case study

Sicherheit & Benutzerfreundlichkeit Hand in Hand
Security Audit und Usability Test bei der Bayerischen Versorgungskammer

Sicherheit und Usability in Einklang zu bringen stellt viele Betreiber von Online-Applikationen vor Herausforderungen – insbesondere, wenn es um den Schutz hochsensibler, personenbezogener Daten wie Versicherungsdaten geht: So entschied sich die Bayerische Versorgungskammer bei ihrem Online-Portal für ein entsprechend sicheres, aber auch komplexes Zugangsverfahren, das viele Anwender vor Probleme stellte. Doch auch bei hohem Schutzbedarf lässt sich die Benutzerfreundlichkeit häufig optimieren. Mit einer Kombination aus Security Audit und Usability Test zeigte plan42 konkrete Strategien auf.

BAYERISCHE VERSORGUNGSKAMMER

plan42 gmbh

Der Kunde

Als größte öffentlich-rechtliche Versorgungsgruppe in Deutschland ist die *Bayerische Versorgungskammer* (BVK) Dienstleistungs- und Kompetenzzentrum für berufsständische und kommunale Altersversorgung. Die BVK führt die Geschäfte von zwölf verschiedenen Vorsorgeeinrichtungen, darunter die der *Bayerischen Ärzteversorgung* (BÄV). Diese ist für Ärzte, Zahnärzte und Tierärzte in Bayern, teilweise auch in Rheinland-Pfalz und im Saarland, zuständig. Für ihre über 80.000 Mitglieder betreibt die BÄV das Online-Portal *BÄV24*, über das die Versicherten ihre Daten einsehen und bei Bedarf bearbeiten können.

Die Herausforderung

Um dem hohen Schutzbedarf der Daten im Online-Portal und den Anforderungen des Bundesdatenschutzgesetzes (BDSG) Rechnung zu tragen, wählte die BÄV ein entsprechend sicheres, aber auch technisch komplexes Verfahren für Registrierung und Anmeldung.

Allerdings übersteigt die gewählte Methode die Computer- und Internetkenntnisse vieler Mitglieder, wie die Anfragen und Beschwerden einiger Versicherten zeigten:

"Einige der Beschwerden hatten die Sorge um mangelnde Sicherheit von Internet-Portalen generell zum Inhalt. Viele Anwender formulierten aber auch ihre Bedenken zu der aus ihrer Sicht zu komplexen Registrierung bzw. Authentifizierung, der übertriebenen Sicherheit des Internet-Portals oder sogar der Schutzwürdigkeit ihrer eigenen personenbezogenen Daten“, so Eckhard Reichelt, IT-Sicherheitsbeauftragter der BVK. „Anzahl und Inhalt der eingehenden Beschwerden und Anfragen von ca. 10 % der Portal-Anwender ließen vermuten, dass einige der Probleme durch mangelnde Usability vor allem in den Prozessen der Erstregistrierung liegen könnten. Diese Vermutung wurde auch durch die entsprechend starke Inanspruchnahme der Hilfe an der Service-Hotline untermauert."

Auch die Anzahl nicht abgeschlossener Registrierungen bestätigt diese Vermutung: Der Anteil an Erstregistrierungen, die nicht zu einer erfolgreichen Anmeldung im Portal führen, sinkt zwar stetig, war aber mit kapp 40 % zu Beginn des Audits noch relativ hoch.

Zur Lösung des Problems entschieden sich die Betreiber für ein externes Audit, das Antworten auf die Kernfragen liefern sollte: Ist das gewählte Sicherheitskonzept dem Schutzbedarf angemessen und richtig umgesetzt?

Wo liegen die konkreten Defizite in Sachen Usability? Und wie lassen sich die Abläufe im Support optimieren? Erklärtes Ziel war es, den Anwenderkomfort zu verbessern – jedoch keinesfalls auf Kosten der Sicherheit.
Die Entscheidung für eine Untersuchung durch ein externes Unternehmen basierte laut Eckhard Reichelt vor allem auf dem Wunsch nach einer unabhängigen, neutralen und nicht vorbelasteten Betrachtung. plan42 erhielt den Auftrag nach einer Ausschreibung.

