Executive Summary

Security Audit 2012

Kunde	Realisator AG
Datum	21.12.2012

| Hauptsitz	Büro Deutschland	Büro Österreich
OneConsult GmbH	Niederlassung der OneConsult GmbH	Niederlassung der OneConsult GmbH
Schützenstrasse 1	Karlstraße 35	Wienerbergstraße 11/12A
8800 Thalwil	80333 München	1100 Wien
Schweiz	Deutschland	Österreich
Tel +41 43 377 22 22	Tel +49 89 452 35 25 25	Tel +43 1 99460 64 69
Fax +41 43 377 22 77	Fax +49 89 452 35 21 10	Fax +43 1 99460 50 00
www.oneconsult.com	www.oneconsult.de	www.oneconsult.at
info@oneconsult.com	info@oneconsult.de	info@oneconsult.at

Project

OneConsult has conducted a detailed security audit in December 2012. The tests included automated security scans and manual penetration tests which were executed from the internal network of Realisator AG (DMZ in Dietikon) and from the Internet. The project has been conducted following the Open Source Security Testing Manual (OSSTMM) which has primarily the following objectives:

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

Security Level and Benchmarking

The objective security level is reflected by the Risk Assessment Value (RAV). The formula is documented within the OSSTMM standard. The effective protection requirements depend on the test vector, the surrounding systems and the assets that need to be protected. Based on the projects conducted by OneConsult, the following benchmark has been defined for manufacturing and the financial services industry. The following graph shows the RAV of the security scan.

Realisator AG: 95.23

50   60   70   80   90   100

Manufacturer

Financial services industry
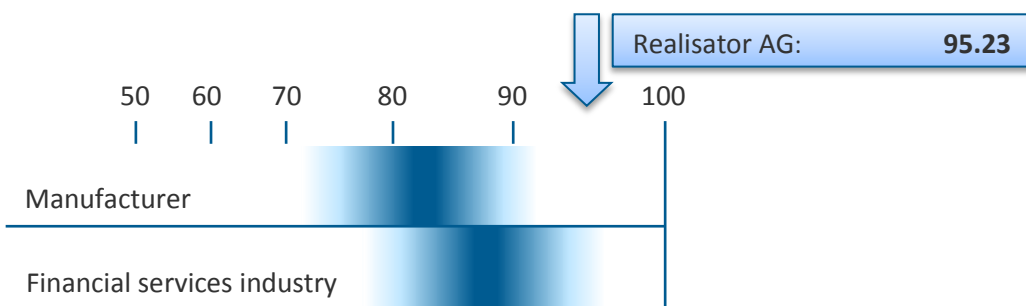
Conclusion

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.

There are no fundamental vulnerabilities allowing unauthorized access to customer data or the infrastructure of Realisator, either within the DMZ in Dietikon as well as from the Internet. On the first run, all ports on every tested system inside of the DMZ were detected as closed. Which has to be rated positively, because all connections are filtered with firewalls and only given connections are allowed. An attacker would have to take over a system within the DMZ in the first place to be able to mount additional attacks against the systems nearby. On a second run, the tester's IP address was whitelisted on the firewall to execute further tests. These tests showed that system hardening is done thoroughly, no critical vulnerabilities were found during the penetration test. Minor adjustments on the webserver and VPN gateway could improve the security level.
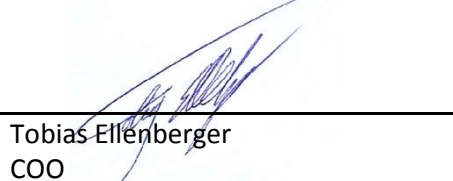
OneConsult would like to kindly thank all involved parties for their cooperation and trust.

OneConsult GmbH

Yves Kraft
Team Leader Consulting & Training

OneConsult GmbH

Tobias Ellenberger
COO