

Executive Summary



IT Security Audit

Client	Realisator AG
Date	20-12-2016



Head Office		Office Germany
Oneconsult AG Schuetzenstrasse 1 8800 Thalwil Switzerland	Oneconsult AG Baerenplatz 7 3011 Bern Switzerland	Subsidiary of Oneconsult AG Karlstrasse 35 80333 Munich Germany
Tel +41 43 377 22 22 Fax +41 43 377 22 77 www.oneconsult.com info@oneconsult.com	Tel +41 31 327 15 15 Fax +41 31 327 15 25 www.oneconsult.com info@oneconsult.com	Tel +49 89 452 35 25 25 Fax +49 89 452 35 21 10 www.oneconsult.de info@oneconsult.de



1 Executive Summary

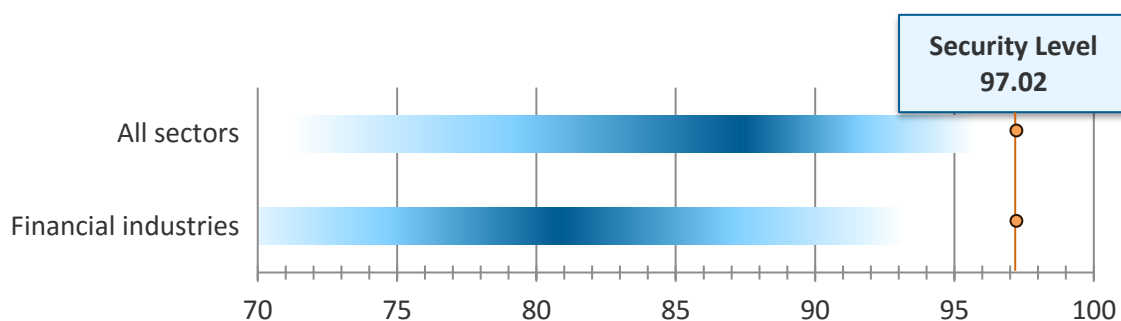
During this IT security audit conducted in December 2016, a security scan and a penetration test were carried out from the internal network on-site at Realisator AG in the internal demilitarized zone. The audit focused on identifying possibilities an attacker may have to gain access to other DMZ servers while already being virtually present in the DMZ.

The project has been conducted following the *Open Source Security Testing Methodology Manual (OSSTMM)* which primarily has the following qualities/goals:

1. Traceability and transparency of the tests and the documentation
2. Guidelines and methodologies about the execution of technical security audits
3. Neutral and objective rating of the security level in the form of a numerical value (RAV)
4. Ethical principles

1.1 Security Scan

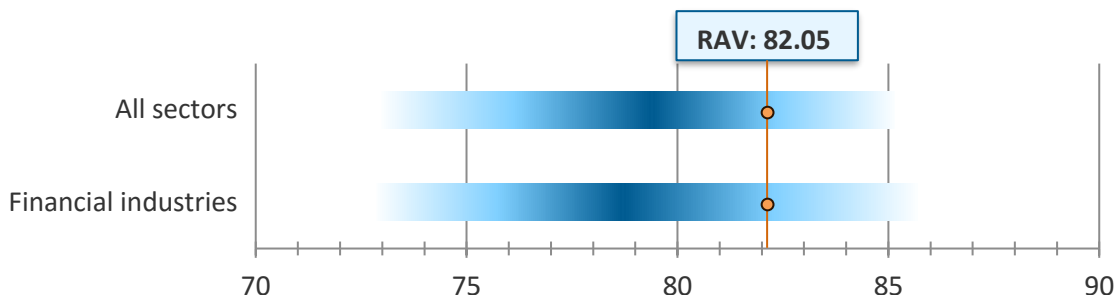
During the security scan, no critical risks were discovered. Thus, the calculated security level is very high also in comparison to past Oneconsult audits (over 750 OSSTMM-compliant projects carried out by Oneconsult):



No risks of the highest category (so called “vulnerabilities”) were discovered. The risks of the second highest category (so called “weaknesses”) all concern encryption with SSL/TLS. As a result, it is highly recommended to only support modern and secure ciphers. This is particularly true for services with confidential information, for example test.easymission.ch or test.easytemp.ch.

1.2 Penetration Test

The penetration test has produced good results, too. The systems are configured with professional competence and reflect the technical know-how of the people in charge. The Risk Assessment Value (RAV) is an in-depth calculation of the effective security based on the OSSTMM standard. The calculated RAV is above average compared to other similar audits. During the penetration test, the IP addresses of the auditors were whitelisted. Due to this, additional risks were found which reduces the calculated RAV value. Hence the effective security of the systems might be slightly higher than the security represented by the RAV value below:



The cooperation between all involved people has been exemplary. At no point during the audit did Oneconsult think that information was concealed or presented in a better light.

Oneconsult would like to kindly thank all involved people for their cooperation and trust.

Oneconsult AG

Rafael Scheel
Senior Penetration Tester, IT-Forensiker &
Security Researcher

Oneconsult AG

Dr. Cathrin Senn
Chief Consulting Officer
Senior Security Consultant