



Master Thesis

im Rahmen des
Universitätslehrganges „Geographical Information Science & Systems“
(UNIGIS MSc) am Interfakultären Fachbereich für Geoinformatik (Z_GIS)
der Paris Lodron-Universität Salzburg

zum Thema

**„Volunteered Geographic Information (VGI): Methodische und
technische Konzeption einer qualitätsgesicherten
Erfassungskomponente“**

vorgelegt von

Dipl.-Ing. (FH) Jörgen Spradau
106903, UNIGIS MSc Jahrgang 2021

Betreuer/in: Dr. Manfred Mittlböck

Zur Erlangung des Grades
„Master of Science – MSc“

Linsengericht, 10. Mai 2023

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit eigenständig verfasst und ohne fremde Hilfe angefertigt habe. Es wurden keine anderen als die angegebenen Quellen und Hilfsmittel verwendet. Verwendete Quellen und Hilfsmittel, wörtlich und inhaltlich, wurden als solche kenntlich gemacht. Diese Arbeit wurde noch keiner anderen Prüfungskommission in dieser oder einer ähnlichen Form vorgelegt oder veröffentlicht.

Linsengericht (Deutschland), 10. Mai 2023

(Jörgen Spradau)

Vorwort

Diese Arbeit entstand im Rahmen der Master Thesis des berufsbegleitenden Fernstudienganges „UNIGIS MSc (Master of Science)“ an der Universität Salzburg und in Zusammenarbeit mit dem Bundesamt für Kartographie und Geodäsie (BKG).

Das BKG ist unter anderem der zentrale Dienstleister für Geodaten innerhalb der Verwaltungsbehörden der Bundesrepublik Deutschland. Zentrales Ziel des BKG ist es, alle notwendigen Belange der Bundesverwaltung im Bereich der Geoinformation abzudecken. Ob krisensituativ oder für die Belange der allgemeinen Verwaltung. Mit dem Ergebnis dieser Arbeit können Dienstleistungen weiter optimiert und zusätzliche zur Verfügung gestellt werden.

Recht herzlich möchte ich mich bei meinem Prüfer und Betreuer Herrn Dr. Manfred Mittlböck der Universität Salzburg bedanken. Für die tatkräftige Unterstützung innerhalb des BKG danke ich Frau Dr. Hopfstock (Abteilungsleiterin), Herrn Dr. Bobrich (Referatsleiter) und Herrn Walther (Referatsleiter). Vor allem möchte ich jedoch auch dem Befürworter und Initiator des Studiums Prof. Dr. Becker (Präsident des BKG) danken.

Selbstverständlich ist das gesamte hervorragende UNIGIS-Team noch zu nennen. Ich habe meinen Horizont definitiv erweitert. Mit jedem einzelnen Modul wurde dieser Wissensstand bereichert. Vielen lieben Dank dafür!

Zu guter Letzt gilt ein spezieller und größter Dank meiner tollen Frau. Sie hat mich jederzeit unterstützt, Dokumente und Arbeiten quergelesen. Zu den einzelnen Themen haben wir uns viel ausgetauscht. Vor allem wegen ihrem Zuspruch, ihrer Unterstützung und ihrem Zurückstecken konnte ich alles meistern.

Danke Kirsten, dass du mir immer wieder die Kraft und die Zeit für das Studium gegeben hast.

Zusammenfassung

Diese Masterarbeit ist das technische Konzept zur methodischen Umsetzung einer qualitätsgesicherten Erfassungskomponente. Mittels eines exemplarischen Vergleichs zweier Erfassungskomponenten / -systemen werden drei Erfassungsmethoden ermöglicht und anschließend bewertet.

Die Forschungsfrage dieser Arbeit beschäftigt sich mit der Fragestellung, wie mittels VGI eine Datenerfassung erfolgen, qualitätsgesichert übernommen und bereitgestellt kann. Hierzu wurden zunächst Anforderungen definiert. Diese Anforderungen entsprechen den obligatorischen Anforderungen und unterteilen sich weiter in drei Sichtweisen. Die allgemeinen Anforderungen entsprechen eher denen, welche aus der Sicht des Endnutzers der Erfassungskomponente entsprechen. Nach weiterer Forschung ergaben sich weitere Anforderungen. Einmal aus Sicht des Datenschutzes und der IT-Sicherheit. Beide zuletzt genannten Anforderungen wurden genauer betrachtet und ergaben weitreichendere Schwerpunkte dieser Arbeit.

Ein zusätzlicher Punkt dieser Arbeit ist das Vergleichen zweier Systeme, die auf Basis definierter Standards Erhebungen und Erfassungen von Geodaten ermöglichen. Die Bereitstellungen in den unterschiedlichen Plattformen wurden miteinander verglichen und zeigten wenige bis keine Unterschiede auf. Lediglich die Art und Weise, wie und mit welchen Mitteln solche Erhebungen in eine Plattform überführt werden, differieren. Hierbei ist Standardisierung und Qualität dieser Arbeit eine zusätzliche Frage. Genauer, „Wie können sich erhobene Daten überführen lassen und wie steht es um die Qualität?“. Der Begriff Qualität wird in diesem gesamten Zusammenhang geklärt. In der Geoinformation sieht man stets die Sicht der Geodaten. Aus der Sicht eines IT-Betriebes ist die Qualitätsfrage jedoch umfänglicher. Unterscheiden lässt sich der Begriff zwischen der technischen und der funktionalen Qualität. Die Qualität der Software und der Bereitstellung ist die technische Qualität, also generell ein IT-Betrieb. Die Qualität der Daten ist, wie gesagt die Geoinformation. Diese Fragen und Verantwortlichkeiten werden anhand von Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geklärt.

Wie genau die Sensoren eines mobilen Endgerätes sind, wurde theoretisch behandelt und lässt sich auch nachvollziehen. Ebenso gilt es für die Nutzergruppierungen und deren Beweggründe Daten zu erfassen. Anhand eines Testverfahrens wurde eine kleinere Gruppe befragt, wie Tester die Erhebungen mittels zwei Alternativen empfanden. Anschließend fand eine Bewertung statt.

Den Schluss dieser Arbeit bildet ein Fazit der Forschung und ist mit einem Ausblick, sowie einer Empfehlung an das BKG verbunden.

Abstract

This master thesis is the technical concept for the methodical implementation of a quality-assured collection component. By means an exemplary comparison of two collection components/-systems. Three collection methods are made possible and subsequently evaluated.

The research question of this thesis deals with the question: "How can data collection be carried out in the meaning of VGI, taken over in a quality-assured manner and made available?" For this purpose, requirements were first defined. These requirements correspond to the mandatory requirements and are divided into three Levels. The general requirements are more like how must the capture component contain for the end user. After further research, this resulted in additional requirements. Once from the perspective of data protection and IT security. Both of the latter requirements were considered more closely and resulted in more far-reaching focal points of this work.

An additional important point of this work is the comparison of two systems that enable the collection and recording of geodata on the basis of standards. The deployments in the different platforms were compared and raises slightly differences. Only the way of publishing such surveys and the transferring to the platforms differ. Here, standardisation and quality of this work is a central question. That is, "How can collected data can be transferred and what about quality?" The term quality is clarified in this context. In Geoinformation, one always sees the view of the geodata. From the perspective of an IT department, however, the question of quality is more far-reaching. A distinction can be made between technical and functional quality. The quality of the software and the provision is the technical quality, i.e. generally an IT operation. The quality of the data is, as said, the geoinformation. The questions and responsibilities are clarified on the basis of guidelines issued by the Federal Office for Information Security (BSI).

How exactly the sensors of a mobile device are has been dealt with theoretically and can also be understood. Likewise, data must be collected for user groupings and their motivations. Using a test procedure, a smaller group was asked how they felt about surveys using two alternatives. This was followed by an evaluation.

In conclusion of this work a conclusion of the research and is connected with an outlook as well as a recommendation to the BKG.

Abkürzungsverzeichnis

App	Applikation/Anwendung, die auf mobilen Endgeräten als auch auf gewöhnlichen PC genutzt werden kann.
BKG	Bundesamt für Kartographie und Geodäsie
BSI	Bundesamt für Sicherheit in der Informationstechnik
CSA	Crowd Sourcing Approach
DLM	Digitales Landschaftsmodell
DSB	Datenschutzbeauftragter
ETL	Extract-Transform-Load
FAIR	Findable, Accessible, Interoperable, Reusable
GA	Geographic Approach
GDI	Geodateninfrastrukturen
GNSS	Global Navigation Satellite System
HTTPS	Hypertext Transfer Protocol Secure
IMAGI	Interministerieller Ausschuss für Geoinformationswesen
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnologie
ODK	OpenDataKit (https://getodk.com)
OGC	Open Geospatial Consortium (https://www.ogc.org/)
OSM	Open Street Map (https://www.openstreetmap.de/)
P	Präsident des BKG
POI	Point of Interest
PWA	Progressive Web App
SA	Social Approach
SaaS	Software-as-a-Service
SQL	Structured Query Language
VGI	Volunteered Geographic Information
WYSIWYG	What You See Is What You Get

Inhaltsverzeichnis

Eigenständigkeitserklärung	i
Vorwort	ii
Zusammenfassung.....	iii
Abstract.....	iv
Abkürzungsverzeichnis.....	v
Inhaltsverzeichnis.....	vi
1 Einleitung	- 1 -
1.1 Motivation.....	- 1 -
1.2 Stand der Forschung.....	- 2 -
1.3 Forschungsziel und Gliederung.....	- 5 -
1.4 Strategie zur geplanten Umsetzung	- 8 -
2 Anforderungen	- 9 -
2.1 Allgemein inhaltliche Anforderungen.....	- 9 -
2.2 Organisatorische/Rechtliche Anforderungen	- 11 -
2.3 Technische Anforderungen (Sicherheitsaspekte)	- 13 -
2.3.1 „IT-Grundschutz“	- 14 -
2.3.2 Sicherheitsrelevante Grundlagen	- 17 -
2.4 Abgrenzungen	- 23 -
3 Methodik.....	- 25 -
3.1 Software	- 25 -
3.1.1 Standard der Erfassungskomponenten.....	- 25 -
3.1.2 Survey123	- 29 -
3.1.3 KoboToolbox.....	- 31 -
3.2 Benutzerführung	- 33 -
3.3 Digitale Erfassungssensoren	- 35 -
3.4 Sammlereigenschaften	- 36 -
3.5 Verantwortlichkeiten.....	- 37 -

3.6	Qualitätssicherung eines VGI-Systems	- 41 -
3.7	Teilnahme und Motivationsgründe der Erfasser	- 46 -
3.8	Resultat	- 46 -
4	Ergebnisse und Diskussion	- 47 -
4.1	Bewertung der VGI-Software.....	- 47 -
4.1.1	Vergleich der technischen Fähigkeiten	- 50 -
4.1.2	Benutzerführung und Usability.....	- 52 -
4.1.3	Sensorgenauigkeiten	- 56 -
4.1.4	Bereitstellung von Erfassungsumfragen	- 57 -
4.2	Erfasser und Verantwortlichkeiten	- 64 -
4.3	Qualitätssicherungsmaßnahmen.....	- 64 -
4.4	Motivationsgründe	- 72 -
4.5	Zusammenfassung.....	- 73 -
5	Fazit/Ausblick	- 74 -
5.1	Empfehlung für das BKG.....	- 75 -
Tabellenverzeichnis.....		lxxvii
Abbildungsverzeichnis.....		lxxviii
Anhang 1		lxxx
Anhang 2		lxxxvii
Anhang 3		lxxxviii
Anhang 4		lxxxix
Literaturverzeichnis.....		xc

1 Einleitung

1.1 Motivation

Im Kontext bereits durchgeführter Analysen zur Machbarkeit einer sogenannten Sammel-App nach diversen anderen Vorreitern, soll diese Arbeit ein Ergebnis liefern, mit dem das BKG nachhaltig neue Wege einleitet. Erkenntnisse aus vorangegangenen Projekten sollen direkt in diese Masterarbeit einfließen. Aus diesem Grund wird die Ursprungsidee einer individuell entwickelten App mit dem Konzept dieser Arbeit abgewandelt.

Das Konzept soll eine nicht-native Anwendung (z.B. eine Progressive Web App (Abkürzungsverzeichnis)) umfassen, die auf mobilen Endgeräten wie Smartphones oder Tablets betrieben und verwendet werden kann. Der Einsatz auf Desktop PCs soll ebenfalls möglich sein. Ein Kernaspekt des Konzeptes sind Webkarten des BKG, die als Kartengrundlage dienen sollen. Auf dieser Basis sollen Nutzende möglichst einfach und schnell Informationen erfassen, korrigieren und ergänzen können. Ein ebenfalls wichtiger Aspekt ist die lizenzkostenfreie Nutzung der App.

Hintergrund und gleichzeitige Motivation zu einer bereitzustellenden Anwendung ist, dass es bereits fest etablierte Apps und vergleichbare Anwendungen, wie z.B. durch OpenStreetMap oder Google Maps, gibt. Diese beschränken sich jedoch vorrangig auf Orte der Freizeitgestaltung (Restaurants, Hotels, Cafés) sowie der Mobilität (Tankstellen, Haltestellen). Gefestigt haben sich die Orte unter dem Begriff „Point Of Interest (Abkürzungsverzeichnis)“. Aber auch Routing und Navigation sind Kernelemente der genannten Anwendungen. Für Bundesbehörden stehen häufig relevante Informationen sowie Verortungen spezieller oder kritischer Infrastrukturen nicht zur Verfügung. Ein Ziel der Anwendung soll daher die Schaffung einer eigenen Erfasser-Community sein. Hierzu soll das Potenzial der großen Gruppe (Community) genutzt werden. Die Community soll somit schnell Lageinformationen für Bundesbehörden und -institutionen erfassen und bereitstellen können. Gefilterte Informationen sollen jedoch auch der Allgemeinheit zur Verfügung gestellt werden. Und damit nicht nur einer selektierten Gruppe.

Vorhandene Erfahrungen aus anderen internen Projekten oder der kartographischen Informationsgewinnung qualifizieren das BKG für eine fachlich korrekte Umsetzung. Zusätzlich ergeben sich auch Vorteile aus dem Betrieb der beschriebenen Anwendung für das BKG. Diese Vorteile reichen von gezielter Datenneuerfassungen bis hin zu möglichen Aktualisierungen durch Mitteilungen von Veränderungen der dargestellten Objekte in Bestandprodukten. Das entspricht der Objekte der realen Welt. Mit diesem Ansatz kann das BKG seiner Rolle als Geodatenbroker für die Bundesverwaltung gerecht werden.

1.2 Stand der Forschung

Bisherige Geodaten obliegen zumeist etablierten Erfassungskriterien und -methoden zu unterschiedlichen Themen. In der Vielzahl von situativen Ereignissen kann das Erfassen von Daten/Informationen auch längere Zeit in Anspruch nehmen. Steigern lässt sich die Vielfalt der Daten, wenn eine Gruppe freiwilliger Erfasser (Mapper) dazu einsetzt wird (Howe, 2006). Das Erfassen durch externe Gruppen heißt „Crowdsourcing“ und kann die Prozesse deutlich beschleunigen. Sofern es richtig umgesetzt wird, entwickelt sich ein hohes Potential an Nutzen und Erfolg (Hammon & Hippner, 2012). Es gibt jedoch auch Risiken in der Überführung der Daten in eine qualitätsgesicherte und geprüfte Datenbasis. Ansätze in wissenschaftlichen Ausarbeitungen gibt es hierzu viele. Aktuelle Forschungsergebnisse werden in dieser Arbeit herangezogen.

OpenStreetMap (Abkürzungsverzeichnis) sammelt zum Beispiel Daten mittels einer großen Anzahl von Erfassern und stellt damit hochdynamische Geodaten zur Verfügung. Eine Aussage zur Qualität ist jedoch schwer zu ermitteln und hängt unter anderem auch von dem jeweiligen Erfasser ab (Mocnik et al., 2018). Etabliert ist das Sammeln räumlicher Daten unter dem Begriff „Volunteered Geographic Information“ (VGI). Was VGI ist und warum Menschen dazu beitragen, wie akkurat die Ergebnisse sind, ob sie die individuelle Privatsphäre gefährden und ob sie konventionelle Quellen ergänzen können stellt M. F. Goodchild in seiner Ausarbeitung, im Jahr 2007, dar (Goodchild, 2007). Goodchild zieht einen Vergleich mit den traditionelleren „citizen sciences“ und erläutert die Rolle von „Amateuren“ in der geografischen Informationsgewinnung. Ein entscheidendes Problem von VGI ist, dass die Metadaten oft gar nicht, unvollständig oder inkorrekt erfasst werden. Dieser Umstand erschwert die Qualitätsbewertung der daraus resultierenden Karten oder Konzepte. Es stellt sich somit die Frage, warum die Erfasser überhaupt VGI betreiben. Erklärungen könnten sein:

1. „self-promotion“/ Selbstdarstellung
2. Inhalt mit Freunden zu teilen, dann aber auch gleichzeitig mit dem ganzen Internet.
3. bei OSM beispielsweise persönliche Zufriedenheit, wenn eine Karte immer vollständiger wird.

VGI wird manchmal als „behauptete Infos“ beschrieben, da sie teils keine Quellenangaben haben und jeder sie bearbeiten kann. Eventuell werden sogar mit Absicht Fehler eingearbeitet. Dies sind wesentliche Aspekte, die bei der Arbeit mit VGI immer mit beachtet werden müssen. Ein weiteres Problem ist, dass es bis heute allgegenwärtig große Unterschiede in der digitalen Infrastruktur gibt. Daher sind viele Regionen aufgrund mangelnder Internetversorgung und Digitalisierung unterrepräsentiert.

