

# Windows and AD-Sanity-Check

## Issue

Most enterprises base on Microsoft systems. Active Directory (AD) is the basis of most modern Microsoft based networks. Via AD central and decentralized services and regulations are controlled. This includes security relevant settings. Appropriate AD setup and configuration is therefore crucial for reliable and secure operation of all involved clients and servers. Best practice requires that Windows stations and AD systems are carefully designed and appropriately protected such that any potential weaknesses cannot be abused.

## Cnlab Services

Cnlab analyze the Windows stations and centralized AD configurations and related administrative processes. The goal is to identify the **vulnerability** to any potential weaknesses, to identify the potential **damage** which can incur if a weakness is exploited, and to assess the related **risk** for the organizations. Further, suggestions for **improvements** are worked out where this seems necessary.

The Cnlab methodology is based on our own experience from more than 10 years in the field, and on the common standards (such as ISO 17799, BSI, OSSTMM). Further, the relevant Microsoft Security Standards are always used for our work.

## Project Sketch

Projects start with an **analysis** phase (interviews, document studies). Based on this, detailed test plans are worked out for a subsequent **verification** phase (automated and manual tests, analysis of AD and policy configurations, analysis of process flows). Results are always documented in a formal **report** which provides a management summary, a description of the review and the obtained results, a list of the performed tests, and a list of the identified weaknesses and the related risks

Work depends on actual network (AD) size and complexity, and on the review focus. Typical smaller network related projects start from 5 days and go up to 15 and more (person) days for more complex scenarios and targets.

## Success Stories

Cnlab has analyzed Microsoft networks and networks and their components since 1997, for major Swiss banks, for public administrations, and for industry users including a number of small and medium enterprises. Reviews have shown weaknesses (in most cases). Based on our engineering background we have always been able to work out improvements which could be implemented within reasonable time and budget, and which could effectively fight the observed weaknesses.

## Cnlab contacts

Detail Information on Windows reviews can be obtained from the following Cnlab representatives:

Thomas Lüthi Tel +41 55 214 33 41

Paul Schöbi Tel +41 55 214 33 33