

Executive Summary



Jahresaudit 2019

Kunde	Realisator AG
Datum	09-Jan-2020



Hauptsitz	Büro Bern	Büro Deutschland
Oneconsult AG Schützenstrasse 1 8800 Thalwil Schweiz Tel +41 43 377 22 22 Fax +41 43 377 22 77 www.oneconsult.com info@oneconsult.com	Oneconsult AG Bärenplatz 7 3011 Bern Schweiz Tel +41 31 327 15 15 Fax +41 31 327 15 25 www.oneconsult.com info@oneconsult.com	Oneconsult Deutschland GmbH Agnes-Pockels-Bogen 1 80992 München Deutschland Tel +49 89 248820 600 Fax +49 89 248820 677 www.oneconsult.com info@oneconsult.com



1 Executive Summary

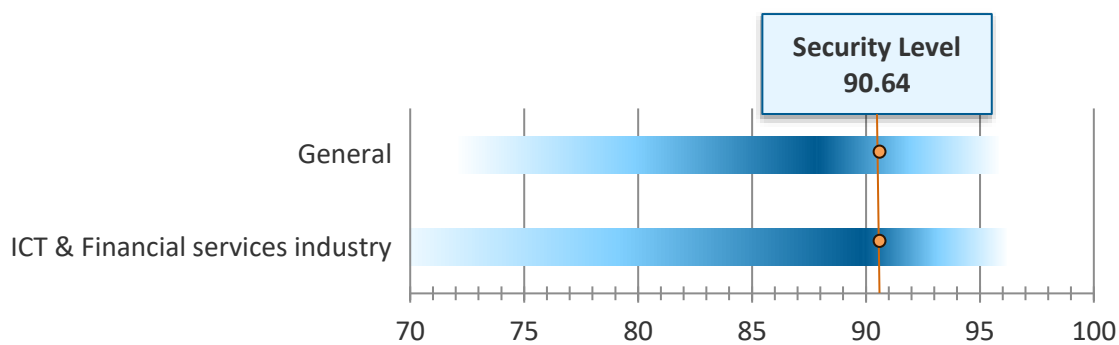
During this IT security audit conducted in December 2019, the security level of the DMZ (demilitarized zone), a part of the IT infrastructure of Realisator AG, was checked from an external and internal perspective by means of technical security tests. Automated vulnerability scans and manual penetration tests were used to search for network vulnerabilities on the systems.

The project has been conducted following the *Open Source Security Testing Methodology Manual (OSSTMM)*, which 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. Based on the projects conducted by Oneconsult in the past years (over 850 OSSTMM-compliant projects), the following benchmark has been defined for the ICT and financial services industries.

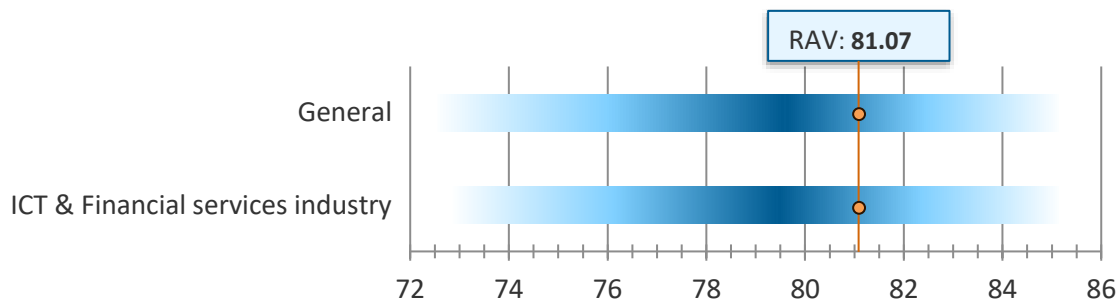


Graph 1: Security level and benchmarking

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.

1.2 Penetration Test

The penetration test of the DMZ (Demilitarized Zone) has produced good results within the scope of the project. The systems are configured with professional competence and reflect the technical know-how of the people in charge. The objective security level is reflected by the Risk Assessment Value (RAV) which is based on the OSSTMM standard. The calculated RAV is above average compared to other similar audits. During the penetration test, the IP address of the auditor was 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:



Graph 2: Risk Assessment Value benchmarking

Note: In practice, a RAV value of 100 is almost impossible. At this point an in-depth cost / benefit analysis (the ratio between the value of the analysed system and the investments in its security) should be performed to evaluate which improvements are worthwhile.

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.

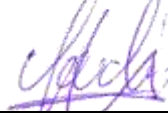
Oneconsult would like to kindly thank all involved people for their cooperation and trust.

Oneconsult AG



Simon Gfeller
Senior Penetration Tester

Oneconsult AG



Claudio Anliker
Team Leader Penetration Testing