Dennoch vollzieht sich mittlerweile ein Wandel von statischen Erfassungsmethoden hin zu dynamischen. Insbesondere das individuelle Fachwissen des Erfassers ist ausschlaggebend für den

Aufbau einer umfangreichen und fachlich korrekten Datenbasis. VGI bietet zwar viele Vorteile (kostenlos, viele Inhalte, ...), jedoch gibt es in vielen Fällen noch allgemeine Qualitätsmängel, da eine einheitliche Qualitätskontrolle schwer umzusetzen ist. Drei Ansätze zur Qualitätssicherung, die während der Datenaufnahme angewendet werden können, wurden durch Goodchild im Jahr 2012 beschrieben (Goodchild & Li, 2012).

Crowd-Sourcing-Approach (CSA)

„Crowdsourcing“ ist die Lösung von Problemen durch die Mitarbeit vieler Personen, ohne dass diese Personen unbedingt qualifiziert sind. „Crowdsourcing“ ist die Fähigkeit einer Gruppe die Fehler anderer zu Erkennen und zu verbessern. Drittens ist „Crowdsourcing“ die Fähigkeit einer Gruppe, der „Wahrheit“ immer näher zu kommen.

Diese drei Fähigkeiten können eingeschränkt sein, da sie von der aktiven Gruppengröße abhängig sind. Auch hängt es von der Art des Objektes oder dem Attribut ab. Dieses kann mal mehr und mal weniger prominent sein.

Gründe für weiterhin entstehende Fehler oder unzureichende Erfassungen sind, dass es tendenziell mehr Erfasser gibt, die lediglich Informationen hinzufügen. Entgegen hierzu stehen die Erfasser, die bestehende Informationen bearbeiten bzw. korrigieren. Hinzu kommt auch, dass es Erfasser gibt, die die lokalen Gegebenheiten wenig bis gar nicht kennen.

Social-Approach (SA)

Die Möglichkeit der Qualitätssicherung durch den SA erfolgt anhand eines Hierarchiesystems. Mapper können verschiedene „Bearbeitungsstufen“ erreichen. Wer mehr mitarbeitet (mappt), kann mehr Verantwortung bekommen und hat mehr Mitbestimmungsrechte. Dieses Hierarchiesystem kann auch durch andere Belohnungsideen ergänzt werden. Die Hierarchien ahmen die Strukturen traditioneller maßgebender Kartierungsagenturen nach. Weniger formell, dafür natürlich freiwillig. Der Ansatz funktioniert besonders gut bei objektiven und replizierbaren Fakten. Sprich, bei repräsentativen Objekten der Karte (z.B. dem Eiffelturm).

Geographic-Approach (GA)

Die GA soll die Qualität in der GI-Welt zusätzlich absichern. Der Ansatz ist der Vergleich zwischen einem vermeintlichen geografischen Sachverhalt und dem allgemein geografischen Wissen. Geographische Sachverhalte sind bestimmten Regeln unterworfen; also was z.B. an einem Ort passieren könnte. Und anhand dieser Regeln kann geprüft werden, ob eine dargestellte geographische Tatsache möglich ist oder nicht.

Allgemein gehört dazu das 'Erste Gesetz der Geographie' von Tobler (1970): „Alle Dinge sind miteinander verbunden, aber nahe Dinge sind mehr miteinander verbunden als entfernte Dinge“. Also gibt es räumliche Abhängigkeiten zwischen Gegebenheiten. Ganz im Sinne, dass einer behaupteten Gegebenheit mit ihrem geographischen Kontext übereinstimmen sollte (horizontaler Zusammenhang). Und dass eine behauptete Gegebenheit mit anderen Gegebenheiten übereinstimmen sollte, die bereits über diesen Ort bekannt ist (vertikaler Zusammenhang). Es gibt sehr verschiedene Regeln, die die Geographie beschreiben. Diese können sehr einfach, aber auch sehr abstrakt sein. Damit sind sie auch schwer einheitlich darzustellen. Erkennbar sind diese Regeln. Diese jedoch in einem Handbuch umsetzbar festzulegen, bleibt schwierig.

Allgemein kann festgehalten werden, dass es unterschiedliche Szenarien zur qualitätsgesicherten Übernahme von erfassten Daten, dritter, gibt. Eine weitere Frage ist, wie diese Informationen erfasst werden können? Möglichkeiten der Erfassungskomponenten gibt es viele. Dies reicht von Eigenentwicklungen über Open Source Software bis hin zu proprietärer kommerzieller Software. Damit verbunden ist aber auch die Frage nach „Wie und womit können Geodaten erfasst werden?“.

Situative Ereignisse grenzen eine Erfassung eher ein. Der Erfasser soll hierzu möglichst die Daten dort aufnehmen, wo er sich gerade befindet. Was sind situative Ereignisse? Geodaten werden insbesondere in Krisensituationen (Beispiel: Überschwemmung im Ahrtal) aktuell und hochverfügbar in unterschiedlichsten Kombinationen sowohl für die Analyse als auch die Visualisierung benötigt. Nutzer sind zum einen die Öffentlichkeit und zum anderen Behörden, einschließlich deren Krisen- und Lagezentren. Hierfür müssen Erhebungsplattformen geschaffen werden, die es ermöglichen, eine möglichst gute Situation der aktuellen Lage zu erheben und Helfern zur Verfügung stellen. Damit wird es ermöglicht, Daten, Dienste und Anwendungen dem jeweiligen Anwender, ad hoc und im zugeschnittenen Format, verfügbar zu machen.

Folglich wäre die Auswahl der Erfassung über ein mobiles Endgerät, gekoppelt mit dessen Sensoren. (Yeon, 2021) beschreibt die Anforderungen an mobile Endgeräte. Bezogen auf einen Anwendungsfall führen (Loola Bokonda et al., 2020) eine Vergleichsanalyse bestehender mobiler Apps durch. Dabei fallen die Apps OpenDataKit (Abkürzungsverzeichnis - <https://getodk.org/>) und KoboToolbox (<https://www.kobotoolbox.org/>) besonders auf. Hersteller kommerzieller Software, wie ESRI (<https://www.esri.de/de-de/home>), setzen sich ebenfalls mit der mobilen Datenerfassung auseinander. Wie weit sich ihre Software auf spezielle Projekte anpassen lässt, beschreiben (Hennig et al., 2020). Die dort erfassten Daten werden zur Qualitätsprüfung und Validierung anders erfasster Geodaten genutzt. Die im Feld erfassten Daten werden hier ohne weitere Kontrolle direkt weiter genutzt. Eine Erfassung von Geodaten mittels mobiler Endgeräte stellt den aktuellen Trend dar. OSM ist bekannt für ein breites Spektrum und eine hohe Anzahl an Volunteers. Ursprünglich beruht die

Erfassungsmethode nicht auf mobilen Endgeräten. Die Idee besteht darin, auf internetbasierten Anwendungen die Erfassung und Nutzung zu ermöglichen. Vor allem herkömmliche Browser eines Desktop-PCs werden hierzu genutzt. Flexibilität in der Erfassung und der Darstellung der Geodaten ist deshalb nicht nur für einen bestimmten Client wichtig. VGI-Methoden beinhalten eine Vielzahl an Möglichkeiten der Erfassung und der Visualisierung. Anwender können grundsätzlich in drei Klassen zugeordnet werden. Hierzu zählen einfache, fortgeschrittene und professionelle Endanwender (Hammon & Hippner, 2012).

Einheitliche Umgebungen, wie Frameworks, bieten große Vorteile. Sie können individuelle Anforderungen auf Administrationsebene und gleichzeitig themenbezogene Erfassungen umsetzen (Pinheiro & Davis, 2018). Außerdem kann die Nutzung einzelner Themenbereiche einer beliebigen Anwendergruppe zugänglich gemacht werden. Dazu müssen aber auch Workflows erarbeitet werden, um in den Frameworks Qualitätssicherungsmechanismen umzusetzen. Mit der Weiterentwicklung serviceorientierter Geoinformationsplattformen steigt der Bedarf an einer Optimierung der qualitätsgesicherten, standortbezogenen Datenerfassung. Das kann die Erfassung auf die Nutzung mobiler Endgeräte eingrenzen. Eine Erfassung mit mobilen Endgeräten ist in der Regel mit thematisch einfachen Objektarten gekoppelt, um eine schnelle und intuitive Bedienung zu gewährleisten.

1.3 Forschungsziel und Gliederung

Die Kernaufgabe dieser Arbeit beschäftigt sich mit folgender Fragestellung: „Wie kann mittels VGI eine Datenerfassung erfolgen, qualitätsgesichert übernommen und bereitgestellt werden?“

Anhand dieser Fragestellung soll in der vorliegenden Arbeit ein beispielhaftes Konzept entwickelt werden, mit dem erfasste Daten von einer Erfasser-Community in die Produkte des BKG einfließen können. Hiermit verbunden ist auch die Frage, wie Dienstleistungen für die Bundesverwaltung bereitgestellt werden können, damit diese ihre eigenen Daten erfassen können.

Hierzu werden folgende operative Teilschritte untersucht:

1. Die technischen Fähigkeiten der „Off-The-Shelf“ Umgebungen aus den Bereichen Open Source und kommerzieller Software werden untersucht. Mit diesen Umgebungen können VGI-Anwendungsfälle zeitnah bearbeitet, verwaltet und als Erfassungswerkzeug bereitgestellt werden.
2. Die gegebene Benutzerführung für mobile Endgeräte anhand des Verhaltens der App wird bewertet.
3. Die Genauigkeiten der mobilen Sensoren werden bewertet.

4. Eine Klassengruppierung der Sammlereigenschaften wird ermittelt.
5. Die Verantwortlichkeiten der Datenverwaltung auf Organisationseinheiten werden geplant, um die verschiedenen Themen der Anwendungsfälle zu überwachen.
6. Um die Qualität zu gewährleisten, müssen Aspekte der Auftragsverwaltung für die Arbeitsabläufe definiert werden. Aktuelle Ansätze der Forschung werden genutzt, um ein Monitoring umzusetzen. Dieses zeigt den aktuellen Status und Fortschritt der Datenerfassungsaufträge an.
7. Untersuchung zu den Motivationsgründen der Erfasser.

Die Teilschritte ergeben folgenden Ablaufplan und die Struktur dieser Arbeit.



Abbildung 1: Gliederung der Arbeit

1.4 Strategie zur geplanten Umsetzung

Anhand des Forschungsziels können die Erfassungswerkzeuge definiert werden. Zum Einsatz und zur Evaluation kommen die Umgebungen von ESRI (Survey123) und KoboToolbox. Beide Umgebungen versprechen den gleichen Ansatz und unterstützen einen Standard mit dem die Teilziele evaluiert werden können. Der Standard lautet XLSForm und wurde im Jahr 2007 mit der Version 1.0 veröffentlicht (<https://qsel.columbia.edu/>). Inhaltlich beschreibt ein XLSForm-Dokument, wie Steuerelemente in einem Formular erscheinen sollen. Zunächst werden die jeweiligen technischen Fähigkeiten der Erfassungskomponenten und die Usability untersucht. Die Qualität und die Überführung in eine gesicherte Geodateninfrastruktur der erfassten Geodaten werden in den weiteren Kapiteln exemplarisch beschrieben. Die Untersuchung der Methoden in Methodik beschrieben und in dem vierten Ergebnisse und Diskussion ergebnisorientiert bewertet. Insgesamt soll das Ziel eine nachhaltige Lösung für die Bereitstellung eines Gesamtsystems zur Erfassung von Geodaten im Feld darstellen.

Auf die Anforderungen des BKG müssen unterschiedliche Dienste/Anwendungen untersucht werden. Eine Wahrscheinlichkeit, dass mobil erfasste Daten fehlerhafte Informationen aufweisen, scheint gegeben zu sein. Hierzu können schlechte Sichtverhältnisse bei Tageslicht, Überforderung des Anwenders mit der mobilen Anwendung oder die nicht optimale Bedienung auf den mobilen Endgeräten führen. Dies sind mögliche Gründe, warum mobile Erfassungssysteme nur begrenzt eingesetzt werden können. Um eine möglichst hohe Anzahl von Erfassern zu erreichen, müssen auch Desktop-PCs mit größeren Bildschirmen und der Nutzung von Tastatur und Maus als herkömmliche Datenerfassung genutzt werden können. Hierbei wird die Qualität der Erhebungsmethoden untersucht, da mittels zusätzlicher Datenlayer die Qualität und die Erfassungsgeschwindigkeit gesteigert werden können.

Informationen werden für drei Anwendungsfälle und Erfassungsmöglichkeiten mobiler Endgeräte und normaler Desktop-PCs erstellt. Folgende drei Bereiche sollen abgedeckt werden:

1. Erfassung von situativen Ereignissen
2. Erfassung von Korrekturen von Bestandsprodukten
3. Erfassung neuer Objektarten für Bestandsprodukte

Diese drei Erfassungsmethoden werden in der vorliegenden Masterarbeit stets wiederverwendet und werden damit häufig in betrachtet.

2 Anforderungen

Aus den zuvor erwähnten Vorreitern des BKG kann sich ein Gesamtprojekt ableiten. Die wesentlichen Punkte der Evaluierung zur Einführung einer Sammel-App werden in der vorliegenden Arbeit behandelt. Eine Gesamtstruktur des Projektes wird nicht weiter erwähnt und erläutert. Essentielle Methoden sind in dieser Veröffentlichung beschrieben. Unter Punkt 2.1 werden die allgemeinen Anforderungen als sogenannte „lose Sammlung“ gelistet. In den Abgrenzungen, unter 2.4, werden erste Definitionen aufgestellt, wie sich diese Arbeit von der allgemeinen Komplexität der Aufgabe abgrenzen soll.

2.1 Allgemein inhaltliche Anforderungen

Die Anforderungen der umzusetzenden Sammel-App können allgemein festgehalten werden und spiegeln die folgenden Punkte wider. Diese ausgewählten Anforderungen sollen für einen ersten Entwurf umgesetzt und evaluiert werden. Grundsätzlich entstammen sie aus Vorläuferprojekten des BKG. Naturgemäß erfolgen sich hieraus weitere Anforderungen, die in Folgeprojekten untersucht werden müssen.

- Die Sammel-App soll eine Progressive Web App (PWA) sein
 - Eine PWA kann über „Add-To-Homescreen“ quasi auf mobilen Endgeräten installiert werden
 - Eine PWA bietet die „Offline“-Funktionalität, also ohne Internetverbindung
- Die PWA muss im Internet verfügbar sein
 - Die Kartendienste der PWA sind im BKG-Portal vorhanden
- Anmeldung
 - Anmeldung beim Herunterladen und beim Synchronisieren
 - Keine erneute Anmeldung, wenn die alte noch gültig ist
 - Nutzen der PWA soll allgemein auch ohne Anmeldung möglich sein
- Ohne Anmeldung am BKG-Portal
 - Jedem anonymen Nutzer Kartendienste zur Verfügung stellen
- Anwendbar auf allen Plattformen (Smartphone Tablet, Desktop-PC)
- Responsive Design –Smartphone/Desktop (IOS und Safari bzw. Android und Chrome auf aktuellen Geräten)

- Erscheinungsbild und Bedienung der PWA ist abhängig vom Endgerät und muss möglicherweise angepasst werden.
- Karte: Zoom, Pan, Locate, (GNSS/Adresssuche/ Freie Positionierung durch Panning, Scrollen und Zoomen der Karte, Positionierung mit Maus/Tastatur und Bildschirmicons)
- Selektion verschiedener Kartenhintergründe (WMS/WMTS/Vektoren (Basemap))
- Nice To Have: Aufruf weiterer externer Fachinformationen zum Thema in zweitem Fenster
- Aufruf Kontakt und Datenschutz / Nutzungsbedingungen
- Informationen hinzufügen und/oder bearbeiten (punkt-, linien-, flächenhafte Geometrien) – erstmal nur Punkte
- Verschiedene Typen wählen
 - Ein Typ entspricht einer Featureklasse
- Freies Platzieren / Attribute eingeben (Texte, Bilder/Foto, Tonaufnahmen, bedingte Attributeingabe)
- Rechtemanagement und Rollenkonzept (user, group, groupadmin)
 - Der Gruppenadmin legt für seinen POI-Typen eine Gruppe im Portal mit der Option an, dass nur Gruppenbesitzer, Manager und Nutzer hinzufügen dürfen. Somit kann er bestimmen, wer der Gruppe hinzugefügt wird und sein Vertreter sein soll.
- Qualitätsprüfung. Wie?

Ergebende Fragen:

- Welche Sicherheitsmechanismen/-vorkehrungen müssen umgesetzt werden?
- Wie kann ein Export / eine Übertragung der erfassten Daten zur QM und weiteren Verarbeitung erfolgen?
- Wie kann die Rückübertragung erfolgen?
- Wie verlaufen mögliche Synchronisationen?
- Wie können Hinweise von Erfassern mitgeteilt werden?
- Wie können Hinweise den Erfassern mitgeteilt werden (responsive Design)?

Anhand der sich ergebenden Fragen und der Anforderungen orientiert sich diese Meisterarbeit und werden sukzessive überprüft.

