Executive Summary

IT Security Audit	
Client	Realisator AG
Date	11-12-2015

REALISATOR

oneconsult®

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

Project

Oneconsult has conduct a IT security audit in November and December 2015. The tests included automated security scans as well as manual penetration tests which were executed from the internal network on the premises of Realisator AG as well as the internet. 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

Security Level

The effective protection requirements depend on the test vector, surrounding systems and assets that need to be protected. Based on the projects conducted by Oneconsult in the past years (over 750 OSSTMM compliant-projects), the following benchmark for the financial services industry may be applied.

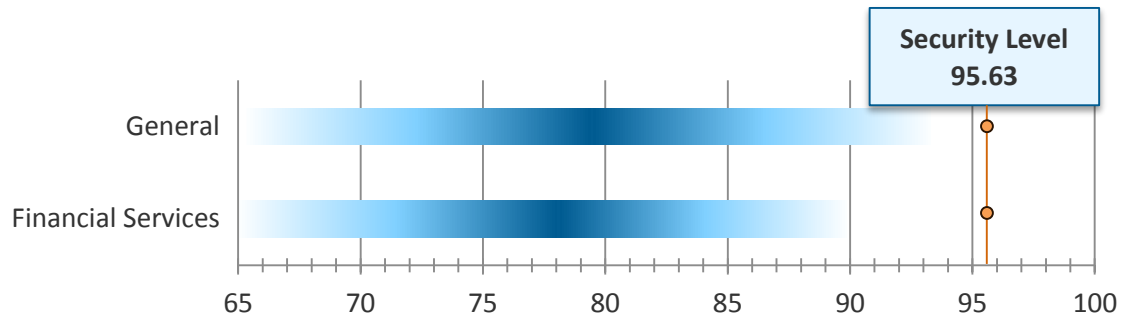

Figure 1 Security Level of the Security Scan

Conclusion

The results of the security audit have shown a good security level 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 audit did not reveal any vulnerabilities that would allow an attacker to access customer data or the infrastructure of Realisator, neither in the demilitarized zone (DMZ) nor from the internet. A first scan of the DMZ did not show any unnecessary visible services. This behaviour greatly reduces the attack surface and is therefore rated positively. All services were then made visible to the auditor to allow a thorough test of all used technologies. The audit shows that in order to access customer data, an attacker would need to circumvent several security measures, as Realisator follows the defence in depth approach.
The hardening of the systems is done thoroughly. Minor adjustments on the webservers could increase the security level.

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

Oneconsult AG

Severin Wischmann
Penetration Tester

Oneconsult AG

Tobias Ellenberger
COO & Partner