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

service could not only be in negative headlines for a while but a complete new development might become necessary. This might be the case because implementing a security concept in the existing system might not be possible at all.

Regarded medium and long term, products which take the security of their users and their data seriously will become successful and sustainable. Leaks are unavoidable – how to deal with these is crucial. Furthermore, minimum requirements for systems and products can be derived from various laws. If the corporate management fails to enforce these, it might slide in a case of legal negligence and legal liability for successful attacks by third parties. This should be reason enough for each project to deal with the issue of IT security seriously. The respective company management needs provide and ensure the corresponding foundation – in its own interest.

IT Security in Projects: From the very beginning!

The critical factor for the issue of security in IT projects is the moment in time. Too often, projects are considered from a business or functional point of view and are realized as a proof-of-concept, without even considering security issues. Prospects and financial forecasts are created. Then, when it comes to the implementation phase, security requirements and privacy requirements emerge – in whatever way. These can destroy the whole business idea, in the worst case. Usually, at least adjustments are needed that will affect the project plan and may be causing a disruptive factor in the project and its team. Depending on how far the proof-of-concept was planned to serve as the technical basis for the actual implementation, a complete redesign may be necessary due to the security and privacy requirements.

If you want to move these requirements to the next release after the go-live, the problems increase tremendously. Of course, this also lets the budget explode accordingly. A retiring project manager can thus also leave his successor a corresponding burden. As practice shows, any compromise in the realization will be unusable and ultimately expensive in the long run.

If there are already signed contracts with suppliers and other partners – for example, for custom developing or hosting services – before security requirements were considered, serious problems are caused for the overall project. All suppliers must be bound to the corresponding security requirements, standard contracts must be verified. Should it not be possible to adjust contracts, for example because contracts are being made with a larger company and/or a certain other dependency exists, then there has to be an own explicit risk management in place. Many web agencies, for instance, make tight price calculations to be competitive. Such agencies usually have to make separate calculations for special requirements of security catalogs. According plannings have to be adopted by the project early on.

A practical example: In an IT project, a web store should be built using standard software. It includes installation and hosting. Further changes to the web store software are not part of the project. The hosting should also include a patch management in addition to hardening the system. This must be provided for the entire life-cycle of the web shop and critical security updates of the shop software have to be applied in a timely manner. If this is not contractually agreed, additional costs will arise. Alternatively, the application owner – the owning company – must run an own process for this and must have correspondingly skilled personnel in charge.

From practical experience, it can be observe that even in companies with an established security organization, this organization is very often used much too late. Meetings of potential project teams, for example, should be accompanied by a security advisor – and by the way a data protection advisor. Thus, corresponding security and data privacy requirements can be recognized early on and no-gos can be avoided. Moreover, security advisors are usually able to discuss easier technical alternatives because of their project experience. The attendance by a security consultant may be advisable even for meetings without technical character or pure idea development.

When projects fail on IT security, then usually because of long-existing requirements which are unknown to the project team or not respected.

Security is a Process

IT security causes running costs. IT security needs permanent staff. The latter needs not necessarily to be full-time. Why is that so? – Security is a process! This applies to all types of IT projects. Here are some practical examples.

Example A

A custom developed web application is put into operation. During operation, security vulnerabilities are reported. There must exist a process to evaluate, check and fix these issues. If the software is custom-developed (in-house), this process needs to be established within the company itself. If software has been delivered by an external supplier, a corresponding contractual agreement must be installed accordingly. The interface between the internal and external processes must be defined, as well as corresponding service level agreements, such as the maximum processing time and the general cost absorption.

Example B

A standard application is hosted on the Internet. All systems have been hardened initially. Through the appearance of newly discovered vulnerabilities in standard software, a patch management process must be established. This includes among others the sighting of patches and the patch deployment. Critical security patches need to be spotted and installed promptly. Depending on the complexity of the application, a separate test system besides the actual production system is necessary to guarantee the proper functioning of the system after applying patches. Also, a regular penetration testing should be mandatory to ensure that no system component is omitted.

Example C

A system not only allows system administrators but also certain applicative roles access to customer data. Therefor, a proper logging of data access has been implemented. Even if an automatism is established which includes a fraud detection, a detection must be reported to a corresponding person to be examined and dealt with. For this, a proper process has to be created and documented. Additionally, regular audits have to be performed – also from the data privacy perspective.

Example D

For the hosting of certain systems, intrusion detection systems have been established. These allow the monitoring of unusual events in system behavior and potential attacks. From certain automatisms apart, it is necessary that suitable staff members monitor alerts and optionally initiate countermeasures.

In addition to these practical examples, for IT security the same is true as for all other things: One learns new things with every new project and, hence, own process will be adjusted accordingly.

IT Security Standards

If you want to set up an IT security process for a project or a whole company, you do not have to start from scratch and you should not. There are many accepted security standards which one can build on. This applies to smaller projects and smaller companies as well. Most large companies usually have a certified IT security process in place and hence project managers receive concrete technical and non-technical requirements for IT security as well as requirements coming from data protection laws. The project manager has to check whether industry-specific standards exist which have to be applied also.