2.2 Organisatorische/Rechtliche Anforderungen

Der Datenschutz spielt bei Datenerhebungen externer eine erhebliche Rolle. So können Informationen von Community-Mitgliedern ermittelt und statistisch ausgewertet werden. Aber auch private Informationen und zuvor besuchte Internetangebote können ermittelt werden und über IP-Adressen rückwirkend personalisiert werden.

Zum Thema Crowdsourcing von Geodaten hat der Interministerielle Ausschuss für Geoinformationswesen (IMAGI) sogenannte Handlungsoptionen zum Umgang und zur Nutzung veröffentlicht (IMAGI, 2019). Urheberrechtliche Aspekte und Datenschutz werden unter anderem auch kritisch betrachtet. Als rechtliche Regelungen für das Urheberrecht werden Miturheberschaft (§ 8 UrhG) oder die Bearbeitung eines bestehenden Werks (§ 24 UrhG) genannt. Offen bleibt jedoch, ob die Erhebungen einer Community überhaupt urheberrechtlich relevant sind, da diese Informationen kein geschütztes Werk im Sinne des Urheberrechtsgesetzes sind. Bezüglich des Datenschutzes gibt es klare Empfehlungen. So heißt es:

„Zu klären ist in jedem Fall, wie die Identität Einzelner gehandhabt werden soll: Als gänzlich anonyme Beteiligte ohne Kontakt zu anderen Mitwirkenden als eine Extremform oder mit vollständiger Offenlegung diverser Fakten als anderes Extrem.“ (IMAGI, 2019)

Für die anonyme Beteiligung sei ein explizites Einverständnis des Datenschutzes zwar „nur“ erschwert, sollte wegen der Transparenz aber umgesetzt werden. Grundsätzlich geht aus den Handlungsoptionen hervor, den Datenschutzbeauftragten (DSB) in neue Projekte von Beginn an einzubeziehen. Datenschutzrechtlich ergeben sich also Konflikte in dem Bereich VGI und der Erfassung von Daten mittels einer Community. Das haben auch jüngste Forschungen und Veröffentlichungen erwiesen. Dunkel et al. (2020) haben die Thematik erforscht und schreiben unter anderem:

„Addressing these privacy conflicts is particularly problematic in natural resource management...“ Dunkel et al. (2020)

Gemäß einer Gesamtprojektstruktur ist der DSB frühzeitig einzubeziehen.

Die allgemeinen Datenschutzerklärungen des BKG erscheinen generell für die Sammel-App ausreichend. Siehe hierzu <https://www.bkg.bund.de/DE/Service/Datenschutz/datenschutz.html>. Speziell der Punkt „4. Verarbeitung von personenbezogenen Daten im Rahmen der

Informationsbereitstellung“ muss geprüft werden. Bezogen auf die einzelnen Anwendungsfälle aus dem 1.4 Strategie zur geplanten Umsetzung dieser Arbeit, muss der Datenschutz sicherlich einzeln betrachtet werden. Aus anderen aktuellen Anlässen werden die allgemeinen Datenschutzbestimmungen angepasst. Der DSB des BKG empfiehlt eine Anpassung gemäß Richtlinien. Speziell der genannte Punkt ist auf dem Prüfstand. Hier dreht es sich um die tatsächliche Verarbeitung personenbezogener Daten bei der Bearbeitung und Bereitstellung von Webkarten. Hierbei handelt es sich konkret darum, dass das BKG keine personenbezogenen Daten bevorratet, um diese mit Standorten in einer Karte zu verbinden.

1. Erfassung von situativen Ereignissen:

Wie in diesem Abschnitt beschrieben, soll diese Art der Erfassung eine Dienstleistung darstellen. Daten sollen nicht von dem BKG kontrolliert bzw. übernommen werden. Aus diesem Grund sollen die Datenschutzrichtlinien dem Kunden, der das Angebot nutzt, obliegen. Sprich, der Kunde handelt im Eigeninteresse und ist selbstständig für die Belange des Datenschutzes zuständig. Der allgemeine Datenschutz des BKG bleibt jedoch bestehen. Es sei darauf hingewiesen, dass Fotos, Videos, Tonaufnahmen, etc. erfasst werden können. Diese sensiblen Informationen müssen datenschutzrechtlich gesondert betrachtet werden. Damit dieser Punkt praktikabel umgesetzt werden kann, muss die erste Frage einer Erfassung mit individuellen Richtlinien versehen sein.

2. Erfassung von Korrekturen von Bestandsprodukten:

Bei dieser Art der Erfassung greifen die Datenschutzrichtlinien und -hinweise des BKG vollumfänglich. Es soll anonym erfasst werden. Somit ist lediglich ein Hinweistext mit Bestätigung notwendig. Zu überlegen wäre hier, ob die Erhebungen wirklich anonym umgesetzt werden sollen. Gründe dagegen wären, einem Community-Mitglied eine Rückmeldung der Bearbeitung zu geben. Ob dies zwingend erforderlich ist, kann lediglich die Erfahrung zeigen. Grundsätzlich sollte diese Erfassung jedoch vollständig anonym erfolgen und nur bei Bedarf bzw. Einwilligung personalisiert werden.

3. Erfassung neuer Objektarten für Bestandsprodukte:

Die Datenschutzrichtlinien und -hinweise des BKG können bei dieser Art der Erfassungsmethode vollumfänglich greifen. Zwar soll personalisiert erfasst werden, die Frage ist jedoch, ob Fotos, Videos oder Tonaufnahmen hierfür wichtig sind. Zusätzliche Fotos sind sicherlich immer sinnvoll für eine Gegenkontrolle und hilfreich für eine Übernahme. Wie macht es jedoch OSM? Die OSM-Community

sammelt und bestätigt Geoinformationen durch eine Gegenkontrolle anderer Mitglieder. Gänzlich ohne Fotos. Das BKG sollte dies ähnlich machen und so wenig Information wie möglich von einer eigenen Community erfassen. Somit sollten die allgemeinen Datenschutzrichtlinien vollumfänglich ausreichen. Eine Bestätigung der Richtlinien ist ohnehin notwendig.

2.3 Technische Anforderungen (Sicherheitsaspekte)

Manuel Höferlin kritisierte, 2021, im Deutschen Bundestag den Entwurf zum „IT-Sicherheitsgesetz“ und begann mit den Worten „Die IT-Sicherheit ist die Achillesferse unserer modernen Gesellschaft...“ (Höferlin, 2021). Selbstverständlich müssen IT-Systeme sicherheitsgeprüft werden. Aber in welchem Umfang?

Für die Umsetzung einer frei zugänglichen Anwendung zur Erfassung und Speicherung von Geodaten einer Community, müssen die Software-Komponenten und IT-Systeme sicherheitstechnisch geprüft werden. In Bezug auf frei zugängliche Geodateninfrastrukturen (GDI) ist eine sichere IT-Infrastruktur unerlässlich. In den vergangenen zwei Jahrzehnten wurde hierauf wenig geachtet. Lediglich eine Verschlüsselung der Internetprotokolle, mittels dem HTTPS-Übertragungsprotokoll, wurde in Erwägung gezogen und umgesetzt. Stets wurde auf eine Interoperabilität von Diensten und Daten geachtet. Das diese Standards in die Jahre gekommen sind und an keiner Stelle über IT-Sicherheit nachgedacht wurde, bemängelt (Matheus, 2018). In seiner Veröffentlichung präsentiert er das Ergebnis eines User/Rollenkonzepts für Web-GIS-Anwendungen mit OGC-Diensten. Verheißungsvoll klingt die Veröffentlichung des e.V. Runder Tisch GIS „Leitfaden - Mobile GIS-Hardware, Software, IT-Sicherheit (Version 2.0)“ (Dr. Klaus Brand, GI Geoinformatik GmbH & Prof. Dr. Matthäus Schilcher, Runder Tisch GIS e.V., 2014). Auf einer Vielzahl von Seiten wird eher rudimentär auf IT-Sicherheit eingegangen. Klare Sachverhalte fehlen. Das mag vielleicht auch an dem Veröffentlichungsdatum liegen. Immerhin finden sich Checklisten allgemeiner Art mit Kategorisierungen in dem Dokument wider. Diese können bei Marktübersichten und Anforderungsmodellen helfen. In folgenden Jahren wurde der Leitfaden weitergeführt. Der aktuellste Leitfaden trägt die Version 4. Jedoch ist das Thema IT-Sicherheit ab der Version 3 kein plakativer Bestandteil des Leitfadens mehr und wirkt insgesamt ausgedünnter und wenig verändert.

Grundsätzlich können IT-Sicherheitsüberprüfungen nach eigenen Kriterien oder nach offiziellen Vorgaben durchgeführt werden. Hierzu bietet sich eine Prüfung offizieller Standards an, damit einer Community gewährleistet werden kann, dass die Anwendung nach direktiven Vorgaben geprüft ist. Im Folgenden Unterkapitel wird der IT-Grundschutz kurz erläutert und aufgezeigt worauf speziell zu achten ist. Anschließend wird darauf hingewiesen, welche sicherheitsrelevanten Grundlagen einzubeziehen sind.

2.3.1 „IT-Grundschutz“

In der aktuellen Zeit der Informationstechnologie stellt der Sicherheitsaspekt eine wesentliche Rolle dar. Immer mehr „Hacker“ versuchen über IT-Infrastrukturen „Herr der Lage“ zu werden. Ein möglicher Grund ist die Erpressung zur Veröffentlichung von Daten und Informationen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit seinem IT-Grundschutz einen Leitfaden zur Verfügung. Hierin werden Methoden veröffentlicht, mit denen sich die Gefährdung von IT-Anwendungen und Systemen in Unternehmen, Behörden oder anderen Organisationen minimieren lassen können. Der sogenannte IT-Grundschutz des BSI ermöglicht es, Sicherheitsmaßnahmen strukturiert zu identifizieren und umzusetzen. Somit können vorab notwendige Maßnahmen lokalisiert und realisiert werden, um einen IT-Sicherheitsvorfall so gering wie möglich zu halten.

Das BSI veröffentlicht damit eine Dokumentensammlung von Standards, die Vorgehensweisen zum Schutz der IT-Infrastrukturen beschreiben. Vorrangiges Ziel des IT-Grundschutzes ist es, die Mindestanforderungen für einen normalen Schutzbedarf von Anwendungen und Systemen zu definieren. Diese Umsetzungsmethoden liefern wesentliche Bausteine für eine möglichst sichere Anwendungsumgebung von IT-Systemen. Mit dem IT-Grundschutz-Kompodium (Bundesamt für Sicherheit in der Informationstechnik, 2023) des BSI werden pauschal die typischen Gefährdungen für die verschiedenen IT-Bereiche dokumentiert. Sind Anwendungen mit einem erhöhten Schutzbedarf vorhanden, lassen sich diese durch erweiterte Analysen in ein Schutzkonzept integrieren. Um den Schutz der Informationstechnik absolut sicherzustellen, empfiehlt sich eine offizielle BSI-Zertifizierung. Diese wird durch BSI lizenzierte Auditoren durchgeführt. Zwingend erforderlich ist die Zertifizierung jedoch nicht, da in Eigenregie mit den BSI-Grundschutz-Standards ein vertrauenswürdiges Sicherheitsniveau erreicht werden kann. In den folgenden vier Dokumenten legt das BSI die Standards fest und richtet sich in diesen unter anderem auch an internationale Normen/Standards.

1. Managementsysteme für Informationssicherheit (ISMS) - BSI-Standard 200-1 (Bundesamt für Sicherheit in der Informationstechnik, 2017a):

Mit diesem Standard wird aufgezeigt, wie Unternehmen, Behörden oder andere Organisationen ein Informationssicherheitsmanagementsystem (ISMS) einführen können. Benötigt wird ein ISMS, um Aufgaben und Rollen zu definieren. Aus den Aufgaben und Rollen können somit Handlungsaktivitäten und ein Monitoring abgeleitet werden. Dies sind wesentliche Punkte, die in diesem Standard festgeschrieben sind.

2. *IT-Grundschutz-Vorgehensweise - BSI-Standard 200-2 (Bundesamt für Sicherheit in der Informationstechnik, 2017b):*

Der BSI-Standard 200-2 enthält diskrete Umsetzungsmethoden für den Einsatz eines ISMS in Unternehmen, Behörden oder anderen Organisationen. Anhand von Best-Practices wird konkret durch einzelne Schritte des Gesamtprozesses geführt. IT-Systeme können direkt zugeordnet werden, damit IT-Grundschutz-Bausteine identifiziert werden. Insgesamt gibt es 111 dieser Bausteine. Das BSI führt die Bausteine unter ständiger Aktualisierung in dem Dokument „IT-Grundschutz-Kompodium“ (Bundesamt für Sicherheit in der Informationstechnik, 2023) fort. Anschließend werden sogenannte IT-Grundschutz-Checks durchgeführt, um mögliche Maßnahmen für den IT-Grundschutz umzusetzen. Die IT-Grundschutz-Bausteine des IT-Grundschutz-Kompodiums lassen sich in zwei Bausteinschichten aufteilen. Einmal in Prozess-Bausteine und zum anderen in System-Bausteine (siehe Abbildung 2).

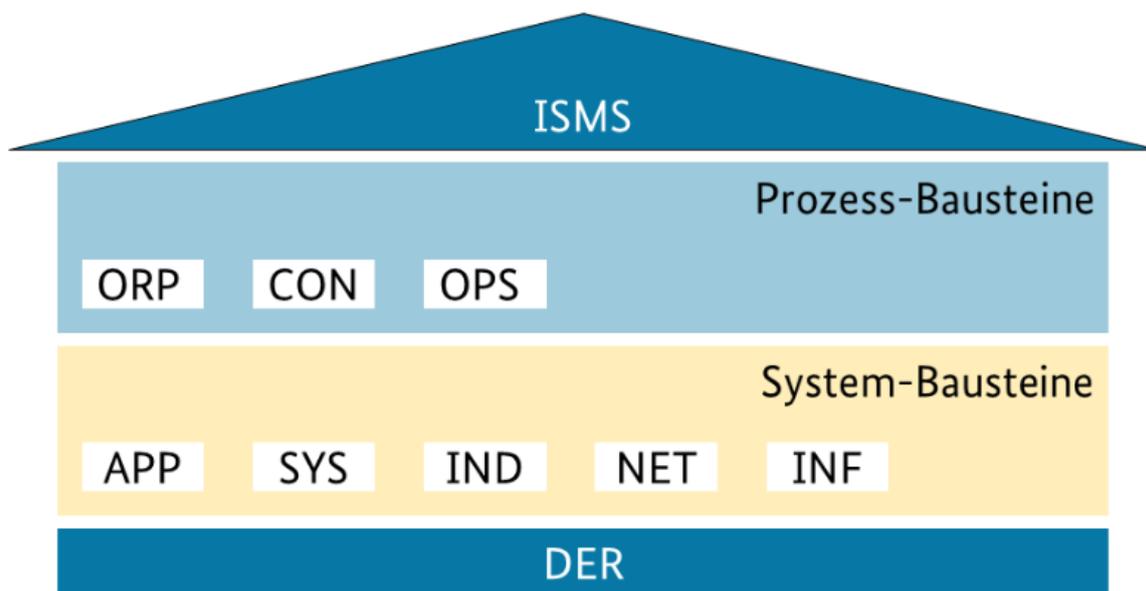


Abbildung 2: IT-Grundschutz-Bausteine (Quelle: BSI)

Zur Erklärung der einzelnen Schichten.

Prozess-Bausteine

ISMS (nach BSI diesem Baustein zugeordnet): Grundlage für alle Aktivitäten im Kontext der Sicherheit

ORP: Organisatorische und personelle Aspekte

CON: Konzeptionelle Aspekte und zu Vorgehensweisen

OPS: Aspekte zum IT-Betrieb

DER (nach BSI diesem Baustein zugeordnet): Behandlung von Sicherheitsvorfällen und zur Vorsorge

System-Bausteine

APP: Aspekte zur Absicherung von Anwendungen und Diensten

SYS: Sicherheitsaspekte von Servern und Desktop-Systemen

IND: Sicherheitsaspekte industrieller IT, wie Prozessleit- und Automatisierungstechnik

NET: Sicherheitsaspekte zur Vernetzung

INF: Sicherheitsaspekte zu baulich-technischen Gegebenheiten, wie Gebäudetechnik

3. Risikoanalyse auf der Basis von IT-Grundschutz - BSI-Standard 200-3 (Bundesamt für Sicherheit in der Informationstechnik, 2017c):

Die Risikoanalyse des BSI identifiziert mögliche Risiken bzw. Gefährdungen und stellt diese in einem ersten Schritt in einer Übersicht zusammen. In einem weiteren Schritt folgt eine Einstufung mit einer Eintrittshäufigkeit und dem verbundenen Schaden. Der dritte Schritt beinhaltet den Umgang mit verbleibenden Restrisiken. Sprich, können die Risiken weiter reduziert werden und wenn ja, wie? Oder, können die Risiken akzeptiert werden? Der vierte und letzte Schritt ist die Konsolidierung der gesamten Risiken. Hieraus resultieren möglicherweise zusätzliche Maßnahmen, die das Sicherheitsniveau von IT-Infrastrukturen belastbarer machen können.

