INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Bachelorarbeit

Evaluation von Open-Source-Werkzeugen zum Management von Sicherheitsdokumenten

Zoya Bosh

INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Bachelorarbeit

Evaluation von Open-Source-Werkzeugen zum Management von Sicherheitsdokumenten

Zoya Bosh

Aufgabensteller:	Priv. Doz. Dr. Wolfgang Hommel
Betreuer:	Felix von Eye Stefan Metzger
Abgabetermin:	09. Mai 2014

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 09. Mai 2014

. . . . . .
(Unterschrift des Kandidaten)

Abstract

Die Erstellung und Aktualisierung der Informationssicherheitsdokumentation ist ein wesentlicher Bestandteil des Informationssicherheitsprozesses. Am Leibniz-Rechenzentrum (LRZ) erstellt man Sicherheitsdokumente für die einzelnen IT-Dienste, dienstspezifische Sicherheitskonzepte genannt. Sie fassen die Information über die dienstspezifischen Sicherheitseigenschaften und implementierten technischen Sicherheitsmaßnahmen zusammen. Um diesen Dokumenten eine einheitliche Struktur zu geben, wurde eine Dokumentvorlage entworfen, die als Muster für die Erstellung dienstspezifischer Sicherheitskonzepte dient. Jedoch benötigt man eine Automatisierung des gesamten Erstellungs-, Freigabe- und Kontrollprozesses. Diese Arbeit beschäftigt sich mit der Konzeptentwicklung für die Verwaltung von Sicherheitskonzepten am Leibniz-Rechenzentrum bzw. mit der Ermittlung der Anforderungen an das benötige Verwaltungssystem. Im Rahmen einer Evaluation müssen die bereits auf dem Markt vorhandenen Softwareprodukte anhand des in der Konzeptentwicklungsphase erstellten Anforderungskatalogs untersucht werden. Außerdem soll eine Entscheidung getroffen werden, ob eine Softwarelösung für die Verwaltung von Sicherheitsdokumenten am LRZ geeignet ist. Bei einem positiven Ergebnis der Marktuntersuchung muss zum Schluss der Arbeit ein Prototyp eines Teils der Sicherheitskonzept-Vorlage auf Basis des ausgewählten Tools implementiert werden.

Inhaltsverzeichnis

1 Einleitung

Vom Leibniz-Rechenzentrum (LRZ) wird ein breites Spektrum von IT-Dienstleistungen für Forschung und Lehre an den Hochschulen in München und Bayern angeboten. Dazu zählen E-Mail, Wireless Local Area Network (WLAN), Virtuelles Privates Netz (VPN), Internet und noch viele andere [Bod13]. Insgesamt sind am LRZ ca. 80 Dienste in Betrieb. Eine wesentliche Aufgabe eines Hochschulrechenzentrums ist die Gewährleistung der IT-Sicherheit. In den letzten Jahren sind Rechenzentren zunehmend Opfer von Angreifern geworden. Laut dem jährlichen "Worldwide Infrastructure Security Report" von Arbor Networks im 2013 sind DDoS-Angriffe auf Infrastruktur und Service von Rechnerzentren dramatisch angestiegen [wis14]. Am LRZ beschäftigt man sich viel mit dem Thema IT-Sicherheit und es werden ständig Sicherheitsrichtlinien gemäß den aktuellen Standards weiterentwickelt.
In diesem Kapitel werden erst die Ist-Situation am LRZ und die Problemstellung erläutert. Danach wird die Art des zu einwickelnden System ermittelt. Das Kapitel schließt mit einem Überblick über den Arbeitsaufbau.

1.1 Motivation

Für jeden Dienst am LRZ muss ein Dokument geführt werden, das sich mit den jeweiligen Sicherheitsaspekten befasst. Dieses Dokument wird am LRZ Sicherheitkonzept (SK) genannt und muss spätestens beim Aufbau eines neuen Dienstes oder bei größeren Änderungen an einem bestehenden Dienst aktualisiert werden. Um die Dokumentation von Sicherheitsprozessen heterogener Dienste besser strukturieren und verwalten zu können, wurde am LRZ eine Sicherheitskonzept-Vorlage (SK-Vorlage) entworfen. Sie sollte als die Grundlage zur Erstellung der dienstspezifischen Sicherheitskonzepte dienen. Das Ziel der Ausarbeitung eines generalisierten vorlagebasierten Ansatzes liegt daran, die schriftliche Arbeit für Dienst-Administratoren zu minimieren und eine einheitliche Struktur des Dokumentes zu erhalten, was eine spätere Auswertung effizienter macht. Zurzeit existiert eine Sicherheitskonzept-Vorlage im PDF-Format und auf ihrer Basis werden Sicherheitskonzepte mit Hilfe eines Texteditors erfasst und danach als PDF-Dateien oder als Papierdokument in einem Ordner abgelegt.

Die Struktur des Dokumentes ist ein Fragebogen, der aus einem Titelblatt und aus drei Kapiteln, die jeweils in Abschnitte unterteilt sind, besteht. Das Titelblatt enthält die Daten, die sich auf das gesamte Dokument beziehen. Das sind der Dienstname des Sicherheitskonzeptes, Angaben zu Autor, Versionsnummer, Bearbeitungsdatum und weitere Metadaten. Das erste Kapitel gibt einen Überblick über den Dienst und seine Eigenschaften: die Umgebung, in der er am LRZ umgesetzt wird, die Zusammenhänge mit anderen Diensten und seine Schwachstellen im IT-Sicherheitskontext. Im zweiten Kapitel sollen die dienstspezifisch eingesetzten Sicherheitsmaßnahmen zusammengefasst werden. Das dritte Kapitel hält ergänzende Informationen fest, die Schnittstellen zu anderen Prozessen darstellen und die

vor allem für das LRZ-Security-Team relevant sind.
Die genauere Gestaltung der Dokumentvorlage ist folgendermaßen aufgebaut:

1. Überblick über den Dienst
   a) Ansprechpartner
   b) Eingesetzte Hardware / Server
   c) Eingesetzte Software
   d) Klassifikation der verarbeiteten Daten
   e) Dienstabhängigkeiten
   f) Kritikalität des Dienstes
   g) Dienstspezifische Risiken
2. Beschreibung der eingesetzten Sicherheitsmaßnahmen
   a) Betriebssystem- und Software-Updates
   b) Dedizierte Sicherheitssoftwares
   c) Zugriff für Administratoren und Benutzer
   d) Datenschutz und Datensicherheit
3. Schnittstellen
   a) Relevante Dokumentation
   b) Anmerkungen für das LRZ-CSIRT[1]
   c) Geplante Änderungen und Erweiterungen
   d) Das Sicherheitskonzept und seine Realisierung

Der Entwicklungsprozess der Vorlage und ihre Beschreibung ist in Artikel "Security Knowledge Management auf Basis einer Dokumentenvorlage für Sicherheitskonzepte" [Hom14] detailliert beschrieben

Die Vorlage ist so ausgearbeitet, dass man nicht viel Zeit mit langen Beschreibungen verbringen muss. Stattdessen kann man die Antwort aus bereits verfügbaren Antwortvarianten auswählen oder einen kurzen Eintrag machen. Das erspart den Dienstadministratoren zeitlichen Aufwand. Daneben können die vorgeschlagenen Antwortalternativen eine gute Hilfe für die schnelle Antwortentscheidung sein, weil nicht immer sofort notwendige Informationen verfügbar sind.

Neben den Vorteilen dieser Lösung existieren jedoch auch Schwachstellen bei ihrer praktischen Umsetzung, die im Folgenden erläutet werden.

Vor allem entsteht eine zahlreiche Menge von Dokumenten, die abzulegen und weiter zu verwalten sind. Es gibt keinen bestimmten Ablageort für die erstellten Sicherheitskonzepte. Das führt zu Unübersichtlichkeit, erschwert die Auswertung der Daten und macht das Sammeln für eine Statistik kaum realisierbar.

[1] CSIRT steht für Computer Secutity Incident Response Team

Da je nach Dienst seine Schwachstellen und Nutzungsbedingungen variieren und weitere Anforderungen an Sicherheitsmaßnahmen folgen, muss ein dienstspezifisches Sicherheitskonzept um bestimmte Abschnitte erweitert oder reduziert werden. Man kann nicht die Tatsache ignorieren, dass in Zukunft eine Dokumentvorlage auf eine große Menge von Abschnitten erweitert werden kann und aus einer endlosen Liste von Fragen besteht. Für Dienstadministratoren bedeutet das, dass sie die Seiten mit den für ihre Dienste irrelevanten Fragen durchblättern und nach dienstcharakteristischen Fragen suchen müssen.

Die Verwaltung des Sicherheitskonzeptes erfolgt dynamisch, was ein häufiges Auftreten von Änderungen und Aktualisierungen bedeutet. Jede notwendige Änderung der Sicherheitskonzept-Vorlage bedeutet, dass sowohl die Vorlage selbst als auch die Sicherheitskonzepte umgeschrieben werden müssen. Außerdem ist das Verweisen auf andere relevante Dokumente oder externe Quellen nicht zuverlässig [Hom14]. Das macht Bearbeitung des Sicherheitskonzeptes mit einem Texteditor unbequem.

Zusätzlich ist es schwer, Zugriffe sowohl auf die Vorlage als auch auf die Sicherheitskonzepte zu kontrollieren. Am Betrieb eines Dienstes sind normalerweise mehrere Akteure beteiligt. Nachdem ein Sicherheitskonzept vom Dienstadministrator erstellt und vom Dienstverantwortlichen freigegeben wird, müssen andere Personen je nach Aufgabe und Rolle auf bestimmte Kapitel zugreifen. Während das Sicherheitskonzept als PDF-Dokument gespeichert wird, ist es unmöglich, den Zugriff nur für einzelne Abschnitte/Kapitel freizugeben und zu kontrollieren.

Aus allen oben geschriebenen Tatsachen folgt, dass zur Unterstützung der Administratoren und Verantwortlichen am LRZ bei der Verwaltung von Sicherheitskonzepten eine technische Lösung nötig ist.

1.2 Web-Content-Management-System

Jetzt muss überlegt werden, was für Art der Programmlösung für die Realisierung von SK-Verwaltung am besten geeignet ist. Aus dem vorherigen Abschnitt können die folgende Merkmale der zu entwickelnden Anwendung ermittelt werden. Die Oberfläche muss eine dynamische Interaktion des Benutzers mit der Anwendung ermöglichen. Da am LRZ ca. 100 Dienstadministratoren tätig sind, ist es erwünscht, dass mehrere Benutzer gleichzeitig und unabhängig voneinander die Anwendung nutzen können. Das heißt, der Mehrbenutzerbetrieb ist nötig. Für Ablage von dienstspezifischen Sicherheitskonzepten ist ein zentraler Ort erforderlich, um die Daten geordnet und möglichst konsistent zu halten. Alle diese Bedürfnisse lassen sich mit Hilfe einer webbasierten Lösung realisieren. Dadurch werden noch weitere Vorteile gewonnen. Alle Aktualisierungen und Änderungen der Software sind zentral durchzuführen, was das Administrieren und Wartung erleichtert. Auf den lokalen Rechner von LRZ müssen keine Installationen von Software ausgeführt werden, was Zeitaufwand spart.
Weiter kann ein Web-Content-Management-System (WCMS) in Betracht kommen, weil die Verwaltung von Inhalten seine Hauptaufgabe ist.

Im klassischen Sinne wird ein WCMS für Erstellung, Verwaltung und Veröffentlichen von

dynamischen Webseiten verwendet werden. Aber in letzter Zeit hat sich die Bedeutung des Begriffs erweitert. Je nach der Ausrichtung lassen sich die WCMS weiter aufspalten. Die Hauptfunktionalitäten bleiben jedoch unabhängig von dem verwalteten Inhalt unverändert und bringen mit sich die folgenden Nutzen und Leistungen.

- Verwaltung und Strukturierung der Inhalte, sowie der kontrollierte Zugriff auf Information sind einige der Hauptaufgaben des Systems. "Durch die Trennung der Inhalten vom Layout wird eine Abstraktion der eigentlichen Information von ihrer Darstellung erreicht." [Zsc01] Die Benutzer brauchen keine HTML-Kenntnissen. Die Darstellung wird auf einer Webseite über eine Vorlage generiert.
- Durch das Speichern der Inhalte in einer zentralen Datenbank wird der gleichzeitige Zugriff mehrerer Personen auf gleicher Datenbasis ermöglicht.
- Die Workflowkomponente unterstützt die Anwender mit der der automatisierten Kontrolle über Abläufe und Aufgabe.

Alle oben beschriebenen Feutures können bei der Entwicklung einer webbasierten Anwendung für die Verwaltung der elektronischen dienstspezifischen Sicherheitskonzepte am LRZ übernommen und genutzt werden. Die Basisfunktionen eines Web-basierenden Verwaltungssystems für Sicherheitskonzept lassen sich folgendermaßen beschreiben:

- Vorlage-Erstellungsprozess: Erst wird eine zentrale Vorlage erstellt und in einer zentralen Datenbank gespeichert.
- Content-Erstellungsprozess: Im zweiten Schritt werden Inhalte über die zentral vorgegebene Vorlage eingegeben und in der Datenbank gespeichert. Ebenso werden bestimmte Inhalte aus bereits bestehenden in die Datenbank importiert.
- Verwaltungsprozess: Mit dem vom WCMS bereitgestelltem Workflow können die berechtigte Personengruppen die in der zentralen Datenbank gespeicherten Informationen gemeinsam nutzen und überarbeiten

1.3 Ziel der Arbeit

Das Ziel dieser Arbeit besteht darin, die Anforderungen zu ermitteln, die eine Programmlösung zur Verwaltung von dienstspezifischen Sicherheitskonzepten am LRZ erfüllen soll. Um die gesamte System-Funktionalität allgemein verständlich zu machen, sollen Nutzungsabläufe einzelner Zielgruppen in der Use-Case-Spezifikation detailliert beschrieben werden. Um Datenschutz von Sicherheitskonzept-Inhalten zu gewährleisten, muss unter Berücksichtigung der Organisationsstruktur des LRZ eine Trennung von Mitarbeitern auf Dienstebene durchgeführt werden. Darüber hinaus ist nicht nur die Funktionalität der Software zu beschreiben, sondern sind auch Qualitätseigenschaften, Leistungen und sonstige Restriktionen zu erheben. Je nach Wichtigkeit müssen die Anforderungen an das System gewichtet werden. Am Ende dieser Arbeitsphase muss ein Anforderungskatalog erstellt werden, der die identifizierten funktionalen und nicht-funktionalen Anforderungen zusammenfasst.

In Rahmen einer Evaluation aktuell am Markt erhältlicher Werkzeuge soll daraufhin die software-technische Umsetzbarkeit der ermittelten Anforderungen untersucht werden. Durch

ein geeignetes Auswahlverfahren muss eine Applikation ausgewählt werden, die die Realisierung des entwickelten Konzeptes ermöglicht. Dabei kann das Ergebnis der durchgeführten Evaluation sowohl positiv als auch negativ sein. Denn ist es denkbar, dass keine Software auf dem Markt vorhanden ist, die die einen Großteil der Anforderungen erfüllt und zu den Bedürfnissen des LRZ passt. Ist das der Fall, dass eine für die Sicherheitskonzeptverwaltung geeignete Anwendung ausgewählt wird, soll auf ihrer Basis ein Prototyp implementiert werden, um Teile der Sicherheitskonzept-Vorlage zu repräsentieren.

1.4 Struktur der Arbeit

Kapitel 2 stellt den Vorgang bei der Konzeptentwicklung vor. Angefangen von der Beschreibung des Use-Cases wird am Ende dieses Kapitels ein Katalog mit den Anforderungen an die zu entwickelnde Anwendung und ihrer Priorisierung präsentiert. In Kapitel 3 wird eine Übersicht von aktuell am Markt erhältlicher Werkzeuge gegeben und die Untersuchung geführt, in wie weit sie den im Kapitel 2 identifizierten Anforderungen entsprechen. Ist im Kapitel 3 eine Anwendung ausgewählt, wird im Kapitel 4 auf ihrer Basis ein Prototyp implementiert. Schließlich werden die Ergebnisse der durchgeführten Arbeit im Kapitel 5 zusammengefasst, ein Fazit gezogen und einen Ausblick auf mögliche zukünftige Aufgaben gegeben.

2 Anforderungen an ein Web-basiertes Verwaltungssystem

Im ersten Kapiteln wurde festgelegt, dass für die Erstellung und Verwaltung von dienstspezifischen Konzepten ein Web-basiertes Managementsystem erforderlich ist. Im nächsten Schritt müssen die konkreten Anforderungen an dieses System erhoben werden, um eine klare Vorstellung über Leistungen des neuen Systems zu bekommen. Bevor man versucht, die gewünschte Funktionalität des Systems zu bestimmen, muss man Antworten auf die folgenden Fragen finden:

1. Wer ist an den Aufgaben beteiligt?

2. Was sind die Hauptaufgaben des Systems?[Kle13]

In diesem Kapitel wird erst die Struktur von LRZ betrachtet und die Personenkreise ermittelt, die ein Interesse am neuen System haben oder von ihm in irgendeiner Weise betroffen sind (engl. Stakeholder). Nach der Identifizierung der Stakeholder werden die Ziele des zu entwickelnden Systems verdeutlicht. Im nächsten Schritt wird mit Hilfe der Anwendungsfälle (engl. Use Cases) die Hauptfunktionalität des neuen Systems geklärt und werden funktionale und nicht-funktionale Anforderungen an das zu entwickelnde System ermittelt. Zum Schluss des Kapitels werden die Anforderungen je nach ihrer Wichtigkeit gewichtet und in einem Anforderungskatalog zusammengefasst.

2.1 Organisationsstruktur des LRZ

Bei der Entwicklung einer unternehmensspezifischen neuen Software soll nicht die Organisationsstruktur außer Acht gelassen werden. Eine Einsichtnahme in den Aufbau der Organisation dient zum besseren Verständnis innerbetrieblicher Abläufe und der Kommunikationsbeziehungen zwischen den organisatorischen Einheiten. Auch der Organisationsaufbau ist bei der Festlegung einer anwendungsspezifischen Zugriffskontrolle zu berücksichtigen.

In diesem Abschnitt wird ein kurzer Überblick über die interne organisatorische Struktur des LRZ und über Dienst- und Aufgabenverteilung gegeben. Das Organigramm 2.1 stellt den Aufbau des LRZ dar[1].

Dem Organigramm ist zu entnehmen, dass das LRZ vom Vorsitzenden des Direktoriums geleitet wird. Das LRZ gliedert sich in folgende vier Abteilungen: Benutzernahe Dienste und Systeme, Hochleistungssysteme, Kommunikationsnetze, Zentrale Dienste[2]. Jede Abteilung wird von einem Abteilungsleiter geführt und ist in weitere Arbeitsgruppen unterteilt. Jede

[1] http://www.lrz.de/wir/organisation/
[2] Stand vom 01. Juli 2013

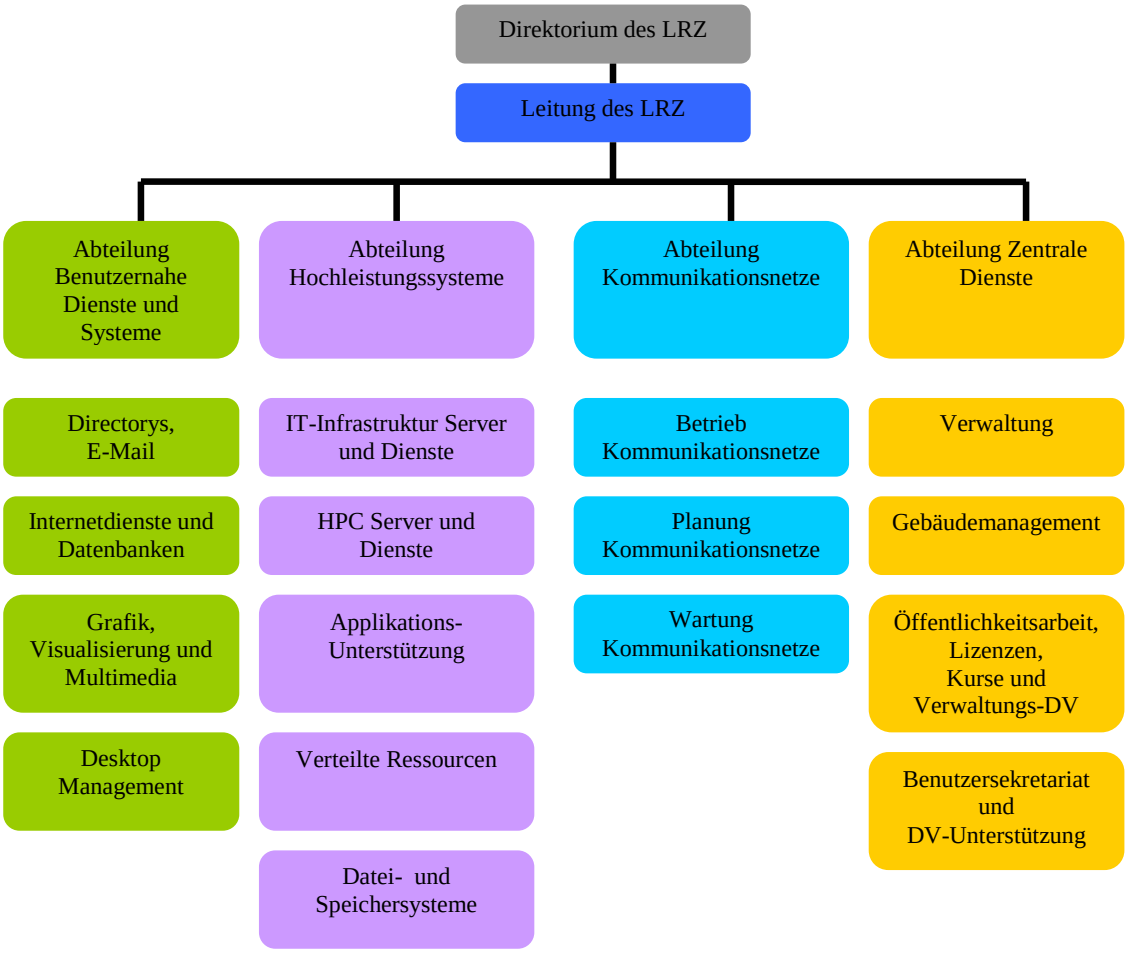


Abbildung 2.1: Die interne Organisationsstruktur des LRZ

Gruppe spezialisiert sich auf eine enge Dienstmenge und wird von einem Gruppenleiter geleitet. Hier folgt eine Kurzbeschreibung der Abteilungen mit ihren Schwerpunkten.

1. Abteilung "Benutzernahe Dienste und Systeme"
Von der Abteilung betreute IT-Infrastruktur-Dienste im Münchner Wissenschaftsnetz (MWN) sind u.a. Verzeichnisdienste für das Identity Management, die Unix-Maillösung sowie die Groupware Microsoft Exchange, die eLearning-Plattformen Moodle für TUM und LMU, das Hosting von Webauftritten und Dokumenten-Managementsystemen, Web-Portallösungen auf klassischer Unix-Basis und Microsoft Sharepoint, hochskalierende Datenbanklösungen, Desktop-Management-Angebote für diverse Arbeitsplatztypen, die gesamte komplexe IT-Infrastruktur für den Bibliotheksverbund Bayern vom Verbundkatalog bis zur Langzeitarchivierung (Rosetta).

2. Abteilung "Hochleistungssysteme"
Zu den Aufgaben der Abteilung "Hochleistungssysteme" gehören der Betrieb aller Hoch- und Höchstleistungsrechner des LRZ bzw. des SuperMUC, der Betrieb der Cluster-Systeme und der Grid-Dienste, Support im Bereich Hochleistungsrechnen, Zuständigkeit für Datenspeicherung bzw. Online-Speicher, Archiv- und Backupsysteme sowie Langzeitarchivierung.

3. Abteilung "Kommunikationsnetze"
Aufgabe der Abteilung "Kommunikationsnetze" ist die Bereitstellung einer stabilen und ausgearbeiteten Netzinfrastruktur. Zudem werden wichtige Netzdienste von der Abteilung bereitgestellt und gepflegt. Dazu gehören vor allem alle Dienste und Protokolle, die in MWN angesetzt sind. Das sind Internet-Protokolle, Namen-Server Dienst, Virtuelle Private Netze und Wireless LAN in MWN und viele andere Dienste, die auf der Webseite des LRZ[3] detailliert beschrieben sind.

4. Abteilung "Zentrale Dienste"
Die Abteilung "Zentrale Dienste" ist zuständig für Softwarelizenzen, Gebäudemanagement, Betreuung der komplexen Rechenzentrumsgebäude-Infrastruktur und Personalausstattung. Die Abteilung bietet und organisiert Kurse zu PC-Software, Hochleistungsrechnen, Grafik, Internet und Visualisierung.

Außerdem werden im LRZ noch folgende längerfristige Arbeitskreise durchgeführt, die einen abteilungsübergreifenden Charakter besitzen: IT-Sicherheit, Koordination der Nutzerkontakte, Grid, ITSM, Informationsmanagement, Visualisierung.

Der Arbeitskreis Visualisierung dient zum Wissensaustausch im Bereich Virtuelle Realität und Visualisierung am LRZ. Der Interessensbereich der Arbeitsgruppe umfängt Grid Computing und Cloud Computing. Dazu ist dieser Arbeitskreis an vielen nationalen und internationalen Grid-Projekten beteiligt. Das IT-Service-Management Team unterstützt Geschäftsprozesse durch Liefer- und IT-Services.

Der ständige Arbeitskreis IT-Sicherheit am LRZ beschäftigt sich auch mit einer Reihe von Themen: Erstellung von Sicherheitsrichtlinien bzw. Erstellung der Vorlage von Betriebs- und

[3] `http://www.lrz.de/services/netzdienste/`

Sicherheitskonzepten, Entwicklung der Security-Awareness-Maßnahmen für LRZ-Mitarbeiter, Erweiterung des Security-Incident-Response-Prozesses. Das Computer Security Incident Response Team (CSIRT) des LRZ ist für die Erkennung, Eingrenzung und auch Aufklärung von hausintern aufgetretenen Sicherheitsvorfällen zuständig. [Zen14].

Insgesamt sind am LRZ ca. 80 Dienste im Betrieb, die von über 100 Dienst-Administratoren bedient und gepflegt werden.

2.2 Stakeholder und Ziele

Nach Betrachtung der allgemeinen Struktur des LRZ kann man zur Identifikation der unmittelbar an Dienstbetrieb und IT-Sicherheit beteiligten Personenkreise übergehen. Im Folgenden wird eine Liste von Personengruppen vorgestellt, die relevant für den Prozess der Erstellung und Verwaltung von Sicherheitskonzepten am LRZ sind. Alle Mitarbeiter des LRZ, die sich mit Diensten beschäftigen oder für die Sicherheit am LRZ verantwortlich sind, sind potenzielle **Endanwender des Systems**. Das ist eine zentrale Gruppe für dieses Projekt, die sich weiter aufspalten lässt.

Jede der vier oben genannten Abteilungen wird von je einem **Abteilungsleiter** geführt. Seine Aufgabe umfasst die fachlich-organisatorische Führung der Abteilung, Koordination mit anderen Fachabteilungen und Anleitung der zugeordneten Angestellten. Wenn man jede Abteilung des LRZ als eine hierarchische Struktur betrachtet, befindet sich der Abteilungsleiter auf der obersten Ebene der Hierarchie. Jede Gruppe innerhalb einer Abteilung hat einen **Gruppenleiter**. Zu seinen Aufgaben zählen das Koordinieren der Arbeitsabläufe innerhalb seiner Gruppe und die Verteilung der Aufgaben an Teammitglieder. Der Gruppenleiter befindet sich in der Abteilungshierarchie unmittelbar unterhalb des Abteilungsleiters. Hierher kann man auch die Leiter der abteilungsübergreifenden Arbeitskreise rechnen. Diese haben ähnliche Funktionen, allerdings außerhalb der Abteilungsstruktur. Der Dienstadministrator betreibt einen oder mehrere Dienste und eine seiner Aufgaben ist die Erstellung des Sicherheitskonzeptes für diesen Dienst. In dieser Arbeit wird der Dienstadministrator als **Dienstbetreiber** bezeichnet, um eine Verwechslung mit Nutzern mit administrativen Berechtigungen (Administratoren) zu vermeiden.

Der abteilungsübergreifende Arbeitskreis IT-Sicherheit ist für die Unterstützung des Sicherheitsprozesses am LRZ zuständig. Die Vorlage für die Erstellung dienstspezifischer Sicherheitskonzepten wurde vom Arbeitskreis entworfen und dem Dienstbetreiber und fachlich Verantwortlichen als Hilfestellung zum Erreichen eines hohen Sicherheitsniveaus im Dienstbetrieb zur Verfügung gestellt. Das Erstellen und Aufrechterhalten von Vorlagen für Sicherheitskonzepte ist eine der Aufgaben dieses Arbeitskreises. Einige der Mitarbeiter dieses Arbeitskreises können bei sich die administrativen Funktionen des zu entwickelnden Systems verwalten. Der **Informationssicherheitsbeauftragter** ist für die gesamte IT-Sicherheitssituation zuständig. Zu seinen Aufgaben gehören Entwickeln, Formulieren und Kontrollieren der Umsetzung der IT-Sicherheitsrichtlinien am LRZ. Außerdem koordiniert und kontrolliert er die Verwaltungsprozess von Sicherheitskonzepten.

Der Fokus der Arbeit des Computer Security Incident Response Teams (CSIRT) liegt auf

der Behandlung von Sicherheitsvorfällen. Die Sicherheitskonzepte können beim Analysieren der konkreten Sicherheitsvorfälle als Einstiegspunkt dienen. Diejenigen Mitarbeiter, die kompletten Lesezugriff auf die Inhalte der Sicherheitskonzepte benötigen, werden im Weiteren als **Operateure** bezeichnet.

Jetzt können die Ziele des zu entwickelnden Systems ermittelt werden, die als Ankerpunkt der weiteren Entwicklung dienen. Die folgenden Hauptziele können genannt werden:

1. Das neue System muss eine einfache und bequeme Erstellung, Verwaltung und konsolidierte Ablage dienstspezifischer Sicherheitskonzepte am LRZ ermöglichen.
2. Mit Hilfe des neuen Systems kann man eine Übersicht der bereits eingesetzten Sicherheitsmaßnahmen bekommen und rechtzeitig die noch existierenden Sicherheitslücken identifizieren. Dadurch kann das Sicherheitsniveau verbessert werden.
3. Durch die festgelegten Zugriffsregeln und Zugriffsbeschränkungen muss der kontrollierte Zugriff auf die Funktionen und Daten gewährleistet werden.

Die in den folgenden Abschnitten ermittelten Anforderungen sollen als Mittel zum Erreichen dieser Ziele dienen.

