Active Directory Security Assessment

Deliverables

Executive Summary

◆ High level summary
◆ Less technical
◆ Results and recommendations

Detailed Report

◆ Detailed documentation of identified risks
◆ Recommendations and best practices
◆ Comments by security experts

Remediation plan

◆ Prioritized risks with help from an expert in the field
◆ Execution times and ownership set

Overview

Time is a resource. Many organizations try to fit all operational needs and maintenance in and sometimes it's not enough. Getting help from acknowledged experts to identify and assess your security posture greatly improves the security. The support you receive helps you plan and prioritize upcoming activities, such as remediation of the identified issues and risks. We will provide your organization with strong recommendations and a plan to achieve a more secure Active Directory.

Key Features

The AD Security Assessment offering has been developed to collect and analyze as many security controls as possible. Your data is analyzed, and risks are identified. The identified risks are then classified by severity, have comments and recommendations attached and are delivered in a prioritized list. At the end of the delivery an executive summary will be presented together with a workshop style meeting where we prioritize and plan the remediation activities.

Agenda

This is a four-day onsite engagement. The four days does not have to be sequential dates. The exact dates are set during a preparation-call.

Day 1: Data collection
Day 2: Data collection continued with interviews
Day 3: Data analysis, Prepare report
Day 4: Executive summary meeting followed by a technical planning and prioritizing meeting.

advania

Delivery Details

Value proposition

Security Awareness

- ◆ Executive presentation
- ◆ Technical explanations

Knowledge Transfer

- ◆ Explanation of findings
- ◆ Discussion about the risks

Next step

- ◆ Remediation plan with prioritized activities

Keeping your systems and policies up to date

- ◆ Measurement of your current configurations

In-Scope

This assessment is focused on Active Directory and related dependencies. The assessment covers one Active Directory forest.

Here are some of the areas that are covered by the assessment:

- Directory Security Settings
- Domain Controller Security Settings
- Privileged Accounts and Groups
- Administrative Delegation Model
- Active Directory Access Control Lists
- Authentication Protocol Settings
- Strategy and Procedure for Back-up
- Strategy and Procedure for Disaster Recovery
- Domain Name Service security
- Extended Security Boundary
- Security Update Management

Out-Scope

This is a security assessment focusing on security risks meaning that the Active Directory health is not in scope. That means that the assessment will not cover Active Directory replication or logical design of site and subnets etc.

Requirements

Specific requirements for performing the delivery is set at a preparation call. The tools will be provided and run by an Advania expert.

advania