4. Notfallmanagement - BSI-Standard 100-4 (Bundesamt für Sicherheit in der Informationstechnik, 2008):

Für den BSI-Standard 100-4 gibt es bereits einen Nachfolger, den BSI-Standard 200-4. Der Nachfolger, mit dem Namen „Business Continuity Management“, ist bislang noch ein Entwurf und wurde grundlegend überarbeitet. Während der BSI-Standard 200-4 noch im Entwurfsstand ist, ist der BSI-Standard 100-4 noch maßgebend. In diesem werden Leitlinien erläutert, wie ein Notfallmanagement aufgestellt werden kann. Ein Notfallmanagement sieht die Aufgaben zur Ausfallsicherheit, Notfall- und Krisenmanagement vor. Die daraus abgeleiteten Handlungsempfehlungen geben den Unternehmen, Behörden oder anderen Organisationen Orientierungen, wie bei einem Ausfall die wichtigsten IT-Systeme wieder aufgenommen werden können. Außerdem werden hiermit die Methoden zur weiteren Schadensbegrenzung dokumentiert.

Explizite Methoden oder Empfehlungen für den Datenschutz stellt der IT-Grundschutz nicht bereit. Es wird jedoch auf eine Einbeziehungspflicht hingewiesen. Datenschutz, siehe 2.2 Organisatorische/Rechtliche Anforderungen.

2.3.2 Sicherheitsrelevante Grundlagen

Die beschriebenen BSI-Standards, aus 2.3.1 „IT-Grundschutz“, mit hinreichenden Empfehlungen, Vorgehensweisen und Maßnahmen geben einen klar definierbaren Rahmen, wie das neue Fachverfahren zur öffentlichen Erfassung von Geodaten sicherheitstechnisch auszusehen hat. Nach IT-Grundschutz ist es erforderlich, dass ein Server lediglich eine IT-Aufgabe innehat. Allgemein und mit anderen Worten, ein Server als Webserver, ein Server für das Frontend und ein Server für das Backend. Nicht nur die System-Architektur, sondern auch die IT-Grundschutz-Bausteine des IT-Grundschutz-Kompodiums lassen sich identifizieren. Mit der Durchführung der grundlegenden Sicherheitsüberprüfung kann beispielhaft in Rahmen dieser Arbeit der IT-Grundschutz geprüft werden. Insgesamt ergibt sich daraus ein Ablaufschema zur Einführung neuer Fachverfahren (Abbildung 3).

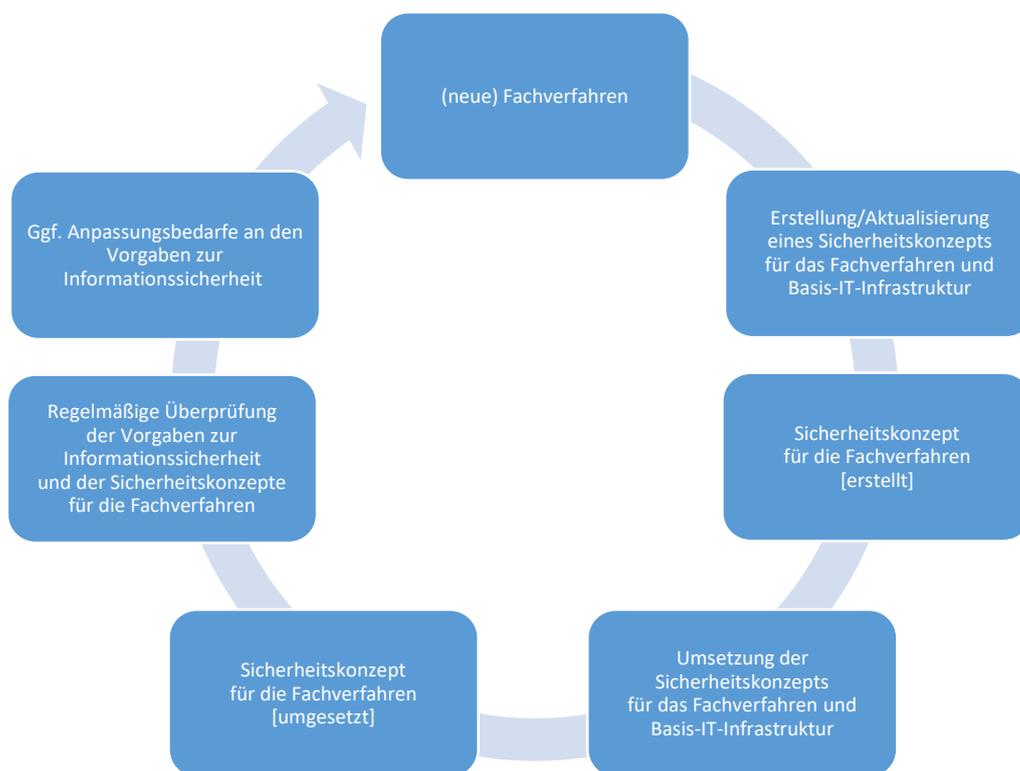


Abbildung 3: Ablaufschema Einführung neuer Fachverfahren

Bevor ein Sicherheitskonzept erstellt werden kann, muss klar sein, welchem Schutzbedarf ein Fachverfahren zugeordnet werden kann bzw. muss. Ein Schutzbedarf wird mit den Fachverfahrensverantwortlichen und dem Informationssicherheitsbeauftragten (ISB) erstellt. Grundsätzlich wird hier eine Schutzbedarfskategorie ermittelt. Normal, hoch oder sehr hoch (Bundesamt für Sicherheit in der Informationstechnik, 2020). Hintergrund ist hier, die Ermittlung eines

entstehenden Schadens bei Verletzung der sog. Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit und einer Einordnung in die entsprechende Kategorie. Wichtig ist die Begründung der Einordnung, um Entscheidungen auch nachhaltig nachzuvollziehen. IT-Systeme stellen Anwendungen bereit, deshalb wird der Schutzbedarf von diesen nach dem Maximalprinzip vererbt. Der höchste Schutzbedarf setzt sich durch. Grundsätzlich sind damit zwei Formen von Effekten zu erkennen.

Kumulationseffekt: Wenn durch Ausfall eines Servers mehrere Anwendungen ausfallen und dadurch größerer Schaden entsteht, kann sich der Schutzbedarf eines Servers erhöhen.

Verteilungseffekt: Der Schutzbedarf eines IT-Systems kann sich auf mehrere Systeme verteilen. Unter anderem auch bei Anwendungen, die einen niedrigen Schutzbedarf besitzen. Dies gilt auch bei der Verarbeitung von personenbezogenen Daten in pseudo-anonymisierter Form.

Aus der Festlegung des Detailgrads und der IT-Systeme kann eine nachfolgende Dokumentation mit Kategorisierungen entstehen.

Folgende IT-Anforderungen einer Webanwendung werden beispielhaft angenommen:

1. Serverbetriebssystem: Windows Server 2022
2. Webserver: Internet Information Server
3. Frontend: PHP und/oder HTML 5 und JavaScript
4. Backend: PostgreSQL mit PostGIS

Aus den angenommenen IT-Anforderungen ergeben sich folgende Dokumente der IT-Grundschutz-Bausteine:

1. OPS_1_1_2_Ordnungsgemaesse_IT_Administration_Edition_2022 (Bundesamt für Sicherheit in der Informationstechnik, 2021b)
2. OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2022 (Bundesamt für Sicherheit in der Informationstechnik, 2021c)
3. SYS_1_1_Allgemeiner_Server_2023 (Bundesamt für Sicherheit in der Informationstechnik, 2022d)
4. SYS_1_2_3_Windows_Server_2023 (Bundesamt für Sicherheit in der Informationstechnik, 2022e)
5. APP_3_1_Webanwendungen_und_Webservices_Edition_2022 (Bundesamt für Sicherheit in der Informationstechnik, 2022a)
6. APP_3_2_Webserver_Edition_2022 (Bundesamt für Sicherheit in der Informationstechnik, 2021a)

Mit diesen Dokumenten ergeben sich Fragestellungen, die für eine Bereitstellung der angedachten Erfassungskomponente relevant sind und betrachtet werden müssen. Aus innerbetrieblichen Gründen

des BKG werden in dieser Arbeit keine Informationen preisgegeben. Die zuvor genannten IT-Anforderungen sind rein exemplarisch. Alle Fragen zur sicherheitsrelevanten Einschätzung stehen jedermann zur Verfügung. Der Detailgrad der Fragen erfolgt in drei Kategorien und orientiert sich an dem Schutzbedarf der Daten und der bereitzustellenden Anwendung. „Basis (=normal)“ stellt das absolute Minimum dar. Der „Standard (=hoch)“ gibt ein mittleres Sicherheitsniveau wider. Das Höchstmaß entspricht der Kategorie „Hoch (=sehr hoch)“. Weiterführende Erklärungen bzw. Erläuterungen befinden sich in den referenzierten Dokumenten.

[Zu OPS_1_1_2_Ordnungsgemaesse_IT_Administration_Edition_2022](#)

Tabelle 1: Fragenkatalog zu OPS_1_1_2

Anforderung	Titel	Kategorie
OPS.1.1.2.A1	ENTFALLEN	Basis
OPS.1.1.2.A2	Vertretungsregelungen und Notfallvorsorge	Basis
OPS.1.1.2.A3	Geregelte Einstellung von IT-Administratoren	Basis
OPS.1.1.2.A4	Beendigung der Tätigkeit als IT-Administrator	Basis
OPS.1.1.2.A5	Nachweisbarkeit von administrativen Tätigkeiten	Basis
OPS.1.1.2.A6	Schutz administrativer Tätigkeiten	Basis
OPS.1.1.2.A7	Regelung der IT-Administrationstätigkeit	Standard
OPS.1.1.2.A8	Administration von Fachanwendungen	Standard
OPS.1.1.2.A9	Ausreichende Ressourcen für den IT-Betrieb	Standard
OPS.1.1.2.A10	Fortbildung und Information	Standard
OPS.1.1.2.A11	Dokumentation von IT-Administrationstätigkeiten	Standard
OPS.1.1.2.A12	Regelungen für Wartungs- und Reparaturarbeiten	Standard
OPS.1.1.2.A13	ENTFALLEN	Standard
OPS.1.1.2.A20	Verwaltung und Inbetriebnahme von Geräten	Standard
OPS.1.1.2.A14	Sicherheitsüberprüfung von Administratoren	Hoch
OPS.1.1.2.A15	Aufteilung von Administrationstätigkeiten	Hoch
OPS.1.1.2.A16	Zugangsbeschränkungen für administrative Zugänge	Hoch
OPS.1.1.2.A17	IT-Administration im Vier-Augen-Prinzip	Hoch
OPS.1.1.2.A18	Durchgängige Protokollierung administrativer Tätigkeiten	Hoch
OPS.1.1.2.A19	Berücksichtigung von Hochverfügbarkeitsanforderungen	Hoch

[OPS_1_1_3_Patch_und_Aenderungsmangement_Edition_2022](#)

Tabelle 2: Fragenkatalog zu OPS_1_1_3

Anforderung	Titel	Kategorie
OPS.1.1.3.A1	Konzept für das Patch- und Änderungsmanagement	Basis
OPS.1.1.3.A2	Festlegung der Zuständigkeiten	Basis
OPS.1.1.3.A3	Konfiguration von Autoupdate-Mechanismen	Basis
OPS.1.1.3.A15	Regelmäßige Aktualisierung von IT-Systemen und Software	Basis
OPS.1.1.3.A16	Regelmäßige Suche nach Informationen zu Patches und Schwachstellen	Basis

OPS.1.1.3.A4	ENTFALLEN	Standard
OPS.1.1.3.A5	Umgang mit Änderungsanforderungen	Standard
OPS.1.1.3.A6	Abstimmung von Änderungsanforderungen	Standard
OPS.1.1.3.A7	Integration des Änderungsmanagements in die Geschäftsprozesse	Standard
OPS.1.1.3.A8	Sicherer Einsatz von Werkzeugen für das Patch- und Änderungsmanagement	Standard
OPS.1.1.3.A9	Test- und Abnahmeverfahren für neue Hardware	Standard
OPS.1.1.3.A10	Sicherstellung der Integrität und Authentizität von Softwarepaketen	Standard
OPS.1.1.3.A11	Kontinuierliche Dokumentation der Informationsverarbeitung	Standard
OPS.1.1.3.A12	Einsatz von Werkzeugen beim Änderungsmanagement	Hoch
OPS.1.1.3.A13	Erfolgsmessung von Änderungsanforderungen	Hoch
OPS.1.1.3.A14	Synchronisierung innerhalb des Änderungsmanagements	Hoch

SYS_1_1_Allgemeiner_Server_2023

Tabelle 3: Fragenkatalog zu SYS_1_1

Anforderung	Titel	Kategorie
SYS.1.1.A1	Geeignete Aufstellung	Basis
SYS.1.1.A2	Benutzerauthentisierung an Servern	Basis
SYS.1.1.A3	ENTFALLEN	Basis
SYS.1.1.A4	ENTFALLEN	Basis
SYS.1.1.A5	Schutz von Schnittstellen	Basis
SYS.1.1.A6	Deaktivierung nicht benötigter Dienste	Basis
SYS.1.1.A7	ENTFALLEN	Basis
SYS.1.1.A8	ENTFALLEN	Basis
SYS.1.1.A9	Einsatz von Virenschutz-Programmen auf Servern	Basis
SYS.1.1.A10	Protokollierung	Basis
SYS.1.1.A11	Festlegung einer Sicherheitsrichtlinie für Server	Standard
SYS.1.1.A12	Planung des Server-Einsatzes	Standard
SYS.1.1.A13	Beschaffung von Servern	Standard
SYS.1.1.A14	ENTFALLEN	Standard
SYS.1.1.A15	Unterbrechungsfreie und stabile Stromversorgung	Standard
SYS.1.1.A16	Sichere Grundkonfiguration von Servern	Standard
SYS.1.1.A17	ENTFALLEN	Standard
SYS.1.1.A18	ENTFALLEN	Standard
SYS.1.1.A19	Einrichtung lokaler Paketfilter	Standard
SYS.1.1.A20	ENTFALLEN	Standard
SYS.1.1.A21	Betriebsdokumentation für Server	Standard
SYS.1.1.A22	Einbindung in die Notfallplanung	Standard
SYS.1.1.A23	Systemüberwachung und Monitoring von Servern	Standard
SYS.1.1.A24	Sicherheitsprüfungen für Server	Standard
SYS.1.1.A25	Geregelte Außerbetriebnahme eines Servers	Standard
SYS.1.1.A35	Erstellung und Pflege eines Betriebshandbuchs	Standard

SYS.1.1.A37	Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten	Standard
SYS.1.1.A26	ENTFALLEN	Hoch
SYS.1.1.A27	Hostbasierte Angriffserkennung	Hoch
SYS.1.1.A28	Steigerung der Verfügbarkeit durch Redundanz	Hoch
SYS.1.1.A29	ENTFALLEN	Hoch
SYS.1.1.A30	Ein Dienst pro Server	Hoch
SYS.1.1.A31	Einsatz von Ausführungskontrolle	Hoch
SYS.1.1.A32	ENTFALLEN	Hoch
SYS.1.1.A33	Aktive Verwaltung der Wurzelzertifikate	Hoch
SYS.1.1.A34	Festplattenverschlüsselung	Hoch
SYS.1.1.A36	Absicherung des Bootvorgangs	Hoch
SYS.1.1.A38	Härtung des Host-Systems mittels Read-Only-Dateisystem	Hoch

[SYS_1_2_3_Windows_Server_2023](#)

Tabelle 4: Fragenkatalog zu SYS_1_2_3

Anforderung	Titel	Kategorie
SYS.1.2.3.A1	Planung von Windows Server 2012	Basis
SYS.1.2.3.A2	Sichere Installation von Windows Server 2012	Basis
SYS.1.2.3.A3	Telemetrie- und Nutzungsdaten unter Windows Server	Basis
SYS.1.2.2.A4	Sichere Konfiguration von Windows Server 2012	Standard
SYS.1.2.2.A5	Schutz vor Schadsoftware auf Windows Server 2012	Standard
SYS.1.2.2.A6	Sichere Authentisierung und Autorisierung in Windows Server 2012	Standard
SYS.1.2.2.A7	ENTFALLEN	Standard
SYS.1.2.2.A8	Schutz der Systemintegrität	Standard
SYS.1.2.2.A9	ENTFALLEN	Standard
SYS.1.2.2.A10	ENTFALLEN	Hoch
SYS.1.2.2.A11	Angriffserkennung bei Windows Server 2012	Hoch
SYS.1.2.2.A12	Redundanz und Hochverfügbarkeit bei Windows Server 2012	Hoch
SYS.1.2.2.A13	ENTFALLEN	Hoch
SYS.1.2.2.A14	Herunterfahren verschlüsselter Server und virtueller Maschinen	Hoch

[APP_3_1_Webanwendungen_und_Webservices_Edition_2022](#)

Tabelle 5: Fragenkatalog zu APP_3_1

Anforderung	Titel	Kategorie
APP.3.1.A1	Authentisierung	Basis
APP.3.1.A2	ENTFALLEN	Basis
APP.3.1.A3	ENTFALLEN	Basis
APP.3.1.A4	Kontrolliertes Einbinden von Dateien und Inhalten	Basis
APP.3.1.A5	ENTFALLEN	Basis