2.3 Beschreibung von Anwendungsfällen und Ableitung funktionaler Anforderungen

Die Anwendungsfälle beschreiben das Verhalten des Systems aus der Sicht des Nutzers. Um eine bestimmte Funktionalität des Systems durchzuführen, muss sie ein Auslöser aufrufen. Die Auslöser, auch Akteure benannt, der zu entwickelnden Anwendung sind die Mitarbeiter des LRZ, die aus der Gruppe von Stakeholder "Endanwender des Systems" ausgewählt werden können. Aus der Beschreibung der Endanwender des Systems und deren Aufgaben lassen sich die folgende Auslöser für die Ausführung der Anwendungsfälle differenzieren:

- Administrator
- Informationssicherheitsbeauftragte
- Dienstverantwortlicher
- Dienstbetreiber
- Operateur

Sobald die Projektziele bestimmt und die Akteure identifiziert wurden, kann man zur Beschreibung der Kernfunktionalität des Systems übergehen.
Die Erstellung des Sicherheitskonzeptes am LRZ kann man grob folgendermaßen skizzieren: Zuerst wird die Sicherheitskonzept-Vorlage erstellt und nach der Überprüfung freigegeben. Auf Basis dieser Vorlage sind dienstspezifische Sicherheitsdokumente zu erstellen. Jedes Sicherheitskonzept muss erst genehmigt und danach freigegeben werden. Nach der Freigabe steht es für die weitere Arbeit zum Beispiel für das CSIRT-Team bereit. Das Diagramm 2.2 stellt diesen Ablauf dar, wobei es zeigt, welche Akteure an welcher Aktivität beteiligt sind.

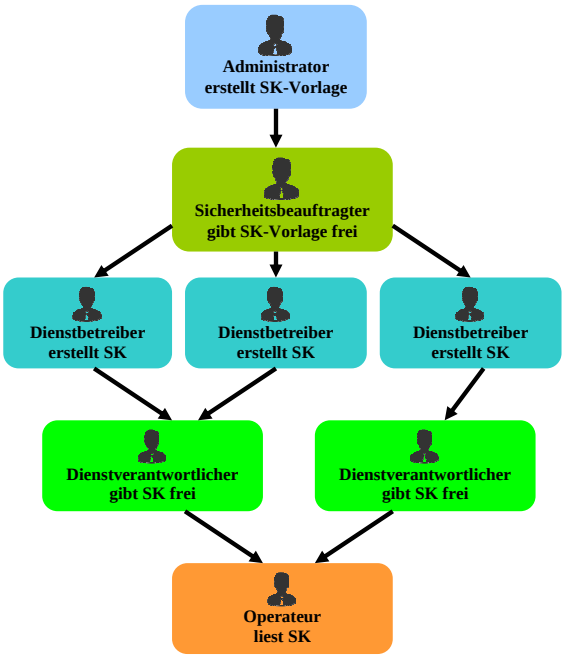


Abbildung 2.2: Ablauf beim Erstellen von Sicherheitskonzepte

Das Aktivitätsdiagramm 2.3 beschreibt den Prozess der Erstellung und Aktualisierung von Sicherheitskonzepten genauer und basiert auf der Abbildung 2 in [Hom14, S. A-14]. Aus diesem Diagramm ist klar ersichtlich, dass die Sicherheitskonzeptverwaltung ein zyklischer Prozess ist. Der Lebenszyklus eines Sicherheitskonzeptes beginnt mit dem Erstellen der Mustervorlage, ihrer Überprüfung und Genehmigung. Nach der Freigabe der Vorlage können dienstspezifische Sicherheitskonzepte erfasst werden. Nach der Überprüfung jedes Dokumentes erfolgt seine Freigabe. Ist es der Fall, dass ein Sicherheitskonzept veraltet ist, ein Sicherheitsvorfall aufgetreten ist oder am Dienst globale Änderungen vorgenommen wurden, muss es überarbeitet und aktualisiert werden. Die gleiche Regel gilt für die Sicherheitskonzept-Vorlage, die regelmäßig auf Aktualität zu prüfen ist.

Nach der Überlegung, welche zentrale Informationen das System verwalten und bearbeiten muss, wurden die folgenden fünf obligatorischen Funktionalitäten definiert:

1. Verwaltung der Sicherheitskonzept-Vorlage
2. Verwaltung der dienstspezifischen Sicherheitskonzepte
3. Rollen- und Rechteverwaltung
4. Dienstverwaltung
5. Benutzerverwaltung

Hinter dem Begriff "Verwaltung" sind die folgenden Fälle zusammengefasst:

- Eine neue Information hinzufügen

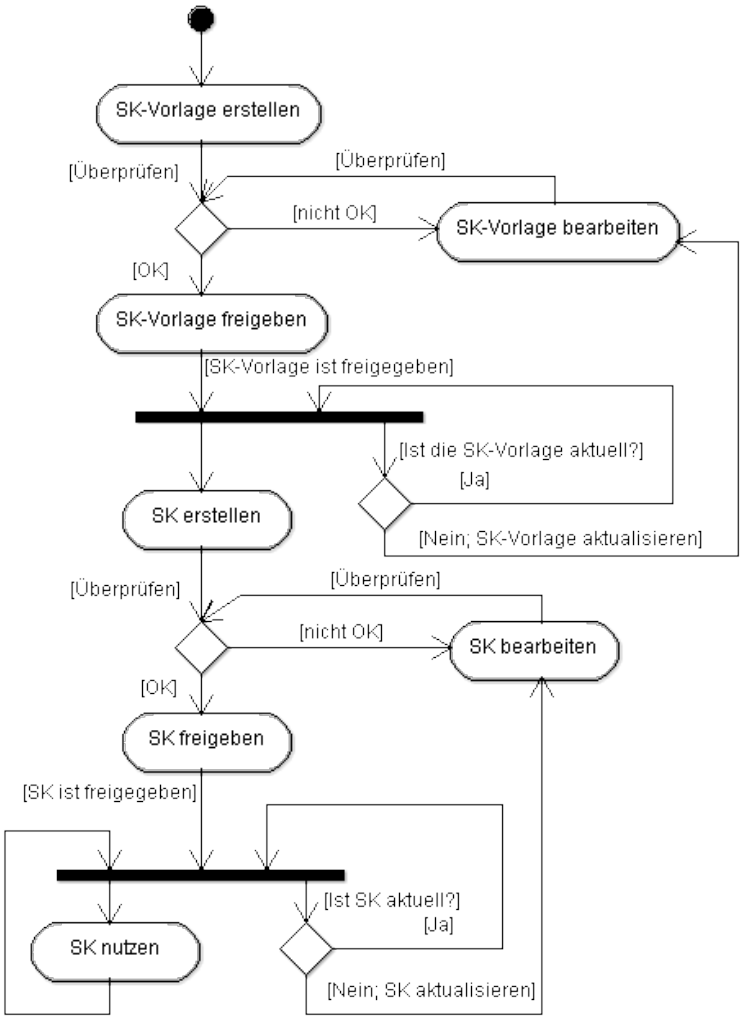


Abbildung 2.3: Aktivitätsdiagramm "Ablauf beim Erstellen und Aktivieren von Sicherheitskonzepte"

- Eine existierende Information nutzen
- Eine existierende Information bearbeiten
- Eine existierende Information löschen

Jetzt werden die fünf oben genannten Hauptfunktionalitäten in einzelne Schritte zerlegt und mit Hilfe von Anwendungsfällen genauer beschrieben. Aus den Anwendungsfällen lassen sich die funktionalen Anforderungen ableiten. Das sind die Anforderungen, die die gewünschten Funktionalitäten eines Systems beschreiben und die Frage "WAS soll das System tun?" beantworten. Im Weiteren werden jeder funktionalen Anforderung der Buchstabe "F" und eine fortlaufende Nummer zugeordnet. Die in diesem Kapitel zu beschreibenden Use Cases sind durchnummeriert und haben das folgenden Format: Use Case-Nummer (UC-Nr.).

2.3.1 Verwaltung einer Sicherheitskonzept-Vorlage

Dieser Abschnitt beschäftigt sich mit der Ermittlung der benötigen Funktionalitäten zur Sicherheitskonzept-Vorlag-Verwaltung. Beim Übertragen der auf dem Papier bestehende Vorlage in elektronische Form, muss die Struktur der zu entwickelnden Vorlage möglichst nah behaltet werden und die Vorteile, die eine webbasierte Lösung anbietet, auszunutzen. Da es sich dabei um Formulare handelt, wird im Folgenden von "Fragen" und "Antworten" gesprochen, wobei "Antworten" den Eingaben der Nutzer entsprechen. Das Verwalten der Vorlage ist Aufgabe des Administrators und der Verwaltungsprozess beginnt eigentlich mit deren Erstellung. Der folgende Anwendungsfall stellt das detaillierte Vorgehen des Erzeugungsprozesses vor.

Anwendungsfall *Erstellen einer neuen Sicherheitskonzept-Vorlage* (UC-1)
Akteur: Administrator
Vorbedingung Sicherheitskonzept-Vorlage existiert im System noch nicht oder ist nicht mehr aktuell
Nachbedingung: Sicherheitskonzept-Vorlage ist erstellt und im System gespeichert
Standardablauf: Der Administrator soll den Befehl zur Erstellung der neuen Sicherheitskonzept-Vorlage wählen. Nachdem das System die entsprechende Nutzeroberfläche angezeigt hat, erzeugt der Administrator eine Fragengruppe (Anwendungsfall *Erstellen einer Fragengruppe*). Danach fügt er eine Frage oder mehrere Fragen hinzu (Anwendungsfall *Erstellen einer Frage*). Soll die Sichtbarkeit der Frage oder der Fragengruppe von den bisher gegebenen Antworten abhängig sein, definiert der Administrator die Bedingung, die erfüllt werden muss (Anwendungsfall *Verknüpfen der Fragen unter Bedingungen*). Die Schritte der Erstellung einer Fragengruppe und einer Frage wiederholen sich, bis die Mustervorlage fertig ist. Danach wird die Sicherheitskonzept-Vorlage im System gespeichert.

Die weiteren drei Use cases verfeinern den oben beschriebenen Anwendungsfall.

Anwendungsfall *Erstellen einer Fragengruppe* (UC-2)
Akteur: Administrator
Vorbedingung: Sicherheitskonzept-Vorlage ist erstellt
Nachbedingung: Eine neue Fragengruppe erstellt und gespeichert
Standardablauf: Der Administrator wählt den Befehl zum Erstellen einer neuen Fragengruppe aus, benennt sie und speichert.

Anwendungsfall *Erstellen einer Frage* (UC-3)
Akteur: Administrator
Vorbedingung: Fragengruppe ist erstellt und gespeichert
Nachbedingung: Eine neue Frage ist erstellt und gespeichert
Standardablauf: Der Administrator wählt den Befehl zum Erstellen einer neuen Fragengruppe aus. Nachdem das System die Eingabefelder angezeigt hat, gibt der Administrator den Text der Frage ein und legt fest, ob die Beantwortung optional oder Pflicht ist. Im nächsten Schritt wählt der Administrator einen Fragentyp aus. Wenn der Fragentyp mehrere Möglichkeiten für eine Antwort erfordert, trägt der Administrator die entsprechenden Antwortvorgaben ein. Soll eine Antwortalternative später mehrere Male vorkommen, speichert der Administrator sie als Schablone. In dem Fall, dass der Wertebereich eines Eingabewertes eingeschränkt sein muss, definiert der Administrator die zulässigen Werte und speichert schlussendlich die Frage.

Anwendungsfall *Anzeigebedingungen definieren* (UC-4)
Akteur: Administrator
Vorbedingung: In der Vorlage sind mindestens zwei Fragen bereits vorhanden.
Nachbedingung: Eine Frage oder Fragengruppe mit einer anderer Frage unter der definierten Anzeigebedingung verknüpft
Standardablauf: Der Administrator wählt eine Frage oder eine Fragengruppe aus, die je nach der gegebenen Antwort angezeigt oder ausgeblendet werden soll. Danach wählt er den Befehl zum Definieren der Anzeigebedingungen aus. Das System bietet eine Liste aller vorher stehenden Fragen zur Auswahl. Der Administrator selektiert eine Frage aus der Liste, wählt eine von der Vergleichsoperationen und die erwartete Antwort oder den erwarteten Wert aus. Schließlich legt der Administrator die Aktion zur Anzeige oder zur Ausblendung fest und speichert die Bedingung.

Aus den oben vorgestellten Anwendungsfällen lassen sich die folgenden Funktionalitäten des Systems nachvollziehen:

1. Das System muss eine Möglichkeit bieten, eine standardisierte Mustervorlage zur Erfassung von Sicherheitskonzepten zu erstellen und zu speichern, ebenso den noch nicht freigegebenen Entwurf zwischen zu speichern. Diese Vorlage muss als Ausgangspunkt für alle weiteren Sicherheitskonzepte dienen. In der Zukunft wird der Inhalt der Vorlage an spezifische Dienste verschiedener Dienstverantwortlicher angepasst. Nach mehreren solchen Änderungen kann die Mustervorlage die Konsistenz verlieren. Deswegen macht es Sinn, eine gemeinsame Vorlage für die Erstellung aller Sicherheitskonzepte, unabhängig vom Dienst, zu verwenden.
   → Anforderung F01: Erstellen und Speichern der Sicherheitskonzept-Vorlage
   → Anforderung F02: Zwischenspeichern des Entwurfs der Sicherheitskonzept-Vorlage

2. Das System muss dem Benutzer eine Möglichkeit bieten, Fragen zu erstellen, sie in Fragengruppen zusammenzufassen und verwalten zu können.
   Da das Sicherheitskonzept in mehrere Kapiteln aufgeteilt ist, die ihrerseits aus Unterabschnitten bestehen, braucht man die entsprechende Funktionalität, um die Struktur der zu entwickelnden Sicherheitsvorlage zu erhalten.

→ Anforderung F03: Erstellen von Fragen
→ Anforderung F04: Gruppieren von Fragen in Fragengruppen

3. Das System muss Fragentypen zur Auswahl stellen.
   Die Fragentypen lassen sich in offene, geschlossene und halboffene Fragen unterteilen. Eine Frage kann als Klartext beantwortet werden (offene Frage), eine begrenzte Anzahl von Antwortalternativen enthalten, z. B. Checkbox, Ja/Nein (geschlossene Frage), oder als Checkbox mit einer offenen Kategorie angegeben werden (eine halboffene Frage). In der aktuellen Sicherheitskonzept-Vorlage werden am häufigsten folgende Varianten vorkommen: Freitextfelder bzw. Freitextfelder mit begrenzter Anzahl von Zeichnen, Multiple Choice mit einer oder mehreren gleichzeitig wählbaren Antwortalternativen (Checkboxen, Radiobuttons, Checkboxen mit einer offenen Kategorie), Tabellen, Datum und Uhrzeit. Da die zu entwickelnde Anwendung vor allem Zeit und Aufwand der LRZ-Mitarbeiter reduzieren soll, müssen diese Typen auch in der Anwendung beibehalten werden. Außerdem können einzelne Eingabewerte beschränkt und insbesondere auf Typ (Integer, String), auf Anzahl der Zeichen oder auf Wertebereich beschränkt werden. Durch eine Eingabewertprüfung wird das Speichern unzulässiger Werte vermieden.
   → Anforderung F05: Auswahl von Fragentypen
   → Anforderung F05.1: Der Fragentyp "Freitext"
   → Anforderung F05.2: Der Fragentyp "Mehrere Antwortalternativen"
   → Anforderung F05.3: Der Fragentyp "Exakt eine Antwortalternative"
   → Anforderung F05.4: Der Fragentyp "Datum"
   → Anforderung F05.5: Der Fragentyp "Uhrzeit"
   → Anforderung F05.6: Der Fragentyp "Tabelle"
   → Anforderung F06.1.1: Beschränken des Eingabewertes auf Typ: Nummer
   → Anforderung F06.1.2: Beschränken des Eingabewertes auf Typ: Buchstaben
   → Anforderung F06.2: Beschränken des Eingabewertes auf Anzahl von Zeichen
   → Anforderung F06.3: Beschränken des Wertebereiches eines Eingabewertes

4. Das System muss eine Möglichkeit bieten, eine obligatorische Frage als Pflichtfrage zu markieren.
   → Anforderung F07: Markieren von Frage als "Pflichtfeld"

5. Das System muss eine Möglichkeit bieten, die logischen Abläufe zu definieren.
   Nicht alle Fragen der Sicherheitskonzept-Vorlage müssen beim Ausfüllen des Sicherheitskonzepts beantwortet werden. Unnötige Fragen machen den Fragenbogen umständlich. Dies kann man mit Hilfe von Verzweigungslogik vermeiden, indem man vordefiniert, welche Fragen oder Fragegruppen unter welchen Bedingungen angezeigt bzw. ausgeblendet werden sollen. Je nach gegebener Antwort kann ein Pfad in einem Fragebogen variieren.
   → Anforderung F08: Verknüpfen einer Frage mit einer Bedingung
   → Anforderung F09: Verknüpfen einer Fragengruppe mit einer Bedingung

6. Das System muss eine Möglichkeit bieten, die Antwortalternativen als Schablone zu speichern.
   Da sich in der aktuellen Vorlage einige Antwortmöglichkeiten oft wiederholen, wäre es hilfreich, diese nur einmalig einzugeben, zu speichern und später mehrmals zu verwen-

den.
→ Anforderung F10: Speichern der Antwortalternativen als Schablone

Die gespeicherte Sicherheitskonzept-Vorlage kann nachgearbeitet oder freigegeben werden. Hat der Administrator die Vorlage vollständig ausgearbeitet, kann sie freigeschaltet werden. Dafür muss erst der Informationssicherheitsbeauftragte des LRZ sie überprüfen. Der Vorgang der Freigabe lässt sich mit dem Use Case *Sicherheitskonzept-Vorlage freigeben* beschreiben.

Anwendungsfall *Sicherheitskonzept-Vorlage freigeben* (UC-5)
Akteur: Informationssicherheitsbeauftragter
Vorbedingung: Eine Sicherheitskonzept-Vorlage ist im System gespeichert und noch nicht freigegeben.
Nachbedingung: Sicherheitskonzept-Vorlage ist freigegeben
Standardablauf: Der Informationssicherheitsbeauftragte öffnet die Vorlage, überprüft und gibt sie frei.
Alternativeablauf: Fehlen in der Vorlage irgendwelche Fragen oder Abschnitte oder soll der Fragebogen noch überarbeitet werden, teilt das der Informationssicherheitsbeauftragte dem Administrator mit.

Aus diesem Use Case kann man das Folgende ableiten:

1. Das System muss eine Möglichkeit bieten, die Sicherheitskonzept-Vorlage zur Vorschau aufzurufen.
   Es ist wichtig, die Vorlage während des Erstellungsprozesses und noch vor der Freigabe aus der Sicht des Benutzers anschauen zu können. Das ermöglicht frühzeitige Fehlerkorrektur und die Vorlage benutzerfreundlicher zu gestalten.
   → Anforderung F11: Aufrufen der Sicherheitskonzept-Vorlage zur Vorschau

2. Das System muss eine Möglichkeit bieten, die Vorlage freizugeben.
   → Anforderung F12: Freigabe der Sicherheitskonzept-Vorlage

Neben der Erstellung einer Form ist es sehr wichtig, eine Gelegenheit zu haben, die Änderungen vorzunehmen. Die Vorlage muss immer auf dem neuesten Stand sein, das heißt, sie muss regelmäßig aktualisiert werden. Weiter unten ist der Ablauf des Vorlagebearbeitungsprozesses zusammengefasst.

Anwendungsfall *Bearbeiten einer Sicherheitskonzept-Vorlage* (UC-6)
Akteur: Administrator
Vorbedingung: Die Sicherheitskonzept-Vorlage ist erstellt
Nachbedingung: Die Änderungen sind erfolgreich im System gespeichert.
Standardablauf: Der Administrator öffnet die Sicherheitskonzept-Vorlage, deaktiviert und bearbeitet sie. Soll die Vorlage ergänzt werden, fügt der Administrator eine neue Fragengruppe(Anwendungsfall *Erstellen einer Fragengruppe*) und/oder eine neue Frage(Anwendungsfall *Eerstellen einer Frage*) hinzu. Soll eine neue Frage/Fragengruppe zwischen bereits existierenden Items hinzugefügt werden, erstellt der Administrator ein neues Item und zieht es an die richtige Stelle. Das System markiert es als "neu". Ist ein Fehler im Fragetext oder im Namen der Fragengruppe aufgetreten, korrigiert er diese. Tritt der Fall auf, dass eine Frage eine neue Antwortalternative braucht, wählt er diese Frage aus und fügt eine weitere Variante hinzu. Ist ein Item (Fragengruppe, Frage oder Antwortalternative) nicht mehr nötig,

löscht es der Administrator. Schließlich speichert er die Änderungen, das System schließt die Vorlage.

Die folgenden Bearbeitungsaufgaben können aus dem Use Case *Sicherheitskonzept-Vorlage bearbeiten* abgeleitet werden:

1. Das System muss die Möglichkeit bieten, die Sicherheitskonzept-Vorlage deaktivieren. Bevor man mit der Bearbeitung der Vorlage anfängt, muss sie zuerst inaktiv sein. Das Deaktivieren der Vorlage ermöglicht während ihrer Bearbeitung mögliche Kollisionen zu vermeiden. Daneben kann eine alte Version der Mustervorlage einfach deaktiviert werden ohne sie zu löschen.
   → Anforderung F13: Deaktivieren der Sicherheitskonzept-Vorlage

2. Das System muss eine Möglichkeit bieten, die Sicherheitskonzept-Vorlage zu bearbeiten.
   Für eine regelmäßige Aktualisierung der Mustervorlage ist eine Bearbeiten-Option notwendig. Das System muss die Mustervorlage zum Ausfüllen bereitstellen, so dass Eingabefelder mit bereits existierendem Text editierbar und alle Optionen (wie Frage-/Fragengruppenerstellung) verfügbar sind.
   → Anforderung F14: Aufrufen der Sicherheitskonzept-Vorlage zum Bearbeiten

3. Das System muss eine Möglichkeit bieten, die Reihenfolge von Fragen und Fragengruppen zu ändern. Es kann sehr nützlich sein, einen neuen Abschnitt nicht am Ende der Vorlage anzuhängen, sondern an der logisch passenden Stelle einzufügen. Eine ähnliche Situation findet sich bei den Fragen.
   → Anforderung F15: Ändern der Reihenfolge der Fragen
   → Anforderung F16: Ändern der Reihenfolge der Fragengruppen

4. Das System muss die Möglichkeit bieten, den Text von Fragen, Fragengruppen und Antwortalternativen zu editieren. Das Korrigieren syntaktischer oder anderer Fehler muss möglich sein.
   → Anforderung F17: Ändern des Fragen- und Fragengruppentextes

5. Das System muss die Möglichkeit bieten, eine Frage um eine neue Antwortalternative zu erweitern. Im Fall, dass ein Fragentyp eine Antwortalternative verlangt, eine mögliche Variante der Antwort jedoch noch fehlt, kann sie hinzugefügt werden.
   → Anforderung F18: Einfügen einer neuen Antwortalternative zu einer Frage

6. Das System muss die Möglichkeit bieten, ein in der Vorlage neu hinzugefügtes Item (Fragengruppe, Frage und Antwortalternative) als "neu" zu markieren. Es wäre sehr hilfreich, wenn der Dienstbetreiber beim Bearbeiten eines dienstspezifischen Sicherheitskonzeptes sofort die Änderungen in der Vorlage sehen könnte.
   → Anforderung F19: Markieren in der Sicherheitskonzept-Vorlage neu hinzugefügter Fragengruppen, Fragen und Antwortalternativen

7. Das System muss die Möglichkeit bieten, Fragengruppe, Frage und Antwortalternative aus der Vorlage zu löschen.
   Das Löschen von Fragen, Fragengruppen und Antwortalternativen kann zum Verlust der bereits gespeicherten Daten im Sicherheitskonzept führen. Bei der Implementierung

muss aufgepasst werden, damit die bereits gespeicherte Information, die von gelöschten Fragen/Fragengruppen abhängig ist, nicht verloren geht.
→ Anforderung F20: Löschen einer Antwortalternative
→ Anforderung F21: Löschen einer Frage
→ Anforderung F22: Löschen einer Fragengruppe

Der Ablauf der Verwaltungsprozesses der Musterforlage ist in Abbildung 2.4 zusammengefasst.

Einen speziellen Fall von Vorlagebearbeitung ist das Bestimmen dienstspezifischer Fragen und Fragengruppen. Der Dienstverantwortliche kann für einen Dienst, für den er zuständig ist, entscheiden, welche Fragengruppen/Fragen in der Mustervorlage für diesen Dienst spezifisch oder irrelevant sind. Der Anwendungsfall für das Bestimmen dienstspezifischer Fragen und Fragengruppen kann folgendermaßen zusammengefasst werden:

Anwendungsfall *Bestimmen von Sichtbarkeit und Relevanz der Fragen und Fragengruppen für einen konkreten Dienst* (UC-7)
Akteur: Dienstverantwortlicher
Vorbedingung: Die Sicherheitskonzept-Vorlage ist erstellt und gespeichert
Nachbedingung: Dienstspezifische Fragen/Fragengruppen markiert und erfolgreich im System gespeichert. Alle für einen konkreten Dienst irrelevanten Fragen/Fragengruppen werden ausgeblendet.
Standardablauf: Der Dienstverantwortliche wählt einen Dienst und danach den entsprechenden Befehl aus, um für diesen Dienst spezifische Fragen/Fragengruppen zu bestimmen. Die Sicherheitskonzept-Vorlage wird geöffnet. Der Dienstverantwortlicher versieht dienstspezifische Fragen und Fragengruppen mit einer Marke. Gibt es Fragen/Fragengruppen, die für diesen Dienst irrelevant sind und bei der Erfassung des Sicherheitskonzeptes nicht angezeigt werden müssen, wählt er diese auszublenden. Schließlich speichert er die Änderungen.

An dem oben dargestellten Anwendungsfall lassen sich die weiteren Anforderungen ableiten:

1. Das System muss die Möglichkeit bieten, die Mustervorlage zum Bestimmen von dienstspezifischen Fragen und Fragengruppen zu öffnen. Die Sicherheitskonzept-Vorlage kann als Liste aller Fragengruppen und Fragen aufgerufen werden, das heißt ohne Eingabefelder. Der Dienstverantwortliche muss eine Entscheidung treffen, welche Fragen und Fragengruppen für einen konkreten Dienst nicht passen. Beim Erstellen eines Sicherheitskonzeptes für diesen konkreten Dienst lassen sich diese Fragengruppen/Fragen nicht anzeigen.
   → Anforderung F23: Öffnen der Sicherheitskonzept-Vorlage zum Bestimmen von dienstspezifischen Fragen und Fragengruppen
   → Anforderung F24: Ein- und Ausblenden dienstspezifischer Fragengruppen/Fragen

2.3.2 Verwaltung von den dienstspezifischen Sicherheitskonzepten

Nachdem die Mustervorlage für alle Sicherheitskonzepte am LRZ im System gespeichert und aktiviert worden ist, kann man nun zur Ausarbeitung eines dienstspezifischen Sicherheitskonzeptes übergehen. Das dienstspezifische Sicherheitskonzept ist nichts anderes als ein

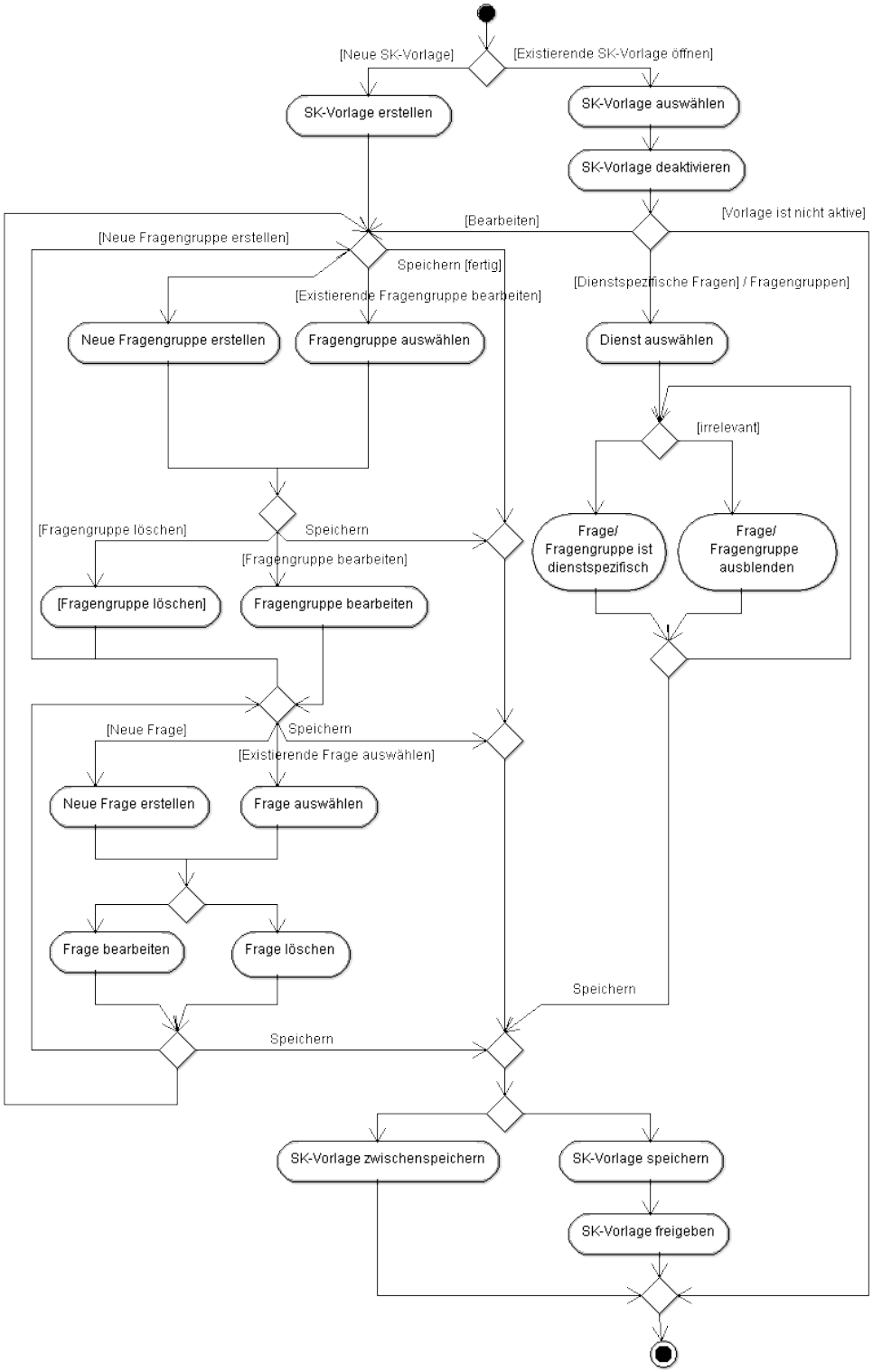


Abbildung 2.4: Aktivitätsdiagramm "Verwalten einer Sicherheitskonzept-Vorlage"

beantwortetes Vorlage-Formular. Um ein Sicherheitskonzept zu erstellen, muss man im Grunde genommen einen Dienst auswählen, einen Fragebogen ausfüllen und die Ergebnisse als separates Dokument abspeichern. Am LRZ wird diese Aufgabe meistens von Dienstadministratoren (Dienstbetreibern) übernommen.

Der nächstfolgende Anwendungsfall beschreibt den Ablauf das Erfassen eines Sicherheitskonzept.