If you do not want to make the "big step" of implementing a standard security process and developing an own security organization, a so-called "Information Security Management System" (ISMS), which is understandable especially for smaller companies – security standards still help: Either for your own software development or dealing with suppliers and partners.

An advantage of the relevant security standards is that they can be used in contracts for reference. This guarantees at least some minimum level of security. If the companies participating in the project are certified according to established security standards, the application of these standards should be integrated into the corresponding contract.

A brief overview of some selected security standards without any claim to completeness:

- ISO/IEC 27001: Probably the most widely used international standard for enterprise-wide information security organizations. The concrete implementation is company- and industry-specific.
- BSI IT-Grundschutz ("IT Baseline Protection"): A concrete implementation catalog issued by the German Federal Office for Information Security (BSI) for ISO/IEC 27001. The IT Baseline Protection also includes a publicly available catalog of concrete technical security requirements on a specification level for various software and hardware components.
- Common Criteria for Information Technology Security Evaluation: An international standard that allows the testing and certification of security requirements in concrete products. This certification process is usually very extensive and costly.
- PCI-DSS and PCI-PA-DSS: This is the credit card industries' standard to be met by companies that use credit card information. This is also publicly available and can be applied to other data as well and thus used in own projects due to the very strong requirements included. The security catalogs contain concrete technical and organizational implementation measures. The standard PA-DSS is specifically for custom-developed products that process credit card information.
- OWASP Top Ten Project: The Open Web Application Security Project (OWASP) is a nonprofit organization which publishes security policies (and more) for free use. In particular, the so-called "Top Ten Project" can be used as a reference for minimum requirements for secure web applications.

Do the same for Data Privacy Laws!

This white paper primarily relates to IT security. However, most problems illustrated equally apply to privacy and data protection requirements. Requirements derived from laws and data regulations also need to be carried out within IT projects as early as possible. They need to be supported and implemented. Because of non-negotiable legal regulations, missing contractual agreements can become self-inflicted "project killers". Like for IT security, an appropriate specialist is also required for data protection – ideally with experience on the technical side. For the technical implementation of these requirements, again, an IT security specialist can be consulted.

Checklist for Project Managers

The following checklist is intended to serve IT project managers as a guide to implement the often overlooked topics of IT security within IT projects. The list is not exhaustive. IT projects differ greatly in their requirements. Should enterprise-wide requirements exist then these are, of course, to be considered in the first place. For international projects, country-specific requirements, in particular coming from data protection laws, have to be considered as well.

Levels of IT Security

Security requirements are defined in various technical levels of a project. Because IT projects differ strongly, the following list is intended only as an aid to pick up according security issues in a project early on. The requirements can be only partially meaningful or not at all for a certain project. A complete security concept, however, should at least consider all of these levels.

Technical levels:

Similar to the OSI model, the various technical levels have to be investigated if applicable for a project.

- Network layer: This includes the network concept (for example, the appropriate segmentation) and all network components such as switches, routers, network firewalls, VLAN settings, and wireless access points. Advanced components could be intrusion detection or intrusion prevention systems (IDS/IPS).
- Virtualization level: Should virtualized components being used, the virtualization management software must be configured and hardened properly. It must also be verified whether an adequate level of security for the project can even be achieved using virtualization. For instance, in some projects virtualized firewalls might be out of question.
- Operating system level and application level: In addition to the actual applications, this also includes used libraries, extensions, runtimes, server components (for example, web server) and middleware components. Operating on up-to-date and secure software must be ensured but also the secure configuration of all components (for example, web server configuration). The general term for this is system hardening. Also included in this category are enhanced security components such as application-level firewalls.

Other topics that must be covered within the project for each technical level:

- Roles and Permissions
- Monitoring and logging (e.g., system behavior, login and access patterns)
- Authentication methods for an adequate level of security (for example, password authentication, two-factor authentication)
- Encryption concept: It is necessary to clarify whether an encryption concept is required for an adequate level of security, for example through the use of database, file, disk, or e-mail encryption solutions.
- Operational safety and reliability
- Access protection and entry control for physical access to IT systems

In-House Development (Secure Programming)

- Custom-developments, whether these take place in-house or are being outsourced, require additional measures to ensure the secure programming of all custom software. One should rely on the security standards mentioned previously. The requirements that arise here are highly dependent on the respective development context and the chosen programming environment. For instance, the security requirements for Windows applications, mobile apps, web applications

or ABAP applications for SAP differ significantly in comparison. Even with mobile apps alone different security concepts arise from the various mobile operating systems (for example, iOS, Android or Windows).

- It has also to be verified if industry-specific security requirements exist, such as PCI PA-DSS for credit card applications. For web-based applications, the general standards of the aforementioned OWASP can be used.