APP.3.1.A6	ENTFALLEN	Basis
APP.3.1.A7	Schutz vor unerlaubter automatisierter Nutzung	Basis
APP.3.1.A14	Schutz vertraulicher Daten	Basis
APP.3.1.A16	ENTFALLEN	Basis
APP.3.1.A19	ENTFALLEN	Basis
APP.3.1.A8	Systemarchitektur	Standard
APP.3.1.A9	Beschaffung von Webanwendungen und Webservices	Standard
APP.3.1.A10	ENTFALLEN	Standard
APP.3.1.A11	Sichere Anbindung von Hintergrundsystemen	Standard
APP.3.1.A12	Sichere Konfiguration	Standard
APP.3.1.A13	ENTFALLEN	Standard
APP.3.1.A15	ENTFALLEN	Standard
APP.3.1.A17	ENTFALLEN	Standard
APP.3.1.A18	ENTFALLEN	Standard
APP.3.1.A21	Sichere HTTP-Konfiguration bei Webanwendungen	Standard
APP.3.1.A22	Penetrationstest und Revision	Standard
APP.3.1.A23	ENTFALLEN	Standard
APP.3.1.A20	Einsatz von Web Application Firewalls	Hoch
APP.3.1.A24	ENTFALLEN	Hoch
APP.3.1.A25	ENTFALLEN	Hoch

APP_3_2_Webserver_Edition_2022

Tabelle 6: Fragenkatalog zu APP_3_2

Anforderung	Titel	Kategorie
APP.3.2.A1	Sichere Konfiguration eines Webserver	Basis
APP.3.2.A2	Schutz der Webserver-Dateien	Basis
APP.3.2.A3	Absicherung von Datei-Uploads und -Downloads	Basis
APP.3.2.A4	Protokollierung von Ereignissen	Basis
APP.3.2.A5	Authentisierung	Basis
APP.3.2.A6	ENTFALLEN	Basis
APP.3.2.A7	Rechtliche Rahmenbedingungen für Webangebote	Basis
APP.3.2.A11	Verschlüsselung über TLS	Basis
APP.3.2.A8	Planung des Einsatzes eines Webserver	Standard
APP.3.2.A9	Festlegung einer Sicherheitsrichtlinie für den Webserver	Standard
APP.3.2.A10	Auswahl eines geeigneten Webhosters	Standard
APP.3.2.A12	Geeigneter Umgang mit Fehlern und Fehlermeldungen	Standard
APP.3.2.A13	Zugriffskontrolle für Webcrawler	Standard
APP.3.2.A14	Integritätsprüfungen und Schutz vor Schadsoftware	Standard
APP.3.2.A16	Penetrationstest und Revision	Standard
APP.3.2.A20	Benennung von Ansprechpartnern	Standard
APP.3.2.A15	Redundanz	Hoch
APP.3.2.A17	ENTFALLEN	Hoch
APP.3.2.A18	Schutz vor Denial-of-Service-Angriffen	Hoch

APP.3.2.A19	ENTFALLEN	Hoch
-------------	-----------	------

Nach Beantwortung der Fragen aus den Tabellen 1 bis 6 ergibt sich ein Gesamteindruck der notwendigen IT-Systeme. Je nachdem wie sich das Ergebnis abzeichnet, kann oder muss nachjustiert werden. Entsprechend ist dies ein iterativer Prozess und wird jeweils dokumentiert, welchem Sicherheitsniveau die Erfassungskomponenten genügen. Gemäß den allgemeinen Anforderungen und den Anforderungen des Datenschutzes reicht die Einstufung „Basis“ für den Anwendungsbetrieb der angedachten Erfassungskomponente. Bei genauerer Betrachtung können auch die Bedarfe der nächsthörenden Kategorie (=Basis) positiv beantwortet werden können. Das Mindestmaß bildet jedoch, dass alle Basis-Fragen positiv beantwortet werden, damit ein Fachverfahren in Betrieb genommen werden kann.

2.4 Abgrenzungen

Aus dem methodischen Ansatz auf Seite - 8 - ergeben sich nachstehende Punkte, die individuelle Abgrenzungen notwendig machen.

1. Erfassung von situativen Ereignissen:

Die Erhebungen der Erfasser müssen nicht in eine BKG-interne Infrastruktur übernommen werden. Sie sind essentiell wichtig und stellen eine Dienstleistung des BKG dar. Wichtig sind diese für individuelle Bedürfnisse von Kunden/Behörden. Der Kunde ist also selbstständig dafür verantwortlich, die erfassten Daten in die eigene Infrastruktur zu übernehmen. Damit stellt das BKG einen Dienst zur Verfügung, ohne im eigenen Interesse zu handeln, bzw. die Daten zu übernehmen. Die Erfassungen können jeglicher Art sein, und umfassen Daten wie, Texte, Bilder/Fotos, Tonaufnahmen, bedingte Attributeingabe.

Wichtig: Die tatsächlich erhobene Daten werden nicht überführt.

2. Erfassung von Korrekturen von Bestandprodukten:

Die Erhebungen der Erfasser müssen nicht 1:1 in eine BKG-interne Infrastruktur übernommen werden. Informationen/Erhebungen dieser Art stellen Auskünfte dar. Diese sollten manuell abgearbeitet werden. Erfasst werden demnach Lageinformationen mit einem Attribut und mindestens einem Text. Nach interner Prüfung können diese Informationen an entsprechende Stellen weitergeleitet werden.

Wichtig: Die tatsächlich erhobene Daten werden nicht überführt.

3. Erfassung neuer Objektarten für Bestandsprodukte:

Die Erhebungen der Erfasser müssen in eine BKG-interne Infrastruktur übernommen werden. Eine erste Kontrolle dieser soll über die Community erfolgen. Die zweite Kontrolle könnte mit OSM-Daten, als Referenzdatensatz, erfolgen. Würde die aufgenommene Geoinformation in OSM existieren, dann wäre keine weitere manuelle Kontrolle notwendig. Würden die Informationen in OSM fehlen, müsste eine manuelle Nachkontrolle erfolgen.

Diese Art der Erfassung erscheint als aufwändigste und muss weiter fokussiert werden. Aufwändig, weil Erfassungsdaten direkt übernommen bzw. überführt werden müssten. Hierzu müssen zusätzlich der Datenschutz und die Informationssicherheit betrachtet werden.

Wichtig: Die tatsächlich erhobenen Daten sollen überführt werden. Hieraus würden sich hohe Anforderungen an die IT ergeben.

3 Methodik

Dieser Abschnitt beschreibt die Methoden zur Beantwortung der operativen Teilziele aus 1.3 Forschungsziel und Gliederung“. Zunächst werden die Softwarekomponenten auf Standards und IT-Bausteine untersucht, um Erfassungsumfragen erstellen zu können. Hersteller bzw. Anbieter zur Bereitstellung von Erfassungsmethoden von Geodaten gibt es diverse. Herauszuheben sind aber Anbieter, die sich an einem Standard orientieren. Aus diesem Grund fiel die Wahl auf ESRI, als kommerziellen Anbieter, und KoboToolbox, als Open Source Lösung. Ob dies „state of the art“ ist, bleibt unbeachtet. Um einen Vergleich herbeizuführen, scheint es praktikabel. Anschließend wird exemplarisch eine Erfassungsumfrage erstellt, damit die Usability in „Benutzerführung und Usability“ bewertet werden kann. Da die Erfassungen grundsätzlich mittels Sensoren mobiler Endgeräte erfolgen, wird im dritten Unterkapitel auf Sensoriken eingegangen. Um Kategorisierungen von Sammlern durchzuführen, wird in dem darauffolgenden Unterkapitel theoretisch eingegangen. Bezogen auf die technischen Anforderungen aus 2.3 Technische Anforderungen (Sicherheitsaspekte)“ werden Rollen zu Verantwortlichkeiten in 3.5 Verantwortlichkeiten“ festgehalten und definiert. Mögliche Sicherheitsmaßnahmen zur Qualität und zur Integration werden daraufhin anhand unterschiedlicher Aspekte behandelt. Abschließend werden die Motivationsgründe der Teilnehmenden auf Basis von Forschungsergebnissen betrachtet.

3.1 Software

Untersucht werden zwei Erfassungssysteme unterschiedlicher Hersteller. Beide Systeme bauen auf einen gleichen Standard. Somit ist ein direkter Vergleich günstig in der Umsetzung.

3.1.1 Standard der Erfassungskomponenten

Die Erfassungskomponenten, die untersucht werden, basieren beide auf einem offenen Standard, XLSForm. Aus diesem Grund können beide Systeme direkt miteinander verglichen werden. In gleicher Weise werden beide Komponenten untersucht und geprüft, ob sie den Standard identisch interpretieren bzw. umsetzen. Den Komponenten wird ein übereinstimmendes XLSForm übermittelt. XLSForm ist ein offener Standard, der von der „Sustainable Engineering Lab der Columbia University“ entwickelt wurde (<https://qsel.columbia.edu/>). Mit XLSForms wird ein praktischer Ansatz verfolgt. Wie der Name es andeutet, basiert der Standard auf Microsoft Excel. Ein großer Vorteil ist, dass eine Großzahl von Anwendern mit Excel vertraut ist. Das Microsoft Office Produkt Excel ist allgegenwärtig und damit einer Vielzahl von Anwendern bekannt. Die Anwender benötigen nicht einmal Programmierkenntnisse. Diesen Zusammenhang und die Erkenntnis sehen auch Brunette und Hartung

(Brunette & Hartung, 2023). Ein inhaltliches Format muss dennoch eingehalten werden. Ein einfaches Beispiel zeigt Abbildung 4, in dem ein Name und die GPS-Koordinaten eines Geschäfts zu erfassen sind. Daraus folgen eine größere Akzeptanz und ein größeres Nutzerumfeld.

type	name	label
text	store_name	What is the name of this store?
geopoint	store_gps	Collect the GPS coordinates of this store.

← | survey | choices | settings | +

Abbildung 4: Beispiel XLSForm (Quelle: <https://xlsform.org/>)

Klar ist damit auch, dass mit dem offenen Standard Um- bzw. Abfragen definiert werden können. Die XLSForm-Dateien werden den IT-Systemen übermittelt, anschließend interpretiert und veröffentlicht. Der XLSForm-Standard ist unter <https://xlsform.org/> erreichbar und fest definiert. Alternativ zu den Excel-Dateien bieten beide Erfassungskomponenten einen WYSIWYG-Editor an. Mit Hilfe von diesem lassen sich einfach per „Drag and Drop“ Elemente in einer visuellen Oberfläche einfügen und anschließend beschriften und formatieren. Quasi ein echtes Klick-System. Somit steht ein zusätzliches Werkzeug zur Verfügung, ohne sich mit Excel und dem inhaltlichen Format auseinanderzusetzen. Eine Umfrage, die mit dem Editor erstellt wurde, kann aus diesem auch in das standardisierte XLSForm-Format exportiert werden. Abbildung 5 zeigt den WYSIWYG-Editor von KoboToolbox exemplarisch.

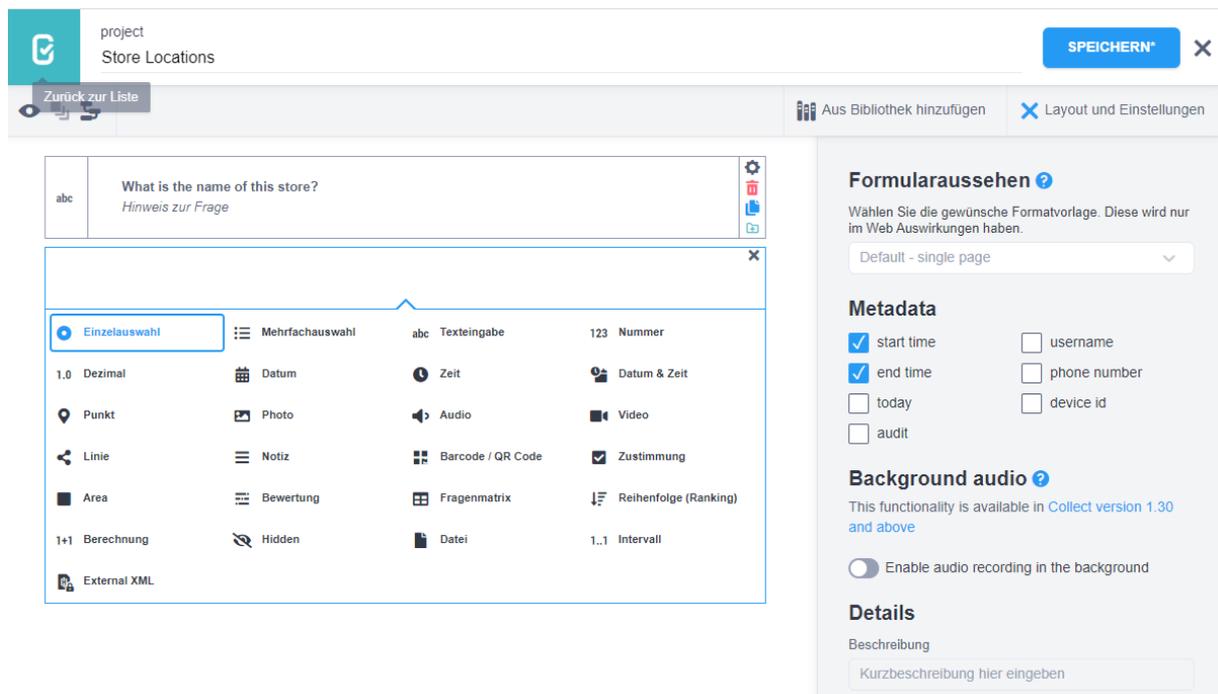


Abbildung 5: Beispiel WYSIWYG-Editor von KoboToolbox

Eine weitere wesentliche Rolle beider Systeme spielt hierbei ENKETO (<https://enketo.org/>). ENKETO ist ein webbasierter Aufsatz, der XLSForms für Anwender über einen Browser nutzbar macht. In den vergangenen COVID-Jahren wurden unzählige Erfassungskomponenten zu dieser Krankheit bereitgestellt. Nicht nur COVID wurde erfasst. Auffallend ist, dass mittels des genannten Standards viele Erhebungen und Forschungen betrieben wurden. Ein wichtiger Aspekt ist, dass eine Erhebung mittels dem Open-Source Ansatz von ENKETO auch OFFLINE erfasst werden kann. Eine Bereitstellung durch ENKETO bedarf lediglich einen aktuellen Browser auf einem Endgerät. Diese Erkenntnis beschreiben auch (Guinez-Molinos et al., 2022). Alle aktuell gängigen Browser und Betriebssysteme werden unterstützt. Damit auch die Arten eines jeweiligen Endgerätes. Bezüglich des Endgerätes wird durch ENKETO die optimale Darstellung gewählt. Ermittelt werden die Auflösung und die Größe des Displays/Bildschirms. So erhält der Endnutzer immer eine individuell angepasste Ansicht, wodurch Entwickler und Bereitsteller keine weiteren Anpassungen durchführen müssen.

Nachdem feststeht, dass beide Komponenten auf gleiche Art arbeiten, kann ein vordefinierter Ablauf erfolgen.

1. XLSForm erstellen
2. Publizieren erfolgt über anhand der Komponenten
3. Community einladen
 - a. An publizierten Umfragen kann über den gewöhnlichen Browser (Mobile Geräte und normale PC's) teilgenommen werden.
4. Das Erfassen beginnt und die Daten werden von der Community bei bestehender Internetverbindung wieder in die Komponenten hochgeladen.
5. Die Analyse der Daten beginnt (siehe Kapitel 4 „Ergebnisse und Diskussion“)

Visuell kann der Ablauf in einem Zyklus dargestellt werden (siehe Abbildung 6). Die Abbildung unterstreicht ein wiederkehrendes Muster, mit dem Um- und Abfragen individuell und unmittelbar zur Verfügung gestellt werden können.

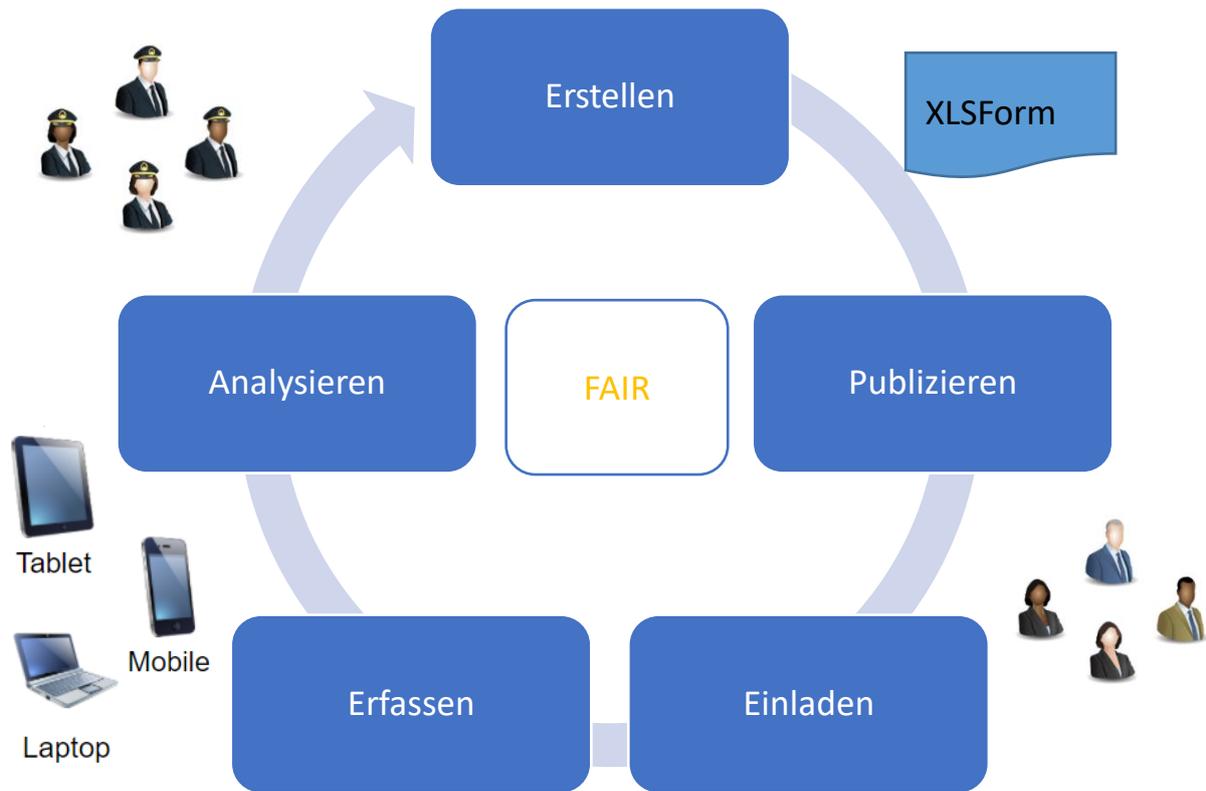


Abbildung 6: Ablaufzyklus der Erfassungskomponenten

Nach dem generellen Ablauf lässt sich ein weiterer Kernaspekt erkennen. 2016 veröffentlichte die Europäische Kommission die GO-FAIR-Initiative. FAIR steht für Findable, Accessible, Interoperable und Reusable. Die FAIR-Prinzipien beinhalten die nachhaltige Wiederverwendbarkeit von Daten.