Anwendungsfall *Erstellen eines Sicherheitskonzeptes* (UC-8)
Akteur: Dienstbetreiber
Vorbedingung: Sicherheitskonzept-Vorlage ist im System vorhanden und freigegeben. Eine Liste von Diensten für diesen Nutzer ist vorgegeben
Nachbedingung: Sicherheitskonzept ist erstellt und gespeichert
Standardablauf: Der Dienstbetreiber wählt einen Dienst aus einer Liste aus, für das er Sicherheitskonzept erstellen will. Nachdem das System überprüft hat, dass noch kein Sicherheitskonzept für diesen Dienst existiert, wählt der Dienstbetreiber den Befehl für eine Sicherheitskonzept-Erstellung aus. Das System zeigt die Vorlage mit Fragen und mit Eingabefeldern für Antworten an. Der Dienstbetreiber füllt den Fragenbogen aus. Schließlich speichert er das Sicherheitskonzept ab. Die Eingaben lassen sich vom System auf Plausibilität überprüfen und danach bestätigt das System die Speicherung.
Alternativeablauf 1: Ist für diesen Dienst bereits ein Sicherheitskonzept vorhanden, zeigt das System für diesen Dienst und das existierende Sicherheitskonzept eine Warnmeldung an.
Alternativeablauf 2: Sollen einige Fragen später beantwortet werden, überspringt der Dienstbetreiber diese und antwortet auf andere. Danach kehrt er zu noch nicht beantworteten Fragen zurück, um die fehlenden Eingaben hinzuzufügen, und danach speichert er das vollständige Sicherheitskonzept oder den Entwurf des Sicherheitskonzepts zwischen.
Alternativeablauf 3: Wenn ein oder mehrere Felder nicht plausibel sind, zeigt das System eine Warnmeldung und markiert diese Felder. Der Dienstbetreiber korrigiert die Eingaben und fordert wiederum die Speicherung an.

Die folgenden Anforderungen lassen sich aus dem Anwendungsfall *Sicherheitskonzept erstellen* herleiten:

1. Das System muss dem Dienstbetreiber eine Liste von Diensten bereitstellen, damit er aus dieser Liste einen oder mehrere Dienste auswählen kann. In der Praxis kann ein Sicherheitskonzept für einen oder für mehrere Dienste erfasst werden. Dabei ist in Betracht zu ziehen, dass die Liste nur aus Diensten bestehen soll, für die der Dienstbetreiber eine Berechtigung hat.
   → Anforderung F25: Bereitstellen von Diensten mit Mehrauswahlmöglichkeit

2. Das System muss eine Möglichkeit bieten, einen dienstspezifischen Sicherheitskonzept für den ausgewählten Dienst zu erstellen, zwischen zu speichern und endgültig zu speichern.
   → Anforderung F26: Erstellen und Speichern eines Sicherheitskonzeptes auf Basis einer Sicherheitskonzept-Vorlage
   → Anforderung F27: Zwischenspeichern des Entwurfs des Sicherheitskonzeptes

3. Das System muss eine Navigationsmöglichkeit im Sicherheitskonzept bieten.

Das System muss dem Dienstbetreiber ermöglichen, in beiden Richtungen von einem Abschnitt zum anderen zu überspringen, damit er mit dem Ausfüllen beliebiger Kapitel anfangen und später zu noch nicht beantworteten Fragen wieder zurückkehren kann.
→ Anforderung F28: Navigation im Sicherheitskonzept von einem Element zum anderen in beiden Richtungen

4. Das System muss die Eingabewerte auf Plausibilität überprüfen.
   Hier wird ein eingegebener Wert mit dem erwarteten Wert auf Übereinstimmung geprüft. Durch die Verifizierung können zum Beispiel Tippfehler frühzeitig ausgeschlossen werden.
   → Anforderung F29: Überprüfen von Eingabewerten auf Plausibilität

5. Das System muss den Anwender über alle erfolgreichen oder erfolglosen Ereignisse informieren.
   Das System muss Meldungen erstellen und ausgeben können, die wichtige Informationen für den Endnutzer der Anwendung enthalten. Ist ein Fehler beim Ausführen einer Aktion aufgetreten oder hat der Nutzer eine Eingabe in einem falschen Format vorgenommen, wird am Bildschirm eine Benachrichtigung ausgegeben. Dadurch kann der Dialog zwischen Nutzer und System ermöglicht und die Nutzerfreundlichkeit erhöht werden.
   → Anforderung F30: Mitteilung des Nutzers über erfolgreiche oder erfolglose Ereignisse

Ähnlich dem oben beschriebenen Verfahren der Vorlagenfreigabe sollte ein Mechanismus für Freigabe des Sicherheitskonzeptes vorgesehen werden. Der Vorgang des Freigabeprozesses des Sicherheitskonzeptes ist im nachfolgenden Use Case beschrieben.

Anwendungsfall *Freigeben eines dienstspezifischen Sicherheitskonzeptes* (UC-9)
Akteur: Dienstverantwortlicher
Vorbedingung: Das Sicherheitskonzept ist im System gespeichert.
Nachbedingung: Das Sicherheitskonzept ist freigegeben
Standardablauf: Der Dienstverantwortliche öffnet das Sicherheitskonzept, überprüft seinen Inhalt und gibt ihn frei.
→ Anforderung F31: Freigabe eines dienstspezifischen Sicherheitskonzeptes
Das Sicherheitskonzept kann zu zwei Zwecken aufgerufen werden: zum Bearbeiten und zum Lesen. Die folgenden zwei Use Cases stellen beide Fälle vor.

Anwendungsfall *Aufrufen eines Sicherheitskonzeptes zum Bearbeiten* (UC-10)
Akteur: Dienstbetreiber
Vorbedingung: Sicherheitskonzept ist im System vorhanden.
Nachbedingung: Änderungen sind vom Sicherheitskonzept gespeichert worden
Standardablauf: Der Dienstbetreiber selektiert das Sicherheitskonzept, das er bearbeiten will, und fordert die Bearbeitung an. Das System stellt das Sicherheitskonzept vor. Wurden neue Fragen, Fragengruppen oder Antwortalternativen seit der letzten Öffnung dieses Sicherheitskonzepts der Sicherheitskonzept-Vorlage hinzugefügt, werden sie als "neu" markiert angezeigt. Sollen noch fehlende Daten eingetragen oder bereits vorhandene Angaben korrigiert werden, sucht der Bearbeiter die Frage und füllt das Eingabefeld aus. Dieser Schritt wiederholt sich, bis alle Änderungen vorgenommen sind. Schließlich wählt der Dienstbetreiber den

Befehl zum Speichern. Das System überprüft die Eingaben auf Plausibilität, speichert und schließt das Sicherheitskonzept.
Alternativeablauf: Der Dienstbetreiber schließt das Sicherheitskonzept ohne zu speichern.

Anwendungsfall *Aufrufen eines Sicherheitskonzeptes zum Lesen* (UC-11)
Akteur: Operateur
Vorbedingung: Das Sicherheitskonzept ist im System vorhanden. Der Dienst, für den das Sicherheitskonzept aufgerufen werden soll, ist ausgewählt
Nachbedingung: Das Sicherheitskonzept ist geschlossen
Standardablauf: Der Leser öffnet das Sicherheitskonzept zum Anschauen. Er sucht den für ihn interessanten Abschnitt heraus und sieht ihn durch. Dieser Schritt kann wiederholt werden. Danach schließt der Leser das Sicherheitskonzept.

Daraus ergeben sich die nächsten Funktionalitäten des Systems:

1. Das System muss die Möglichkeit bieten, die dienstspezifischen Sicherheitskonzepte in zwei Modi aufrufen zu können: zum Bearbeiten und zum Lesen. Für den Bearbeiten-Modus lässt sich das Sicherheitskonzept so öffnen, dass der Text der Fragen bzw. der Fragengruppen und der Antwortalternativen nur zum Lesen und die Eingabefelder mit den eingegebenen Antworten zum Editieren bereitgestellt sind. Beim Lesen-Modus sind keine Änderungen möglich, aber der Text der Fragen und entsprechenden Antworten darauf sollte angezeigt werden.
   → Anforderung F32: Aufrufen des Sicherheitskonzeptes zum Bearbeiten
   → Anforderung F32.1: Anzeigen aller Antwortalternativen beim Öffnen des Sicherheitskonzeptes zum Bearbeiten
   → Anforderung F33: Aufrufen des Sicherheitskonzeptes zum Lesen
   → Anforderung F34: Anzeigen von Text der Frage bzw. Fragengruppe beim Öffnen des Sicherheitskonzeptes

2. Das System muss die Möglichkeit bieten, ein dienstspezifisches Sicherheitskonzept schließen zu können.
   Ist eine Änderung fehlerhaft eingetragen worden und muss sie nicht gespeichert werden, schließt der Dienstbetreiber das Sicherheitskonzept, ohne es zu speichern.
   → Anforderung F35: Schließen des Sicherheitskonzeptes ohne zu speichern

Der Nutzer kann das Anzeigen aller im System gespeicherter Sicherheitskonzepte anfordern. Je nach seinen Berechtigungen wird vom System eine Übersicht aller Sicherheitskonzepte gegeben. Öfter ist es aber nötig, ein konkretes Dokument zu finden. Die folgenden zwei Anwendungsfälle beschreiben diese Situationen.

Anwendungsfall *Anzeigen aller Sicherheitskonzepte* (UC-12)
Akteur: Operateur
Vorbedingung: -
Nachbedingung: Alle im System vorhandenen Sicherheitskonzeptes, die ein konkreter Nutzer sehen darf, werden angezeigt
Standardablauf: Der Leser fordert vom System, alle Sicherheitskonzeptes zu zeigen. Das System gibt eine Übersicht an.

Anwendungsfall *Suchen nach einem dienstspezifischen SK* (UC-13)
Akteur: Operateur
Vorbedingung: -
Nachbedingung: Ein oder mehrere Sicherheitskonzepte sind gefunden
Standardablauf: Der Leser gibt die Kriterien an, nach denen ein oder mehrere Sicherheitskonzepte gesucht werden sollen, und fordert die Suche an. Das System zeigt das Ergebnis an.

Aus dem oben beschriebenen Ablauf lassen sich die nachfolgenden zwei Anforderungen ableiten.

1. Das System muss eine Suchoption anbieten.
   Für das schnelle Herausfinden eines erforderlichen Sicherheitskonzeptes ist es nützlich, einen Filtermechanismus im System zu haben. Die Suchkriterien sind Dienst, Name des Sicherheitskonzeptes, Erstellungs- und Bearbeitungsdatum, Sicherheitskonzepterersteller. Diese können nach Bedarf erweitern werden.
   → Anforderung F36: Anzeigen aller dienstspezifischer Sicherheitskonzepte (je nach Berechtigung)
   → Anforderung F37: Suchen nach einem Sicherheitskonzept, das bestimmte Kriterien erfüllt

Oft ist es notwendig, ein Dokument auszudrucken oder in ein anderes Programm zu exportieren. Entsprechend dem Ziel des Exports verwendet man verschiedene Dateiformate. Der nächste Anwendungsfall präsentiert das Exportverfahren in ein beliebiges Format.

Anwendungsfall *Exportieren eines Sicherheitskonzeptes in eine Datei* (UC-14)
Akteur: Dienstverantwortlicher
Vorbedingung: Sicherheitskonzept ist im System vorhanden
Nachbedingung: Sicherheitskonzept in eine Datei erfolgreich exportiert
Standardablauf: Der Dienstverantwortliche wählt ein Sicherheitskonzept und das Dateiformat für Export und fordert das Exportieren an. Das System erstellt eine neue Datei mit dem ausgewählten Format.

Die folgenden Anforderungen lassen sich aus dem Anwendungsfall *Exportieren eines Sicherheitskonzeptes in eine Datei* ableiten:

1. Das System muss eine Möglichkeit bieten, das Sicherheitskonzept zu exportieren.
   An dieser Stelle muss man überlegen, welche Dateiformate für die zu entwickelnde Anwendung nützlich und sinnvoll sind. Vor allem muss eine Druckversion vorhanden sein. Das heißt, Export eines Sicherheitskonzeptes in ein PDF-Format muss möglich sein. Im Folgenden ist ein wichtiger Punkt der Datenaustausch zwischen verschiedenen Programmen. Da in Zukunft Export der Sicherheitskonzeptes ohne vertrauliche Daten oder Übernahme aus anderen Systemen einzelner Details, wie IP-Konfigurationen, Hardware-Rackpositionen und so weiter geplant sind, müssen mehrere für eine Datenübertragung geeignete Formate berücksichtigt werden [Hom14]. Als ein universales Metaformat gilt XML, das im Zusammenhang mit vielen Office Programmen, wie MS Excel und MS Word, eingesetzt werden oder über Internet Datentransport leisten kann. Für den Austausch von Daten zwischen verschiedenen Betriebssystemen können Textdateien(.txt oder .csv) benutzt werden.

→ Anforderung F38: Exportieren des Sicherheitskonzeptes in eine PDF-Datei
→ Anforderung F39: Exportieren des Sicherheitskonzeptes in eine XML-Datei
→ Anforderung F40: Exportieren des Sicherheitskonzeptes in eine Text-Datei
→ Anforderung F41: Exportieren des Sicherheitskonzeptes in eine HTML-Datei
→ Anforderung F42: Exportieren des Sicherheitskonzeptes in eine RTF/Word-Datei
→ Anforderung F43: Import-Schnittstelle

Die Abbildung 2.5 repräsentiert das Aktivitätsdiagramm, das den Verwaltungsprozess der Sicherheitskonzepte beschreibt. Der Vorgang beginnt mit der Auswahl eines Dienstes. Danach muss eine Entscheidung getroffen werden, was weiter gemacht wird: ein neues Sicherheitskonzept erstellen oder ein existierendes Sicherheitskonzept suchen. Entsprechend dem selektierten Befehl lässt sich die entsprechende Seite anzeigen. Ist noch kein Sicherheitskonzept für den selektierten Dienst im System vorhanden, wird die Vorlage zum Ausfüllen bereitgestellt. Sind die Änderungen in ein dienstspezifisches Konzept einzutragen, wird dies zum Bearbeiten aufgerufen. Dabei kann man dem Aktivitätsdiagramm entnehmen, dass das Editieren ein Sonderfall des Erstellverfahrens ist. Anschließend muss eine Fragengruppe ausgewählt werden. Die Abbildung zeigt, dass es von einer Frage zur anderen einen freien Übergang gibt. Ebenso existiert ein Übergang zu einer vorherigen und zu einer nachfolgenden Fragengruppe. Muss die Arbeit mit dem Sicherheitskonzept beendet werden, stellt die Anwendung zwei Möglichkeiten um sie abzuschließen zur Verfügung: Das Sicherheitskonzept kann zur weiteren Bearbeitung zwischengespeichert oder endgültig gespeichert werden. Im zweiten Fall führt das System eine Überprüfung durch, ob alle Eingaben plausibel sind. Sind sie unkorrekt, bekommt der Nutzer eine Warnmeldung und das Sicherheitskonzept ist zur Korrektur bereit. Ansonsten ist der Ablauf beendet.

2.3.3 Rollen- und Rechteverwaltung

Wie schon erwähnt, haben die Nutzer des zu entwickelnden Systems verschiedene Aufgaben und einen unterschiedlichen Verantwortungsgrad. Deswegen ist es wichtig zu unterscheiden, welcher Nutzer auf welche Ressourcen des Systems (Dateien, Funktionen, etc.) zugreifen darf. Eine weit verbreitete Zugriffskontrollstrategie ist die rollenbasierte Zugriffskontrolle (role-based access control, RBAC). Die Grundidee liegt darin, dass diese statt Vergabe von Rechten an jeden einzelnen Nutzer an eine bestimmte Rolle geknüpft wird. Der Benutzer bekommt Berechtigungen, indem er eine Rolle zugewiesen bekommt.

Nach einiger Zeit passiert es oft, dass die Einstellungen, die am Anfang eingesetzt wurden, nicht mehr passen. Das kann auch seine Rolle betreffen. Vor Beginn der Arbeit an der Anwendung legt der Administrator die Rollen samt Berechtigungen entsprechend der Vereinbarung beispielsweise mit dem Informationssicherheitsbeauftragten fest. Doch können später Änderungen in der Organisationsstruktur vom LRZ oder Sicherheitsrichtlinien auftreten. Um die Anwendungsfunktionalität und vor allem das Berechtigungskonzept von solchen Restrukturierungen unabhängig zu machen, sind das Hinzufügen neuer Rollen und eine flexible Berechtigungsvergabe zu realisieren. Die folgenden Anwendungsfälle beschreiben die Vorfälle, die eine flexible Rollenverwaltung ermöglichen.

Anwendungsfall *Anlegen und Speichern einer neuen Rolle* (UC-15)
Akteur: Administrator
Vorbedingung: Administrator befindet sich im Rollen-Einstellungsbereich

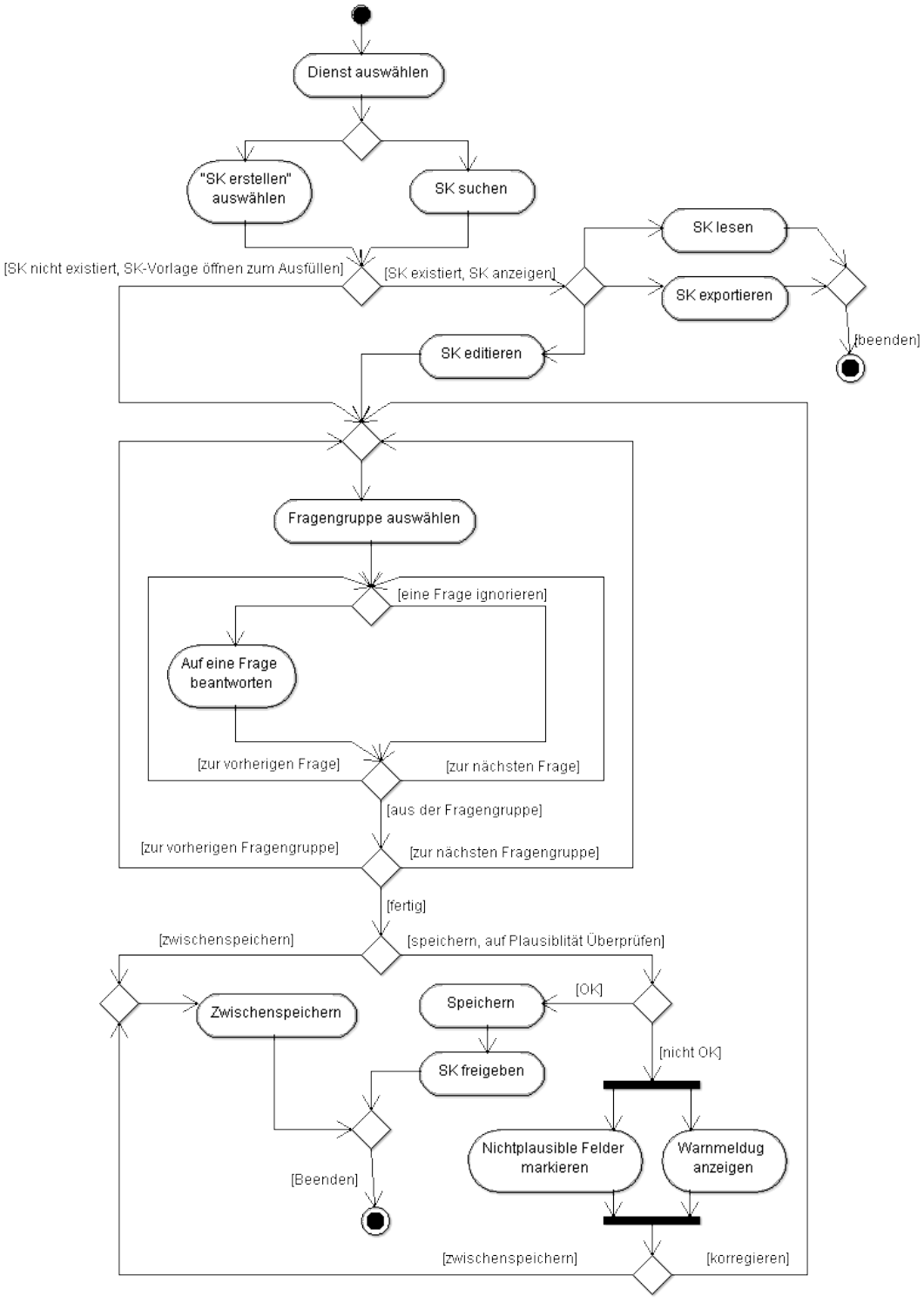


Abbildung 2.5: Aktivitätsdiagramm "Verwalten der Sicherheitskonzepte"

Nachbedingung: Eine neue Rolle ist angelegt. Die Rechte für diese Rolle bestimmt
Standardablauf: Der Administrator wählt einen Befehl zum Anlegen einer neuen Rolle aus, benennt die Rolle und fügt die Rechte zu dieser Rolle hinzu. Daneben entscheidet er, ob sie die Rolle mit administrativen Berechtigungen ist. Schließlich speichert er die Eingaben.

Anwendungsfall *Bearbeiten einer Rolle* (UC-16)
Akteur: Administrator
Vorbedingung: Administrator befindet sich im Rollen-Einstellungsbereich
Nachbedingung: Die Änderungen sind gespeichert
Standardablauf: Der Administrator wählt eine Rolle aus und danach den Befehl zum Bearbeiten. Er selektiert aus der vorgelegten Liste mit den Berechtigungen diejenigen, die der Rolle zugewiesen sind, und bestätigt ihre Übernahme. Sollen irgendwelche Rechte aus der Rolle entfernt werden, hakt der Administrator sie ab und bestätigt ihre Herausnahme. Nach Bedarf gibt der Administrator der Rolle einen neuen Name. Am Ende speichert er die Rollenmodifikation.

Aus den beiden Szenarios ergeben sich die folgen Anforderungen:

1. Das System muss einen rollen-basierten Zugriff unterstützen.
   Entsprechend wird es erwartet, dass das System über Rollenverwaltungsoptionen verfügt.
   → Anforderung F44: Anlegen und Speichern einer neuen Rolle
   → Anforderung F45: Bearbeiten einer Rolle
   → Anforderung F46: Löschen einer Rolle

2. Das System muss eine gewisse Menge an Berechtigungen bereitstellen. Im Unterschied zu Rollen können Berechtigungen nicht einfach hinzugefügt oder gelöscht werden. Das liegt daran, dass Rechte den im System vorhandenen Funktionalitäten entsprechen und normalerweise beim Entwicklungsprozess festgelegt werden. Aber die Flexibilität des Zugriffskonzeptes wird durch Hinzunahme oder Entfernen von Rechten bei einer Rolle erreicht.
   → Anforderung F47: Bereitstellen der Berechtigungen
   → Anforderung F48: Knüpfen der Berechtigungen an einer Rolle
   → Anforderung F49: Entfernen der Berechtigungen aus einer Rolle

Wie oben erwähnt, müssen Berechtigungen zum Programmierzeitpunkt vordefiniert werden. Welche Aufgaben im zu entwickelnden System sollen zulassungsbeschränkt sein? Bereits aus den oben beschriebenen Use Cases können einige Rechte formuliert werden. Alle Funktionalitäten, die sich auf einzelne Anwendungsfälle verteilen lassen, werden als potenzielle Berechtigungen angesehen. Ausgenommen sind diejenige Aktivitäten, die ein Use Case verfeinern und nur als Bestandteil dieses ausführbar sind. Dazu gehören UC-2 , UC-3 und UC-4. Dabei ist zu beachten, dass eine zu feine Rechteverteilung schnell zur Unübersichtlichkeit führen kann. Hier die Auflistung der Anforderungen für ein Berechtigungskonzept:

→ Anforderung F50.1: Das Recht eine Sicherheitskonzept-Vorlage zu erstellen
→ Anforderung F50.2: Das Recht eine Sicherheitskonzept-Vorlage zu bearbeiten
Obwohl die Use Cases UC-1 und UC-5 der Administrator ausführt, kann es später passieren, dass der Subadministrator das Eintragen von Änderungen übernimmt. Auf jeden Fall ist es besser diese beiden Funktionalitäten getrennt zu halten.

→ Anforderung F50.3: Das Recht eine Sicherheitskonzept-Vorlage freizugeben
Die Freigabe einer Vorlage darf eine begrenzte Anzahl von Nutzern durchführen. Dieses Argument weist auf die Notwendigkeit hin, die Freigabe als separates Recht zuweisen zu können.

→ Anforderung F50.4: Das Recht dienstspezifische Fragen und Fragengruppen einer Sicherheitskonzept-Vorlage hinzuzufügen
→ Anforderung F50.5: Das Recht dienstspezifische Fragen und Fragengruppen in einer Sicherheitskonzept-Vorlage zu bestimmen
Diese beiden Aufgaben können vom Dienstverantwortlichen übernommen werden. Das Hinzufügen neuer dienstspezifischen Fragen und Fragengruppen führt zur Änderung der Vorlagenstruktur.

→ Anforderung F50.6: Das Recht ein dienstspezifisches Sicherheitskonzept zu erstellen
→ Anforderung F50.7: Das Recht ein dienstspezifisches Sicherheitskonzept zu bearbeiten
→ Anforderung F50.8: Das Recht ein dienstspezifisches Sicherheitskonzept freizugeben
Ähnlich wie die Trennung von Berechtigungen für die Sicherheitskonzept-Vorlageverwaltung, sind die Rechte für die Sicherheitskonzeptverwaltung definiert.

→ Anforderung F50.9: Das Recht ein dienstspezifisches Sicherheitskonzept zu exportieren
Welche Inhalte von Sicherheitskonzeptes exportiert und an Dritte übergeben werden können, darf wiederum nur ein begrenzter Kreis von Nutzern entscheiden. Deswegen muss das Exportieren als ein autonomes Recht bestimmt werden.

→ Anforderung F50.10: Das Recht ein dienstspezifisches Sicherheitskonzept zu lesen
Dieses Recht gibt Gelegenheit den Inhalt von Sicherheitskonzeptes durchzulesen. Es ist denkbar, dass alle Nutzer, die den Zugang zur in Entwicklung befindlichen Anwendung haben werden, eventuell ein Leserecht erhalten.

→ Anforderung F50.11: Das Recht eine neue Rolle anzulegen
Beim Anlegen einer neuen Rolle müssen gleichzeitig deren Berechtigungen definiert werden. Normalerweise dürfen nur Administratoren neue Rollen anlegen, da durch die Rechtebestimmung die Zugriffskontrolle auf die Aufgabenebene erfolgt.

→ Anforderung F50.12: Das Recht Administratorrollen an andere Benutzer zu delegieren
→ Anforderung F50.13: Das Recht Rollen (außer Administratorrollen) an andere Benutzer zu delegieren
Da in der Regel der Administrator über alle oder fast alle Rechte verfügt, sollte man vorsichtig mit dem Zuweisen von Administratorrollen sein. Aus Sicherheitsgründen muss die Vergabe von Rollen mit administrativen Berechtigungen von einer streng begrenzten Anzahl an Personen erfolgen und die Anzahl derjenigen Nutzer, denen solche Rollen zugewiesen werden, ist möglichst zu beschränken. Diese Beschränkungen gelten nicht für andere Rollen, diese können nicht nur von Administratoren verteilt werden. Deswegen teilt man hier die Rollenvergabe in zwei separate Funktionen.

→ Anforderung F50.14: Das Recht einen Dienst hinzufügen und bearbeiten
→ Anforderung F50.15: Das Recht einen Dienst löschen

Die Dienste können sowohl von einem Administrator als auch von einem Dienstverantwortlichen hinzugefügt werden. Im Gegenzug sollte mit dem Entfernen von Diensten vorsichtig umgegangen werden. Da es im zu entwickelnden Konzept viele Funktionalitäten gibt, die nur nach der Dienstauswahl ausgeführt werden können, kann das zufällige Löschen eines Dienstes unerwünschte Ergebnisse herbeiführen. Zum Beispiel die Unmöglichkeit das Sicherheitskonzept für diesen Dienst aufzurufen oder in der Vorlage dienstspezifische Fragen zu kennzeichnen. Aus diesen Gründen muss man die Berechtigung, Dienste zu löschen, von anderen Dienstmanipulationen trennen.

→ Anforderung F50.16: Das Recht Dienste den Benutzern zuzuweisen
Das Zuweisen von Diensten an den Benutzer ist vergleichbar mit der Rollenvergabe. Die Verantwortlichen müssen entscheiden, für welche Dienste der betreffende Benutzer Optionen der Anwendung nutzen darf.
→ Anforderung F50.17: Das Recht einen neuen Benutzer hinzufügen und zu bearbeiten
→ Anforderung F50.18: Das Recht einen Benutzer zu löschen
Es werden wieder Rechte zum Verwalten und Löschen getrennt.

Da die Zuständigkeiten und Aufgaben in jeder Abteilung des LRZ hierarchisch geordnet sind, können die Rollen auch hierarchisch aufgebaut werden. In dem RBAC1-Model lässt sich die Rollenhierarchie folgendermaßen definieren: $y \leq x$, was bedeutet: Rolle x erbt alle Rechte von Rolle y, d.h. "x darf alles was y darf (und mehr)" [sz104]. Auf Basis dieses Zugriffskontrolle-Modells (RBAC1) lassen sich die Rollen für das neue System bestimmen.

Das System muss von mindestens einer Person administriert sein. Dafür braucht man einen **Administrator**. Er hat alle Rechte im System. Aus der Abteilungsstruktur folgt, dass jeder Abteilungsleiter die administrativen Berechtigungen haben darf, da er sich auf der obersten Ebene der Hierarchie befindet. Aber er ist nur für seine Abteilung zuständig. Dies führt zu der Entscheidung, noch eine Rolle mit administrativen Berechtigungen, **Subadmin**, anzulegen, die aber auf einige Aufgaben beschränkt ist. Dann müssen die Aufgaben von Gruppen- und Teamleiter in einer Rolle, der des **Dienstverantwortlicher**, zusammengefasst werden. Sein Zuständigkeitsbereich erstreckt sich auf eine Gruppe und er hat noch weniger Rechten als ein Subadministrator. Die Mitarbeiter, die sich direkt mit den Diensten beschäftigen, können der Rolle **Dienstbetreibern** zugeteilt werden. Auf der unteren Ebene der Hierarchie befindet sich die Rolle mit den minimalen Rechten, in dieser Arbeit **Operateur** genannt. Dazu gehören die Nutzer, die keine Sicherheitskonzepte verwalten und sie nur lesen dürfen. Diese Rollen können nach RBAC1-Modell in der folgenden Reihenfolge angeordnet werden:
Leser < Dienstbetreiber < Dienstwerantwortlicher < Subadmin < Admin

Solche hierarchische Rollenstruktur ist ein Vorschlag. Durch die flexible Berechtigungsvergabe können Rollen nach einem anderen entsprechenden den Bedürfnissen des LRZ Schema verteilt werden.

2.3.4 Dienstverwaltung

Ein Sicherheitskonzept wird für einen Dienst erstellt. Es dokumentiert seinen aktuellen Stand und seine Eigenschaften. Der Dienst im zu entwickelnden Konzept hat eine große Bedeutung. Dieser Abschnitt beschreibt die Abläufe in der Dienstverwaltung.

Es folgen die Use Cases, die das Erstellen von Diensten und Dienstgruppen beschreiben.

Anwendungsfall *Erstellen einer neuen Dienstgruppe*(UC-17)
Akteur: Administrator
Vorbedingung: Die Dienstgruppe ist noch nicht im System eingetragen
Nachbedingung: Eine neue Dienstgruppe ist im System gespeichert
Standardablauf: Der Administrator erstellt eine neue Dienstgruppe, vergibt ihr einen Name, schreibt bei Bedarf einen Kommentar und speichert sie.

