

Executive Summary

Realisator AG is proactively aware of the security risks and threats facing it in modern times. Best practices, together with a well designed and maintained network infrastructure focusing on security & safety ensure that the standards required are kept. Additionally, externally handled security auditing tasks are done on a regular basis. The security testing allows for potential and existing flaws in the environment to be detected early on and effective counter-measures implemented in a fast & timely manner. This reduces the time-frame for successful attacks to be limited to a minimum.

In addition, the physical security of the environment is limited to key personnel. Access to the server room with the sensitive hosts is restricted with a magnetic key. All devices, Internet and network connections are equipped with fail-over separation including offsite failover and uninterruptible power supply. The consequences of a hardware or software based malfunction has been reduced to a minimum.



Security auditing is a means to determine the potential and existing flaws in the current environment. Extensive testing with attack techniques were used to detect any issues. Targeted penetration tests were conducted in December 2010 indicating a high security level. Given the size of Realisator AG, the amount of customers and the potential risk of attacks, **the security environment of Realisator AG can be classified as “reaching excellent”**. The security level applied can be compared to the security level of a banking environment.

Questions & Answers

Are external attackers able to access, change or steal sensitive data?	
No, within the given security assessment no further access attempts to sensitive data was possible.	

Was the possible and desired level of security reached?	
Yes, the high level of security was maintained again. All of the involved parties did a good job.	

Which kind of security risks are remaining?	
The topic of social hacking (e.g. phishing) is still newsworthy. It remains important to make the users aware of the threats in the Internet of today.	

Which threats are we facing in general?	
Information technology heavily relies on progressing technologies. It is always important to get the best effort in usability and security at the same time.	



Zürich, 12/17/2010

Mr. Marc Ruef (Lead Auditor)