1. **Findable**, bezieht sich auf die Auffindbarkeit von Daten.
2. **Accessible**, bezieht sich auf die nachhaltige Zugänglichkeit von Daten.
3. **Interoperabel**, bezieht sich auf die Interoperabilität von Daten und sichert die.
4. **Reusable**, umfasst die Wiederverwendbarkeit von Daten.

In diesem Zusammenhang wurde auch Crowdsourcing als ein wichtiger Punkt thematisiert. In aktuellen Forschungen und Veröffentlichungen wird belegt, dass der Ablaufzyklus aus Abbildung 6 den FAIR-Prinzipien entspricht. Viele Forschungseinrichtungen nutzen heterogene Systeme, die Daten mit ähnlichen Methoden erfassen. Bei einer Umsetzung mit KoboToolbox oder ODK entspricht dies den FAIR-Prinzipien des Datenmanagements, so Senagi & Tonnang (2022). In dem Zeitraum von 2014 bis 2020 konnten zum Thema Crowdsourcing und FAIR EU-Projektmittel, mit dem Ziel der Beteiligung von EU-Bürgern, beantragt werden.

“The aim of the project is to foster the successful inclusion of EU mobile citizens in their host EU country’s civic and political life through the provision of a holistic approach to tackling obstacles they face when exercising their rights.”

<https://ecas.org/wp-content/uploads/2018/04/ToR-Crowdsourcing-platform.pdf>

Im Folgenden werden die Softwaresysteme und die Bereitstellung von Umfragen behandelt.

3.1.2 Survey123

Survey123 ist eine Erfassungskomponente mit der Daten vor Ort und formularbasiert erfasst werden können. Ganz einfach mit dem Smartphone oder Tablet vor Ort oder mittels eine Desktop-PC’s von einem anderen Ort. Die erfassten Informationen stehen dann übergreifend zur Verfügung und können von berechtigten Personen, z.B. Einsatzkräften, sowohl unterwegs als auch von dem Arbeitsplatzrechner (Desktop-PC) im Büro genutzt werden.

Mit Survey123 bietet der kommerzielle GIS-Hersteller ESRI eine Erfassungskomponente an, die sich in das Gesamtkonzept des Herstellers integrieren lässt. Dieses Gesamtkonzept von ESRI läuft unter dem Oberbegriff „ArcGIS Enterprise“. ESRI selbst wirbt mit den Schlagworten „Sichere Bereitstellung im Unternehmen“, „Datenmanagement“, „Kartenerstellung und Visualisierung“ und „Analyse und Erkundung“. Hinter diesen Schlagworten verbirgt sich eine Vielzahl an einzelnen IT-Systemen, die sich modular gestalten. Grundvoraussetzung ist ein User-basiertes Kontrollsystem. Entweder über ESRI oder über ein eigens gehostetes System. Die Zugriffskontrolle erfolgt für gewöhnlich über sog. „Named-User“. Was nichts anderes heißt, als dass der Anwender den Systemen bekannt sein muss. Öffentliche Zugriffe, für Jedermann und ohne Registrierung, sind dennoch möglich. Systeme, die Jedermann zur Verfügung stehen, sind im Sicherheitskontext weniger günstig. Gerade im Hinblick auf die Gesamtumgebung können mit freizugänglichen Anwendungen erhebliche Lasten auf das Gesamtsystem erzeugt werden. Gerade diese Abhängigkeiten können kontraproduktiv sein, weshalb nicht nur eine sog. horizontale, sondern auch vertikale Skalierung der gesamten Infrastruktur in Betracht gezogen werden muss. Vertikale Skalierung bedeutet, dass die Anzahl einer Gesamtinfrastruktur (eines Clusters) multipliziert wird, um eine Verarbeitungskapazität zu steigern. Bei der horizontalen Skalierung werden innerhalb eines Clusters weitere Systeme derselben Größe hinzugefügt.

Abbildung 7 zeigt die benötigte und allgemeine Architektur der Infrastruktur von Survey123 und eines Clusters.

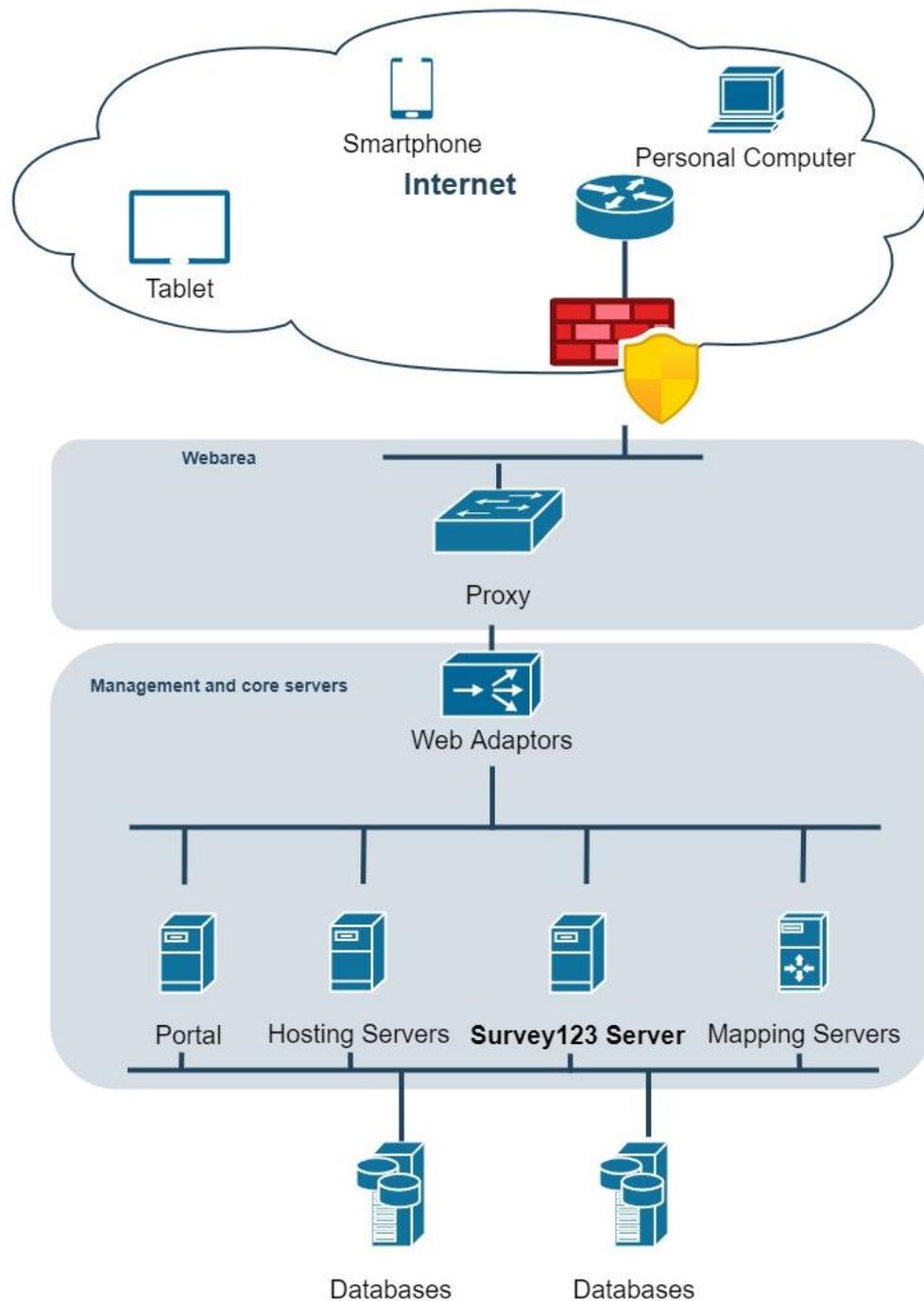


Abbildung 7: Architektur ESRI Survey123 (nach: ESRI)

Survey123 ist nach ESRI ein sog. „Hosting Server“. Generell veröffentlicht ESRI wenige Detail-Informationen über mögliche IT-Architekturen. Nach der abgeleiteten IT-Architektur von ESRI können vier Ebenen identifiziert werden. Einmal der „End-User“ über das Internet, der über einen Zugriffspunkt (Proxy) auf die Infrastruktur zugreift. Das wird obligatorisch über das HTTPS-Protokoll gemacht und ist damit eine verschlüsselte Verbindung zwischen dem Endnutzer und dem Verbindungsknoten zu der ESRI-Umgebung. Weiter vermittelt wird der jeweilige Zugriff über diverse ESRI-Web-Adaptoren, die die Systeme auf Lasten ausbalancieren und in die nächste Ebene vermitteln

sollen. In der nachfolgenden Systemebene bildet eine Portallösung die Zentrale. Hier werden Anwendungen verwaltet und die User-Kontrolle eingestellt. „Mapping-Servers“ stellen individuelle Darstellungsdienste (WMS-Dienste) dar. Weitere abhängige Dienste sind „Hosting Servers“, wie z.B. Server zur Analyse von Geodaten. Als solch einen Dienst lässt sich auch Survey123 identifizieren. Auf gleicher Ebene operieren und kommunizieren mehrere Server miteinander und stellen somit eine gesamte Plattform dar. Die unterste Ebene bildet die Datenhaltung. Also, eine, bzw. mehrere, Datenbanken oder andere Datenspeicherformen. Das ganze Konstrukt entspricht grundsätzlich dem Ansatz des IT-Grundschutzes, ein Server hat eine Aufgabe. Individuell umsetzen muss das jedes Unternehmen für sich. Auf Basis eines allgemeinen IT-Verstandes, kann festgehalten werden, dass die notwendigen und einzelnen Komponenten gekapselt werden können.

3.1.3 KoboToolbox

KoboToolbox ist nahezu identisch zu Survey123 von ESRI. Formularbasiert können Daten erhoben bzw. erfasst werden. Unterschiede gibt es kaum, da beide auf dem gleichen Standard basieren, nämlich dem XLSForm und der Webkomponente ENKETO. Im Gegensatz zu ESRI kennt man KoboToolbox weniger. Das mag daran liegen, dass der Hersteller eine unabhängige gemeinnützige Organisation ist. 2005 wurde Kobo von der „Harvard Humanitarian Initiative in Cambridge, Massachusetts“ gegründet und die KoboToolbox dient bis heute vorrangig humanitärer Forschungen. Mittlerweile gibt es jedoch diverse hochrangige Partner und Unterstützer. Genannt seien hier z.B. „United Nations Refugee Agency (UNHCR)“ oder das „United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA)“. Aber auch kleinere Organisationen, wie die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) beteiligen sich aktiv und zählen zu den Partnern. KoboToolbox ist eine „Free and Open Source Software“, die vor allem von ihren zahlreichen Partnern für eine langfristige Nachhaltigkeit unterstützt wird. Da es sich um freie und offene Software handelt, ist KoboToolbox auch in der OSM-Community uneingeschränkt beliebt.

Die Merkmale von KoboToolbox gleichen Survey123. So kann mit mobilen Endgeräten, als auch mit Desktop-PC's, erfasst werden. Online, wie Offline. Berechtigten steht ebenso der Gesamtüberblick der Daten zur Verfügung.

Anders als bei Survey123 umfasst KoboToolbox lediglich die Erfassungskomponente mit den dazugehörigen IT-Systemen. Eine große Plattform mit unterschiedlich agierenden Systemen gibt es nicht. Auf den Internetseiten (<https://kobotoolbox.org>) wird mit den Worten „Einfache Datenerfassung, in jedem Kontext, für jeden“ geworben. Das sog. KISS-Prinzip (Keep It Simple and Smart) lässt sich dadurch ableiten. Das KISS-Prinzip steht für eine möglichst einfache und minimalistische Problemlösung. Bei der Veredelung von Geodaten kann eine möglichst klar

strukturierte und minimalistische Anwendung oftmals mehr Gewinn und Akzeptanz bringen, als eine überfrachtete.

Unter anderem findet sich auch das Thema Sicherheit wieder. „Sicher und flexibel“ heißt es auf den Internetseiten. Hierunter verbirgt sich u.a. die Zugriffskontrolle. Mit KoboToolbox lassen sich Erfassungsprojekte und deren Daten mit differenzierten Berechtigungsoptionen teilen. „Named-User“ und anonyme Anwender können unterschiedliche Arten des Zugriffs erhalten. Wie bereits bei Survey123 erwähnt, ist der „Jedermann-Zugriff“ mit Sicherheitslücken behaftet. Eine flexible Skalierung des Systems ist durch die grundsätzliche Docker-Containerisierung gegeben. Abbildung 8 zeigt den Aufbau der „multiple Composable“ IT-Architektur, die Lastspitzen auffangen kann. Was ist eine „multiple Composable“ IT-Architektur? Übersetzt bedeutet es eine zusammengesetzte Infrastruktur. Also nichts anderes als ein gesamter Container, der wiederum aus einzelnen System-Containern besteht und in sich als ein Ganzes agiert. In einer Composable Infrastructure werden Rechen-, Datenspeicher- und Netzwerkressourcen von ihren physischen Orten abstrahiert und können über eine webbasierte Schnittstelle verwaltet werden. Bei der Composable Infrastructure werden Ressourcen zentralisiert zusammengefasst, so dass diese zentral verwaltet werden können. Das heißt, wenn die IT-Abteilung eine neue Software benötigt, kann die erforderliche Infrastruktur unter Verwendung dieser Templates erstellt werden. Im Gegensatz zu virtuellen Maschinen verwenden

Container das zugehörige Hostbetriebssystem, anstatt ein eigenes bereitzustellen.

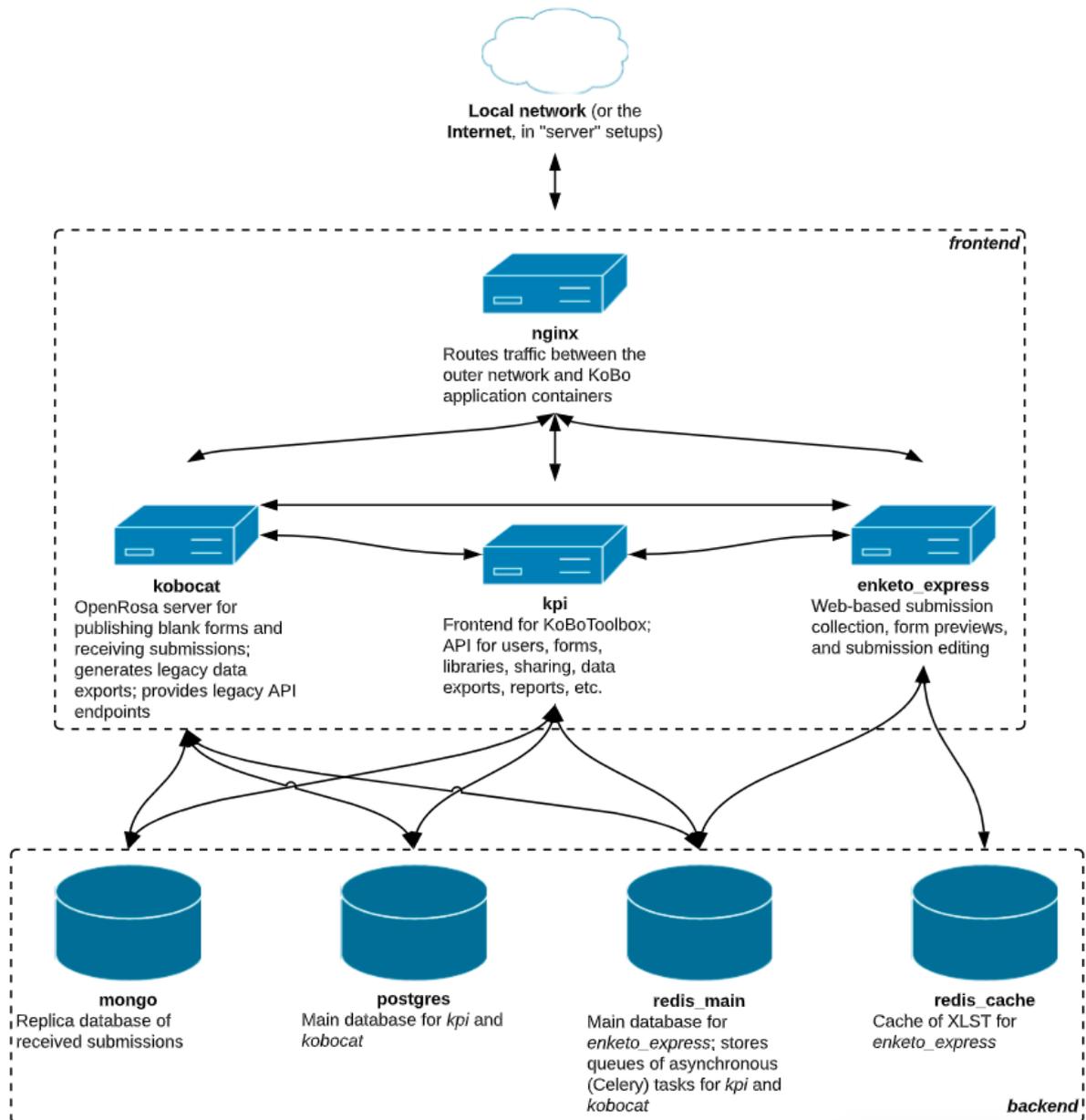


Abbildung 8: Architektur KoboToolbox (Quelle: https://support.kobotoolbox.org/software_architecture.html)

3.2 Benutzerführung

Eine Bewertung durch End-Nutzer wurde im Vorfeld umgesetzt. Im Vorfeld heißt, dass die bereitgestellte Anwendung KoboToolbox aus Kapitel 3.1.3 „KoboToolbox“ so umgesetzt wurde, dass Bewertungen und Kommentare einer Vorerprobung eingeflossen sind. Ziel hiervon war es, die Systeme kennenzulernen und End-Nutzer frühzeitig einzubinden. Die Herangehensweise war das Erstellen einer Anwendung, mit der neue Objekte erfasst werden können. Unter anderem sollte geprüft werden, ob es sich besser darstellt, alle Fragen einer Erhebung anhand einer einzelnen Seite zu erfassen. Oder, ob

pro Erhebungsfrage eine einzelne Seite besser geeignet erscheint. Hinzu kam auch die Betrachtung mit der Zustimmung der Datenschutzrichtlinien. Die Ergebnisse und Bewertung befinden sich in 4.1 Bewertung der VGI-Software“.

Der Ablauf wurde folgendermaßen definiert (siehe Abbildung 9):

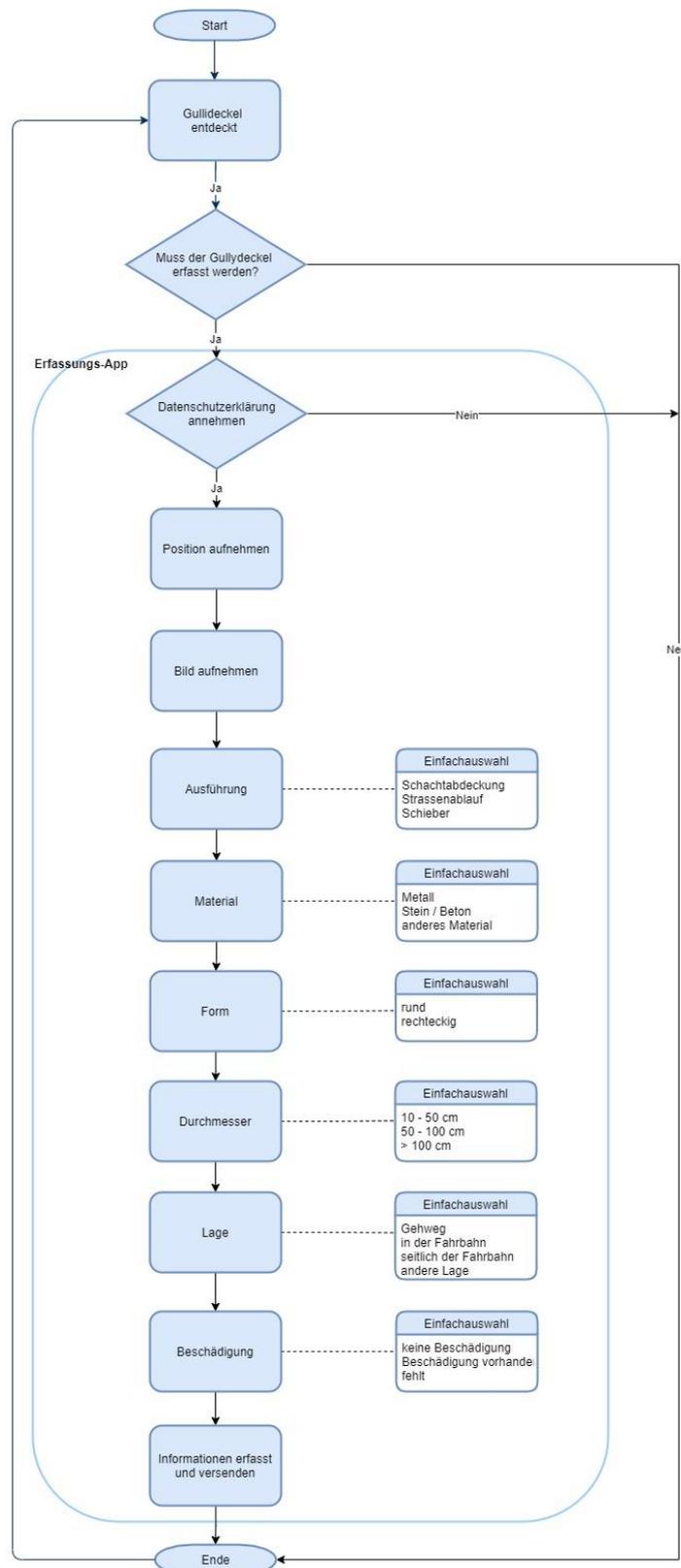


Abbildung 9: Ablauf eines Testszenarios

Eine Auswertung und weitere Empfehlung befindet sich im Kapitel 4.1 „Bewertung der VGI-Software“.

3.3 Digitale Erfassungssensoren

Unter Sensoren sind die Empfangseinheiten des „Global Navigation Satellite System (GNSS)“ eines mobilen Endgerätes zu verstehen. Mit dem globalen Navigationssatellitensystem wird auf den mobilen Endgeräten eine Positionsbestimmung ermöglicht. In zahlreichen Studien werden die Empfänger stets wiederkehrend auf die Positionierungsgenauigkeiten geprüft. In einer aktuellen Veröffentlichung, vom Oktober 2022, werden drei unterschiedliche Empfängertypen unter erschwerten Bedingungen verglichen. Huang et al. (2022) vergleichen professionelle Empfänger, mittelklassige Handempfänger und die Empfangseinheiten zweier Smartphones. Die Empfänger wurden in einem Mischwald (Nadel- und Laubwald) gegen getestet. Zur Genauigkeitsbewertung wurden die Ergebnisse von 57 Aufnahmepunkten mit unterschiedlichen Abschattungen herangezogen. Als Ergebnis wurde festgehalten, dass aktuelle Smartphones unter erschwerten Bedingungen eine Genauigkeit von bis zu 2,5m in horizontaler Richtung erreichen. Bezogen auf die Anwendungsfälle dieser Arbeit ist die Genauigkeit, die Huang et al. (2022) ermittelt haben, absolut ausreichend. Gerade wenn man überlegt, dass eine Community Daten erfassen soll und diese keine Geodäten sind und somit keine Präzisionsvermessung erstellen.

3.4 Sammlereigenschaften

Goodchild (2007) stellt vor was VGI ist. Er erklärt warum Menschen dazu beitragen, wie akkurat die Ergebnisse sind, ob sie die individuelle Privatsphäre gefährden und ob sie konventionelle Quellen ergänzen können. In seiner Veröffentlichung zieht er einen Vergleich mit den traditionelleren „citizen sciences“ und erläutert die Rolle von Amateuren in der geografischen Informationsgewinnung.

Bei VGI handelt es sich um Informationen die Personen freiwillig sammeln, bearbeiten und kostenlos bereitstellen. Dabei ist es egal, welche Personen an dieser kollaborativen Datengewinnung teilnehmen: „user-generated-content“. So bildet VGI ein Gegenstück zur kommerziell erworbenen Datengewinnung. Plattformen, wie OSM, beinhalten mittlerweile sehr viel Inhalt. OSM bildet Geodaten sehr detailliert ab und kann potentiell eine große Lücke in einem harmonisierten Welt Datensatz schließen. GoogleMaps dagegen nutzt kommerzielle Daten.

Eine der Technologien, die VGI erst so möglich gemacht haben ist das Web 2.0. Hiermit wurde es populär, dass Nutzer Inhalte erstellen, der wiederum von anderen bearbeitet werden kann. Weitere Technologien haben das zusätzlich unterstützt. Diese sind u.a. Geotags, GPS, Grafiken, Breitband. Die Technologien haben die Entwicklung verschiedener Konzepte ermöglicht, welche die „Rohdaten“ sammeln und weiterverarbeiten. Ein entscheidendes Problem von VGI ist, dass die Metadaten oft unvollständig oder nicht korrekt erfasst werden. Dieser Umstand erschwert die Qualitätsbewertung/-abschätzung der resultierenden Ergebnisse bzw. Erhebungen. Es stellt sich damit die Frage, warum User überhaupt VGI betreiben.

Erklärungen könnten sein (siehe auch 1.2 „Stand der Forschung“):

1. „self-promotion“/ Selbstdarstellung
2. Inhalte mit Freunden zu teilen, dann aber auch gleichzeitig mit dem ganzen Internet.
3. bei OSM beispielsweise persönliche Zufriedenheit, wenn eine Karte immer vollständiger wird.

VGI wird manchmal als „behaftete Informationen“ beschrieben, da sie teils keine Quellenangaben haben und jeder sie bearbeiten kann. Eventuell können sogar mit Absicht Fehler eingearbeitet werden. Vor allem die absichtlichen Fehler sind Aspekte, die bei der Arbeit mit VGI immer beachtet werden müssen. Ein weiteres Problem ist, dass es regional immer noch große Unterschiede in der digitalen Infrastruktur gibt. Daher gibt es Gebiete, die aufgrund mangelnder Anbindung unterrepräsentiert sind. Allgemein lässt sich auch festhalten, dass sprachliche Barrieren Erhebungen eingrenzen können.

3.5 Verantwortlichkeiten

Bevor Verantwortlichkeiten allen Beteiligten zugeordnet werden können, müssen die Rollen klar definiert werden. Das muss aus Sicht des Ganzen geschehen. Einen sehr guten Einstieg hierzu geben die Grundschutzdokumente des BSI. Für einen besseren Überblick soll die folgende Abbildung der Stakeholder dienen.



Abbildung 10: Interne BKG-Stakeholder

Die Rollen und Aufgaben der Stakeholder aus Abbildung 10 können folgend festgelegt werden und entsprechen den Grundschutzdokumenten des BSI.

Initiator (Präsident): Der Präsident ist kein unmittelbarer Funktionär in der Bereitstellung einer Erfassungsplattform von Geodaten. Er ist der Initiator, verfolgt strategische Ziele und ist damit also der Vorantreiber.

Verantwortlichkeit: In Bezug auf dieses Fachverfahren keine.

Fachverfahrensverantwortliche: Fachverfahrensverantwortliche Personen spielen eine wesentliche und zentrale Rolle. Auch der IT-Grundschutz dokumentiert das. Sogenannte Fachverantwortliche sind für Geschäftsprozesse zuständig. Sie kennen die Abhängigkeiten und die Komplexität innerhalb ihres Prozesses, der sich jedoch von dem IT-Betrieb abgrenzt. Fachverantwortliche sind für ihre Verfahren die Organisatoren und stellen das Bindeglied zwischen Endanwendern und der IT-Abteilung her. Sie

erstellen gemeinsam mit dem ISB ein Sicherheitskonzept und arbeiten dem DSB in Datenschutzfragen zu. Technisch gesehen muss ein Fachverfahrensverantwortlicher ein notwendiges Grundverständnis der IT haben und bei einem möglichen IT-Stillstand die richtigen IT-Administratoren kontaktieren. Nach obligatorischen Software-Updates muss der Fachverantwortliche sein Verfahren testen und im besten Fall „grünes Licht“ geben. Die Dokumente des BSI sind von allgemeiner Natur. In der Welt der Geoinformation muss man die Rollen klarer definieren, als in einer Verwaltungsorganisation. Bezogen auf die Geoinformation sind Fachverantwortliche Personen näher an eine IT-Abteilung gekoppelt. Ein Beispiel dazu sind Geodatenbanken. Die Administration, Installationen und Backups der Geodatenbanken und deren Betriebssysteme umfassen Aufgaben einer IT-Abteilung. Die Modelle und Strukturen, wie die Geodaten gespeichert werden sollen, sind wiederum Aufgaben eines Fachverantwortlichen, der die Geschäftsmodelle und Ideen umsetzt. Also das „Customizing“. Hiermit verbunden sind Fragen wie, „Wie können Daten erfasst werden und wie kann ich die erfassten Daten weiternutzen?“. Die Sicht, wie eine IT-Infrastruktur sicher ist und auf welchen Säulen sie steht, ist weniger wichtig. Als Fachverfahrensverantwortliche bezeichnet man also Personen, die sich mit einem Thema und Prozessen auseinandersetzen, um eine Thematik in ihrem Bereich zu lösen und generell zur Verfügung stellen. In einer Welt der digitalen Informationstechnologie beschäftigen sich solche Personen eher mit Dingen, wie eine Anwendung aussehen könnte und ob Nutzer damit umgehen können. Wichtige Fragen wie, „Hat meine Anwendung ein Nachhaltigkeitsziel?“ und „Wie sieht mein Workflow aus?“ beschäftigen einen Fachverfahrensverantwortlichen.

Als Koordinator für sein Fachverfahren hält der Verantwortliche Kontakte zu ISB, DSB, IT-Abteilung und zu den Anwendern. Genau mit diesem Thema hat sich auch das BSI befasst. Abbildung 11 ist dem IT-Grundschutz nachempfunden und steht in dem Dokument „BSI-Standard 200-2 IT-Grundschutz-Methodik“ (Bundesamt für Sicherheit in der Informationstechnik, 2017b).

Verantwortlichkeit: In Bezug auf dieses Fachverfahren leitet und koordiniert der Fachverfahrensverantwortliche. Er hält alle Stricke zusammen, so dass die Erfassungskomponente reibungslos als SaaS läuft. Außerdem kann er Erhebungen gestalten und Endanwendern zur Verfügung stellen.

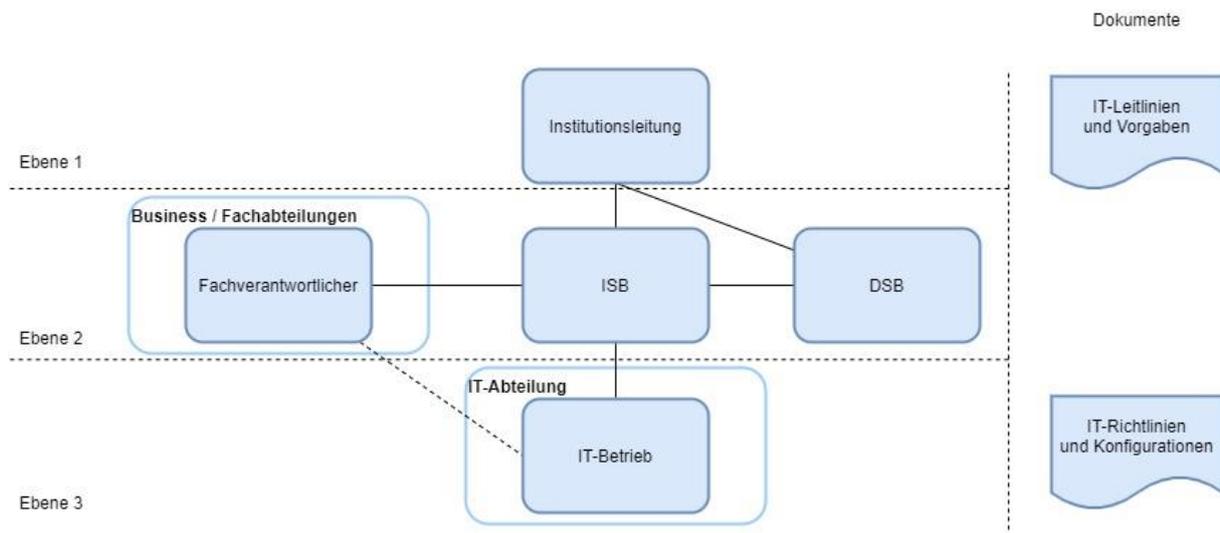


Abbildung 11: Aufbau der Organisation (nach: BSI-IT-Grundschutz)

ISB: Die Rolle und die Aufgaben des ISB sind in den IT-Grundschutzdokumenten klar definiert. So steht in der Veröffentlichung des BSI (Bundesamt für Sicherheit in der Informationstechnik, 2017b): „Der ISB ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Institution“. Das bedeutet, dass der ISB die Bereitstellung dieser Erfassungskomponente mitzusteuern hat. Dies beinhaltet auch die Koordinierung zur Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts, anderer Teilkonzepte und System-Sicherheitsrichtlinien. Alle Sicherheitsmaßnahmen muss er initiieren und überprüfen, um der Leitungsebene einen Bericht zu erstellen. Eine Freigabe dieser Kollaborationsplattform kann nur durch den ISB erfolgen.