Anwendungsfall *Erstellen eines neuen Dienstes*(UC-18)
Akteur: Administrator
Vorbedingung: Der Dienst ist noch nicht ins System eingetragen
Nachbedingung: Ein neuer Dienst ist ins System eingetragen und einer Dienstgruppe hinzugefügt.
Standardablauf: Der Administrator wählt eine Dienstgruppe aus, erstellt innerhalb dieser Gruppe einen neuen Dienst, benennt ihn, gibt einen Kommentar ab und speichert ihn. Wenn mehrere Dienste zu dieser Dienstgruppe gehören, wiederholt der Administrator den letzten Schritt.

Aus den oben dargestellten Abläufen lassen sich die folgenden Anforderungen ableiten:

1. Das System muss die Möglichkeit bieten, Dienste anzulegen und sie zu gruppieren. Dabei kann jeder Dienst nur exakt einer Gruppe zugeordnet werden. Eine Dienstgruppe kann aus einem oder mehreren Diensten bestehen.
   → Anforderung F51: Erstellen und Speichern einer neuen Dienstgruppe
   → Anforderung F52: Erstellen und Speichern eines neuen Dienstes
   → Anforderung F53: Einfügen eines Dienstes in eine Dienstgruppe
   Daneben muss die Bearbeitung von Diensten und Dienstgruppen ermöglicht werden. Mit Bearbeitung ist das Umbenennen sowie das Abgeben von Kommentaren gemeint.
   → Anforderung F54: Bearbeiten eines Dienstes
   → Anforderung F55: Bearbeiten einer Dienstgruppe

2. Das System muss die Möglichkeit bieten, einen Dienst von einer Dienstgruppe in eine andere zu überführen.
   Da unter "Dienste" sowohl Sicherheitskonzeptes und Fragen als auch Rollen und Nutzer zusammengefasst werden, ist ein Dienst eine sehr wichtige Einheit im gesamten Konzept. Jeder Dienst darf nicht einfach gelöscht und danach wieder neu erstellt werden. Beim Wechseln der Gruppe bleibt die Dienstidentität unveränderbar.
   → Anforderung F56: Überführen eines Dienstes von einer Dienstgruppe in eine andere
   Neben den Erstellenfunktionen müssen natürlich Funktionen für Bearbeiten und Löschen der Dienste vorhanden sein. Das Löschen eines Dienstes muss normalerweise vermieden und kann nur vom Administrator durchgeführt werden.
   → Anforderung F57: Löschen eines Dienstes

Obwohl sich die Verwaltung von Diensten auf die oben genannten Funktionen begrenzt, darf man die Rolle eines Dienstes nicht unterschätzen. Er ist eng mit dem Sicherheitskonzept und mit den Benutzern verknüpft. Im nächsten Abschnitt wird näher auf den Zusammenhang von Diensten, Benutzer und Rollen eingegangen.

2.3.5 Benutzerverwaltung

Ein Verwaltungssystem ist ohne Benutzerverwaltung kaum vorstellbar. Sie beginnt mit der Registrierung eines Benutzers im System. Normalerweise steht dem Benutzer eine Option zum Erstellen eines Accounts zum Verfügung. Dort können persönliche Daten gespeichert und bearbeitet werden. Der minimalen Satz besteht aus Name, Vorname, Benutzername, Passwort und E-Mail-Adresse. Da am LRZ alle Daten von Mitarbeitern zentral gespeichert sind, reichen die oben genannten Metadaten für eine neue Anwendung aus. Für das System ist es vor allem wichtig, dass neue Benutzer im System gespeichert und ihm eine Identifikationsnummer (ID) zugeordnet wird. Das System "erkennt" den Benutzer an seiner ID und stellt ihm gemäß seinen Berechtigungen eine entsprechende Oberfläche sowie Funktionen zur Verfügung. Dagegen erkennen die Nutzer einander an ihrem Namen und Vornamen. Login und Passwort sind beim Einloggen ins System nötig und eine E-Mail-Adresse für die Benachrichtigungs- und Erinnerungsfunktion.

Wie bereits erwähnt, ist die gesamte Information über LRZ-Mitarbeiter, ihre Kontaktdaten und Benutzer-Account-Daten (ID-Logins und Passwörter) auf einem Server zentral gespeichert und dort von einem Administrator verwaltet. Es gibt viele Vorteile dieser Lösung. Einige davon sind, dass ein Benutzer sich nur ein Passwort merken muss und die Verwaltung aller Benutzerdaten zentral erfolgt, was Zeitaufwand und Speicherressourcen spart. Die zu entwickelnde Anwendung sollte sowohl die Aufnahme von Benutzern aus einem externen Verzeichnissystem als auch das Anlegen eines neuen Benutzers und seines Benutzer-Account unmittelbar im System berücksichtigen.

Die folgenden Schritte beschreiben den Ablauf bei der Benutzerregistrierung.

Anwendungsfall *Registrieren eines neuen Benutzers* (UC-18)
Akteur: Administrator
Vorbedingung: Ein neuer Benutzer ist noch nicht im System registriert.
Nachbedingung: Ein neuer Benutzer wurde im System erfolgreich gespeichert. Ihm werden eine Dienstgruppe und eine Rolle für diese Dienstgruppe zugewiesen. Der Benutzer hat einen Login und ein Passwort für den Zugang zum System.
Standardablauf: Der Administrator wählt den Befehl für das Hinzufügen eines neuen Benutzers aus und schickt die Anfrage mit dem Namen des Nutzers über den Proxy-User an den LDAP-Server. Nachdem er eine positive Antwort bekommen hat, speichert er die ID des Benutzers im System. Dann weist er dem Benutzer eine Gruppe von Diensten zu und vergibt für jede Dienstgruppe eine oder mehrere Rollen. Das System speichert die Eingaben und schickt eine Bestätigung für den Zugang zum System per Mail an einen neuen Benutzer.
Alternativeablauf: Ist das Benutzen von LDAP aus irgendwelchen Gründen nicht möglich, gibt der Administrator die Kontaktdaten des neuen Benutzers, Login und Password an und speichert sie im System. Dann folgen die Schritte der Dienst- und Rollenvergabe (wie beim Standardablauf).

Die nächstfolgenden Anforderungen lassen sich aus dem Use Case *Registrieren eines neuen Benutzers* ableiten:

1. Das System sollte die Möglichkeit bieten, für die Authentifizierung von Benutzern ein externes Authentifizierungssystem zu nutzen.

Integrieren einer LDAP-Schnittstelle für den Zugriff auf Verzeichnisdienste bietet mehrere Vorteilen. Einmal zentral erfasste Mitarbeiterdaten müssen nicht zusätzlich in einer neuen Anwendung erfasst werden. Die Verwaltung der Nutzerdaten, also z. B. Kontaktdaten, Login-IDs und Passwörter, wird nicht vom Administrator der Anwendung, sondern von einem Administrator eines Verzeichnisdienstes durchgeführt.
→ Anforderung F58: Eine integrierte LDAP-Schnittstelle für die Authentifizierung von Benutzer

2. Das System sollte die Möglichkeit bieten, einen neuen Benutzer anzulegen.
   → Anforderung F59: Anlegen der persönlichen Daten des Benutzers
   Wie oben schon erwähnt, ist die Eingabe von Vorname, Nachname und E-Mail völlig ausreichend.
   → Anforderung F60: Anlegen von Login und Passwort für für den Benutzer
   → Anforderung F61: Der Zugriff auf die Daten erfolgt passwortgeschützt
   Nach der erfolgreichen Authentifizierung des Benutzers wird eine Liste von Diensten bereitgestellt, für die er gemäß seinen Berechtigungen seine Aufgaben erfüllen kann.
   → Anforderung F62: Zuweisen von Dienstgruppe(n) an einen Benutzer
   → Anforderung F63: Zuweisen einer Rolle an eine Dienstgruppe

3. Das System muss die Möglichkeit bieten, eine E-Mail an den Benutzer zu senden
   → Anforderung F64: Integrierte E-Mail-Funktion
   → Anforderung F65: Benachrichtigung- und Erinnerungsfunktion per Mail

Da in der Regel die Mitarbeiter einer Abteilung aus Sicherheitsgründen nicht auf die Dokumentation von Diensten anderer Abteilung zugreifen dürfen, ist es nicht ausreichend, nur Berechtigungen für den Zugriff auf Aufgaben zu definieren. Die Zugriffskontrolle soll zweidimensional angelegt sein. Einerseits soll dem Benutzer je nach seiner Rolle der Zugriff auf bestimmte Funktionen des Systems beschränkt werden. Anderseits darf der Benutzer nur auf Dienste zugreifen, für die er Rechte hat. Durch Zuweisung von Diensten auf jeden im System einzutragenden Benutzer, entsprechend seiner Zuständigkeit für diese, und Vergabe einer Rolle für diese Dienste, erreicht man die angeforderte Zugriffskontrolle.

Das untenstehende Bild 2.6 stellt diesen Vorgang dar. Dem Benutzer sind zwei Gruppen von Diensten zugewiesen: eine blau und eine grüne. Die blaue Gruppe enthält zwei Dienste, die grüne umfasst einen Dienst. Für jeden dieser Dienste bekommt der Nutzer eine Rolle mit Aufgaben. Daneben ist eine (rote) Rolle für beide Dienstgruppen, grün und blau, vergeben. Jetzt darf der Nutzer entsprechend den Rollen die Sicherheitskonzepte für die Dienste aus der blauen Gruppe erstellen und bearbeiten, das Sicherheitskonzept für den Dienst aus der grünen Gruppe durchlesen und alle Sicherheitskonzepte freigeben.
Daraus folgt, dass es das System ermöglichen muss, den Zugriff auf die Aufgaben und die Dienste gleichzeitig kontrollieren zu können.
→ Anforderung F66: Zweidimensionale Zugriffskontrolle durch Zuweisung von Rollen und Diensten
Um diesen Zugriffskonzept zu ermöglichen, sollen im System die entsprechenden Funktionen vorgesehen werden.
Nachdem der Benutzer erfolgreich registriert ist, darf er sich ins System einloggen. Der nachfolgende Anwendungsfall stellt das Login-Verfahren dar.

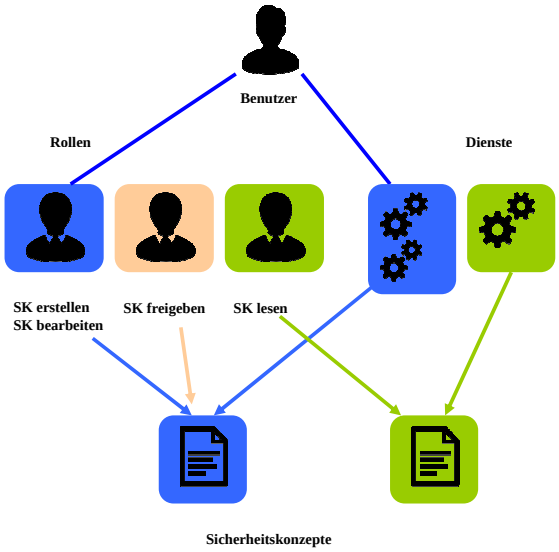


Abbildung 2.6: Zweidimensionale Zugriffskontrolle

Anwendungsfall *Einloggen ins System*(UC-19)
Akteur: unautorisierter Benutzer
Vorbedingung: Das System bietet Eingabefelder für Login und Passwort.
Nachbedingung: Der Benutzer ist im System erfolgreich authentifiziert und autorisiert
Standardablauf: Das System fordert Login- und Passworteingabe an. Der Benutzer gibt Login und Passwort ein. Ist der Benutzer identifiziert und ist das eingegebene Passwort valide, bekommt der Benutzer einen Zugang auf die Anwendung. Das System überprüft, für welche Dienste der Benutzer Berechtigungen hat und zeigt die Liste von diesen Diensten an.
Alternativeablauf: Ist Login oder Passwort falsch, gibt das System eine Fehlermeldung aus. Der Benutzer bekommt keinen Zugang auf das System.

Das Anlegen von Rollen und Diensten sowie das Registrieren eines Benutzers sind im Aktivitätsdiagramm 2.7 zusammengefasst. Aus dem Diagramm folgt, dass Rollen, Dienste und Benutzer parallel hinzugefügt werden können. Aber eine Dienstzuweisung kann nur dann erfolgen, wenn es mindestens einen Dienst im System gibt.

Aus den dargelegten Anwendungsfällen wurden die funktionalen Anforderungen abgeleitet, mit denen sich die Systemfunktionalität vollständig beschrieben lässt. Neben den funktionalen Anforderungen gibt es auch nicht-funktionale Eigenschaften des System, deren Bedeutung jedoch ebenfalls sehr groß ist. Im nächsten Abschnitt wird auf die nicht-funktionalen Anforderungen genauer eingegangen.

2.4 Nicht-funktionale Anforderungen

Nicht-funktionale Anforderungen beziehen sich nicht auf eine Funktionalität des Systems, sondern auf das gesamte System, in dem die geforderte Funktionalität zu erbringen ist. In diesem Abschnitt werden nicht-funktionale Anforderungen formuliert, jede von denen wird

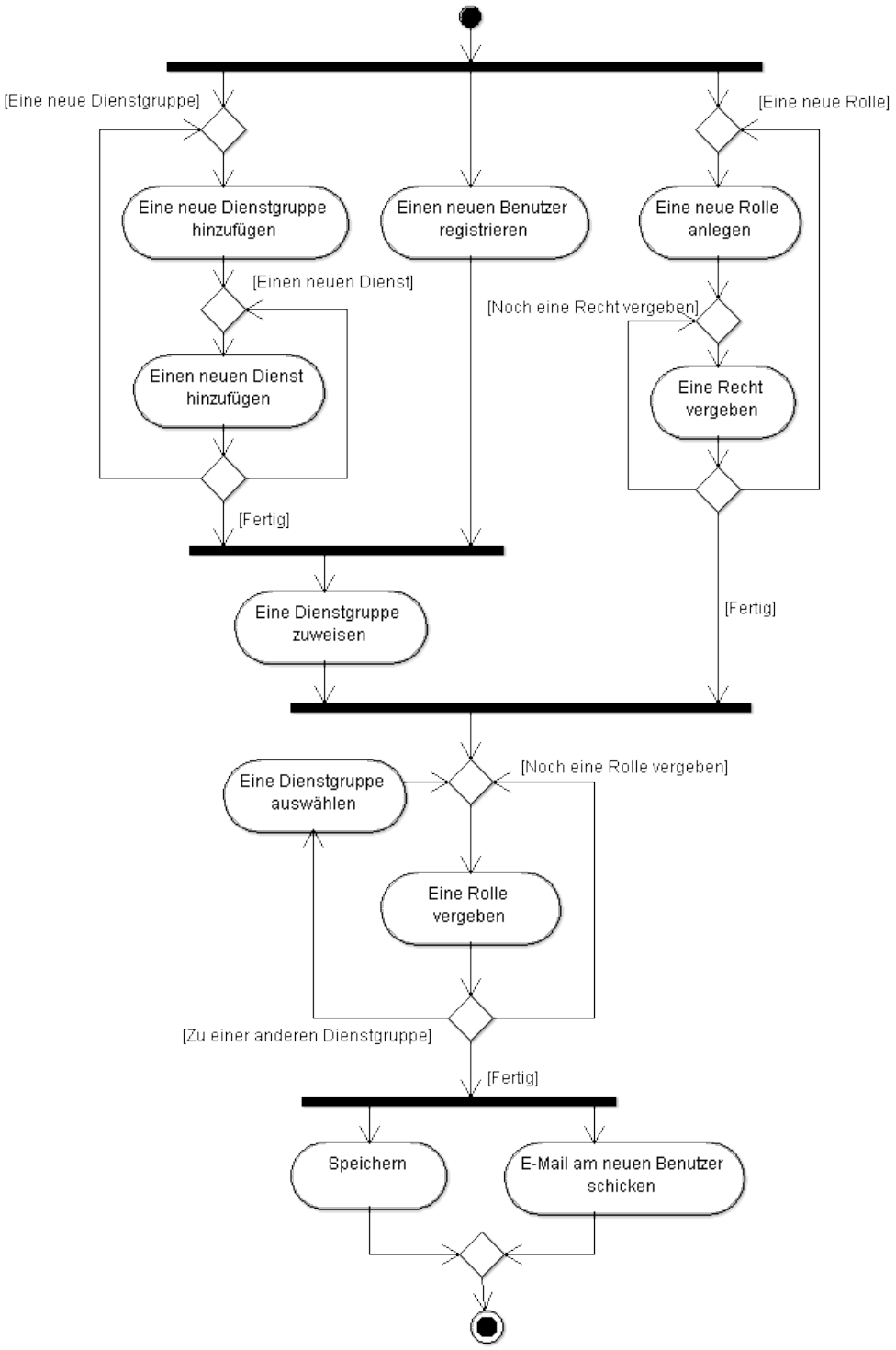


Abbildung 2.7: Aktivitätsdiagramm "Benutzer registrieren"

mit den Buchstaben "NF" und ihrer Nummer bezeichnet.

Technische Anforderungen:

Da es sich um vertrauliche Dokumentation handelt, müssen die Sicherheitskonzepte lokal im LRZ verwaltet und gespeichert werden (keine Cloud-Dienste, keine Online-Speicher).
→ Anforderung NF01: Die Anwendung muss auf einem System des LRZ installiert werden

Das LRZ verfügt über 2.000 bis 2.500 Linux-Server und ca.100 bis 150 Windows-Server. Deswegen wäre es wünschenswert, dass das neue System mit dem Betriebssystem Linux bzw. Debian und SUSE kompatibel wäre.
→ Wünschenswert NF02: Die Anwendung soll auf einer Linux-Plattform lauffähig sein

Qualitätsanforderungen:

Die Software muss nicht nur funktional sein, sondern sich auch auf dem aktuellen Stand der Technik befinden.
→ Anforderung NF03: Software muss dem aktuellen Stand der Softwaremöglichkeiten entsprechen
→ Anforderung NF04: Die Anwendung muss fehlerfrei funktionieren

Kulturelle Anforderungen:

Am LRZ sind sowohl deutschsprachige als auch internationale englischsprachige Mitarbeiter tätig. Deswegen ist mindestens eine von beiden Sprachen Voraussetzung und sind beide wünschenswert.
→ Anforderung NF05.1: Die Anwendung muss die deutsche oder die englische Sprache unterstützen.
→ Anforderung NF05.2: Die Anwendung muss Deutsche und Englische Sprache unterstützen

Benutzerfreundlichkeit:
Der Anwendung muss über eine Benutzeroberfläche verfügen, so dass ein Benutzer ohne Programmierkenntnissen die Anwendung bedienen und alle Funktionalitäten nutzen kann.
→ Anforderung NF06: Das System darf vom Benutzer keine Programmierkenntnisse verlangen
→ Anforderung NF07: Die Anwendung muss eine intuitiv bedienbare Benutzeroberfläche haben
→ Anforderung NF08: Die Dokumentation zur Installation der Anwendung muss vorhanden sein
Eine mangelhafte Installationsanweisung erhöht den Zeitaufwand.
→ Anforderung NF09: Ein Benutzerhandbuch muss vorhanden sein
→ Anforderung NF10: Die Bedienung des Systems muss leicht erlernbar sein. Die ausreichende und gut geschriebene Dokumentation vereinfacht den Lehrprozess
→ Anforderung NF11:Anpassungen an LRZ Corporate Identity (Logo, Firmenfarben)
Im Arbeitsprozess des LRZ ist es wichtig, dass mehrere Benutzer gleichzeitig auf die gespeicherten Daten zugreifen können. Aber die Datenkonsistenz muss gesichert und kontrolliert werden.
→ Anforderung NF12: Mehrbenutzer Betrieb

Wirtschaftliche Randbedingungen:

Unter den wirtschaftlichen Randbedingungen versteht man hier alle Kosten, die zum Erwerb und für den Einsatz einer Software erforderlich sind. Da im Rahmen dieser Arbeit keinen Budget für das Evaluation-Phase vorgesehen ist, sollen Auswahl-, Installation- und Testverfahren keine Kosten mit sich bringen.
→ Anforderung NF13: Kostenlos

Rechtliche Randbedingungen:

Vom LRZ ist geplant, der Quellcode der zu entwickelnden Anwendung unter Public License zu veröffentlichen. Das heißt, der Quellcode kann von den Anwendern genutzt, verändert und mittels klarer Lizenzregelungen auch weiter verteilt werden. Neben dem freien Zugang zum Quellcode bringt Open-Source-Software eine Unterstützung durch eine breite Community mit sich. Einige der Vorteilen der kollaborativen Entwicklung sind kontinuierliche Erweiterungen des Produkts, frühzeitige Erkennung und schnelle Behebung der Fehler.
→ Anforderung NF14: Open Source

Weitere Rahmenbedungungen:

Die Anwendung sollte keine Begrenzung von Ressourcen verlangen. Da die bereits vorhandene Sicherheitskonzept-Vorlage aus circa 140 Fragen und Unterfragen besteht und in Zukunft noch erweitert werden soll, ist keine Beschränkung hinsichtlich der Anzahl von Fragen erwünscht. Das betrifft auch die Anzahl der dienstspezifischen Sicherheitskonzepte, da das LRZ derzeit rund 80 Dienste umfasst. Dementsprechend sollte die Anzahl der Mitarbeiter nicht beschränkt werden.
→ Anforderung NF15: Unbegrenzte Anzahl der Fragen
→ Anforderung NF16: Unbegrenzte Anzahl von Sicherheitskonzept
→ Anforderung NF17: Unbegrenzte Anzahl von Benutzern

Im nächsten Kapitel werden alle ermittelten Anforderungen in einem Katalog zusammengefasst.

2.5 Priorisieren der Anforderungen

Im Rahmen dieser Arbeit wurde insgesamt über 100 Anforderungen ermittelt. Aber nicht alle Anforderungen sind gleich wichtig. Es gibt die zwingend erforderlichen Anforderungen, die wichtigsten Leistungsmerkmale der Software identifizieren. Sie sind entscheidend. Ganz anderer Fall sind die Kriterien, die obwohl gewünscht sind und erhöhen die Zufriedenheit des Benutzers, aber ohne sie die Hauptziele erreicht werden können. Für die Praxis ist es üblich, dass nicht alle Wünsche realisierbar sind. Um Anforderungen in einer langen Kriterienliste von ein ander nach Wichtigkeit zu trennen und zu betonen, setzt man unter den gesammelten Kriterien Prioritäten. Es gibt mehrere Methoden für Strukturierung und Klassifikation von Anforderungen.[4] In dieser Arbeit wird ein einfaches Schema verwendet. Die

[4] z.B. MoSCoW-Analyse
MoSCow steht für:
M = Must = unbedingt erforderlich

Anforderungen werden in zwei Gruppen geteilt: MUSS-Anforderungen und Anforderungen, die wünschenswert sind.
Im Weiteren wird es begründet und festgestellt, welche der Anforderungen zwingend erforderlich und welche Punkte optional sind.

Die Grundlegende Aufgaben zum Erstellen, Speichern, Aufrufen, Bearbeiten, Löschen und Freigeben von Sicherheitskonzept-Vorlage und von Sicherheitskonzepten sind MUSS-Anforderungen. Das sind die wichtigsten Operationen bei der Verwaltung von Dokumenten.

Da die Mustervorlage hat Form eines Formulars, gehören die grundlegende Funktionalitäten zum Formularbilden auch zu wichtigen Kriterien. Das sind Fragen- und Fragengruppenerstellung, Fragetypenauswahl und logische Verknüpfung der Fragen mit einander. Wobei in der Dokumentvorlage Freitext, Mehrfachauswahl und eine Antwortalternative am häufigsten vorkommen. Mit diesen drei grundlegenden Fragenarten und mit der Voraussetzung, dass die Fragen sich je nach gegebener Antwort anzeigen lassen, erreicht man eine dynamische Struktur des Fragebogens. Alle weiteren Fragetypen obwohl erwünscht sind, aber sind nicht notwendig und können mit Hilfe eines von drei oben erwähnten Typen ersetzt werden. Beispielweise kann Datum in einem Freitextfeld eingegeben werden. Verwaltungsoperationen von allen Formularelementen gehören zu erforderlichen Anforderungen. Beispiele sind dafür Hinzufügen einer neuen Antwortalternative oder die Änderung des Fragetextes.

Die Beschränkung der Eingabewerten auf bestimmten Kriterien und Überprüfung der Eingaben auf Plausibilität sind wünschenswert. Es ist nett zu haben eine Möglichkeit, die Reihenfolge der Fragen- und Fragengruppen zu ändern. Obwohl die Mitteilung des Benutzers über Aktivitäten des Systems und das Markieren von Pflichtfeldern oder neuen hinzugefügten Fragen erhöhen die Benutzerfreundlichkeit der Anwendung, sind aber optional.

Einen wichtigen Punkt ist die Navigation in einem Dokument. Da es um einen ziemlich langen Dokument handelt, muss die Sprung von Abschnitt zum Abschnitt möglich sein. Daneben ist das Zwischenspeichern eines teilweise ausgefüllten Dokument erforderlich.

Man benötigt mindestens eine Exportmöglichkeit. Hierbei wurde der PDF-Export gewählt, da man oft eine Druck-Version des Dokuments benötigt. Zudem muss die Berechtigung für das Exportieren berücksichtigt werden, weil Sicherheitskonzepte vertrauliche Daten enthalten können. Das Exportieren in andere Dateiformate ist optional. Importieren und Suchen von Sicherheitsdokumenten, Speichern von Antwortalternativen als Schablonen, Kopieren von Fragen und Fragengruppen - alle diese Optionen erleichtern die Arbeit und sind als die wünschenswerten Anforderungen gewichtet.

Einer der wichtigsten Teile des Konzeptes ist Zugriffskontrolle auf die gespeicherten Daten. Deswegen ist Möglichkeit die Rechte für den Benutzer zu bestimmen und sie an der Rollen zu vergeben ist notwendig. Die Berechtigungen für Verwaltungsaktionen (siehe oben) sind erforderlich. Die Beispiele sind das Recht zum Erstellen der Vorlage, das Recht die

S = Should = sollte umgesetzt werden, wenn alle Must-Anforderungen trotzdem erfüllt werden können
C = Could = kann umgesetzt werden, wenn die Erfüllung von höherwertigen Anforderungen nicht beeinträchtigt wird
W = Won't = wird diesmal nicht umgesetzt, aber für die Zukunft vorgemerkt [Klü12]

Vorlage zu Löschen oder Freigeben. Die wichtigste Tatsache ist, dass Zugriff auf zwei Ebene kontrolliert ist: Auf Dienst- und auf Aufgabe-Ebene. Dienst-Anlegen und -Verwalten sind notwendig für die Trennung von Mandanten und von dienstspezifischen Dokumenten.

Es ist offensichtlich, dass Verwaltung von Benutzern eine MUSS-Anforderung ist. Benutzer müssen angelegt, bearbeitet und gelöscht werden können. Außerdem müssen ihm Zugangsdaten für Zugang ins System vergeben werden. Eine integrierte E-Mail ist wünschenswert, da ihre Präsenz die Kommunikation zwischen dem Benutzer und System vereinfacht. Außerdem ist eine integrierte LDAP-Schnittschtelle gern gesehen.

Die Unterstützung Deutscher oder Englischer Sprache ist eine Voraussetzung. Ebenfalls ist die Installation der Anwendung auf dem System des LRZ zwingend erforderlich. Das Vorgehen bei der Installation muss eindeutig dokumentiert. Da für das Projekt keinen Budget vorhanden ist, müssen die Entwicklung und die Umsetzung der Software keine Kosten verlangen. Die Veröffentlichung der Programmlösung muss unter einer der OpenSource License erfolgen.

Alle ermittelten Anforderungen mit gesetzten Prioritäten sind in der Tabelle 2.8 zusammengefasst. Die unverzichtbare Anforderungen werden mit Buchstabe "A" (steht für "Anforderung") und die wünschenswerte Anforderungen mit Buchstabe "W" (steht für "Wünschenswert") gekennzeichnet.

