Whitepaper

HISSEN IT

About implementing security in IT projects properly – A Guideline

IT Security for Project Managers

Despite many accepted IT security standards, many IT projects fail at IT security. What needs to be considered, what mistakes and pitfalls to avoid.

IT Security in Projects and Products

By definition IT projects include the construction of a system of information technology. This may be the pure installation of existing solutions or the complete new development of custom components. A combination is also possible, such as when standard or open source software is enhanced by custom developed extensions. Whether at the end a product is created or an IT system which is otherwise used commercially, IT security plays a central role for the project's success. This also applies to systems in which IT plays only a secondary role for the whole product, such as the operator interface of a central heating device. Also, projects like building and hosting a standard web store are concerned with the subject of IT security to the same extent.

IT security is a matter for companies of all sizes. In most cases, big corporations have already implemented certain security standards, which enable IT projects to meet highest security requirements in a standardized way. By experience, smaller and medium-sized companies do not have that luxury. Mostly because tight budgets leave little room for security issues or the corresponding know-how is missing and cannot be procured easily.

Enforce IT Security in Projects

Most IT projects have a tight budget. Only in rare cases, a project manager has access to unlimited financial resources. This applies to projects of both large and small businesses alike but usually the smaller the company the bigger the problem.

If security cannot be used as a (unique) selling point for a product or for the development of a system, the project manager often has a hard job to acquire a proper and adequate budget for security issues. That is because:

- Security cannot be seen (superficially).
- Security does not make the system faster.
- Security does not make the system easier to use.
- Security complicates the processes involved in operating the system.

A provocative question could be: Why spend money on something that deteriorates the final product? To make matters worse, in most cases, the people involved in the project have little technical understanding for the topic of security or dangerous superficial knowledge. This is understandable. IT security is one of the most complicated topics at all. An expert in this field requires not only appropriate education and training but also years of practical experience in order to implement adequate security issues in a meaningful way.

The added value of IT security cannot be regarded in the short term. A microsite for a week-long campaign might remain completely unnoticed by hackers. Nevertheless, it would be negligent to exclude IT security explicitly in such a project. On the other hand, what happens if projects lack to address security? A successfully launched web service, for instance, is inevitably going to attract hackers after some time of success. It can lose reputation very quickly when vulnerabilities are disclosed. If security has been undervalued in the project, it can be very difficult to then fix leaks in a sustainable way. As a result, the