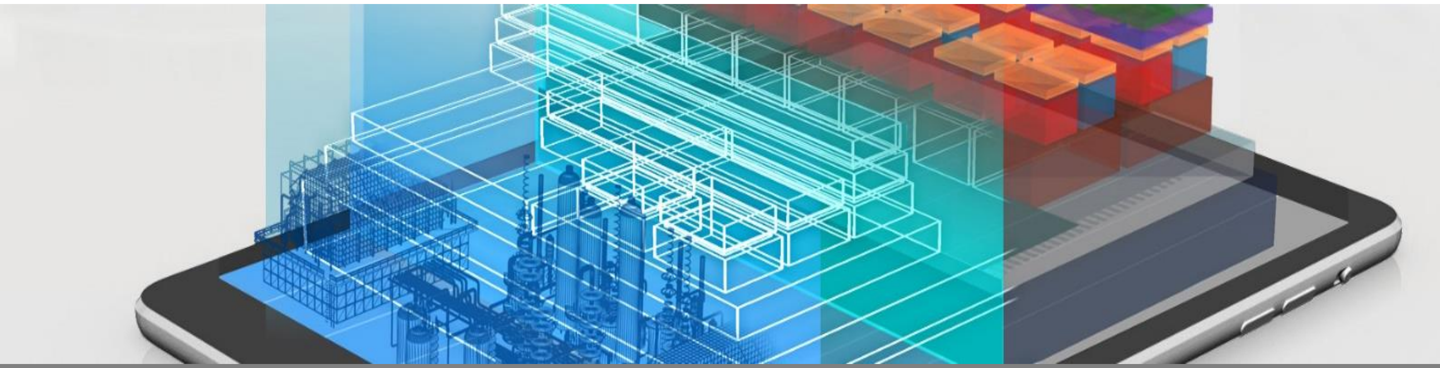
mgm

CASE STUDY



Scalable Security Support in a Highly Agile and Distributed Software Project

This case study describes the introduction of a scalable and flexible security approach into a highly agile insurance project with low security budget. The early integration enabled a security-by-design approach which was easily adapted as the project grew. With the introduction of a Security Representaitve the project was additionally enabled to make security decisions on their own, allowing for overall security despite the tight budget.

Initial Situation

For a large insurance provider, a portal was to be implemented that enhances document creation for brokers and replaces a legacy paper process. Initially, a small project team with an agile development approach was chosen for this task.

Goals & Requirements

Right from the start, the project was designed to add security to the development process. However, since the initial project setup was small and the budget was not as flexible, an 8h/week contract for security support was negotiated.

We depict in the following how we used our lean security approach for an efficient and flexible security support against the background of a limited time scale.

Approach

Despite the tight budget constraints, our goal was to integrate security as comprehensively as possible into the development process. This intention was further highlighted by the project's high agility and great flexibility in the face of frequently changing requirements.

Why mgm security partners?

The described case study depicts an instance of our overall achievement: With our lean-security-by-design approach, we contribute to the goal to go live on time with all intended security features at calculable cost.

Contact

Maximiliane Zirm

089/358680-834
Maximiliane.Zirm@mgm-sp.com

The approach we took was based on the lean security concept, where a security specialist works together with a so-called "security representative in project" or “security champion”. This role is taken up by a regular team member and enables them to take the necessary security actions without deep involvement of the specialist. In this project, the security representative role was given to the technical project manager.

To help with the authorisation of the security representative and to simplify tracking of the ticket's security relevance, a field was added to the project’s ticketing system, categorizing the security requirements of a ticket from none to high. In a dedicated weekly call between the specialist and the representative, the tickets were rated and appropriate measures were discussed (ranging from "has to pass a code review" of high-tickets to declaring features as "not security relevant")

Also, since the project was using SCRUM, the participation of the security specialist in selected regular meetings (like grooming and planning) helped to bring security awareness to the whole team and clarify any open questions.

Scalability

In the course of the project, the team grew from 6 to over 20 members and from 2 to 4 different locations. Also, instead of one portal, numerous instances for different use cases were developed. This change also affected the established security process. Here, the flexibility of the lean security approach paid off.

The process of individual ticket rating had to be adapted as the load of tickets became too much to handle. Instead, a “shift left” was performed. Rating now took place not on ticket level but on requirement level, together with the business analysts in a dedicated meeting.

Moreover, testing all new features in all new portals manually was not feasible anymore. Instead, automated approaches for certain use cases were installed – especially in the area of access control, where requirements and implementations changed constantly.

The early implementation of a security process and enablement of the whole team and the representative in particular made those changes possible and helped divide the security workload efficiently without having to increase the budget.

Lessons learned

Among the lessons learned from this project we would like to point out the following:

- Early implementation of a security process helps setting the basis for later changes in the project
- Enablement of security representatives helps taking away responsibility of the security specialist and makes scalability of security processes easier for the whole team
- The excellent results of the external penetration test as well as the satisfaction of the customer showed, that the flexible lean security approach can lead to a highly successful result even with the restrictions of a low security budget.