Nummer	Beschreibung	Priorität
Funktionale Anforderungen		
Verwaltung der Sicherheitskonzept -Vorlage		
F01	Erstellen und Speichern der Sicherheitskonzept-Vorlage	A
F02	Zwischenspeichern des Entwurfs der Sicherheitskonzept-Vorlage	A
F03	Erstellen von Fragen	A
F04	Gruppieren von Fragen in Fragengruppen	A
F05	Auswahl von Fragentypen	A
F05.1	Der Fragentyp „Freitext“	A
F05.2	Der Fragentyp „Mehrere Antwortalternativen“	A
F05.3	Der Fragentyp „Exakt eine Antwortalternative“	A
F05.4	Der Fragentyp „Datum“	W
F05.5	Der Fragentyp „Uhrzeit“	W
F05.6	Der Fragentyp „Tabelle“	W
F06.1.1	Beschränken des Eingabewertes auf Typ: Nummer	W
F06.1.2	Beschränken des Eingabewertes auf Typ: Buchstaben	W
F06.2	Beschränken des Eingabewertes auf Anzahl von Zeichen	W
F06.3	Beschränken des Wertebereiches eines Eingabewertes	W
F07	Markieren von Frage als „Pflichtfeld“	W
F08	Verknüpfen einer Frage mit einer Bedingung	A
F09	Verknüpfen einer Fragegruppe mit einer Bedingung	W
F10	Speichern der Antwortalternativen als Schablone	W
F11	Aufrufen der Sicherheitskonzept-Vorlage zur Vorschau	A
F12	Freigabe der Sicherheitskonzept-Vorlage	A
F13	Deaktivieren der Sicherheitskonzept-Vorlage	W
F14	Aufrufen der Sicherheitskonzept-Vorlage zum Bearbeiten	A
F15	Ändern der Reihenfolge der Fragen	W
F16	Ändern der Reihenfolge der Fragengruppen	W
F17	Ändern des Fragen- und Fragengruppentextes	A
F18	Einfügen einer neuen Antwortalternative zu einer Frage	A
F19	Markieren neu hinzugefügter in der Sicherheitskonzept-Vorlage Fragengruppen, Fragen und Antwortalternativen.	W
F20	Löschen einer Antwortalternative	A
F21	Löschen einer Frage	A
F22	Löschen einer Fragengruppe	A
F23	Öffnen der Sicherheitskonzept-Vorlage zum Bestimmen von dienstspezifischen Fragen und Fragengruppen	W
F24	Ein- und Ausblenden von dienstspezifischen Fragengruppen/Fragen	W
Verwaltung der dienstspezifischen Sicherheitskonzepte		
F25	Bereitstellen von Diensten mit Mehrauswahlmöglichkeit	A
F26	Erstellen und Speichern eines Sicherheitskonzeptes auf Basis von Sicherheitskonzept-Vorlage	A
F27	Zwischenspeichern des Entwurfs des Sicherheitskonzeptes	A
F28	Navigation im Sicherheitskonzept von einem Element zu anderem in beiden Richtungen	A
F29	Überprüfen von Eingabewerten auf Plausibilität	W
F30	Mitteilung des Nutzers über erfolgreiche oder erfolglose Ereignisse	W
F31	Freigabe eines dienstspezifischen Sicherheitskonzeptes	A

Abbildung 2.8: Anforderungskatalog 1/3

Nummer	Beschreibung	Priorität
F32	Aufrufen des Sicherheitskonzeptes zum Bearbeiten	A
F32.1	Anzeigen aller Antwortalternativen beim Öffnen des Sicherheitskonzeptes zum Bearbeiten	A
F33	Aufrufen des Sicherheitskonzeptes zum Lesen	A
F34	Anzeigen von Text der Frage-/Fragengruppe beim Öffnen des Sicherheitskonzeptes	A
F35	Schließen des Sicherheitskonzeptes ohne zu speichern	W
F36	Anzeigen aller dienstspezifischen Sicherheitskonzepte (je nach Berechtigung)	A
F37	Suchen nach einem Sicherheitskonzept, das bestimmten Kriterien erfüllt	W
F38	Exportieren des Sicherheitskonzeptes in eine PDF-Datei	A
F39	Exportieren des Sicherheitskonzeptes in eine XML-Datei	W
F40	Exportieren des Sicherheitskonzeptes in eine Text-Datei	W
F41	Exportieren des Sicherheitskonzeptes in eine HTML-Datei	W
F42	Exportieren des Sicherheitskonzeptes in eine RTF/Word-Datei	W
F43	Import-Schnittstelle	W
Rollen- und Rechteverwaltung		
F44	Anlegen und Speichern einer neuen Rolle	A
F45	Bearbeiten einer Rolle	A
F46	Löschen einer Rolle	A
F47	Bereitstellen der Berechtigungen	A
F48	Knüpfen der Berechtigungen an einer Rolle	A
F49	Entfernen der Berechtigungen aus einer Rolle	A
F50.1	Das Recht eine Sicherheitskonzept -Vorlage zu erstellen	A
F50.2	Das Recht eine Sicherheitskonzept -Vorlage zu bearbeiten	A
F50.3	Das Recht eine Sicherheitskonzept -Vorlage freizugeben	A
F50.4	Das Recht dienstspezifische Fragen und Fragengruppen einer Sicherheitskonzept-Vorlage hinzufügen	W
F50.5	Das Recht dienstspezifische Fragen und Fragengruppen in Sicherheitskonzept-Vorlage bestimmen	W
F50.6	Das Recht ein dienstspezifisches Sicherheitskonzept zu erstellen	A
F50.7	Das Recht ein dienstspezifisches Sicherheitskonzept zu bearbeiten	A
F50.8	Das Recht ein dienstspezifisches Sicherheitskonzept freizugeben	A
F50.9	Das Recht ein dienstspezifisches Sicherheitskonzept zu exportieren	A
F50.10	Das Recht ein dienstspezifisches Sicherheitskonzept zu lesen	A
F50.11	Das Recht eine neue Rolle anzulegen	A
F50.12	Das Recht Administratorrollen an andere Benutzer zu delegieren	A
F50.13	Das Recht Rollen (außer Administratorrollen) an andere Benutzer zu delegieren	A
F50.14	Das Recht einen Dienst hinzufügen und bearbeiten	A
F50.15	Das Recht einen Dienst löschen	A
F50.16	Das Recht Dienste den Benutzern zu zuweisen	A
F50.17	Das Recht einen neuen Benutzer hinzufügen und bearbeiten	A
F50.18	Das Recht einen Benutzer löschen	A
Dienstverwaltung		
F51	Erstellen und Speichern einer neuen Dienstgruppe	A

Abbildung 2.9: Anforderungskatalog 2/3

Nummer	Beschreibung	Priorität
F52	Erstellen und Speichern eines neuen Dienstes	A
F53	Einfügen eines Dienstes in eine Dienstgruppe	A
F54	Bearbeiten eines Dienstes	A
F55	Bearbeiten einer Dienstgruppe	A
F56	Überführen eines Dienstes von einer Dienstgruppe in eine andere	A
F57	Löschen eines Dienstes	A
Benutzerverwaltung		
F58	Eine integrierte LDAP-Schnittstelle für die Authentifizierung von Benutzer	W
F59	Anlegen der persönlichen Daten des Benutzers	W
F60	Anlegen von Login und Passwort für den Benutzer	A
F61	Der Zugriff auf die Daten erfolgt passwortgeschützt	A
F62	Zuweisen von Dienstgruppe(n) an einen Benutzer	A
F63	Zuweisen einer Rolle an eine Dienstgruppe	A
F64	Integrierte E-Mail-Funktion	W
F65	Benachrichtigung- und Erinnerungsfunktion per Mail	W
F66	Zweidimensionale Zugriffskontrolle durch Zuweisung von Rollen und Diensten	A
Nicht-funktionale Anforderungen		
NF01	Die Anwendung muss auf einem System des LRZ installiert werden	A
NF02	Die Anwendung soll auf einer Linux-Plattform lauffähig sein	W
NF03	Software muss dem aktuellen Stand der Softwaremöglichkeiten entsprechen	A
NF04	Die Anwendung muss fehlerfrei funktionieren	A
NF05.1	Die Anwendung muss deutsche oder englische Sprache unterstützen	A
NF05.2	Die Anwendung muss deutsche und englische Sprache unterstützen	W
NF06	Das System darf vom Benutzer keine Programmierkenntnisse verlangen	A
NF07	Die Anwendung muss eine intuitiv bedienbare Benutzeroberfläche haben	W
NF08	Die Dokumentation zur Installation der Anwendung muss vorhanden sein.	A
NF09	Ein Benutzerhandbuch muss vorhanden sein	W
NF10	Die Bedingung des Systems muss leicht erlernbar sein.	W
NF11	Anpassungen an LRZ- Corporate Identity (Logo, Firmenfarben)	W
NF12	Mehrbenutzer Betrieb	A
NF13	Kostenlos	A
NF14	Open Source	A
NF15	Unbegrenzte Anzahl der Fragen	A
NF16	Unbegrenzte Anzahl von Sicherheitskonzepten	A
NF17	Unbegrenzte Anzahl von Benutzer	A

Abbildung 2.10: Anforderungskatalog 3/3

3 Evaluation

Nachdem die Anforderungen an der gewünschten Applikation festgestellt und ihre Leistungen und Funktionalität ermittelt wurden, kann man in die nächste Phase der Entwicklung übergehen. Oft ist es sinnvoll, vor dem Entwicklungsanfang einer neuen Software, einen Blick auf den Markt zu werfen. Die Wahrscheinlichkeit, dass ein Produkt den vielen angeforderten Kriterien entspricht, ist groß. Der heutigen Markt hat Tendenz sich ständig zu verändern und erweitern. Neben den steigenden Bedürfnissen erhöht sich auch das Angebot der Softwareprodukte. Oft überlappen sich die Leistungen der breit gefächerten Lösungssätze. In dieser Arbeit soll eine von am Markt angebotenen Softwarelösungen ausgewählt werden, die für Verwaltung der dienstspezifischen Sicherheitskonzepte am LRZ geeignet ist. Diese Kapitel beschäftigen sich mit Untersuchung der auf dem Markt vorhandenen Softwareprodukten und Auswahl eines davon durch ein strukturiertes Vorgehen.

3.1 Vorgehensweise

Ausgehend von ermittelten im Kapitel 2 der endgültige Kriterienkatalog wird im Weiteren 3-Stufige Auswahlverfahren durchgeführt[1]. In jeder Stufe sind von der Software zu erfüllende Kriterienrahmen anzulegen , so dass schnell und objektiv diejenige Produkte herauszufiltern, die am besten geeignet sind, um die oben definierten Hauptziele zu erreichen.

Stufe 1: Vorauswahl

Kriterien für eine grobe und schnelle Auswahl sind einzelne funktionale Anforderungen, die das Erreichen der Hauptfunktionalität des Systems ermöglichen. Dazu gehören das Erstellen eines Fragenbogens und Erfassung der Dokumenten auf seiner Basis.

Stufe 2: Feinauswahl

Für den Ausschluss ungeeigneter Systeme werden in dieser Phase entscheidende Kriterien einige nicht-funktionale Anforderungen verwendet. Sie beziehen sich vor allem auf das System im Ganzen.

Die folgenden Kriterien sind in der Feinauswahlphase zu erfüllen:

1. Die Anwendung muss auf einem System des LRZ installiert werden können (NF01)
   Das ist ein sehr wichtiger Punkt, da alle Informationen innerhalb des LRZ verarbeitet werden müssen. Mit diesem Kriterium scheiden alle Tools aus, bei denen Ressourcen auf dem Server eines Herstellers oder in einer public Cloud zu speichern sind.

[1] 3-Stufige Auswahlverfahren wurde in Anlehnung an [Klü07] durchgeführt

2. Die Anwendung muss deutsche oder englische Sprache unterstützen (NF05.1)
   Obwohl die meisten Programmen in englischer und viele der innerhalb einer Internetrecherche gefundenen Tools in deutscher Sprache erhältlich sind, gibt es eine Menge von Software nur in anderen Sprachen, welche ausgefiltert werden müssen.

3. Das System darf vom Benutzer keine Programmierkenntnisse verlangen (NF06)
   Einige Tools bieten die vorgefertigten Programmcode, aber diese Codestücke müssen noch logisch verbunden werden, oder eine Benutzeroberfläche soll noch aufgebaut werden, um die Funktionalität des Tools nutzen zu können. Weiterhin gibt es Programme, die Codeeingaben unmittelbar in Felder verlangen. Alle diese Varianten passen nicht zum Zweck dieser Arbeit.

4. Kostenlos (NF13)
   Die Bestimmung des Kostenrahmens ist wichtig, um sofort Produkte zu beseitigen, die wegen verlangten Kosten weiter in Rahmen dieser Arbeit nicht umgesetzt werden können.

5. Unbegrenzte Anzahl der Fragen (NF15), von Sicherheitskonzepten (NF16) und von Benutzer (NF17)
   Die meisten Softwareanbieter bieten kostenlose Einstiegsangebote oder Testversionen an, die jedoch generell sehr stark eingeschränkt sind. Oft werden die Anzahl der Fragenbogen, der Fragen oder der Teilnehmer limitiert, so dass das angedachte Projekt nicht umsetzbar ist.

6. OpenSource (NF14)
   Damit Änderungen, Behebung eines Programmfehlers oder Erweiterung des Quelltextes möglich sind, muss die Lizenz, unter der die Software freigegeben ist, entsprechende Modifikation erlauben.

7. Software muss dem aktuellen Stand der Softwaremöglichkeiten entsprechen (NF03)
   Um jene Tools auszufiltern, die seit langer Zeit nicht mehr aktiv sind, wird hier Updatestand als Auswahlkriterium angewendet. GESIS (Leibniz-Institut für Sozialwissenschaften)[2] empfehlt bei der Auswahl der Software darauf zu achten, wie aktiv die Entwicklercommunity ist [oss12]. In dieser Arbeit wird angenommen, dass das letzte Update nicht später als 2007 vorgenommen worden sein sollte.

Stufe 3: Endauswahl

In dieser Phase werden die in Stufe 2 vorselektierten Tools genauer betrachtet. Anhand des Anforderungskatalogs werden diese Tools überprüft. Die Ergebnisse müssen empirisch evaluiert sein. Schlussendlich wird eine Applikation ausgewählt, die meisten sowohl funktionalen als auch nichtfunktionalen Bedürfnisse abdeckt.

3.2 Auswahl des Tools

Der Ausgangspunkt des Auswahlprozesses ist der endgültige Kriterienkatalog. Mit Hilfe der für jede Stufe vordefinierten Randbedingungen lässt sich die Zahl der in Frage kommenden

[2] www.gesis.org/en/home/

Programme Schritt für Schritt reduzieren. Die Abbildung 3.1 skizziert die unten detailliert beschriebene Vorgehensweise.

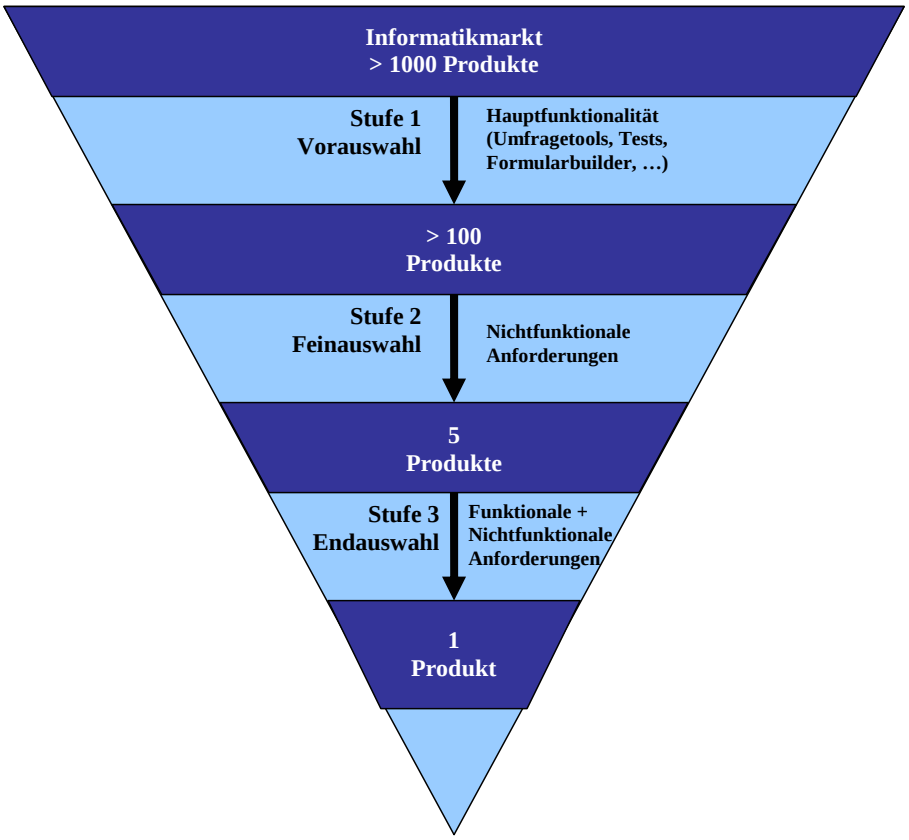


Abbildung 3.1: Auswahlverfahren

3.2.1 Stufe 1. Vorauswahl

Nach der Überlegung, welche Programme aus welchen Branchen die für Vorauswahlphase ausgewählten funktionellen Anforderungen erfüllen könnten, wurden folgenden Arten der Software herausgesucht: Umfragetools bzw. Survey Managemet Systeme, Formularbuilder und Programme zum Erstellen von Tests und Quizzes. Das Angebot im Internet ist riesig und unübersichtlich.

Die WebSM Website[3] ist den methodischen Fragen von Web-Befragungen gewidmet. Die Web Datenbank Survey Bibliography[4] bietet 334 Online Survey Softwares[5].
Verschiedene Rewies und Übersichten des Marktes erweitern die Anzahl der Produkte innerhalb der Survey-Familie. Eine Recherche im Internet bringt noch weitere Ergebnisse. Aus

[3]The University of Ljubljana, Faculty of Social Science, Centre for Methodology and informatics
[4] http://www.websm.org/c/1283/Software/?preid=0
[5]Stand 29.03.14

diesem umfangreichen Angebot müssen jetzt alle nicht geeignete Produkte ausgesondert werden, um den Anteil der weiter zu untersuchenden Software zu reduzieren.

3.2.2 Stufe 2: Feinauswahl

Die Erfüllung der oben formulierten Kriterien ist notwendige Voraussetzung für eine detaillierte Analyse in der nächsten Stufe. Eine Zusammenfassung dieser Kriterien ist unten angegeben.

1. Auf einem System am LRZ installierbar
2. Deutsche oder englische Sprache unterstützt
3. Keine Programmierkenntnisse nötig
4. Kostenlos
5. Unbegrenzte Anzahl der Fragen, von Sicherheitskonzepten und von Benutzern
6. OpenSource
7. Entspricht dem aktuellen Stand der Softwaremöglichkeiten

WebSM ermöglich es, mit einer sehr bequemen Eingabemaske sehr schnell anhand vieler dieser Kriterien Software aussortieren. Es ist aber nicht immer möglich, Tools mit den benötigen Eigenschaften schnell auszusuchen. Die meisten Softwareauswahl-Platformen orientieren sich an kommerziellen Lösungen und können in dieser Arbeit wegen Anforderung NF13 kaum benutzt werden. Normalerweise kann man erst nach dem Besuch der Software-Webseite entscheiden, ob das Tool allen gewünschten Kriterien entspricht. Es ist ein sehr aufwendiger Prozess. In dieser Stufe der Auswahl wurden über 100 Tools auf die Anforderungsabdeckung hin überprüft. Deswegen werden hier nur einige angeführt, um das ganzes Verfahren zu veranschaulichen. Es gibt Tools, die sehr beliebt sind und in mehreren Top-Listen vorkommen. Anhand der Bewertung einiger dieser Tools ist die Vorgehensweise dieser Stufe dargestellt. Die Tabelle 3.2 stellt die Ergebnisse der Evaluirung von Applications in der Phase 2 vor.
In der Stufe 2 sind die folgenden Tools ausgewählt:

1. LimeSurvey[6]
2. Opensurveypilot[7]
3. Web Survey Toolbox[8]
4. TestMaker[9]
5. FormTools[10] - Community Edition (CE)

Bei der Endauswahl werden sie genauer betrachtet, und ihr Abdeckungsgrad wird möglichst exakt ermitteln.

[6] http://www.limesurvey.org/de/
[7] sourceforge.net/projekts/osp/
[8] http://open.jira.com/wiki/display/WST/Home
[9] http://www.global-assess.rwth-aachen.de/testmaker-wiki/de/index.php/Hauptseite
[10] http://www.formtools.org/

	Poll Daddy	Survey Monkey	The Survey System	Lime Survey	Quastion Pro	OpenSurveyPilot	Web Survey Toolbox	els PHP Web Quiz	TextMaker	Wufoo	FormTools	JotForm
Auf einem System des LRZ installierbar	-	-	+	+	-	+	+	+	+	-	+	-
Deutsche oder Englische Sprache unterstützt	+	+	+	+	+	+	+	+	+	+	+	+
Keine Programmierkenntnisse nötig	+	+	+	+	+	+	+	+	+	+	+	+
Kostenlos	+	+	-	+	+	+	+	+	+	-	+	+
Unbegrenzte Anzahl der Fragen	+	-	+	+	+	+	+	+	+	+	+	+
Unbegrenzte Anzahl von Sicherheitskozepten	+	-	+	+	-	+	+	+	+	-	+	-
Unbegrenzte Anzahl von Benutzer	-	-	+	+	-	+	+	+	+	-	+	-
Open Source	-	-	-	+	-	+	+	-	+	-	+	-
Entspricht dem aktuellen Stand der Softwaremöglichkeiten	+	+	+	+	+	+	+	+	+	+	+	+
Auswahlergebnisse				+		+	+		+		+	

Abbildung 3.2: Ergebnisse der Feinauswahl

3.2.3 Stufe 3. Endauswahl

Nachdem die auf den ersten Blick passenden Tools ausgesucht wurden, können sie näher im Betracht kommen. Nachstehend eine kurze Vorstellung der ausgewählten Applikationen.

LimeSurvey ist ein Umfrage-Tool, das es erlaubt, Umfragen verschiedener Komplexität zu erstellen, in einer Datenbank zu speichern und weiter zu verwalten. Die Software wird aktiv weiterentwickelt und bietet umfangreiche Features. LimeSurvey ist mittels PHP realisiert und greift für die Datenhaltung auf eine MySQL- oder PostgreSQL-Datenbank zurück. LimeSurvey ist unter den Bedingungen der GNU General Public License (GNU GPL) veröffentlicht. Es ist OpenSource und kostenlos.

TestMaker "ist eine webbasierte Software zur Darstellung, Durchführung und Auswertung von psychometrischen Tests"[utm09]. Das Programm wurde am Lehrstuhl für Betriebs- und Organisationspsychologie der RWTH Aachen entwickelt. Für den Einsatz von TestMaker sind weder Programmier- noch HTML-Kenntnisse erforderlich. Die Software TestMaker ist in Programmiersprache PHP geschrieben und unter den Bedingungen der GNU GPL (Version 2.0) der Free Software Foundation veröffentlicht. Sie kann sowohl lokal auf dem eigenen Rechner als auch auf einem Webserver eingerichtet werden.

FormTools ist ein in PHP und MySQL geschriebenes Form-Framework. Es erlaubt sowie einfache und mehrseitige interaktive Formulare und bietet Werkzeuge für die Verwaltung und Bearbeitung von Formulardaten. Form Tools ist unter der GNU GPL verfügbar. Source Code kann kostenlos heruntergeladen und geändert werden. Die Software ist in zwei Versionen verfügbar: eine kostenlose Version, die im Weiteren betrachtet werden, und Premium Form Builder Module. Die freie FormTools-Version enthält alle Funktionen zum Verwalten der Formularen.

Opensurveypilot ist ein webbasiertes Open-Source-System zur Erstellung und Auswertung von Stimmabgaben, Umfragen oder der empirischen Sozialforschung. Es ist ein kleines in PHP geschriebenes Projekt, das nicht mehr weiterentwickelt wird. Der Opensurveypilot läuft auf dem Linux System mit Apache Webserver und mySQL Datenbank. Die Software darf unter der Mozilla Public License 1.1 (MPL 1.1) ausgeführt werden.

Web Survey Toolbox ist ein freies Open-Source-Tool, das sich an der Online-Forschung orientiert. Ein Feature ist das Verwalten und Ausführen von Umfragen. Die Software ist mit JSP, Java, JavaScript, PL/SQL realisiert. Web Survey Toolbox darf unter der GNU GPL (Version 2.0) frei verwendet werden.

Alle fünf Softwarelösungen wurden installiert und anhand des Anforderungskatalogs getestet. LimeSurvey, Opensurveypilot, TestMaker und FormTools sind in der Scriptsprache PHP und Web Survey Toolbox ist in der Programmiersprache Java geschrieben. Alle Tools brauchen zum Ausführen Apache Web-Server und eine Datenbank, zum Beispiel MySQL. Ziel des Auswahlverfahrens war es, eine Lösung mit passender Funktionalität möglichst schnell zu finden. Da sowohl Java und PHP, als auch alle für die Installation benötige Software-Komponenten plattformunabhängig sind, spielt es keine Rolle unter welchem Betriebssystem die ausgewählte Web-Anwendungen laufen. Sie können in jedem Browser auf einem beliebigen Betriebsystem ausgeführt werden. Deswegen wurde entschieden, die Anwendungen, bei denen es möglich ist, mit der Hilfe von XAMPP[11] unter Windows XP zu testen. XAMPP ist ein OpenSource-Softwarepaket, das die vorkonfigurierten Webserver Apache, MySQL, Perl und PHP enthält. Es ist als ein Testsystem gedacht und eignet sich ideal zum schnellen Testen der Web-Anwendungen. Windows XP wurde ausgewählt, weil fast alle ausgewählte Anwendungen Installation-Anleitungen nur für eine Windows-Umgebung haben. Um den Zeitaufwand zu reduzieren wurde entschieden, in der Linux-Umgebung nur das passende Tool zu testen.

LimeSurvey, Opensurveypilot, TestMaker und FormTools wurden in folgender Testumgebung installiert:

- Windows XP 32 Bit
- XAMPP der Version 1.7.3

Web Survey Toolbox wurde in folgender Testumgebung installiert:

- Windows XP 32 Bit
- Java JDK 1.7
- Apache Tomcat 6.0.20
- MySQL 5.6

Für die Installation der ausgewählten Anwendungen wurde der Source-Code heruntergeladen und in einem Ordner auf dem Server entpackt. Fast alle getesteten Anwendungen unterstützen die automatische Installation beim ersten Aufruf im Webbrowser. Es wird ein Installationsscript ausgeführt, das die Applikationsparameter konfiguriert. Genaue Installation-Anweisungen sind auf folgenden Webseiten zu finden[12].

[11] https://www.apachefriends.org/index.html

[12] Installation-Anweisungen: TestMaker: `http://www.global-assess.rwth-aachen.de/testmaker-wiki/en/index.php/Installation`,

Das Testen hat ergeben, dass alle über Features zu Fragenbogen-, Fragen- und Fragengruppenerstellung, zur Fragentypauswahl und zum Ändern der Frage- und Fragengruppenreihenfolge verfügen. Dementsprechend sind die Anforderungen F01-F05 vollständig erfüllt. Die unterstützenden Fragentypen unterscheiden sich je nach Applikation. Features wie Freitexteingabe, Checkboxen oder Radiobuttons bieten alle fünf Tools. FormTools und LimeSurvey ermöglichen die Eingabe sowohl von Datum als auch der Uhrzeit. Tabellen erstellen ist möglich mit LimeSurvey und OpenSurveyPilot.
Die Einschränken der Texteingabe auf Nummern ist mit FormTools, LimeSurvey und Web Survey Toolbox möglich. In FormTools, LimeSurvey und Web Survey Toolbox lässt sich die Benutzereingabe zudem auf Buchstaben beschränken.

Mit allen Applikationen außer Web Survey Toolbox können Pflichtfelder gekennzeichnet werden. In keinen Tool ist eine Markierung der neuen hinzugefügten Fragen vorgesehen. Trotzdem ist es möglich, solche Fragen per Hand mit farbigen oder textuellen Markierungen zu versehen. Dies ermöglichen LimeSurvey, FormTools und Web Survey Toolbox.

Verzweigungslogik bieten Tools wie LimeSurvey und TestMaker. Mit TestMaker lassen sich sowohl Fragen als auch Fragegruppen über eine Bedingung miteinander verknüpfen. LimeSurvey ermöglicht nur die Verknüpfung der Fragen. Anzeigenbedingungen für die Fragegruppen können jedoch indirekt definiert werden, indem man für alle Fragen dieser Gruppe eine gleiche Bedingung angibt.

Eine wichtige Anforderung zum Bearbeiten der Sicherheitskonzept-Vorlage (Anforderung F13) ist möglich in allen Tools außer LimeSurvey. Obwohl man im LimeSurvey in einer freigegebenen Sicherheitskonzept-Vorlage den Text der Frage oder Fragengruppe editieren kann, können keine neue Fragen, Fragengruppen und Antwortmöglichkeiten hinzugefügt werden. Das ist der größte Nachteil von LimeSurvey aus der Sicht des ausgearbeiteten Konzeptes für das LRZ. Es gibt allerdings einen Umweg, der teilweise dieses Problem löst, weswegen alle Anforderungen, die mit dem Bearbeiten der Vorlage zu tun haben, als teilweise erfüllt gekennzeichnet sind. Die Idee liegt darin, dass nur nach dem Deaktivieren eine freigegebene Umfrage sich ändern lässt. Die bereits vorhandenen Antworten für diese Umfrage sollen vor dem Deaktivieren exportiert werden, damit sie nicht verloren gehen. Das Deaktivieren wird für die Sicherheitskonzept-Vorlage bedeuten, dass die entsprechende Datenbanktabelle als "old" markiert wird. Alle Fragen, Gruppen und Parameter sind somit wieder veränderbar. Statt der alten Tabelle wird nach der Bearbeitung eine neue angelegt. Das bedeutet, dass eine neue Sicherheitskonzept-Vorlage erstellt wird und alle früher verfassten Sicherheitskonzepte nicht mehr angezeigt werden können.

Alle fünf ausgewählten Tools ermöglichen die Erstellung und Speicherung eines Reportes mit den Antworten auf Basis eines Fragebogens. Somit ist die Anforderung F26 erfüllt. Aber der Vorgang des Fragenbogenausfüllens unterscheidet sich je nach Applikation und entspricht nicht immer den Anforderungen aus dem Kriterienkatalog. So ist es nicht möglich, mit Open-

LimeSurvey `https://manual.limesurvey.org/installation/de`,
OpenSurveyPilot: `https://community.apachefriends.org/f/viewtopic.php?t=8040`,
FormTools: `http://docs.formtools.org/installation/?page=index`,
Web Survey Toolbox: `https://open.jira.com/wiki/display/WST/Installation+Directions`

SurveyPilot ein teilweise ausgefülltes Sicherheitskonzept zu speichern und später zum weiteren Ausfüllen abzurufen (Anforderungen F27 und F32). Web Survey Toolbox erfüllt diese Anforderungen bloß zum Teil. Pflichtfelder können nur indirekt (zum Beispiel mit der Farbe) gekennzeichnet werden, das heißt es wird keine Überprüfung vom System durchgeführt, trotzdem kann ein Sicherheiskonzept zwischengespeichert werden. Obwohl das gleiche Sicherheitskonzept nicht mehr zum Beantworten abrufbar ist, können die Ergebnisse direkt im Report bearbeitet und nachgetragen werden. Diese Lösung hat den Nachteil, dass der ganze Fragentext und alle Antwortalternativen nicht angezeigt werden (Anforderung F32.1) und der ganze Report im Format einer Datenbanktabelle dargestellt wird.

Während das Springen von einer Frage zu nächsten oder zur vorherigen Frage ohne Verlust der bereits angegebenen Antworten (Anforderung F28) in FormTools und in Limeurvey realisierbar ist, kann man mit den übrigen drei Tools nur zu nächstfolgender Frage springen. Bei Web Survey Toolbox ist es möglich, diese Anforderung teilweise zu realisieren, indem man alle Fragen auf einer Seite platziert. Dann können sie unabhängig von deren Reihenfolge beantwortet werden. Mit TestMaker können die Fragen nur nacheinander beantwortet werden, wobei auch nur jeweils eine Frage pro Seite angezeigt wird.
FormTools verfügt über eine komplexe und flexible Struktur der Views. Die Views lassen sich je nach Zugriffseinstellungen anzeigen oder verstecken.

Alle Tools außer OpenSurveyPilot verfügen über Filtermechanismen, die das Suchen der Dokumenten nach bestimmten Kriterien ermöglicht (Anforderung F37).

FormTools und LimeSurvey bieten die Möglichkeit, die erstellten Sicherheitskonzepte in eine PDF-Datei zu exportieren (Anforderung F38) oder als ein eigenständiges Dokument abzulegen und auszudrucken. LimeSurvey stellt zusätzlich das Speichern eines Sicherheitskonzept im XML-, HTML-, Text- und Microsoft Word-Format (Anforderungen 39-42). TextMaker ermöglicht das Export in eine Text-Datei.

Das Rollenkonzept wird mehr oder weniger von allen fünf Applikationen unterstützt. Eine neue Rolle anzulegen und zu verwalten ermöglichen LimeSurvey, Test Maker und Web Survey Toolbox (Anforderungen F44-F46). FormTools bietet zum Anfang der Arbeit zwei so genannte Menüs an: eines für Administratoren und eines für alle Benutzer. Das Menü des Administrators kann angepasst, aber nicht gelöscht werden. Benutzermenüs können hinzugefügt, bearbeitet und gelöscht werden. Im Unterschied zu den oben genannten Tools gibt es keine Möglichkeit, mit OpenSurveyPilot neue Rollen hinzufügen. Jedem Benutzer kann eine oder mehrere von vier vordefinierten Rollen (Gast, Anwender, Projektleiter und Administrator) zugewiesen sein. Alle fünf Tools bieten auch eine Reihe der Berechtigungen, die mit einer Rolle verknüpft oder von ihr entfernt werden können (Anforderungen F47-F49). Die Berechtigung zum Erstellen und Bearbeiten der Vorlage bieten alle Applikationen an. Bei FormTools hat diese Rechte nur der Administrator. Genauer sind Berechtigungen in einer Tabelle zusammen gefasst.

Die Abhängigkeit der Fragenbogen und der Benutzer von Diensten lassen sich mit Hilfe der ausgewählten Tools schwer oder kaum realisieren. Deswegen alle Anforderungen des Dienstverwaltung-Teils (Anforderungen F51-F57) als nicht erfüllt bewertet. Auch die aus anderen Unterteilen des Kriterienkatalogs dienstbezogenen Anforderungen sind als nicht erfüllt

markiert.
Der Zugriff auf das System erfolgt bei allen Tools passwortgeschützt (Anforderung F61). LimeSurvey hat eine integrierte LDAP-Schnittstelle, die eine zentrale Verwaltung Authentifizierung der Benutzer ermöglicht (Anforderung F58). Während des Tests sind bei einigen Tools Fehler aufgetreten. In TextMaker ergibt sich ein Fehler beim Anlegen einer Antwortalternative, deswegen ist die Anforderung F18 nur als teilweise erfüllt markiert. LimeSurvey und FormTools scheinen fehlerfrei.

