

Management Summary

Initial situation

In this project, the security level of the DMZ (Demilitarized Zone), a part of the IT infrastructure of Realisator AG, was checked from an internal perspective by means of technical security audits. Automated vulnerability scans and manual penetration tests were used to search for network vulnerabilities on the systems. These tests are repeated annually.

Goals of the audit

The aim of the audit was to show how vulnerable the DMZ infrastructure is from the inside. The tests were conducted with regard to the scenarios of possible exfiltration of data as well as the possibility of malware infection within the DMZ.

Security Scan DMZ

Detected risks

The security scan was carried out on 04 December 2018 within the DMZ. No critical vulnerabilities were discovered within the DMZ.

Security level and benchmarking

The objective security level of systems examined in the form of an automated security scan is reflected in the security level.

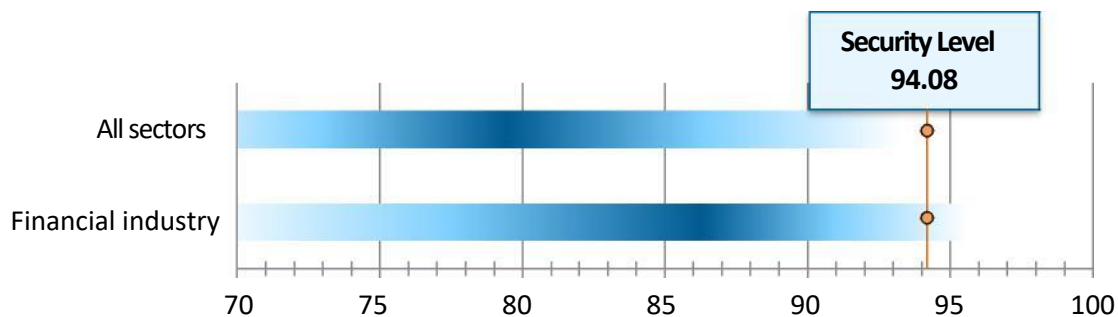


Abbildung 1: Security Level and benchmarking

The security level of the DMZ is rated as high. However, it has to be pointed out explicitly that a security scan is not equivalent to a full penetration test, which searches more intensively for security gaps. Particularly for web servers, which are usually more vulnerable due to their high attack surface, further risks could possibly exist. However, the security level can be increased by implementing the recommended measures.

Penetration Test DMZ

Security level

The objective security level of the object under investigation is reflected in the Risk Assessment Value (RAV).

The effective protection requirement depends on the test vector, the surrounding systems and the values to be protected. On the basis of the projects carried out by Oneconsult in recent years (basis: more than 850 OSSTMM-compliant projects), the following benchmarking can be established for the

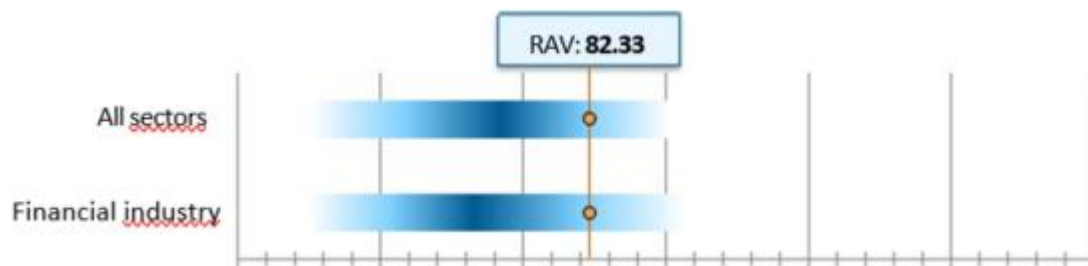


Abbildung 2: Risk Assessment Value Benchmarking

Note: A RAV of 100 can hardly be achieved in practice. At this point, the cost-benefit ratio (i.e. the value of the object under investigation (protected property, asset) in relation to the investment costs in its security) must be taken into account.

Conclusion

The penetration test and the security scan of the DMZ (Demilitarized Zone) 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 achieved security level is high. The infection risk for malware is low for a system within the DMZ from and through systems in the DMZ, which is the core statement after a test within this scope and with this testing results.

The examined environment, the DMZ, is tested annually by different auditors. This is one important reason for only few risks found. No critical vulnerabilities were detected during the test and the total number of risks found was also low.

The above Risk Assessment Value (RAV) for the penetration test and the security level for the security scan are above average. However, it should be considered that the examined network is not very large and does not provide many functions, which constitutes a small attack surface. A small attack surface is beneficial from a security perspective. The systems have not been tested from the internet.

No risks of the category "Vulnerability" (= most dangerous level) were detected. Nevertheless, some risks were discovered. The identified risks concern the configuration of the TLS servers and the TLS certificates in use. The TLS configuration could be further improved by disabling weak encryption algorithms.

Oneconsult recommends to re-evaluate at least the aforementioned risks as soon as possible.

All risks and measures for the various test vectors are listed in the [full report](#).

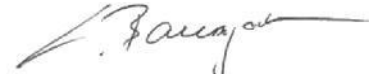
Cooperation with all parties involved was exemplary. Oneconsult would like to thank you very much for the trust you have placed in us.

Oneconsult AG

A handwritten signature in blue ink, appearing to read "Fabian Schewetofksi".

Fabian Schewetofksi
Security Consultant & Penetration Tester

Oneconsult AG

A handwritten signature in blue ink, appearing to read "Christoph Baumgartner".

Christoph Baumgartner
Chief Executive Officer