in this checklist category can help identify exposures within Active Directory that attackers can leverage to compromise the environment. Regularly validating AD accounts and objects and having an updated list of their permissions and privileges is essential for good security hygiene. Identifying and remediating vulnerabilities that attackers can target is vital to maintaining a hardened and secure AD infrastructure.

ACCOUNT ISSUES

Account policies and settings can determine the extent to which attackers can exploit a particular AD identity. Organizations should audit and assess each account to ensure they have only the necessary permission required to accomplish their functions, especially for privileged accounts and accounts with delegated administrative privileges (shadow admin accounts). Organizations should also periodically review existing password policies to validate that these are sufficient for their risk profile. Credentials stored on endpoints can lead to theft and reuse, so security teams should periodically review and remove any AD credentials stored on endpoints that allow privileged access to sensitive or critical systems and data.

ATTACK DETECTION

Many organizations lack controls to detect attack activities targeting AD data, such as data harvesting and privilege escalation attacks. Organizations should establish mechanisms to identify when attackers target AD, such as auditing and reviewing AD changes for activities indicating an attack. They should have a means of detecting AD data harvesting, particularly regarding privileged accounts, and identify attackers who attempt to deploy rogue domain controllers or modify settings with DCSync and DCShadow attacks.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications and MITRE® Shield, and its capabilities tightly align to the MITRE ATT&CK® Framework. Attivo has won over 130 awards for its technology innovation and leadership.
www.attivonetworks.com