Ergebnisse der Evaluation

Zum Schluss der Endauswahlphase wurde eine empirische Bewertung der Tools durchgeführt. Dafür wurde einen Bewertungsschlüssel festgelegt, der in der Tabelle 3.1 dargestellt. Aus der

+	Erfüllt	2 Punkte
+ -	Teilweise erfüllt	1 Punkt
-	Nicht erfüllt	0 Punkte

Tabelle 3.1: Bewertungsschussel

Tabelle folgt, dass beim vollständigen Erfüllen der Anforderung bekam das Tool zwei Punkte, beim nicht völligen Erfüllen - ein Punkt. In der Fall, wann die angeforderten Funktionalität fällte, wurde keine Punkte für das entsprechende Kriterium vergeben. Die grafische Darstellung (+, +-, -) ist in der Tabelle "Evaluation von Software" 3.4 benutzt, in der die Test- und Bewertungsergebnisse zusammengefasst sind.
Da beim Softwareauswahl die MUSS-Anforderungen entscheidend sind, wurden in dieser

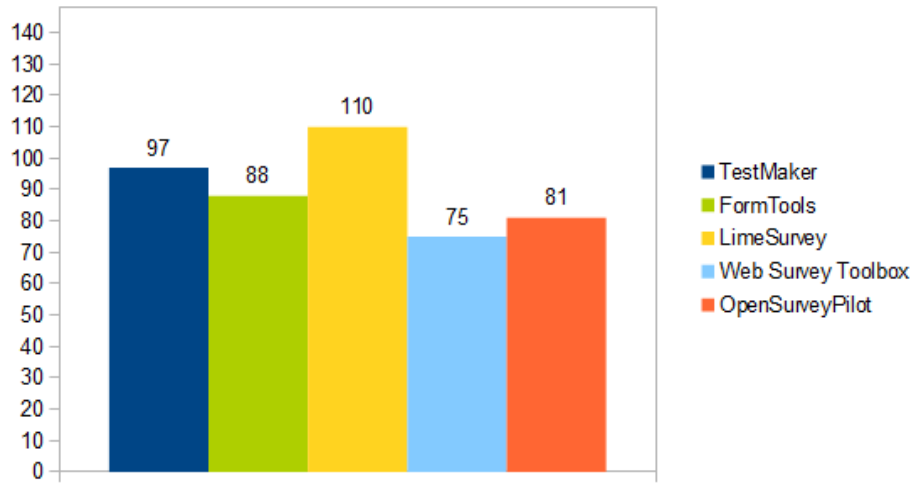


Abbildung 3.3: Erfüllungsgrad der MUSS-Anforderungen

Arbeit nur die zwingend erforderliche Anforderungen (bezeichnete mit dem Buchstabe "A" und grün in der Tabelle 3.4) berücksichtigt und für jedes Tool die vergebene Punkte zusammengerechnet.

Das Diagramm 3.3 stellt die Ergebnisse der Endauswahl-Phase grafisch dar. Die Bewertungsergebnisse sind wie folgt: TestMaker - 97 Punkte, FormTools - 88 Punkte , LimeSurvey - 110 Punkte, Web Surwey Toolbox - 75 Punkte und OpenSurveyPilot - 81 Punkte. Daraus folgt, dass LimeSurvey von fünf selektierten Tools die am besten passende Lösung ist. Aus der 148 möglichen Punkten hat er 110 Punkte erzielt, was einem Prozentsatz von 74, 3 Prozent entspricht.

Nr.	Beschreibung	TestMaker	FormTools	LimeSurvey	Web Survey Toolbox	OpenSurvey Pilot	Priorität
Funktionale Anforderungen							
Verwaltung der Sicherheitskonzept-Vorlage							
F01	Erstellen und Speichern der Sicherheitskonzept-Vorlage	+	+	+	+	+	A
F02	Zwischenspeichern des Entwurfs der Sicherheitskonzept-Vorlage	+	+	+	+	+	A
F03	Erstellen von Fragen	+	+	+	+	+	A
F04	Gruppieren von Fragen in Fragengruppen	+	+	+	+	+	A
F05	Auswahl von Fragentypen	+	+	+	+	+	A
F05.1	Der Fragentyp „Freitext“	+	+	+	+	+	A
F05.2	Der Fragentyp „Mehrere Antwortalternativen“	+	+	+	+	+	A
F05.3	Der Fragentyp „Exakt eine Antwortalternative“	+	+	+	+	+	A
F05.4	Der Fragentyp „Datum“	-	+	+	-	-	W
F05.5	Der Fragentyp „Uhrzeit“	-	+	+	-	-	W
F05.6	Der Fragentyp „Tabelle“	-	-	+	-	+	W
F06.1.1	Beschränken des Eingabewertes auf Typ: Nummer	-	+	+	+	+	W
F06.1.1	Beschränken des Eingabewertes auf Typ: Buchstaben	-	+	+	+	-	W
F06.2	Beschränken des Eingabewertes auf Anzahl von Zeichen	-	+	+	-	-	W
F06.3	Beschränken des Wertebereiches eines Eingabewertes	-	-	-	-	-	W
F07	Markieren von Frage als „Pflichtfeld“	+	+	+	-	+	W
F08	Verknüpfen einer Frage mit einer Bedingung	+	-	+	-	-	A

Abbildung 3.4: Ergebnisse der Endauswahl 1/7

Nr.	Beschreibung	TestMaker	FormTools	LimeSurvey	Web Survey Toolbox	OpenSurveyPilot	Priorität
F09	Verknüpfen einer Fragegruppe mit einer Bedingung	+	-	-	-	-	W
F10	Speichern der Antwortalternativen als Schablone	+	-	+	-	-	W
F11	Aufrufen der Sicherheitskonzept-Vorlage zur Vorschau	+	+	+	+	+	A
F12	Freigabe der Sicherheitskonzept-Vorlage	+	+	+	+	+	A
F13	Deaktivieren der Sicherheitskonzept-Vorlage	+	+	+	+	+	W
F14	Aufrufen der Sicherheitskonzept-Vorlage zum Bearbeiten	+	+	+-	+	+	A
F15	Ändern der Reihenfolge der Fragen	+	+	+	+	+	W
F16	Ändern der Reihenfolge der Fragengruppen	+	+	+	+	+	W
F17	Ändern des Fragen- und Fragengruppentextes	+	+	+	+	+	A
F18	Einfügen einer neuen Antwortalternative zu einer Frage	+-	+	+-	+	+	A
F19	Markieren neu hinzugefügter in der Sicherheitskonzept-Vorlage Fragengruppen, Fragen und Antwortalternativen.	-	+-	+-	+-	-	W
F20	Löschen einer Antwortalternative	+	+	+	+	+	A
F21	Löschen einer Frage	+	+	+	+	+	A
F22	Löschen einer Fragengruppe	+	+	+	+	+	A
F23	Öffnen der Sicherheitskonzept -Vorlage zum Bestimmen von dienstspezifischen Fragen und Fragengruppen	-	-	-	-	-	W
F24	Ein- und Ausblenden von dienstspezifischen Fragengruppen/Fragen	-	+-	+-	-	-	W

Abbildung 3.5: Ergebnisse der Endauswahl 2/7

Nr.	Beschreibung	TestMaker	FormTools	LimeSurvey	Web Survey Toolbox	OpenSurvey Pilot	Priorität
Verwaltung der dienstspezifischen Sicherheitskonzepte							
F25	Bereitstellen von Diensten mit Mehrauswahlmöglichkeit	-	-	-	-	-	A
F26	Erstellen und Speichern eines Sicherheitskonzeptes auf Basis von Sicherheitskonzept-Vorlage	+	+	+	+	+	A
F27	Zwischenspeichern des Entwurfs des Sicherheitskonzeptes	+	+	+	+-	-	A
F28	Navigation im Sicherheitskonzept von einem Element zu anderem in beiden Richtungen	-	+	+	+-	-	A
F29	Überprüfen der Eingabewerten auf Plausibilität	+-	+	+	+	+	W
F30	Mitteilung des Nutzers über erfolgreiche oder erfolglose Ereignisse	+	+	+	+	+	W
F31	Freigabe eines dienstspezifischen Sicherheitskonzeptes	-	+	-	-	-	A
F32	Aufrufen des Sicherheitskonzeptes zum Bearbeiten	-	+	+	+-	-	A
F32.1	Anzeigen aller Antwortalternativen beim Öffnen des Sicherheitskonzeptes zum Bearbeiten	+	+	+	-	+	A
F33	Aufrufen des Sicherheitskonzeptes zum Lesen	+	+	+	+	+	A
F34	Anzeigen von Text der Frage-/Fragengruppe beim Öffnen des Sicherheitskonzeptes	+	+	+	+	+	A
F35	Schließen des Sicherheitskonzeptes ohne zu speichern	+	+	+-	+	+	W
F36	Anzeigen aller dienstspezifischen Sicherheitskonzepte (je nach Berechtigung)	+	+	+	+-	+-	A

Abbildung 3.6: Ergebnisse der Endauswahl 3/7

Nr.	Beschreibung	TestMaker	FormTools	LimeSurvey	Web Survey Toolbox	OpenSurvey Pilot	Priorität
F37	Suchen nach einem Sicherheitskonzept, das bestimmten Kriterien erfüllt	+	+	+	+	-	W
F38	Exportieren des Sicherheitskonzeptes in eine PDF-Datei	-	+	+	-	-	A
F39	Exportieren des Sicherheitskonzeptes in eine XML-Datei	-	-	+	-	-	W
F40	Exportieren des Sicherheitskonzeptes in eine Text-Datei	+	-	-	-	-	W
F41	Exportieren des Sicherheitskonzeptes in eine HTML-Datei	-	-	+	-	-	W
F42	Exportieren des Sicherheitskonzeptes in eine RTF/Word-Datei	-	-	+	-	-	W
F43	Import-Schnittstelle	-	-	+	-	-	W
	Rollen- und Rechteverwaltung						
F44	Anlegen und Speichern einer neuen Rolle	+	-	+	+	-	A
F45	Bearbeiten einer Rolle	+	+-	+	+	-	A
F46	Löschen einer Rolle	+	+-	+	+	-	A
F47	Bereitstellen der Berechtigungen	+	+-	+	+-	+	A
F48	Knüpfen der Berechtigungen an einer Rolle	+	+-	+	-	+	A
F49	Entfernen der Berechtigungen aus einer Rolle	+	+-	+	-	+	A
F50.1	Das Recht eine Sicherheitskonzept-Vorlage zu erstellen	+	-	+	-	+	A
F50.2	Das Recht eine Sicherheitskonzept - Vorlage zu bearbeiten	+	-	+	-	+	A
F50.3	Das Recht eine Sicherheitskonzept - Vorlage freizugeben	-	-	-	-	-	A
F50.4	Das Recht dienstspezifische Fragen und Fragengruppen in Sicherheitskonzept - Vorlage hinzufügen	-	-	-	-	-	W

Abbildung 3.7: Ergebnisse der Endauswahl 4/7

Nr.	Beschreibung	TestMaker	FormTools	LimeSurvey	Web Survey Toolbox	OpenSurveyPilot	Priorität
F50.5	Das Recht dienstspezifische Fragen und Fragengruppen in Sicherheitskonzept - Vorlage bestimmen	+	+	+	-	+	W
F50.6	Das Recht ein dienstspezifisches Sicherheitskonzept zu erstellen	-	+-	+	-	+	A
F50.7	Das Recht ein dienstspezifisches Sicherheitskonzept zu bearbeiten	-	-	+	-	-	A
F50.8	Das Recht ein dienstspezifisches Sicherheitskonzept freizugeben	+	+-	-	-	-	A
F50.9	Das Recht ein dienstspezifisches Sicherheitskonzept zu exportieren	+	+-	+	-	+	A
F50.10	Das Recht ein dienstspezifisches Sicherheitskonzept zu lesen	+	-	+	-	-	A
F50.11	Das Recht eine neue Rolle anzulegen	+	-	+	-	-	A
F50.12	Das Recht Administratorrollen an andere Benutzer zu delegieren	+	-	+	-	-	A
F50.13	Das Recht Rollen (außer Administratorrollen) an andere Benutzer zu delegieren	-	-	-	-	-	A
F50.14	Das Recht einen Dienst hinzufügen und bearbeiten	-	-	-	-	-	A
F50.15	Das Recht einen Dienst löschen	-	-	-	-	-	A
F50.16	Das Recht Dienste den Benutzern zu zuweisen	-	-	-	-	-	A
F50.17	Das Recht einen neuen Benutzer hinzufügen und bearbeiten	-	-	+	-	-	A
F50.18	Das Recht einen Benutzer löschen	-	-	+	-	-	A
	Dienstverwaltung						
F51	Erstellen und Speichern einer neuen Dienstgruppe	-	-	-	-	-	A
F52	Erstellen und Speichern eines neuen Dienstes	-	-	-	-	-	A

Abbildung 3.8: Ergebnisse der Endauswahl 5/7

Nr.	Beschreibung	TestMaker	FormTools	LimeSurvey	Web Survey Toolbox	OpenSurvey Pilot	Priorität
F53	Einfügen eines Dienstes in eine Dienstgruppe	-	-	-	-	-	A
F54	Bearbeiten eines Dienstes	-	-	-	-	-	A
F55	Bearbeiten einer Dienstgruppe	-	-	-	-	-	A
F56	Ziehen eines Dienstes von einer Dienstgruppe in eine andere	-	-	-	-	-	A
F57	Löschen eines Dienstes	-	-	-	-	-	A
	Benutzerverwaltung						
F58	Eine integrierte LDAP-Schnittstelle für die Authentifizierung von Benutzer	-	-	+	-	-	W
F59	Anlegen der persönlichen Daten des Benutzers	+	+	+-	+	+	W
F60	Anlegen von Login und Passwort für den Benutzer	+	+	+	+	+	A
F61	Der Zugriff auf die Daten erfolgt passwortgeschützt	+	+	+	+	+	A
F62	Zuweisen von Dienstgruppe(n) an einen Benutzer	-	-	-	-	-	A
F63	Zuweisen einer Rolle an eine Dienstgruppe	-	-	-	-	-	A
F64	Integrierte E-Mail-Funktion	+	+	+	+	+	W
F65	Benachrichtigung- und Erinnerungsfunktion per Mail	-	-	+	-	-	W
F66	Zweidimensionale Zugriffskontrolle durch Zuweisung von Rollen und Diensten	-	-	-	-	-	A
	Nicht-funktionale Anforderungen						
NF01	Die Anwendung muss auf einem System des LRZ installiert werden	+	+	+	+	+	A
NF02	Die Anwendung soll auf einer Linux-Plattform lauffähig sein	+	+	+	+	+	W

Abbildung 3.9: Ergebnisse der Endauswahl 6/7

Nr.	Beschreibung	TestMaker	FormTools	LimeSurvey	Web Survey Toolbox	OpenSurvey Pilot	Priorität
NF03	Software muss dem aktuellen Stand der Softwaremöglichkeiten entsprechen	+	+	+	+	+	A
NF04	Die Anwendung muss fehlerfrei funktionieren	-	+	+	-	-	A
NF05.1	Die Anwendung muss deutsche oder englische Sprache unterstützen	+	+	+	+	+	A
NF05.2	Die Anwendung muss deutsche und englische Sprache unterstützen	+	-	+	-	+	W
NF06	Das System darf vom Benutzer keine Programmierkenntnisse verlangen	+	+	+	+	+	A
NF07	Die Anwendung muss eine intuitiv bedienbare Benutzeroberfläche haben	+	+	+	+	+	W
NF08	Die Dokumentation zur Installation der Anwendung muss vorhanden sein.	+	+	+	+	+	A
NF09	Ein Benutzerhandbuch muss vorhanden sein	+	+	+	-	-	W
NF10	Die Bedingung des Systems muss leicht erlernbar sein.	+	+-	+	+	+	W
NF11	Anpassungen an LRZ-Corporate Identity (Logo, Firmenfarben)	+	+	+	+	+	W
NF12	Mehrbenutzer Betrieb	+	+	+	+	+	A
NF13	Kostenlos	+	+	+	+	+	A
NF14	Open Source	+	+	+	+	+	A
NF15	Unbegrenzte Anzahl der Fragen	+	+	+	+	+	A
NF16	Unbegrenzte Anzahl von Sicherheitskonzepten	+	+	+	+	+	A
NF17	Unbegrenzte Anzahl von Benutzer	+	+	+	+	+	A
	Bewertungsergebnisse	**97**	**88**	**110**	**75**	**81**	

Abbildung 3.10: Ergebnisse der Endauswahl 7/7

4 Prototypenbau

In diesem Kapitel wird die Verwaltung der Sicherheitskonzepte mit Hilfe eines Prototyps demonstriert. Als Werkzeug dafür wird das Tool LimeSurvey verwendet, da es im Kapitel 3 als am besten passendes Tool für die Bedürfnisse des LRZ bewertet wurde.

Die prototypische Implementierung zielt auf die frühzeitige Erkennung der Schwachstellen des entwickelnden Konzeptes und auf die Ermittlung der noch fehlenden Anforderungen. Damit kann man die richtige Entscheidung über weitere Entwicklungsschritte treffen. Ob der erstellte Prototyp nur durch wenige geringfügige Modifikationen zur endgültigen Anwendung weiterentwickelt werden kann oder er bloß nach erheblichen Veränderungen den im Kapitel 3 gestellten Zielen entsprechen wird, kann man mit Hilfe des Prototyps beurteilen.

4.1 Über LimeSurvey

LimeSurvey orientiert sich vor allem auf die Gestaltung und Durchführung von Online-Umfragen, Datenerhebung und Datenverwaltung. Zur Gestaltung der Fragenbogen stehen die Umfrage-, Gruppe- und Frageerstellung-Funktionen zur Verfügung. Zur flexiblen Einstellung der Umfrage bietet LimeSurvey mehr als 30 Fragentypen, Ausdrucksmanager, drei verschiedene Umfragemodi (Frage-für-Frage, Gruppe-für-Gruppe, alles in eins) und viele weitere Features an. Die Zugriffskontrolle erfolgt im LimeSurvey mittels Rechtevergabe an registrierten Benutzern und durch Zugangsschlüsselgenerieren und -Vergabe an Teilnehmer. Die beide Methode haben verschiedene Zwecke. Unter "Benutzer" werden die Personen verstanden, die in das System anmelden und je nach Berechtigungen die Umfragen und gesammelte Daten verwalten können. Im Unterschied zu den Benutzer bekommen Teilnehmer den Zugang nur zur Befragung, indem sie persönliche Zugangsschlüssel per E-Mail erhalten. LimeSurvey verfügt über Import- und Export-Funktion (Text, CSV, MS Excel, PDF, SPSS, R, queXML), Authentifikation-Plugin und weitere Schnittstellen.

LimeSurvey hat eine detaillierte Bedingungsanleitung, die in mehreren Sprachen geschrieben ist[1]. Außerdem gibt es im Internet zahlreiche Handbücher mit Screenshots[2]. Deswegen wird in dieser Arbeit nicht die Beschreibung aller Funktionalitäten von LimeSurvey angegangen. Stattdessen werden ein konkreter Prototyp und die für seinen Aufbau benötigten Optionen betrachtet.

[1] `https://manual.limesurvey.org/LimeSurvey_Manual`

[2] Beispiele für Handbuch: `http://www.statistik.cc/limesurvey/limesurvey.pdf`, `http://www.ph-heidelberg.de/fileadmin/wp/wp-laporte/scripte/ErsteSchritte_-_LimeSurvey.pdf`

4.2 Umgebungsbeschreibung und erste Schritte

Das LRZ hat verschiedene Betriebssysteme im Einsatz. Aber die Anzahl der Rechner mit Linux übertrifft die Anzahl der Rechner mit anderen Betriebssystemen. Debian und SuSE sind dabei die häufigsten Linux-Distributionen. Aus diesem Grund wurde eine der beiden Distributionen, nämlich Debian 6.0.6, für die Erstellung des Prototyps gewählt. Die Installation und Einrichtung von Debian liegt außerhalb dieser Arbeit. Deswegen wurde für Tests eine vorgefertigte Installation benutzt, die man von der Seite `http://virtualboxes.org/images/debian/` herunterladen kann. Auf der Seite kann man auch verschiedene Versionen von Debian-Linux herunterladen und die benötigten Zugangsdaten finden.

LimeSurvey braucht für den Start einen Webserver mit der Unterstützung von PHP und eine Datenbank. Nach einer Überlegung wurde entschieden, als Webserver Apache HTTP Server zu nutzen und als Datenbank MySQL Server. Es ist sinnvoll, alle Komponenten aus dem Debian-Repository zu nehmen. Damit ist die Verwendung der aktuellsten Versionen von Komponenten garantiert. Zum Zeitpunkt des Tests waren dies folgende Versionen:

- Apache HTTP Server 2.4.9[3]
- MySQL Server 5.6.17[4]
- PHP5[5]

Die Installation erfolgt in folgenden Schritten[6]:

1. Installation von MySQL

   ```
   apt-get install mysql-server mysql-client
   ```

   Nach der Installation wird nach dem Namen und dem Passwort des MySQL-Root-Benutzers gefragt.

2. Installation von Webserver

   ```
   apt-get install apache2
   ```

   Root-Verzeichnis für die Documenten ist /var/www. Die Konfiguration wird der Datei /etc/apache2/apache2.conf entnommen.

3. Installation von PHP-Framework mit der benötigten Bibliotheken

   ```
   apt-get install php5 libapache2-mod-php5 php5-mysql php5-ldap php5-imap
   ```

4. Webserver neustarten

   ```
   /etc/init.d/apache2 restart
   ```

[3] `httpd.apache.org`
[4] `www.mysql.de`
[5] `www.php.net`
[6] `http://www.howtoforge.com/installing-apache2-with-php5-and-mysql-support-on-debian-wheezy`

Nachdem alle benötigten Komponenten installiert sind, kann man die letzte Version von LimeSurvey von der offiziellen Webseite herunterladen[7]. Zurzeit ist die aktuelle Version LimeSurvey 2.05[8]. Den Inhalt des Archives muss man mit der Hilfe des Archiv-Managers in das Verzeichnis /var/www entpacken. Bei Bedarf muss man Zugriffsrechte für das Verzeichnis /var/www/limesurvey einrichten, da der Webserver Schreibrechte für das Verzeichnis braucht.

Durch das Ausführen von "http://domain.com/limesurvey/" im Webbrowser startet das Installationsprogramm von LimeSurvey automatisch (siehe Abbildung 4.1). Jetzt werden Schritt für Schritt die Anweisungen zum Einstellen ausgegeben. Die ersten Schritte sind die Sprachauswahl und die Lizenzbestätigung. Danach folgt die Überprüfung, ob alle mi-

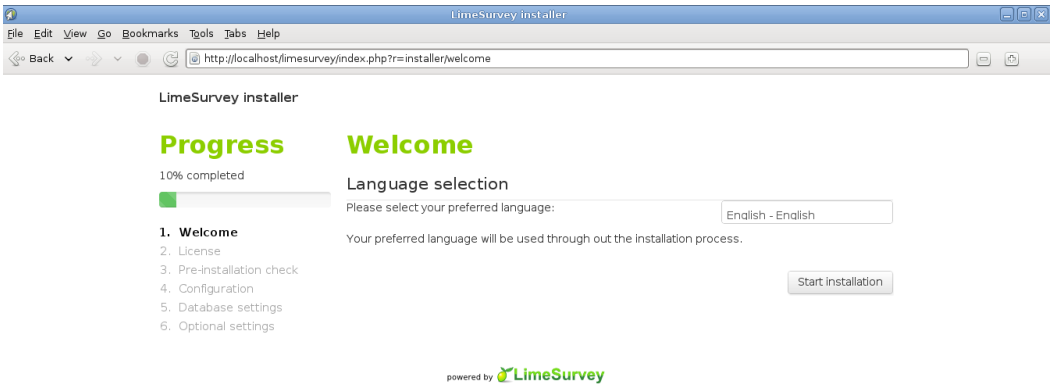


Abbildung 4.1: Beginn der Installation von LimeSurvey

nimal erforderlichen Systemanforderungen für die Installation erfüllt sind (siehe Abbildung 4.2). Mit dem nächsten Schritt wird die Datenbank-Konfiguration vorgenommen, indem Datenbanktyp (hier: MySQL), Datenbank-Location (hier: localhost), Datenbankbenutzer und Password (hier: root/toor) und der Name der Datenbank mit der optionalen Eingabe der Tabellen-Präfix angefragt werden (siehe Abbildung 4.3). Danach wird eine Datenbank erstellt. Schließlich kann der Administrator-Account mit Login-Name und Login-Kennwort (hier: admin/admin) erstellt werden (siehe Abbildung 4.4).

Nachdem das Installationsprogramm fertig ist, kann die Administrationsseite "http://domain.com/limesurvey/admin/" im Webbrowser[9] geöffnet werden. Es wird ein Anmeldefenster geöffnet und nach Benutzername und Kennwort gefragt. Jetzt kann man sich mit früher eingegebenen Administrator-Zugangsdaten im System anmelden. Die Abbildung 4.5 stellt die Login-Seite dar.

[7] `http://www.limesurvey.org/de/herunterladen`
[8] limesurvey205plus-build140414.tar.gz
[9] In dieser Arbeit wurde Ephiphany Web Browser benutzt

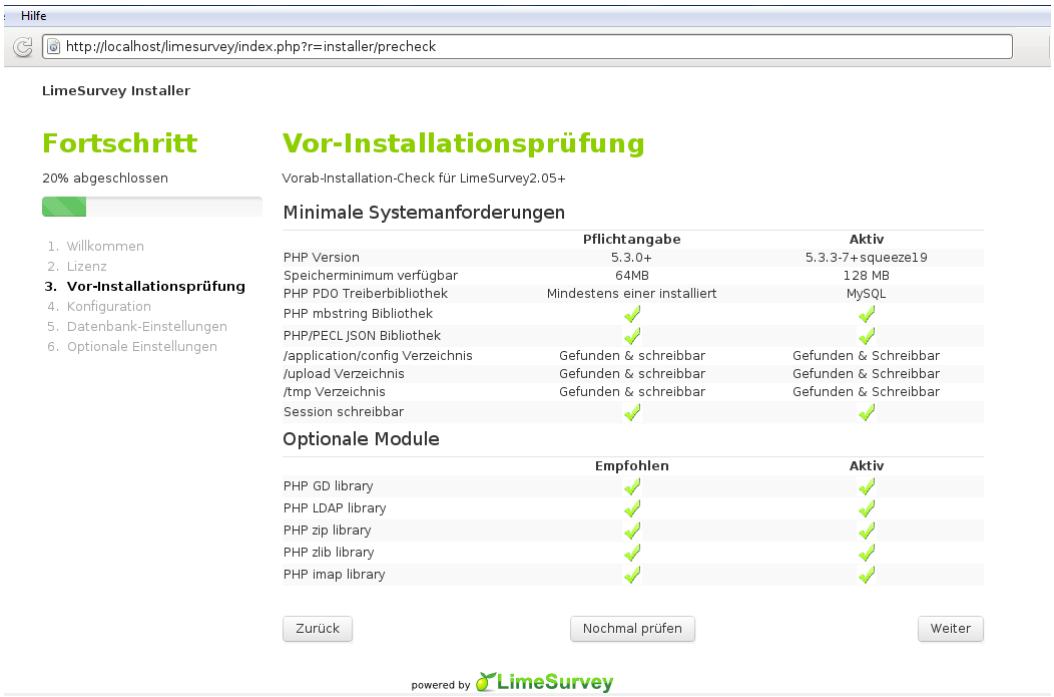


Abbildung 4.2: Installation von LimeSurvey: Vor-Installationsprüfung

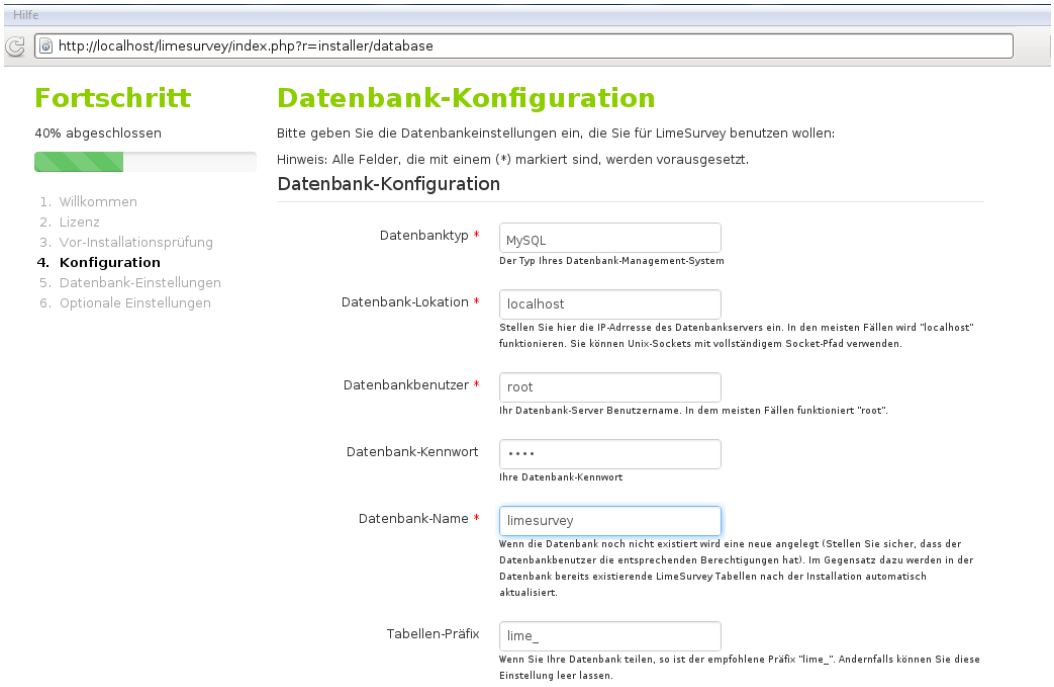


Abbildung 4.3: Installation von LimeSurvey: Datenbank-Konfiguration

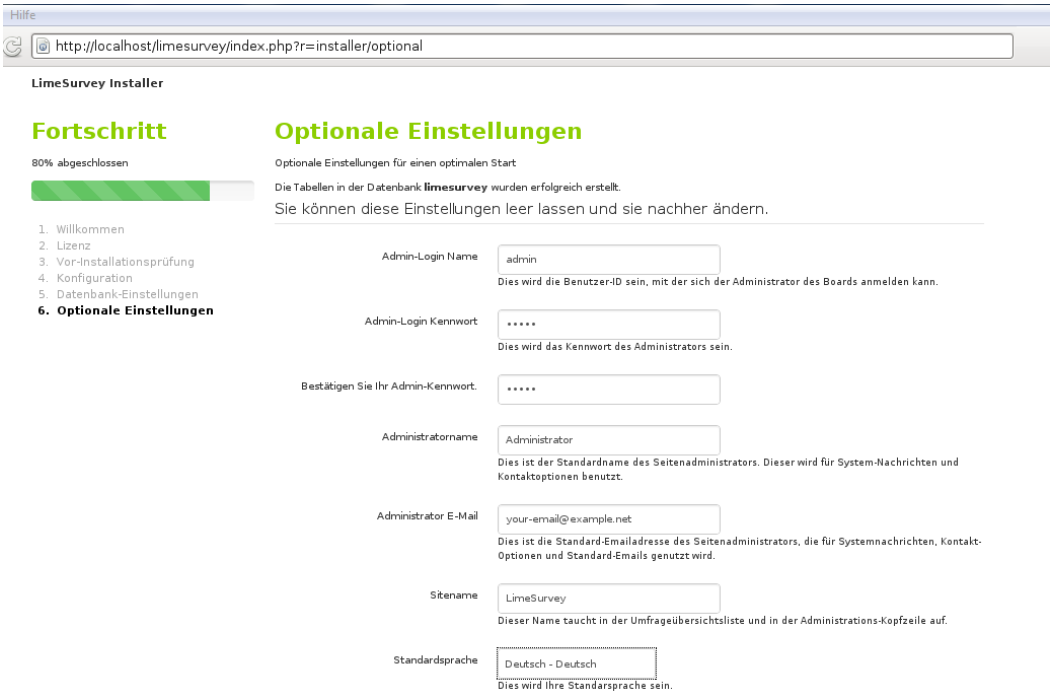


Abbildung 4.4: Installation von LimeSurvey: Anlegen eines Administratoraccounts

Abbildung 4.5: LimeSurvey: Anmelderseite

4.3 Prototypische Implementierung der Sicherheitskonzept-Vorlage

Jetzt ist LimeSurvey installiert und kann man zum Prototypenbau übergehen. Zur Veranschaulichung aller nötigen für Verwaltung der Vorlage und Sicherheitskonzepten Funktionen genügt es, einen Abschnitt der Vorlage zu nehmen. Nach den nachfolgenden Überlegungen wurden für die Repräsentation das Titelblatt und das erste Kapitel genommen. Zunächst enthält der Anfang des Dokuments grundlegende Informationen zum Sicherheitskonzept und zum Dienst, was beim Erstellen des Prototyps eines Sicherheitskonzeptes das Verständnis erleichtert. Außerdem enthalten die beiden Abschnitte alle in der Vorlage enthaltenen Fragetypen (Freie Texte, Checkboxen, Tabellen, Arrays, Datums- und Zeiteingaben) und sind strukturell komplizierter als die nachfolgenden zwei Kapitel aufgebaut. Die ausgewählten Abschnitte sind am meisten zur Demonstration der ganzen Vorlage geeignet. Im Weiteren werden die Teile des Prototyps mit Hilfe der Screenshots repräsentiert und ihre Implementierung genauer betrachtet. Für den Fragen mit mehr Mals wiederholten und bereits beschriebenen Fragentypen werden nur Screenshots angegeben.