Das Vorgehen

„Bei dieser Aufgabenstellung hätte ein klassisches Security Audit zu kurz gegriffen“, so Marc Heinzmann, ISO-27001-Auditor von plan42. „Daher wurde es um einen Usability Test erweitert.“
Zu Beginn des Projekts stand eine eingehende Untersuchung des Sicherheitskonzepts und dessen Umsetzung. Dazu prüften die Auditoren von plan42 alle relevanten Dokumente anhand formaler Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie Best-Practice-Regeln. Lücken des Konzepts und Schwächen implementierter Maßnahmen ließen sich so systematisch aufdecken.
Vor-Ort-Interviews verschafften den Fachleuten einen Einblick in die Sichtweise der betroffenen Mitarbeiter. Durch die Befragung von Vertretern aus verschiedensten Fachbereichen, darunter Benutzer-Service, Sicherheitsmanagement und Öffentlichkeitsarbeit, war es möglich, die Situation aus verschiedenen Perspektiven zu beleuchten.
Kernstück der Untersuchung war ein Test des Online-Portals aus Sicht des Endanwenders. Mit Hilfe von Testkonten vollzogen die Auditoren den Registrierungs- und Anmeldevorgang Schritt für Schritt nach und konnten so Usability-Defizite identifizieren, die sich auch ohne Abstriche bei der Sicherheit beheben lassen.

Das Ergebnis

Die Prüfung ergab schnell, dass bei Sicherheitskonzept und Implementierung nur eingeschränkt Verbesserungspotential besteht: „Die Abweichungen im Sicherheitskonzept vom BSI-Prüfschema für ISO-27001-Audits würden in erster Linie bei einer ISO-27001-Zertifizierung auf Basis von IT-Grundschutz eine Rolle spielen. Für das Sicherheitsniveau und die Benutzerfreundlichkeit sind sie kaum relevant“, stellt Marc Heinzmann fest. Auch beim Zugangsverfahren sieht er wenig Spielraum: „Aus meiner Sicht gibt es hier derzeit keine kostengünstigere Alternative, die gleichwertigen Schutz bietet.“
Allerdings zeigte sich im Test des Online-Portals ein deutlicher Optimierungsbedarf bei Benutzerführung und Hilfsdokumenten. Hier gibt es insbesondere Defizite bei Struktur, Verständlichkeit und Vollständigkeit der Informationen, was die Abläufe für den Anwender zusätzlich erschwert. Im Umkehrschluss bedeutet dies: Mit zielgruppengerechter Benutzerhilfe ließen sich Usability-Schwachstellen in weiten Teilen ausgleichen – und zwar ohne Beeinträchtigung der Sicherheit.
Auch in Sachen Organisation lässt sich der Anwenderkomfort steigern: So kann ein verbesserter Informationsfluss zwischen den Abteilungen dazu beitragen, Versicherten bei Problemen und Anfragen optimale Unterstützung zu bieten.

Zu allen gefundenen Defiziten wurden Lösungsvorschläge und Priorisierungsempfehlungen erarbeitet und diese der BÄV nach Abschluss des Projekts präsentiert.
Eckhard Reichelt zieht ein positives Fazit: „Die im Audit formulierten Feststellungen bestätigten einerseits viele der bereits vermuteten Ursachen, zeigten allerdings auch noch einige weitere, bis dahin noch nicht erkannte Problemstellungen auf. Nachdem erste Maßnahmen umgesetzt wurden, zeigt sich bereits eine Verbesserung in der Akzeptanz der Anwender.
Der Mehrwert dieses Audits besteht einerseits in der direkten Verbesserung der aktuellen Portal-Prozesse und andererseits in einer gestiegenen Sicherheit des Vorgehens bei der Entwicklung weiterer Portale. Eine derartige Überprüfung hätte zwar auch intern durchgeführt werden können, durch Vorkenntnisse aus der Entwicklungsphase des Pilot-Portals BÄV24 und daraus möglicher Vorbelegungen wäre eine neutrale Betrachtung jedoch deutlich schwieriger umsetzbar gewesen.“

Der Blick von außen hat sich also gelohnt und gezeigt, dass sich Sicherheit und Benutzerfreundlichkeit nicht zwangsläufig ausschließen – sofern das Gesamtkonzept auf den Endnutzer abgestimmt ist.

plan42

plan42 ist ein Beratungsunternehmen, das sich auf die Bereiche IT Service & Security Management sowie Open Source Business Solutions spezialisiert hat. Von der Prozessanalyse über die Beratung und Konzeption bis hin zur Realisierung – plan42 verbindet technische Expertise mit praxisbewährten Konzepten aus den Bereichen IT Service & Security Management.

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