Project Idea and Project Development

- After the establishment of the project or product idea, first drafts are discussed with IT security specialists and privacy specialists.
- Requirements and comments of the specialists are included in the project documentation and are presented to the project team. Resulting questions and modified implementation ideas are optionally re-discussed with the specialists.

Project Kick-Off

- To the project kick-off, all project participants are invited including the security and data protection specialists. Ideally, the specialists serve the project team as a direct or at least indirect contact for the entire project.

Creating the Security Concept

- If you are part of a large company with an established IT security process, you will already know the security requirements for your IT project. Usually, these must be compiled for each IT project individually: A suitable, custom catalog of requirements – since different IT projects differ strongly in nature and content. Requirements do not apply for all projects. Also, projects can have new requirements to satisfy, including legal requirements, because of their subject matter.
- In case you do not have security requirements given, you need to create a requirement catalog on your own or with external aid. It is advisable to separate the role of the security specialists from an executive role. It makes no sense, for example, to have a web agency control their own, self-defined security requirements. This is only meaningful for the agency's internal processes, but not for you as a buyer of a service. Please note that usually, an independent, external security specialist will have the smallest percentage of your total project budget. If you define the catalog of security requirements on your own, you can refer to one of the aforementioned established security standards or relate to them. Depending on the project scope, it might be useful to use a particular subset only. Alternatively, you can also search for other established security standards published in your industry or branch.
- A smaller company, for example, that purchases a web shop from a web agency, should include the aforementioned "OWASP Top Ten" as a minimum requirement set in its contract. Moreover, questions about the security of the web hosting have to be fulfilled: Is the agency hosting itself or is it using an established 3rd party service? Who implements the patch management (OS level, application level)?

External Suppliers

- If external service providers are involved, for example, for hosting, design, installation, software development or supplying standard software, they will also being contractually committed to IT security. Contracts have to include certain specific minimum requirements. It has to be taken into account how vulnerabilities are processed that occur after launching – maybe causing additional costs. A corresponding bug fixing has to be established. If external components miss the security requirements at delivery, the bug fixing should take place with no costs.

Technical Acceptance Tests

- Whether custom-developed or delivered by external service providers, each project has to be technically accepted and approved. In addition to the pure functional acceptance, the technical IT security acceptance is a must in every IT project. For this purpose, at least a random sample of version statuses has to be taken to identify, for example, outdated software and therefrom trying to assess the basic quality of the delivered service. Ideally, an acceptance test would include a full penetration test prior to the purchase. This can be done not only for web-based applications, but in a modified form also for desktop applications, mobile apps and other services such as mail servers.
- The acceptance test always refers to the previously agreed security requirements. What has not been agreed on, either cannot be claimed or creates additional costs.

Ongoing Security Processes

The following list is intended to serve as a broad overview of the permanent security processes in the operational area of IT systems:

- Patch management: All used components of the overall system must be monitored regarding their patch levels and must be updated when security implications arise. These components include but are not limited to: firewalls, operating systems, middleware components, web servers, application server runtimes, applications in general.
- Regular penetration testing: Due to changing threats and new attacks, a regular penetration testing should be part of the operation process. The frequency of the pentests depends on the project, recommended in general however is at least once a year. It is advisable to switch the penetration tester at certain intervals to avoid monotonous test behavior. For retests, it is of course time and cost efficient to use the same penetration tester.
- Monitoring of security-related queries: Operative accesses like administrative actions and logs of security components such as intrusion detection systems, application-level firewalls or the like must be spotted regularly. Security-critical events must be sent to appropriate personnel and processed by those.
- Monitoring of applicative queries against abuse: Data access, such as to customer data, by employees must be auditable, but also concrete suspicious cases have to be detected in a timely manner. Therefore, implemented access controls at the application level must be checked in a meaningful process suitable for the project.

Operational Reliability

- If you require special measures of reliability (failure safety) and high availability, you will usually need another specialist in the administrative area. At least, it should be defined in the project what the maximum tolerable downtimes for IT systems are. If third parties are responsible for such cases, they must be bound by contract to the corresponding recovery processes and service level agreements.
- Another key issue is backup & restore. This particularly includes but is not limited to all changing (user) data from databases, NAS and other storage locations. Even if it is complex, the correct functioning of a backup can only be verified by a restoration attempt on a non-installed system. This is the only way to make sure if one is prepared for a worst case scenario. While you might not want to regularly perform this process, it should be performed at least once prior to the project's go-live.

Conclusion

IT security is a complex undertaking. Even experienced project managers cannot fulfill this topic alone and

require professional support. In small businesses, the budget shortage can require to handle the issue of security without external help. Here, security standards can help to control suppliers and partners accordingly. Therefor, the aforementioned key issues have to be considered. However, in general, it is crucial to define adequate project-specific requirements.

IT projects of all sizes must respect the principle of integrating IT security and data protection requirements in the very early stages of the project. Omissions in this area can lead to project shipwrecks or at least lead to high follow-up costs.