Nach der erfolgreichen Anmeldung als Administrator im System wurde einige globale Einstellungen vorgenommen. So bekam die Hauptseite den Überschrift "System für Verwaltung von dienstspezifischen Sicherheitskonzepten". Die Basissprache des Verwaltungssystems ist Deutsch. Für das System wurde den Stil "darkblue" gewählt. Außerdem wurde noch eine von zehn vorgegebenen Präsentationsschablonen zur Demonstration von Fragenbogen gewählt. Die Designvorlage "vallendar" hat den Vorteil, dass ein Logo auf dem Dokument angezeigt wird und selbstverständlich auf das Logo des LRZ geändert werden kann. Daneben ist die Schablone in blau, weiß und grau gestaltet und widerspricht nicht dem Erscheinungsbild des LRZ. Beide Designstile sind gut kombiniert mit einander. Nach diesen Einstellungen ist die Seite wie folgt aussieht (siehe Abbildung 4.6).

Abbildung 4.6: Die Hauptseite des Systems

Für den Prototyp der Dokumentvorlage wurden ein neuer Fragebogen angelegt und im angebotenen Fenster die folgenden allgemeinen Einstellungen vorgenommen:

- Titel "Sicherheitskonzept-Vorlage v1.0.0[10]"
- Kurze Beschreibung "Diese Dokumentvorlage dient zum Erstellen von dienstspezifischen Sicherheitskonzepten"

[10] v1.0.0 steht für den Versionsnummer der verwendeten Dokumentvorlage

- Einen Begrüßungstext "Willkommen! Sie können sofort mit dem Erstellen eines dienstspezifischen Sicherheitskonzepts anfangen. Sie können jederzeit die Arbeit aussetzen und später fortsetzen."
- Antworten auf diese Umfrage sind NICHT anonymisiert
- Es wird eine Gruppe pro Seite (Gruppe für Gruppe) angezeigt
- Ein vollständiges Frageverzeichnis wird angezeigt
- Springen zwischen Fragen hin und her ist erlaubt
- Teilnehmer können eine teilweise fertig gestellte Umfrage zwischenspeichern

Alle diese Einstellungen können später verändert werden. Außerdem wurde das Logotyp des LRZ auf der Willkommen- und Fragenbogen-Seiten platziert, indem das Logobild im Ordner "vallendar"[11] angelegt wurde. Um das Logo auf Willkomenseite anzuzeigen, wurde die Zeile

```
<img src="{TEMPLATEURL}logoLRZ.png" align="right">
```

in Datei welcome.pstpl hinzugefügt. Für die Fragebogenseite musste man in der Datei survey.pstpl die bereits existierende Logo-Datei auf Logo des LRZ[12] ändern.

LimeSurvey bietet eine Option, die Vorschau und Test der Umfrage während ihres Erstellungsprozesses ermöglicht. Beim Aufrufen dieser Option lässt sich die Vorlage in einem neuen Browser-Fenster öffnen. Die Abbildung 4.7 stellt die erste Seite der erstellten Vorlage aus Sicht des Benutzers dar.

Abbildung 4.7: Prototyp der ersten Seite der Sicherheitskonzept-Vorlage

Nach dem Anlegen der Vorlage wurden nacheinander die Fragengruppen des zur Repräsentation ausgewählten Abschnittes angelegt. Ausgehend aus der Besonderheit von LimeSurvey, mit dem das Untergruppenanlegen unmöglich ist, wurde die Struktur der Vorlage mit ihrer Kapitel-, Abschnitt- und Unterabschnitt-Verteilung vereinfacht. Aus Unterabschnitten

[11] Pfad: limesurvey/templates/vallendar
[12] logoLRZ.png

wurden Gruppen gebildet und Kapitel- und Abschnitt-Benennung ignoriert. Das Fragenverzeichis (oder Fragenindex) bietet dem Benutzer einen Übersicht über den Inhalt des Fragenbogens. Es wird auf der rechten Seite angezeigt und gibt die Möglichkeit den Benutzer zwischen den beliebigen Abschnitten hin und her springen. Die Abbildung 4.8 stellt das Inhaltsverzeichnis der prototypisch erstellten Vorlage dar.

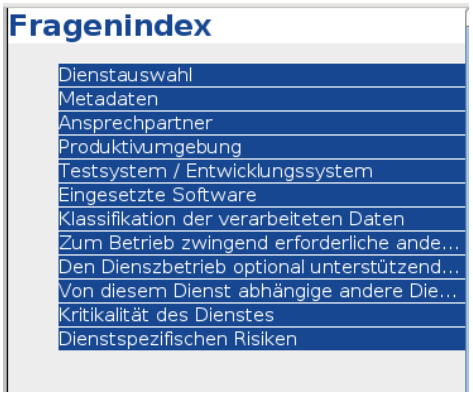
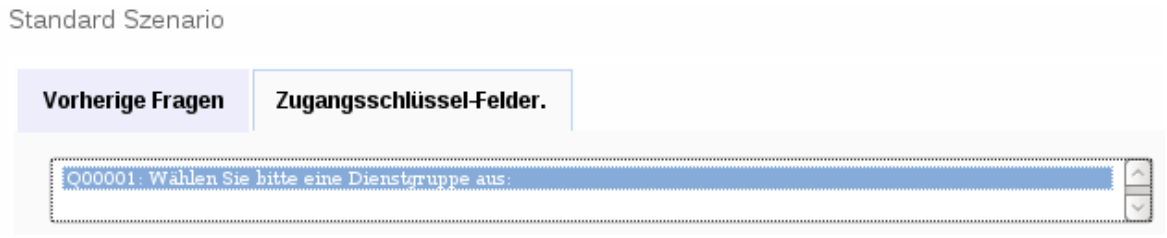


Abbildung 4.8: Prototyp der Sicherheitskonzept-Vorlage: Das Inhaltsverzeichnis

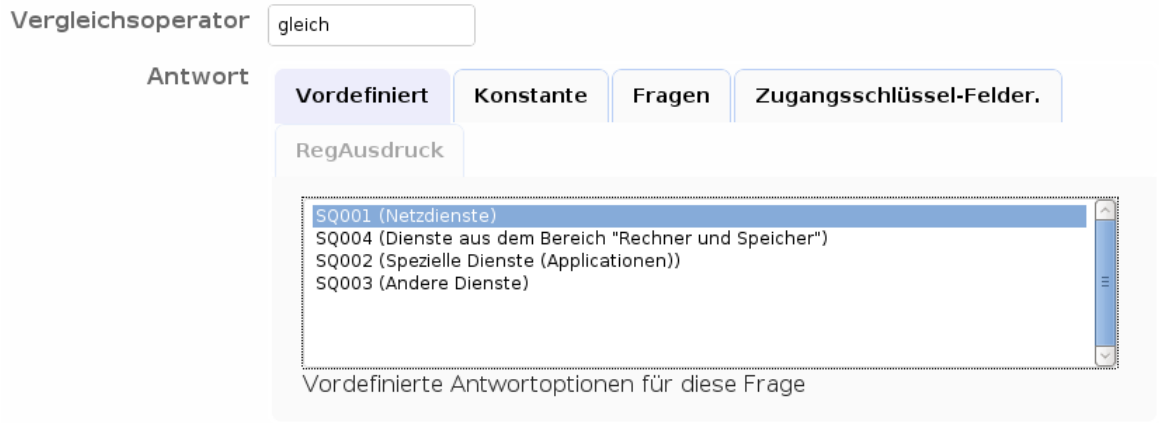
Innerhalb jeder Fragengruppe wurden Fragen formuliert. Neben der eigentlichen Frage muss man auch einen eindeutigen Code manuell angeben, über den Limesurvey später die Antworten zuordnet. In der ersten Fragegruppe "Dienstauswahl" muss man den Dienst auswählen, für den das Sicherheitskonzept zu erfassten ist. Alle am LRZ betriebenen Dienste müssen vom Administrator angegeben werden. Die Liste der Dienste kann man als Checkboxen oder als Auswahlliste angeben. Hier wurde für die erste Variante entschieden, weil diese für eine oder mehrere Dienste das Erstellen eines Sicherheitskonzeptes ermöglicht. Um eine lange und übersichtliche Aufzählung von ungefähr 80 Diensten zu vermeiden, wurden sie gruppiert. Erst wird nach der Dienstgruppe gefragt und danach werden je nach der Antwort dazugehörige Dienste angezeigt. Dies wird mit der Hilfe eines sogenannten Bedingungs-Designers erreicht. Die Abbildung 4.9 stellt das detaillierte Vorgehen beim Bedingungsdefinition für die Frage "Dienstname" mit dem Code Q00002 dar. Diese konkrete Frage enthält die Liste der Diensten, die in Netzinfrastruktur eingesetzt sind, und muss angezeigt werden nur wenn in der vorherigen Frage die Gruppe "Netzdienste" selektiert ist. Indem für diese eine vorherige Frage und eine entsprechende Antwortalternative selektiert werden und daneben ein Vergleichsoperator bestimmt wird, wird eine Anzeigebedingung hinzugefügt. Die Abbildung 4.10 zeigt die Vorlage aus Sicht des Benutzers und stellt der dynamische Aufbau der angezeigten Fragen dar. Es ist zu bemerken, dass beide Fragen Pflichtfelder sind. Dies wird durch das rote Sternchen links von der Frage signalisiert.

Nach der Auswahl des Dienstes wird auf nächsten Seiten den Überschrift angezeigt "Sicherheitskonzept für *Dienstname*". Wobei der Name generisch zugewiesen wird. Dieser Effekt wird erreicht mit Hilfe des Ausdrucksmanagers von LimeSurvey[13]. Die Antwort ist eine Variable und der Ausdrucksmanager erlaubt auf Variablen über die Frage-Nummer zu beziehen. Je nach dem Fragentyp und nach dem verwendeten Funktionen, ermöglicht der Ausdrucksmanager auf bestimmte Eigenschaften der Fragen zuzugreifen. So mit der Variable der Form

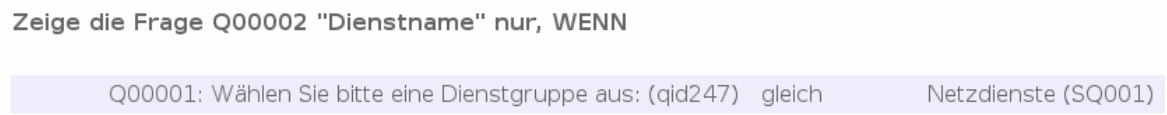
[13] `https://manual.limesurvey.org/Expression_Manager/de#Zugang_zu_Variablen`



(a) Auswahl der vorherigen Frage

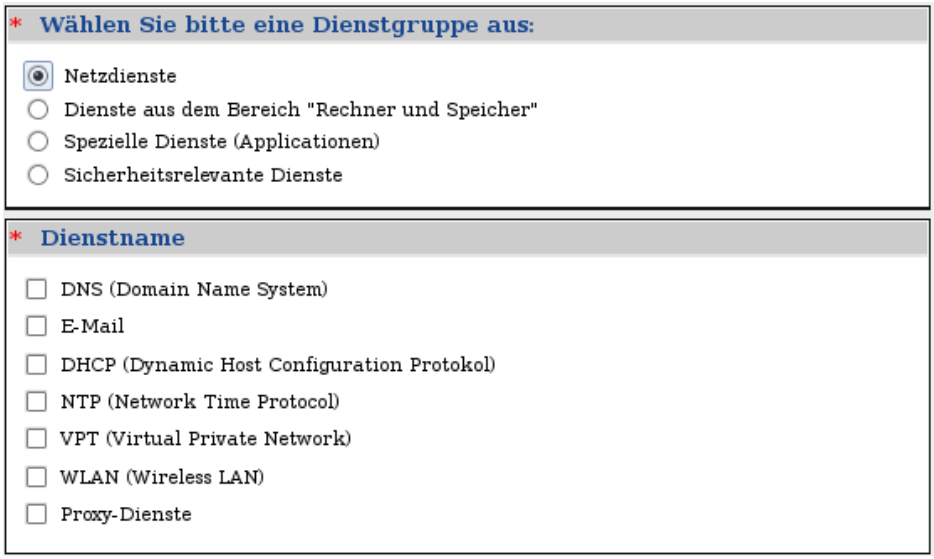


(b) Auswahl des Vergleichsoperators und der Antwort der vorheriger Frage

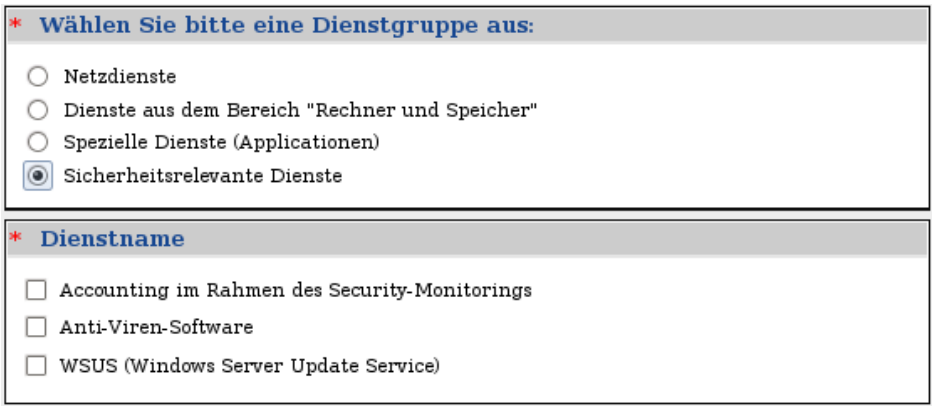


(c) Die hinzugefügte Bedingung

Abbildung 4.9: Prototyp der Sicherheitskonzept-Vorlage: Definition der elementaren Bedingung



(a) Die Gruppe "Netzdienste" ausgewählt



(b) Die Gruppe "Sicherheitsrelevante Dienste" ausgewählt

Abbildung 4.10: Prototyp der Sicherheitskonzept-Vorlage: Die Auswahl einer Dienstgruppe und das Anzeigen dazugehöriger Dienste

`{Q00002_SQ001.shown}`

lässt sich den Wert der Antwortalternative anzeigen. Q00002 und SQ001 stehen für Frage- und Subfrage-Code und shown-Funktion zeigt den Fragenwert (hier: DNS (Domain Name System)). Durch das Hinzufügen der Variablen mit allen Fragen-Coden in der Datei survey.pstl, die das obere Kopfteil (engl. Header) des Fragebogens repräsentiert, wird der Überschrift "Sicherheitskonzepte für *Dienstname*" bedingt auf der Basis anderer Werte angezeigt. Die Abbildung 4.11 stellt die Änderung des Seitenüberschrifteis bei der Auswahl verschiedener Dienste dar.

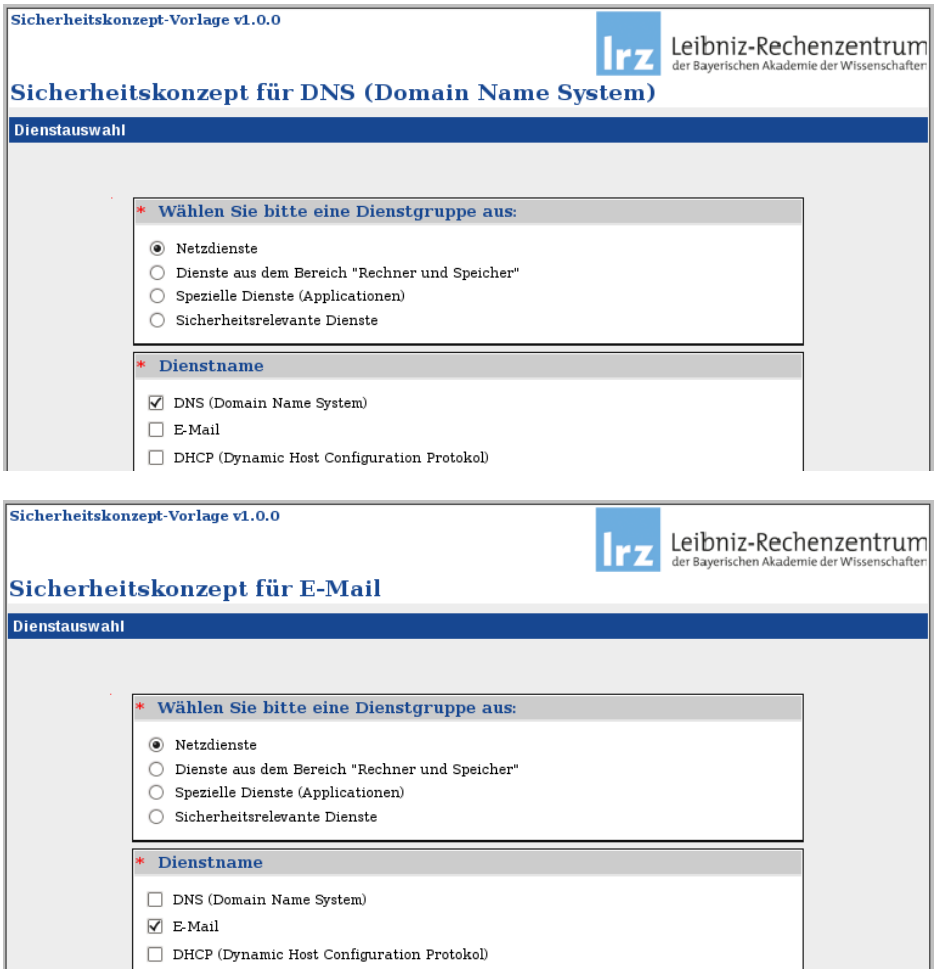


Abbildung 4.11: Prototyp der Sicherheitskonzept-Vorlage: Dynamische Änderung des Überschriftes

Die nächste Fragengruppe heißt "Metadaten". Sie wird im Folgenden genauer betrachtet, weil sie aus der Fragen verschiedener Typen besteht. Zur Autorenangabe wurde ein Fragentyp ausgewählt, der mehrfache kurze Texte nebeneinander platziert. Da während des Ausfüllens kein neues Textfeld hinzugefügt werden kann und die Anzahl der Autoren eher selten drei überschreitet, wurden drei Felder angelegt. Mindestens eines von ihnen ist auszufüllen. Diese Bedingung wird durch die Eingabe der minimalen Antwortanzahl in den erweiterten Einstellungen der Frage. Die Abbildung 4.12 demonstriert das Anlegen der Frage "Autor", das

Festlegen der Frageneigenschaften und das Anzeigen der Frage aus Sichten des Administrators und des Benutzers. Nach gleichem Prinzip sind die Felder für Verteiler des Sicherheitskonzeptes aufgebaut.

Eine Alternative dieser Lösung ist die Frage "Freigegeben von", diese bietet Mehrfachauswahlfelder mit Kommentar. Hier ist die Frage als "Pflichtfrage" eingestellt und mindestens eine Antwortalternative muss ausgewählt und kommentiert werden (siehe Abbildung 4.13). Die Vertraulichkeitsstufe lässt sich gut mit den Radiobuttons darstellen, da nur eine Antwortauswahl möglich ist.

Das Datum der nächsten Aktualisierung des Sicherheitskonzeptes muss im Format "Monat/Jahr" dargestellt werden. Zu diesem Zweck stellt LimeSurvey einen speziellen Typ "Datum/Zeit" zur Verfügung. Je nach Bedarf kann das Format variieren. Dafür muss man in erweiterten Einstellungen ein bestimmtes Datum/Zeit-Format in der Form "d/dd m/mm yy/yyyy H/HH M/MM" für "Tag/Monat/Jahr/Stunde/Minute" angeben. Das Datum der letzten Änderung muss genauer angegeben werden, und zwar im Format "dd mm yyyy". In einem weiteren Abschnitt soll eine kritische Dauerzeit beim Dienstausfall Stunden und Minuten angegeben werden. Die Einstellung des Formates der Frage muss man auf "HH MM" setzen. Die Abbildung 4.14 stellt die verschiedene Möglichkeiten Datum und Zeit anzugeben dar.

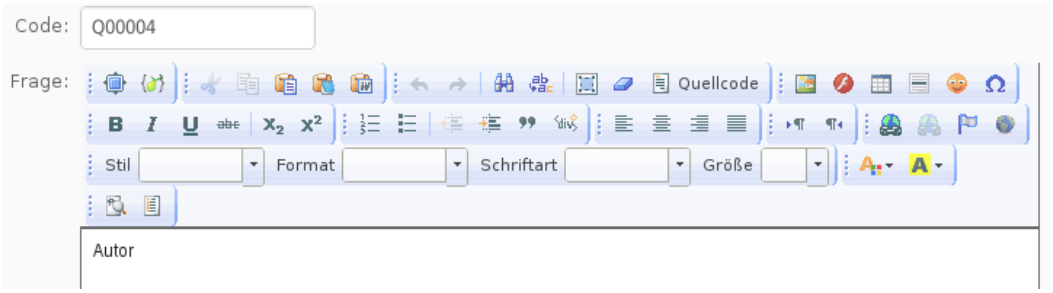
Beim Übergang zur nächsten Gruppe von Fragen durch das Drucken auf "Weiter"-Knopf werden alle Pflichtfelder auf Vorhandensein der Antworten geprüft.

Der nächsten Abschnitt der Vorlage besteht aus einer Tabelle (siehe Abbildung 4.1), in der die Ansprechpartners je nach ihrer Zuständigkeit genannt werden müssen. Aus der Ab-

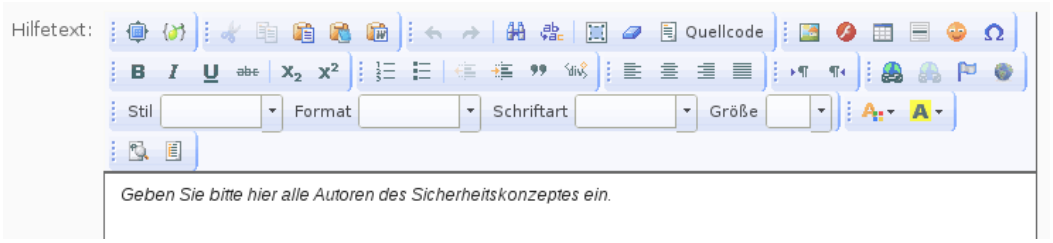
Zuständig für	**Name des Ansprechpartners**	**Tel. oder E-Mail**
Hardware		
Betriebssystem		
Netzanschluss		
Dienstbetrieb		
Herstellersupport		
PKI / Zertifikate		
Sicherheitsvorfälle		
...		

Tabelle 4.1: Die Tabelle "Ansprechpartner"

bildung folgt, dass die Spalte "Zuständig für" mit den vorgeschlagenen Angaben ausgefüllt ist. Das sollte das Ausfüllen vereinfachen. Außerdem können bei Bedarf weiter Zeilen ergänzt werden. LimeSurvey verfügt über die Matrixfragen-Typen, mit denen sich Tabelle mit verschiedenen Angabegemäßen realisieren lassen. Beispielweise die Tabelle für Ansprechpartner muss die Textangaben erhalten. Die Nachteil der Matrixen-Typen in LimeSurvey liegt darin, dass keine neue Zeile während des Beantwortens hinzugefügt werden können. Außerdem können in der Tabelle keine Einträge vorgegeben werden. Deswegen ist eine der möglichen Lösungen sieht folgendermaßen aus (siehe Abbildung 4.15): es wird angenommen, dass für

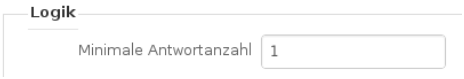


(a) Eingabe des Fragencodes und des Fragentextes

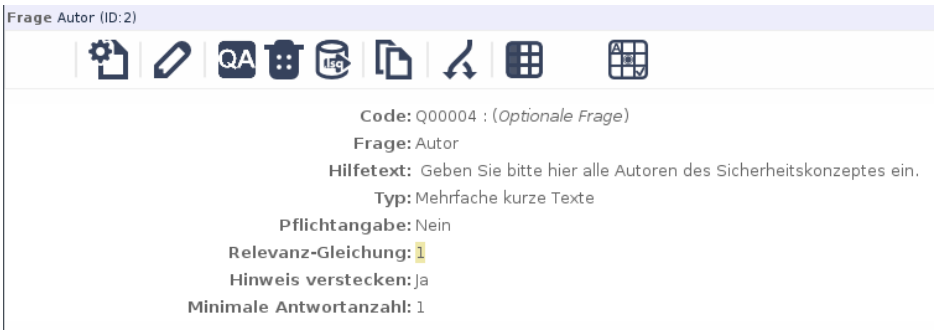


(b) Eingabe des Hilfetextes

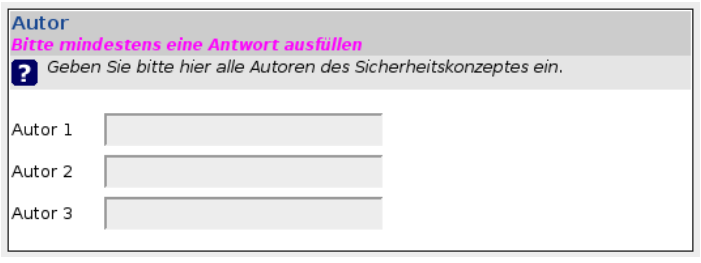
(c) Bestimmen der Frageeigenschaften



(d) Eingabe der minimalen Anzahl der Pflichteingaben



(e) Frage aus der Sicht des Administrators



(f) Frage aus der Sicht des Benutzers

Abbildung 4.12: Prototyp der Sicherheitskonzept-Vorlage: Das Vorgehen beim Anlegen der Frage ”Autor”

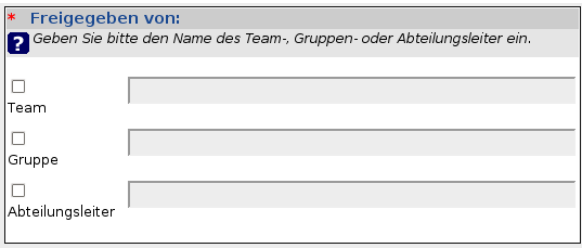
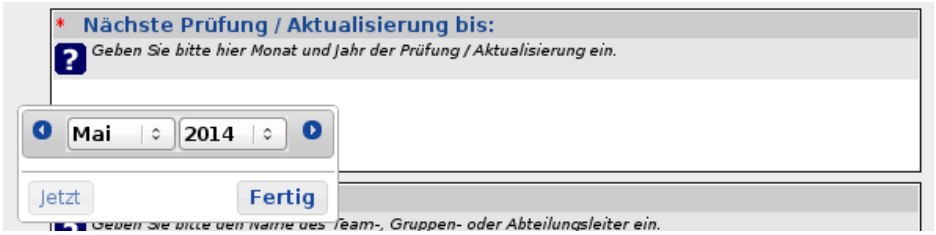


Abbildung 4.13: Prototyp der Sicherheitskonzept-Vorlage: Die Frage "Freigegeben von:" aus der Sicht des Benutzers



(a) Die Frage "Nächste Prüfung / Aktualisierung" erwartet die Angabe im Format "Monat/Jahr"

(b) Die Frage "Letzte Änderung" erwartet die Angabe im Format "Tag/Monat/Jahr"

(c) Die Frage "Kritische Dauerzeit beim Dienstausfall" erwartet die Angabe im Format "Stunde/Minute"

Abbildung 4.14: Prototyp der Sicherheitskonzept-Vorlage: Die Fragen des Datum/Zeit-Types

einen Dienst unwahrscheinlich mehr als 8 Ansprechpartner angegeben kann und eine Matrize mit den entsprechend der oben gezeigten Tabelle Spalten und mit acht Zeilen erstellt. Daneben ist eine Spalte "Kommentar" für zusätzliche Information hinzugefügt. Hinweise zum Ausfüllen der Vorlage können mit dem Fragentyp "Textanzeige" erfasst werden.
Die nachfolgende Gruppe der Fragen befasst sich mit den wichtigen Eckdaten der zur Diensterbringung eingesetzten Maschinen, die sich in physische Hardware und virtuelle Maschine (VM) unterteilen lassen. Je nach dem Typ der Maschine unterscheiden sich einige Umgebungscharakteristiken. Ist das Typ der Maschine "physisch", sind Standort, Rackreihe und Rack anzugeben. Bei virtuellen Maschinen gibt man VMware-Cluster und VMware-Host an. Durch die Definition von Bedingungen nach dem bereits beschriebenen Vorgang

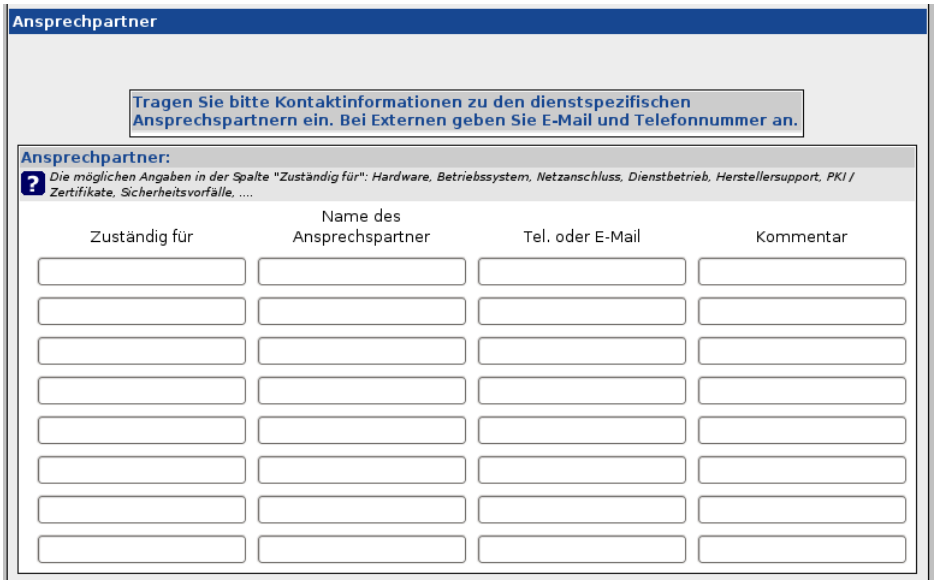


Abbildung 4.15: Prototyp der Sicherheitskonzept-Vorlage: Die Tabelle für die Frage "Ansprechpartner"

werden die entsprechenden Fragen angezeigt. Der Dienst kann aus mehreren grundlegend verschiedenen konfigurierten Maschinen bestehen. In diesem Fall müssen die Felder entsprechend vervielfältigt werden können. In dieser Arbeit wird dieser Abschnitt folgendermaßen realisiert (siehe Abbildung 4.16).

