Active Directory Review

A RICOH Company

Active Directory is at the core of any corporate network and underpins the whole business, but it is complicated to configure correctly. Mistakes in configuration can expose sizeable gaps in your network security because Active Directory defines a vast majority of the security measures applied to the broadest collection of elements that form the technical backbone of your company.

With our strong, proven background in Active Directory configuration, administration and support, MTI consultants are able to review implementation of the directory to determine the overall security of your environment. Our review scrutinises the protection provided to the directory, users, computers and the services it serves.

The Service

The Active Directory Review is designed to highlight the most common critical issues directly affecting security and operations. When remediated correctly, these issues will greatly increase the security of the Active Directory, its host platform and the reliant infrastructure.

The review is designed to examine the configuration of the directory in two focus areas: Security and Functionality.

Stage 1: Information gathering

The project initiation gathers information from all stakeholders about your organisation, its technological layout and current state of operation. Information is grouped into six key areas: Naming, Employees, Systems Overview, Administration overview, Locations and links and Current reported or suspected Active Directory issues.

Stage 2: Security

Security starts with the Forest and then focuses on a few small, but crucial, endpoint settings.

The Forest: The largest security realm in the Active Directory and primary security boundary. The forest will be examined for major configuration issues and security concerns. Multiple forests are addressed separately.

The domain: The domain is the largest security boundary within an Active Directory forest.

Domain controllers: As the host service for the Active Directory, the security of domain controllers is paramount to the entire directory.

Role Based Authority Maturity: Seeks to determine the presence and effectiveness of role-based authority within the Active Directory and connected systems.

Empowered accounts: Accounts that have any level of administrative authority in the system are the targets for attacks because they are stepping stones towards full system access and malicious control.

Passwords: Policies control the creation and management of passwords. The domain enforces these policies in a variety of ways and we assess the policy, whether password filters have been assigned to the domain, and how administrators manage administrative passwords.

Member SAM management: The local SAM database is the core of member system security. Effective management of member SAMs by the directory greatly increases member security and prevents its use as an attack vector against the directory.

Access controls: Every object in the Active Directory has its own access control list (ACL). We check the System Default in place for the Root and other significant objects.

Group policy: A highly effective mechanism for extending configuration control from the directory to member systems and reinforcing that control over time.

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Stage 3: Functionality

Object management: We report on the existence of objects that have not been accessed in a relevant time scale (such as user accounts that have not been used for a login for greater than 90 days).

Documentation: We assess the existence and availability of architecture and process documentation with a high-level review to ensure they are suitable (this is not a full detailed review of all policies and procedures).

Log settings: We assess general log file health, sizing and storage and examine log entries for critical events and certain patterns (such as brute force attacks).

Sites and subnet configuration: The directory's mechanism for understanding the physical layout of the infrastructure and allowing all connected systems to use available network pathways effectively.

DNS: DNS availability and stability are essential to the safe function of the directory.

Deliverables

At the end of the review, the customer will receive:

- A full and detailed report documenting the findings.
- Suggested mitigation for critical findings for security and functional issues.
- Summaries of the business and technical risk that make the results accessible to all stakeholders. The results will be formally presented by a senior consultant.

Outcomes & Benefits:

Our Active Directory Review Assessment:

- Identifies the most common critical issues directly affecting security and operations.
- Outlines remediation measures that will greatly increase the security of the Active Directory, its host platform and the reliant infrastructure.
- Provides peace of mind by discovering critical issues and outlining how they can be addressed.

Why MTI?

MTI has been securing customer environments for more than 30 years. We have developed a wealth of knowledge and skills in the tactics used by malicious users to gain access to corporate networks. As the threat landscape expands to include technologies such as the web, cloud and Active Directory, we have evolved our expertise to help identify new risks to your business and outline remediation measures to counter them.

If required, you can take advantage of our expertise to implement the necessary remediation measures via our professional services operation.

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation