case study

Security and Usability Hand in Hand
Security Audit and Usability Test at Bayerische Versorgungskammer

Reconciling security and usability is often a challenge for online application providers – especially when it comes to protecting highly sensitive, personal data such as insurance details. Facing this challenge, the German pension provider Bayerische Versorgungskammer decided to implement an appropriately secure but also complex access procedure, confronting a number of users with difficulties. However, there is often potential for usability improvement, even in high-protection environments. Combining a security audit with a usability test, plan42 developed concrete optimization strategies.

BAYERISCHE VERSORGUNGSKAMMER

plan42 gmbh

The Client

Germany's largest public pension provider group, Bayerische Versorgungskammer (BVK), is a service and competence centre for profession-based pension providers. BVK manages twelve different providers including Bayerische Ärzteversorgung (BÄV), which is responsible for physicians, dentists, and veterinarians in Germany. BÄV runs the web portal BÄV24, enabling its over 80,000 insurants to view and modify their data online.

The Challenge

Considering the high protection requirements of the data stored in the web portal as well as applicable privacy regulations, BÄV chose a registration and login procedure that provides the required level of security, but at the same time is rather complex in technical terms. As a result, the new method exceeds the computer and internet skills of many users, as a number of incoming requests and complaint revealed: „Some BÄV insurants worried about insufficient security of web portals in general, but many users also thought that our registration and authentication procedures were too complex or that exaggerated security controls were implemented. Others even questioned the need to protect their own personal data", explains Eckhard Reichelt, IT Security Manager at BVK.

„Considering the amount and content of incoming complaints and requests from about 10% of our portal users, we concluded that some of the problems might be caused by insufficient registration usability, an assumption substantiated by a relatively large number of people who made use of our service hotline."

The number of incomplete registrations also supports this assumption: Although the number of new registered users not successfully logging into the portal has constantly decreased, this ratio was as high as 40% at the beginning of the audit.

To tackle the problem, BÄV decided to commission an external audit in order to receive answers to the key questions: Is the implemented security concept appropriate with regard to the protection requirements, and is it implemented correctly? Which procedures lack usability? And how can support procedures be optimised?

The declared objective was to improve user experience – but not at the expense of security.
According to Mr. Reichelt, the decision to hire an external company was mainly driven by the idea of an independent, neutral, and unbiased examination. plan42 was commissioned following a tendering procedure.

The Procedure

“A normal security audit would not have been sufficient for this task“, explains Marc Heinzmann, ISO 27001 auditor at plan42. “This is why it was combined with a usability test.”

At the beginning of the project, the security concept and its implementation were examined in detail. For that purpose, the plan42 auditors reviewed all relevant documents against formal requirements defined by the German Federal Office for Information Security (BSI) as well as against best-practice guidelines. This procedure allowed the auditors to systematically disclose gaps in the concept and deficiencies of implemented controls.

On-site interviews allowed the security experts to gain insight into the views of affected employees. Answers from representatives of various departments including user service, security management and public relations showed the individual perspectives on the situation.

Key element of the examination was a web portal test from the users’ perspective. By means of test accounts, the auditors completed registration and login procedures step by step, which enabled them to identify usability deficiencies that could be eliminated without compromising security.

The Result

As the audit quickly revealed, there is only little room for improving the security concept and its implementation: „Security concept deviations from the BSI testing scheme would mainly play a role in an ISO 27001 certification procedure. They hardly affect the security level and usability“, states Mr. Heinzmann.

Similarly, he sees little possibilities to optimise the access method: „In my opinion, there is currently no cost-effective alternative providing the same level of security“.

However, the web portal test revealed a considerable need for optimising user guidance and help documents. The deficits are mainly related to the structure, comprehensibility, and completeness of the information, which additionally complicates the procedures for the users. The reverse conclusion is: Help documentation suitable for the target group could compensate many usability deficits – without impairing security.

In addition, organisational changes could enhance user experience as well: An improved information flow between the departments would help providing optimal support to users who report problems or have questions.

For all findings identified during the examination, the auditors developed suggestions to eliminate the issues as well as prioritisation recommendations. At the end of the project, Mr. Reichelt draws a positive conclusion:

“On the one hand, the findings from the audit confirmed various causes we had already suspected. On the other hand, however, the audit revealed a number of other, previously undetected issues. The implementation of initial measures has already caused user acceptance to increase.

This audit is not only valuable for the direct improvement of current portal processes, but also for the design of additional portals. Although it would have been possible to conduct such an examination internally, existing knowledge from the development phase of our pilot portal BAEV24 and the potential bias resulting from it would have made a neutral examination much more challenging.“

So, the view from the outside was worth it and has shown that security and usability are not necessarily mutually exclusive – provided that the overall concept is tailored to the end user.

plan42

plan42 is a consulting firm specialised on IT service & security management and open source business solutions. Process analysis, consulting, conception, and implementation – plan42 combines technical expertise and best-practice concepts of IT service & security management.

+49 89 307657-16 info@plan42.com www.plan42.com