

# Case Study

## Security & 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, 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 security consultants developed detailed optimisation strategies.



### The Client

The largest public pension provider group in Germany, *Bayerische Versorgungskammer* (BVK), is a service and competence centre for various profession-based and municipal pension providers. BVK manages twelve different providers including *Bayerische Ärzteversorgung* (BÄV), which is responsible for physicians, dentists, and veterinarians, mostly in Bavaria but also in other parts of Germany.

BÄV runs the web portal *BÄV24*, enabling its over 80,000 insureds to access and, if required, modify their data online.

### The Challenge

Considering the high protection requirements of the data stored in the web portal as well as various applicable privacy regulations, BÄV decided to implement a registration and login procedure that provides the required level of security; however its utilisation is rather complex in technical terms. As a result, the new method exceeds the computer and internet skills of many potential portal users, as a number of incoming requests and complaints revealed:

„Some BÄV insureds worried about insufficient security on web portals in general. However, many users also found that our registration and authentication procedures were too complex or that the implemented security controls were over the top. Others even completely 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 as well as the fact that we received support requests from about 10% of our portal users, we concluded that some of the problems might be caused by insufficient registration usability. This was an assumption that was substantiated by a relatively large number of people who made use of our service hotline.“

The number of incomplete registration procedures also supports Mr. Reichelt's conclusion: Although the number of new registrations that did not result in successful access to the BÄV24 web portal has been constantly decreasing, this ratio was still as high as 40% when the audit project was started.

To tackle this issue, 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?
- Is it implemented correctly?
- Which procedures lack usability?
- And how can support procedures be optimised?

The declared objective of this project was to improve user experience – but not at the expense of security.

According to Mr. Reichelt, the decision to hire an external security consulting company was mainly driven by the idea of conducting an independent, neutral, and unbiased examination of the web portal. The IT business consulting company plan42 was commissioned following a tendering procedure.

## The Methodology

“A normal security audit would not have been sufficient for this kind of 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 and checked them 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 not only gaps in the concept but also deficiencies of implemented security controls.

On-site interviews allowed the security experts to gain insight into the views of affected BÄV 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 only little room for optimising the authentication 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 for 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.

The results were summarised in a final report: for all findings identified during the examination, the auditors included detailed suggestions to eliminate the issues as well as recommendations regarding the prioritisation of required action.

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 controls has already caused user acceptance to increase.

This audit is not only valuable for the direct improvement of current web portal processes, but also for the design of additional portals in the future. 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 Management, IT Security Management & Business Solutions. Process analysis, consulting, conception, and implementation – plan42 combines technical expertise and best-practice concepts of IT Service & Security Management.