Erst wird gefragt, ob die Eckdaten nur für eine Maschine oder für mehrere anzugeben sind. Bei mehrere Maschinen werden zusätzliche Felder sichtbar. Die Auswahl des Maschinentyps lässt sich gut mit dem Einfachauswahl-Typ, der nur eine mögliche Eingabe bietet, realisieren. Die Felder für IP-Adressen und DNS sind vom Typ "Lange freie Text", was mehrere Eingaben in einem Feld ermöglicht. Die Abbildung 4.17 veranschaulicht die Fragen, die je nach dem ausgewählten Maschinentyp angezeigt werden. Für die Frage "Standort der physischen Maschinen" wurde einen Typ 'Mehrfachauswahl" ausgewählt, der noch auf eine selbe zu auszufüllenden Feld erweitert. Dadurch hat der Benutzer eine Möglichkeit, einen nicht vorgeschlagen in der Vorlage Antwort hinzufügen. Mit dem Textfeld, der sich auf nummerische Werte begrenzt, wird es besorgt, dass beim Rackreihe-Angabe nur die Ziffer eingetragenen können. Die Frage "Rack" verlangt die Buchstabeneinträge. Diese und weitere Einschränkungen der Eingabewerten kann man mit Hilfe der regulären Ausdrücken[14] erreichen. Um eine bestehende aus Buchstaben Eingabe zu verlangen muss man in der Feld "Validierung" den folgenden Ausdruck eintragen: /[A-Za-z]+/.

Für die Angabe von Daten weiterer Maschinen sollen alle Fragen des Abschnittes "Produktivumgebung" vom Administrator kopiert und beim Auswahl "mehrere Maschinen" dem Benutzer angezeigt werden. Ähnlich diesem Abschnitt lässt sich die Fragengruppe "Testsystem / Entwicklungssystem" aufbauen. Erst wird gefragt, ob überhaupt eine Test- oder Entwicklungssystem im Einsatz kommt. Ist die Frage "Ja" beantwortet, werden die Fragen

[14] `https://manual.limesurvey.org/Using_regular_expressions/de`

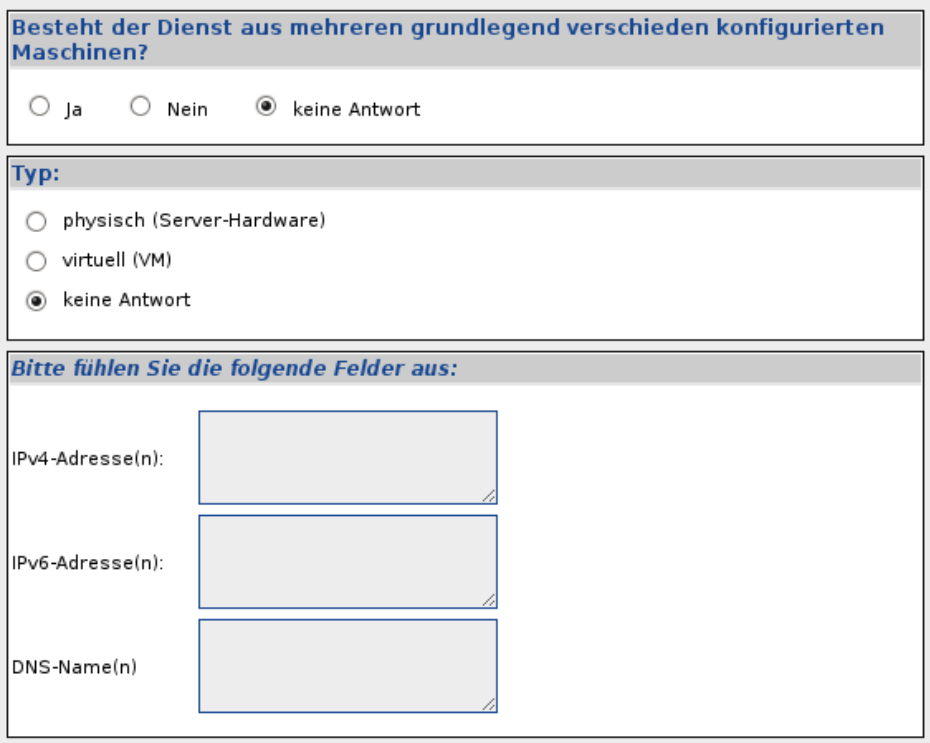
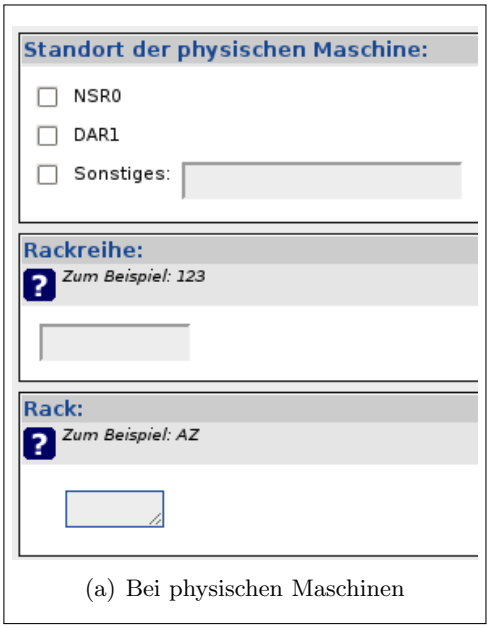
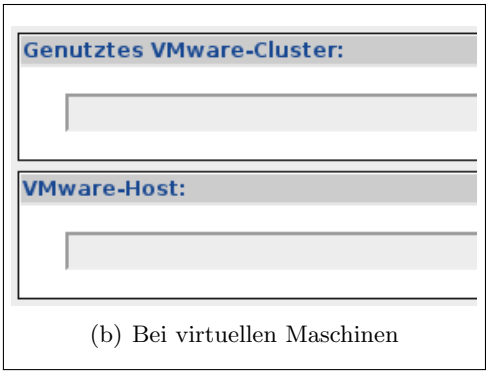


Abbildung 4.16: Prototyp der Sicherheitskonzept-Vorlage: Der Abschnitt "Produktivumgebung"



(a) Bei physischen Maschinen



(b) Bei virtuellen Maschinen

Abbildung 4.17: Prototyp der Sicherheitskonzept-Vorlage: Die Fragen, die sich je nach dem ausgewählten Maschinentyp anzeigen lassen

aus vorherigen Abschnitt angezeigt. Im anderen Fall wird man zur nächsten Fragengruppe, in der es über eingesetzten Software geht, übergegangen. Dort muss man Information über das Betriebssystem, Name und Version der Software in Textfelder eingetragen.

Der Abschnitt "Klassifikation der Verarbeiteten Daten" besteht aus der Fragen, die sich mit den oben beschriebenen Fragentypen realisieren. In den nächsten zwei Abschnitten sollen die zum Dienstbetrieb erforderliche und unterstützende andere Dienste mit ihren wichtigsten Eckdaten genannt werden. Dies wird durch eine Auflistung der vorgegebenen Antwortmöglichkeiten realisiert. Wobei jeweils Dienst ist eine Frage des Typs "Ja/Nein". Ist bei einem Dienst "Ja" beantwortet, wird in der nächsten angezeigten Frage den Textfeld zum Eckdatenangabe angefragt. Ist der Dienst nicht in der Liste, kann er in einem freiem Textfeld am Ende der Fragengruppe eingetragen werden. Auf ähnlicher Weise kann der Abschnitt für den abhängigen von diesem Dienst implementiert werden.

In dem nächstfolgenden Teil muss die Kritikalität des Dienstes beurteilt werden, indem die Fragen über Benutzergruppen und welche Auswirkungen Ausfallzeiten haben. In der letzte Frage soll Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit beurteilt werden. Zu diesem Zweck passt gut das Fragentyp "Matrix". Auf X-Achse wird einen Wert angegeben, auf der Y-Achse sind die drei Grundziele der IT-Sicherheit. Der letzten Abschnitt des Prototyps enthält Information über mögliche Risiken des Dienstes.

Damit die Dienstverantwortlichen den Fragenbogen ausfüllen können, muss die Vorlage freigegeben werden. Dieser Freigabeprozess heißt in LimeSurvey "Umfrageaktivieren". Nach dem Aktivieren sind die Änderungen der Vorlage stark begrenzt. Es besteht die Möglichkeit Fragentext oder -Reihenfolge zu ändern, aber es können keine neuen Fragen hinzugefügt werden. Deswegen soll die Vorlage vor der Aktivierung sorgfältig überprüft werden.

Nachdem der Prototyp der Dokumentvorlage erstellt und freigegeben ist, kann man zum prototypischen Erstellen des Sicherheitskonzeptes übergehen. Dafür führt man die Umfrage aus. Für den Prototyp wurde das Sicherheitskonzept für das "Accounting im Rahmen des Security-Monitorings" erstellt, da ein ausgefülltes im PDF Beispiel für diesen Dienst vorlag.

Nach der Dienstname-Auswahl wurden die Metadaten für das Sicherheitskonzept ausgefüllt. Die folgenden drei Abbildungen zeigen die eingetragenen Antworten auf die Fragen aus der verschiedenen Abschnitten der Vorlage. Die Abbildung 4.18 repräsentiert einige ausgefüllten Felder aus dem Metadaten-Abschnitt. Die Abbildung 4.19 stellt die ausgefüllte Tabelle "Ansprechpartner" (siehe auch die Abbildung 4.15) dar. Die Abbildung 4.20 zeigt der Produktivumgebungsabschnitt. Schrittweise wurde der Prototyp der Vorlage ausgefüllt und gespeichert.

Alle Sicherheitskonzepte, sowohl die vollständig ausgefüllten als auch die zwischengespeicherten, können angesehen werden. Die Abbildung 4.21 gibt einen Überblick über verschiedene Möglichkeiten zum Anzeigen der erfassten Sicherheitskonzepte. Die Antworten werden in der Form angezeigt, wie in der Abbildung 4.21 dargestellt ist. Man kann sehen, dass für jede Frage eine eigene Zeile angelegt wird, in der die Antwort, wenn sie vorhanden ist, angezeigt wird. Es gibt eine Möglichkeit, das Sicherheitskonzept in eine Datei, zum Beispiel in eine PDF- oder Microsoft Word-Datei, zu exportieren und dann zu lesen.

(a) Angaben zu den Autoren und zum Vertraulichkeitsgrad des Sicherheitskonzeptes

(b) Angaben zu den Verteiler des Sicherheitskonzeptes

Abbildung 4.18: Prototyp des Sicherheitskonzeptes: Die ausgefüllten Metadaten

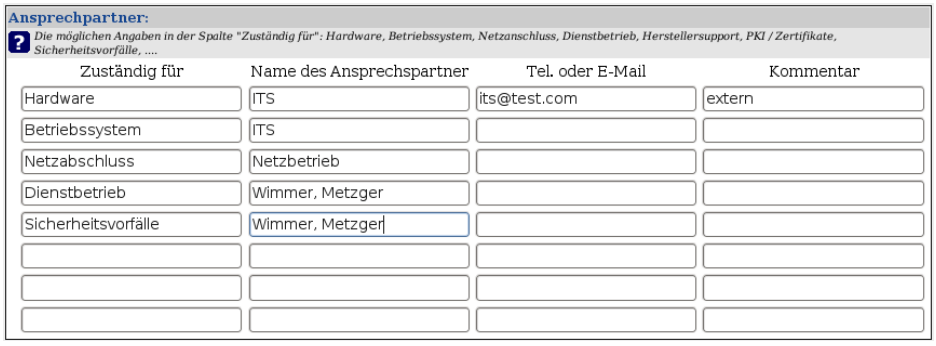


Abbildung 4.19: Prototyp des Sicherheitskonzeptes: Die ausgefüllte Tabelle "Ansprechpartner"

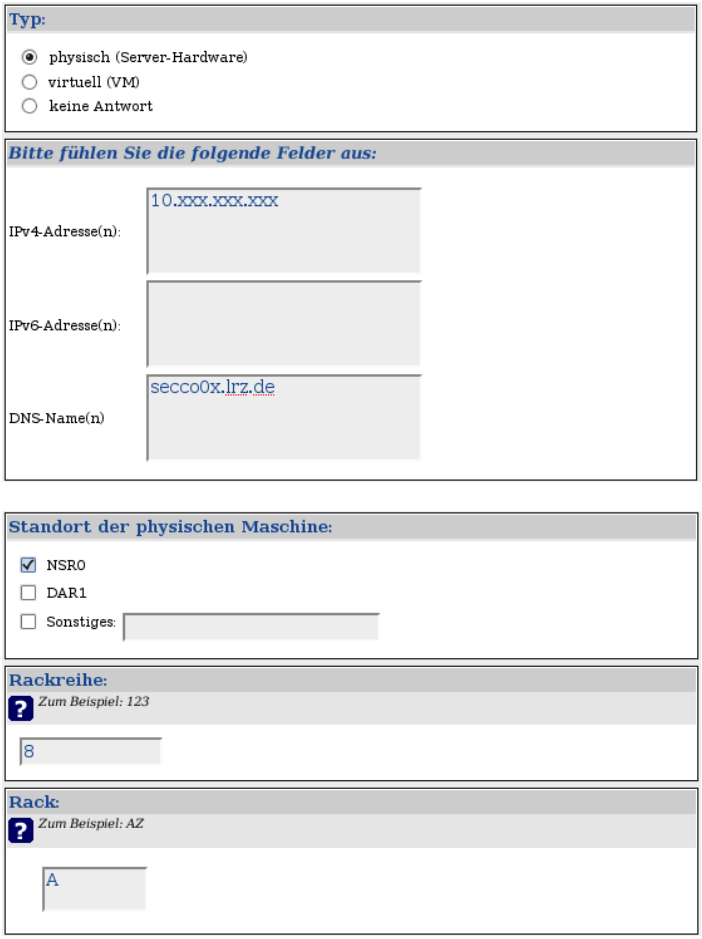


Abbildung 4.20: Prototyp des Sicherheitskonzeptes: Angaben zur Produktivumgebung des Dienstes

[Q00023] Typ:	physisch (Server-Hardware) [SQ3]
[Q00024_SQ001] Bitte fühlen Sie die folgende Felder aus:(IPv4-Adresse(n):)	10.xxx.xxx.xxx
[Q00024_SQ002] Bitte fühlen Sie die folgende Felder aus:(IPv6-Adresse(n):)	
[Q00024_SQ003] Bitte fühlen Sie die folgende Felder aus:(DNS-Name(n))	secco0x.lrz.de
[Q00025_SQ001] Standort der physischen Maschine:(NSR0)	Ja [Y]
[Q00025_SQ002] Standort der physischen Maschine:(DAR1)	
[Q00025_other] Standort der physischen Maschine:(Sonstiges)	
[Q00026] Rackreihe:	8
[Q00027] Rack:	A

(a) Ansehen der Antwortdetails im System

Bitte fühlen Sie die folgende Felder aus: [DNS-Name(n)]	secco0x.lrz.de
Standort der physischen Maschine: [NSR0]	Ja
Standort der physischen Maschine: [DAR1]	Nein
Standort der physischen Maschine: [Sonstiges]	
Rackreihe:	8.0000000000
Rack:	A

(b) Ansehen der Antwortdetails nach dem Export in Microsoft-Word-Datei

Abbildung 4.21: Prototyp des Sicherheitskonzeptes: Ansehen der Antwortdetails

Zum Schluß der Prototypenbau wird es im nächsten Abschnitt eine Zusammenfassung vorgestellt.

4.4 Beurteilung von LimeSurvey anhand des entwickelnden Konzeptes

Die prototypische Implementierung des Konzepts hat gezeigt, dass die Verwaltung von Sicherheitskonzepten mit LimeSurvey möglich ist. LimeSurvey hat sicherlich viele Vorteile, die beim Verwalten von dynamischen Sicherheitsdokumenten benötigt werden können. Die wichtigsten Vorteile sind:

- Unbegrenzte Anzahl von Fragen, Fragenbögen und Benutzern
- Über 30 verschiedene Fragentypen, die durch weitere Einstellungen angepasst werden können
- Auf Bedingungen basierte Verzweigungslogik
- Speichern und Wiederverwenden von Antwortalternativen als Schablone
- Kopieren und Wiederverwenden der Fragen und des Fragenbogens
- Testen der Vorlage während des Erstellungsprozesses
- Benutzerverwaltung mit gezielter Rechtevergabe auf Fragenbogenbasis

- LDAP-Schnittstelle für Import der Benutzerdaten und für Benutzerauthentifizierung
- Import-/Export-Schnittstelle mit Unterstützung vieler Formate

Neben allen Vorteilen gibt es aber auch viele Probleme. Einige davon können indirekt gelöst werden.

Problem 1: Nach dem Aktivieren der Vorlage ist das Hinzufügen von Fragengruppen, Fragen und vordefinierten Antworten nicht mehr möglich. Um den Fragenbogen bearbeiten zu können, muss er deaktiviert werden. Aber nach dem Deaktivieren sind alle gespeicherten Antworten in eine separate Archiv-Tabelle verschoben und nicht mehr abrufbar.
Lösung: Die zu bearbeitende Vorlage kann kopiert und auf dieser Kopie alle nötigen Änderungen vorgenommen werden. Dabei können die Ergebnisse aus der alten Vorlage exportiert und in die neue Vorlage importiert werden. Für dieses Ziel bietet LimeSurvey VV-Import und VV-Export[15] an. Dann kann die kopierte und geänderte Vorlage als eine neue Version der Sicherheitskonzept-Vorlage angesehen werden.

Problem 2: Die Realisierung der zweidimensionalen Zugriffskontrolle, wie im entwickelnden Konzept vorgeschlagen, ist unmöglich. Es gibt in LimeSurvey keine Angabe- und Steuerungsstruktur für Dienste. Während die Zugriffe auf den Fragenbogen für Dienst-Administratoren mit Hilfe von Zugangsschlüsseln gesteuert werden können, ist die Zugriffskontrolle auf die erstellten Sicherheitskonzepte trivial. Obwohl die Berechtigungen zum Erstellen, Anzeigen, Aktualisieren, Löschen, Exportieren und Importieren von Antworten vorhanden sind, gibt es keine Möglichkeit sie auf der Dienstebene zu trennen. Die Benutzer, die beispielsweise nur Lese-Berechtigung für die Antworten der Sicherheitskonzept-Vorlage bekommen haben, können alle Sicherheitskonzepte unabhängig von den Diensten anschauen.
Lösung: Erstellen mehrerer Sicherheitskonzeptvorlagen und Anpassen jeder nach Dienstspezifika. Beispiele hierfür sind "Sicherheitskonzept-Vorlage für E-Mail-Dienste", "Sicherheitskonzept-Vorlage für Verzeichnisdienste" und so weiter. Dadurch wird die Trennung von Benutzern sowohl auf der Aufgaben-Ebene als auch auf Dienstgruppen-Ebene erreicht. Die Aufgabenberechtigungen müssen für jede dienstspezifische Vorlage neu vergeben werden. Mit dieser Lösung lässt sich die Verwaltung von dienstspezifische Fragen gut realisieren. Jede dienstspezifische Vorlage wird in sich neben den allgemeinen Fragen auch die dienstrelevanten Fragen enthalten.

Die folgenden Nachteile können nicht ohne Umschreiben von Teilen von LimeSurvey umgegangen werden:

- Gruppen können nicht in weiteren Gruppen zusammengefasst werden
- Dynamik des Fragenbogens kann nur teilweise erreicht werden
  Während des Ausfüllens des Fragenbogens ist es möglich, bei einigen Fragentypen (Liste, Mehrfachauswahl) nur einen eigenen Eintrag hinzuzufügen. Beim Matrix-Fragentyp besteht keine solche Möglichkeit.
- Validierung der eingetragenen Daten verlangt oft Programmierkenntnisse bzw. Kenntnisse von regulären Ausdrücken (engl. Regular Expressions).

[15] `https://manual.limesurvey.org/Exporting_results/de`

Das Fazit aller obenstehenden Ausführungen lautet, dass die Verwaltung von Sicherheitskonzepten am LRZ mit LimeSurvey nach den benötigten Code-Modifikationen möglich wäre.

5 Resümee der Arbeit

In diesem Kapitel werden die Ergebnisse der Arbeit zusammengefasst und ein Fazit gezogen. Den Abschluss dieses Kapitels bildet einen Ausblick auf mögliche Ansatzpunkte für nachfolgende Untersuchungen und weitere Entwicklungsmöglichkeiten des Projekts.

5.1 Zusammenfassung

Diese Arbeit hat sich mit der Entwicklung eines Konzepts für eine Web-Anwendung, die Erstellung und Verwaltung der dienstspezifischen Sicherheitskonzepte am LRZ ermöglichen kann, beschäftigt. Zuerst wurden die Voraussetzungen für die Entwicklung eines Verwaltungssystems für Sicherheitskonzepte zusammengefasst. Dann wurden entsprechend den Wünschen und Bedürfnissen der LRZ-Mitarbeiter die möglichen Abläufe bei Verwaltung und Aktualisierung der Sicherheitskonzepte modelliert und in Form von Anwendungsfällen dargestellt. Schrittweise wurden die Anforderungen aus den Use Cases abgeleitet und in einem Katalog zusammengefasst. Durch Prioritätensetzung der Anforderungen wurde die Notwendigkeit der Umsetzung in die Programmlösung bestimmt. Nach der Entwicklung des Konzeptes folgte eine Analyse der auf dem Markt erhältlichen Anwendungen. Das Ziel der Marktuntersuchung war, entweder eine Programmlösung zu finden, die für die Verwaltung der Sicherheitskonzepte geeignet ist, oder die Existenz einer solchen Lösung auszuschließen. Da vom Security-Team geplant wurde, die Anwendung für die Verwaltung von Sicherheitskonzepten als Open-Source zu positionieren, beschränkte sich die Marktuntersuchung auf Open-Source-Tools. Im Rahmen der Auswahlverfahren wurden zuerst fünf Programme ausgewählt, testiert und anhand des erstellten Anforderungskatalogs 2.8 verglichen und bewertet. Die Zusammenfassung der Evaluierungsergebnisse repräsentiert die Tabelle 3.4. Zum Schluss wurde ein Programm, LimeSurvey, laut den empirischen Ergebnissen der Evaluation als am besten geeignete Lösung ausgewählt. Mit seiner Hilfe wurden repräsentative Teile der Sicherheitskonzeptvorlage prototypisch implementiert.

5.2 Fazit

Das Resultat der Evaluierung hat ergeben, dass - obwohl ziemlich viele Anwendungen die geforderten Funktionalitäten teilweise besitzen - keine Software alle unverzichtbaren Anforderungen erfüllt. Der im Kapitel 4 beschriebene Prototyp auf Basis von LimeSurvey bestätigt diese Tatsache. Obwohl die meisten Funktionalitäten für Vorlage- und Sicherheitskonzeptverwaltung in LimeSurvey vorhanden sind und fehlende Funktionen auch auf andere Weise realisiert werden können, lassen sich im Abschnitt 2.2 definierte Hauptziele nur teilweise mit Hilfe von LimeSurvey erreichen. Die größte Schwierigkeit liegt in der Umsetzung der erforderlichen Zugriffskontrolle, die im Abschnitt 2.3.3 beschrieben ist.

Es ist offensichtlich, dass das Ergebnis der Umsetzung des entwickelten Konzeptes mit Hilfe

von LimeSurvey befriedigend ist. Für eine Nutzung dieses Systems am LRZ ist aber eine ernsthafte Verbesserung erforderlich. Das Fazit dieser Arbeit ist, dass eine weitere Arbeit zum Thema der Verwaltung der dienstspezifischen Sicherheitskonzepte notwendig ist. Im nächsten Abschnitt werden mögliche Entwicklungs- und Forschungsrichtungen vorgeschlagen.

5.3 Ausblick

Die zukünftigen Arbeiten beschäftigen sich mit den folgenden weiteren Aufgaben, die in dieser Arbeit nicht berücksichtigt wurden.

- Das Testen des Prototyps auf Basis von LimeSurvey am LRZ.
  Wie im Abschnitt 4.2 geschrieben, wurde LimeSurvey für die Erstellung eines Prototyps auf einem lokalen Rechner installiert. Der nächste Schritt wäre, dieses prototypisch implementierte System auf einem Rechner am LRZ laufen zu lassen und zu testen.

- Die weitere Entwicklung von LimeSurvey entsprechend den Bedürfnissen des LRZ.
  Wie oben bereits erwähnt wurde, deckt LimeSurvey nur 74,3 Prozent der erforderlichen Funktionen ab. Da der Sourcecode von LimeSurvey OpenSource ist und für die Weiterentwicklung zur Verfügung steht, kann das Tool an die Bedürfnisse des LRZ angepasst werden.

- Anbinden der LDAP-Schnittstelle an LimeSurvey und testen am LDAP-Server des LRZ.
  Eine neue Version von LimeSurvey, die kurz vor Ende dieser Arbeit veröffentlicht wurde, bietet einen LDAP-Plugin AuthLDAP v2.05+ für Authentication[1]. Laut der Anforderung F58 ist Authentifizieren und Verwaltung der Benutzerdaten mit LDAP wünschenswert. Deswegen ist eine Aufgabe der nachfolgender Arbeiten das Testen von LimeSurvey mit dem installierten LDAP-Plugin am LRZ und die Durchführung der Benutzerauthentifizierung.

- Den vorliegenden Anforderungskatalog mit weiteren Kriterien verfeinern.
  In Rahmen dieser Arbeit wurde vor allem auf die Grundfunktionalität des Systems eingegangen und vor allem auf Ermittlung der Muss-Anforderungen fokussiert. Deswegen ist die Erweiterung des Anforderungskatalogs um weitere Kriterien eine mögliche weitere Aufgabe zum Thema der Verwaltung von Sicherheitskonzepten am LRZ. Beispielhaft wurde in dieser Arbeit auf statistische Auswertungs–Funktionen nicht näher eingegangen. In einer zukünftigen Arbeit könnte überlegt werden, welche Anfragen auf gespeicherte Daten sinnvoll sind, um eine Statistik über die Sicherheitssituation am LRZ zu ermöglichen, und auf welche Weise diese statistischen Berichte präsentiert werden sollen.

- Untersuchung der weiteren Software auf dem Markt.
  In Rahmen der Auswahlverfahren wurden bestimmten Kriterien definiert, um die Anzahl der zu untersuchenden Tools einzugrenzen. Zum Beispiel wurde angenommen, dass die Umsetzung der Software keine Kosten mit sich bringen darf. Wenn in Zukunft die weitere Untersuchung des Marktes finanziell unterstützt wird, ist es denkbar, die nicht

[1] `http://manual.limesurvey.org/Authentication_plugins`

in dieser Arbeit betrachteten Programme anhand des Anforderungskatalogs zu bewerten. Außerdem können die neuen zum Zeitpunkt dieses Schreibens nicht bekannten Programme nach dem Vorgehen, das im Kapitel 3.1 beschrieben ist, evaluiert werden.

- Die Entwicklung einer spezifischen Software, die genau an die Bedürfnisse des LRZ angepasst und später nach Bedarf um neue Funktionalitäten und Schnittstellen erweitert werden kann.

Die in Kapitel 2 erstellten Anforderungskataloge, Aktivitätsdiagramme und Szenarien können ein Hilfsmittel für die weitere Untersuchung und Entwicklung sein.

Abbildungsverzeichnis

Literaturverzeichnis

[Bod13] Bode, Arndt: *Das Leibniz-Rechenzentrum IT-Dienste für Forschung und Lehre in München, Bayern, Deutschland und Europa*, 2013. https://git.lrz.de/?p=secdoc.git;a=blob;f=papers/dfn-cert_workshop_2014.pdf;h=aa61207126afb7151668548a03ddf725119cd89b;hb=HEAD.

[Hom14] Hommel, Wolfgang, Metzger Stefan Reiser Helmut und von Eye Felix: *Security Knowledge Management auf Basis einer Dokumentenvorlage für Sicherheitskonzepte*, 2014. http://git.lrz.de/secdoc.

[Klü07] Klüpfel, Sebastian und Mayer, Tim: *Checkliste und Kriterienkatalog zur Unterstützung der Softwareauswahl in Kleinst-und Kleinbetrieben*, 2007. file:///C:/Documents%20and%20Settings/jask/%D0%9C%D0%BE%D0%B8%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B/Downloads/Checkliste_und_Kriterienkatalog_zur_Unterstuetzung_der_Softwareauswahl.pdf.

[Klü12] Klüpfel, Sebastian, Lang Michael und Amberg Michael: *IT-Projektmanagementmethoden. Best Practices von Scrum bis PRINCE2.* Symposion Publishing Gmbh, Düsseldorf, 1. Auflage, 2012.

[Kle13] Kleuker, Stephan: *Grundkurs Software-Engineering mit UML. Der pragmatische Weg zu erfolgreichen Softwareprojekten.* Springer Vieweg Verlag, 3. Auflage, 2013.

[oss12] *Open Source Software for Online Surveys*, 2012. refhttp://www.gesis.org/unser-angebot/studien-planen/online-umfragen/software-fuer-online-befragungen/freie-software-open-source/.

[sz104] *Systemsicherheit, Zugriffsschutz Teil 1*, 2004. http://www.inf.fu-berlin.de/lehre/SS04/SySi/folien/Zugriffsschutz_Teil1.pdf.

[utm09] *Über TestMaker*, 2009. http://www.global-assess.rwth-aachen.de/testmaker2/index.php?page=about.

[wis14] *Worldwide Infrastructure Security Report*, 2014. http://www.arbornetworks.com/resources/infrastructure-security-report.

[Zen14] Zender, Christoph und Apostolescu, Victor: *Jahrbuch 2013*, 2014. http://www.lrz.de/wir/berichte/jbkomm/jahrbuch_2013.pdf.

[Zsc01] Zschau, Oliver, Traub Dennis und Zahradka Rik: *Web Content Management. Webseites professionell planen und betreiben.* Galileo Press, 2. Auflage, 2001.