Verantwortlichkeit: In Bezug auf dieses Fachverfahren kommuniziert, kontrolliert, berät und unterstützt er zu den Sicherheitsanforderungen, die sich aus dem IT-Grundschutz ergeben. Er gibt schlussendlich ein Sicherheitskonzept frei und wacht über sein ISMS.

DSB: Der DSB hat eine etwas untergeordnete Rolle, die jedoch nicht unwichtiger als die des ISB ist. Denn auch aus Datenschutzgründen muss die geplante Anwendung freigegeben werden. Die Rolle des DSB wird ebenfalls in den Dokumenten des BSI allgemein festgehalten. Hier steht unter anderem: „Er ist an datenschutzrelevanten Vorgängen zu beteiligen und Planungen, die den Umgang mit personenbezogenen Daten betreffen, sind ihm bekannt zu geben. Bei Bedarf muss er von anderen Mitarbeitern mit weitergehenden rechtlichen oder technischen Kenntnissen unterstützt werden.“

Verantwortlichkeit: Bezogen auf dieses neue Fachverfahren kommuniziert, kontrolliert, berät und unterstützt er zu den Datenschutzanforderungen. Er gibt schlussendlich ein Datenschutzkonzept frei.

IT-Abteilung: Zentrale Aufgabe in der Bereitstellung der Komponenten ist die IT-Abteilung. Schlussendlich muss diese die geforderte Komponente zur Verfügung stellen. Inhaltlich und fachlich ist es keine Aufgabe der IT-Abteilung. Ihre Aufgabe besteht darin, dass die Systeme zur Verfügung stehen und genutzt werden können. Basierend auf einem Konzept der Fachverfahrensverantwortlichen, der Freigabe des ISB und des DSB setzt die IT-Abteilung die geforderte Umgebung um. Gemäß Grundschutzdokumenten des BSI und weiteren Richtlinien des ISB stellt die IT-Abteilung den IT-Betrieb sicher und muss die Erfassungskomponente als Software-as-a-Service (SaaS) zur Verfügung stellen.

Verantwortlichkeit: Die IT-Abteilung installiert alle notwendigen IT-Systeme und achtet dabei auf die Richtlinien des ISB. Schlussendlich sorgt die IT-Abteilung für den IT-Betrieb, stellt diesen sicher und übergibt die fertige Erfassungskomponente dem Fachverfahrensverantwortlichen.

Auftraggeber: Wer ist in dem Zusammenhang einer Erfassungskomponente der Auftraggeber? Als Auftraggeber kann man den Präsidenten oder die IT-Abteilung sehen. Aber auch den Fachverfahrensverantwortlichen. In dem Fall der betrachteten Erfassungskomponenten ist der Auftraggeber derjenige, der Erhebungen dem Endanwender zur Verfügung stellt. Grundsätzlich können das zwar auch der Fachverantwortliche sein, aber auch andere Auftraggeber bzw. jede beliebige Person. Ein Beispiel: Ein Auftraggeber nimmt Kontakt mit dem Fachverantwortlichen auf, da er zum Beispiel eine Erhebung veröffentlichen möchte, mit der Bäume aufgenommen werden sollen. Da der Auftraggeber vom Fach ist, weiß er genau, welche Bäume erfasst werden sollen. Der Fachverantwortliche räumt dem Auftraggeber hiermit entsprechende Rechte ein, so dass dieser seine Erfassung selbstständig aufbauen und veröffentlichen kann. Hiermit ist der Auftraggeber in der Lage „Herr“ über die erfassten Daten seiner Community zu sein. Als Geodatendienstleister der Bundesverwaltung können Auftraggeber lediglich Personen der öffentlichen Bundesverwaltung sein. Auftraggeber können aber auch andere angestellte Personen des BKG sein.

Verantwortlichkeit: Nutzt die ihm freigestellte Infrastruktur als SaaS und kann einer Community Erhebungen zur Verfügung stellen.

Endanwender/Sammler: Endanwender spielen keine aktive Rolle. Ihre Erwartungshaltung ist eher, dass etwas bereitgestellt wird, mit dem diese möglichst einfach und praktisch Geodaten erfassen können.

Verantwortlichkeit: In Bezug auf dieses Fachverfahren keine. Er ist lediglich der Erfasser von Geodaten und nutzt die Kollaborationsplattform.

3.6 Qualitätssicherung eines VGI-Systems

Eine große Herausforderung stellt die Übernahme erfasster Daten und deren Qualität dar. Nicht nur die Qualität der erfassten Daten muss hier betrachtet werden. Die Qualität umfasst vielmehr und muss als ein Ganzes gesehen werden. Aus der Sicht der Geoinformation werden diesbezüglich stets die Qualitätsanforderungen nach der ISO 19000er-Reihe betrachtet. Diese ISO-Standards beschreiben Normen der Geoinformation. Also, wie können Geodaten standardisiert bereitgestellt und beschrieben werden. In Bezug auf die Prinzipien der Qualität stellt die Standardisierung ein Dokument aus dem Jahr 2013 bereit „Geographic information — Data quality (ISO 19157:2013)“ (ISO/TC 211 Geographic information/Geomatics. (2013)). Dieser Standard ist somit 10 Jahre alt. Andere Qualitätsstandards der ISO, die auf diesen verweisen, sind noch älter. Dennoch geben diese „veralteten“ Standards den Stand der Geoinformation wider. Wenig betrachtet wird in diesen Standards die allgemeine IT-Infrastruktur. In der Vergangenheit wurden diesbezüglich fast keine Bemühungen unternommen, zwei Sichtweisen in einen Einklang zu bringen. Die Sicht der Geoinformation und der allgemeinen IT. Im Gegenteil! Jeder hatte seine eigene Agenda. In Anbetracht, der in 2.3 Technische Anforderungen (Sicherheitsaspekte)“ erwähnten Sicherheitsthemen, müssen unterschiedliche Qualitätsaspekte betrachtet werden. Sliwinski und Koch (Bernard/Fitzke/Wagner, 2004) haben die Qualitätsdimensionen von Shapiro, Varian (Shapiro & Varian, 1999) und Grönroos (Grönroos, 1993) in funktionale und technische Qualitätsdimensionen eingegliedert (siehe Abbildung 12). Jedoch stammen diese Qualitätsdimensionen aus noch früheren Zeiten und geben lediglich einen Überblick aus Sicht der Geoinformation. Der Grundgedanke die Dimensionen in fachliche und technische Qualitätsdimensionen einzustufen scheint richtig. Heute muss der „Blick“ aber tiefer gehen. Die technischen Qualitätsdimensionen sollten weiter untergliedert werden. Wie in 2.3 Technische Anforderungen (Sicherheitsaspekte) beschrieben benötigt es noch die Sicht der Bereitstellung durch einen IT-Betrieb.

Tabelle 29.1: Qualitätsdimensionen von SHAPIRO & VARIAN (1998, 1999) eingeordnet in die Qualitätstypologie nach GRÖNROOS (1984)

Qualitätsdimension	Ausprägung	
Annehmlichkeit	Einschränkung der Zugangsperioden, -dauer oder -form zu den Informationen	Funktionale Qualitätsdimensionen
Flexibilität der Nutzbarkeit	Einschränkung der Möglichkeiten, die Informationen zu speichern, zu vervielfältigen, zu drucken oder anderweitig zu übertragen	
Anwendergemeinschaft	Bereitstellung von Informationsanwendungen, die es ermöglichen, Informationen innerhalb einer Anwendergemeinschaft auszutauschen	
Belästigung	Freischaltung von Informationsanwendungen mit Werbeblendungen	
Schnelligkeit	Einschränkung der Zugangsgeschwindigkeit zu Informationen	
Kundenservice	Angebot unterschiedlicher Kundenserviceleistungen und unterschiedlicher Zugangsmodi	
Vollständigkeit	Einschränkung des Generalisierungsgrades von Informationen (Detaildarstellung / Übersichtsdarstellung), ihres geographischen oder thematischen Umfangs sowie ihrer Aktualität	Technische Qualitätsdimensionen
Datenprozessierung / Funktionalität	Einschränkung der angebotenen Anwendungsfunktionalitäten, die eine Nutzung von Automatisierungen, Manipulationen und spezialisierter Prozessierungsfunktionalitäten unterbinden	
Nutzerschnittstelle	Einschränkung der graphischen Nutzerschnittstelle und der Anwenderinteraktion	
Bildaufflösung	Einschränkung der Bildauflösung von rasterbasierten Informationen	

Abbildung 12: Qualitätsaspekte (Bernard/Fitzke/Wagner, 2004)

Hiermit wurden technische und funktionale Qualitätsanforderungen einmalig festgehalten. Die technische Qualität umfasst nach Bernard/Fitzke/Wagner das, was ein Endanwender erhält. Während die funktionale Qualität dem entspricht, wie der Endanwender die Information erhält. Dieser Ansatz scheint gut, jedoch sehr allgemein und auch veraltet. Zum heutigen Stand reicht dies nicht aus. Der Grundgedanke gibt jedoch einen guten Anhaltspunkt.

Heute wird expliziter zwischen Qualitäten von Softwareentwicklung und -bereitstellung unterschieden. Hinzu kommt der Punkt der Qualität der Daten. Es müssen drei Qualitätsanforderungen untersucht werden.

1. Qualität der Software

Das BSI hat weitreichende Anforderungen an Software. In dem Dokument „CON.8: Software-Entwicklung“, (CON.8: Software-Entwicklung, 2021) stehen klare Richtlinien, woran sich Entwickler bzw. Softwareprodukte zu halten haben. Die Zielsetzung dieses Dokuments ist zwar auf Eigenentwicklungen ausgerichtet, muss aber auch beim Einsatz von Software anderer angewendet werden. Ehemals bezogen sich die BSI-Dokumente auf einen ISO-Standard, der in den aktuellen

Dokumenten keine weitere Erwähnung findet. Genannt sei hier der ISO 9126. Dieser Standard ist von der Standardisierungskommission mittlerweile durch andere abstrakte Standardisierungen aktualisiert worden. Dennoch kann dieser Standard allgemein herangezogen werden, da er in Neuerungen überführt wurde. Der grundsätzliche und noch verständliche Ansatz zeigt Abbildung 13.

Qualitätsmerkmale von Softwaresystemen (ISO 9126)

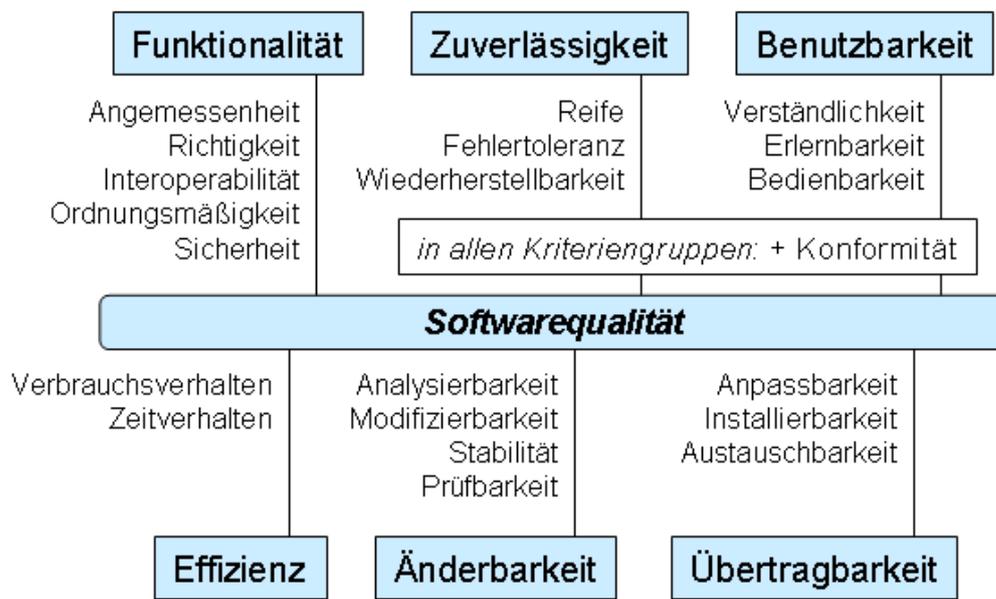


Abbildung 13: Softwarequalitätsmerkmale (nach ISO 9126)

Aus Abbildung 13 werden folgende Qualitätsmerkmale für Software als Produkt nach ISO 9126 (ISO/IEC JTC 1/SC 7 Software and systems engineering. (2001)) aufgeführt:

Änderbarkeit/Wartbarkeit: Welchen Aufwand erfordert die Durchführung vorgegebener Änderungen an der Software? Aufwand, der zur Durchführung vorgegebener Änderungen notwendig ist. Änderungen können Korrekturen, Verbesserungen oder Anpassungen an Änderungen der Umgebung, der Anforderungen oder der funktionalen Spezifikationen einschließen.

- *Analysierbarkeit:* Aufwand, um Mängel oder Ursachen von Versagen zu diagnostizieren oder um änderungsbedürftige Teile zu bestimmen.
- *Konformität:* Grad, in dem die Software Normen oder Vereinbarungen zur Änderbarkeit erfüllt.
- *Modifizierbarkeit:* Aufwand zur Ausführung von Verbesserungen, zur Fehlerbeseitigung oder Anpassung an Umgebungsänderungen.
- *Stabilität:* Wahrscheinlichkeit des Auftretens unerwarteter Wirkungen von Änderungen.
- *Testbarkeit:* Aufwand, der zur Prüfung der geänderten Software notwendig ist.

Gebrauchstauglichkeit (Produkt)/Benutzbarkeit: Welchen Aufwand fordert der Einsatz der Software von den Benutzern und wie wird er von diesen beurteilt? Aufwand, der zur Benutzung erforderlich ist, und individuelle Beurteilung der Benutzung durch eine festgelegte oder vorausgesetzte Benutzergruppe (Software-Ergonomie).

- *Attraktivität:* Anziehungskraft der Anwendung gegenüber dem Benutzer.
- *Benutzerfreundlichkeit/Bedienbarkeit:* Aufwand für den Benutzer, die Anwendung zu bedienen.
- *Erlernbarkeit:* Aufwand für den Benutzer, die Anwendung zu erlernen (zum Beispiel Bedienung, Ein-, Ausgabe).
- *Konformität:* Grad, in dem die Software Normen oder Vereinbarungen zur Benutzbarkeit erfüllt.
- *Verständlichkeit:* Aufwand für den Benutzer, das Konzept und die Anwendung zu verstehen.

Effizienz (Informatik): Wie ist das Verhältnis zwischen Leistungsniveau der Software und eingesetzten Betriebsmitteln? Verhältnis zwischen dem Leistungsniveau der Software und dem Umfang der eingesetzten Betriebsmittel unter festgelegten Bedingungen.

- *Konformität:* Grad, in dem die Software Normen oder Vereinbarungen zur Effizienz erfüllt.
- *Leistung:* Antwort- und Verarbeitungszeiten sowie Durchsatz bei der Funktionsausführung.
- *Komplexität:* Anzahl und Dauer der benötigten Betriebsmittel bei der Erfüllung der Funktionen. Ressourcenverbrauch, wie CPU-Zeit, Festplattenzugriffe usw.

Funktionalität: Inwieweit besitzt die Software die geforderten Funktionen? Vorhandensein von Funktionen mit festgelegten Eigenschaften. Diese Funktionen erfüllen die definierten Anforderungen.

- *Angemessenheit:* Eignung von Funktionen für spezifizierte Aufgaben, zum Beispiel aufgabenorientierte Zusammensetzung von Funktionen aus Teilfunktionen.
- *Informationssicherheit:* Fähigkeit, unberechtigten Zugriff, sowohl versehentlich als auch vorsätzlich, auf Programme und Daten zu verhindern.
- *Interoperabilität:* Fähigkeit, mit vorgegebenen Systemen zusammenzuwirken.
- *Konformität:* Fähigkeit des Softwareprodukts, Standards, Konventionen oder gesetzliche Bestimmungen und ähnliche Vorschriften bezogen auf die Funktionalität einzuhalten.
- *Ordnungsmäßigkeit:* Merkmale von Software, die bewirken, dass die Software anwendungsspezifische Normen oder Vereinbarungen oder gesetzliche Bestimmungen und ähnliche Vorschriften erfüllt.

- *Richtigkeit*: Liefern der richtigen oder vereinbarten Ergebnisse oder Wirkungen, zum Beispiel die benötigte Genauigkeit von berechneten Werten.

Plattformunabhängigkeit / Übertragbarkeit: Wie leicht lässt sich die Software in eine andere Umgebung übertragen? Eignung der Software, von der Umgebung in eine andere übertragen werden zu können. Umgebung kann organisatorische Umgebung, Hardware- oder Software-Umgebung sein.

- *Anpassbarkeit*: Fähigkeit der Software, diese an verschiedene Umgebungen anzupassen.
- *Austauschbarkeit*: Möglichkeit, diese Software anstelle einer spezifizierten anderen in der Umgebung jener Software zu verwenden, sowie der dafür notwendige Aufwand.
- *Installierbarkeit*: Aufwand, der zum Installieren der Software in einer festgelegten Umgebung notwendig ist.
- *Koexistenz*: Fähigkeit der Software neben einer anderen mit ähnlichen oder gleichen Funktionen zu arbeiten.
- *Konformität*: Grad, in dem die Software Normen oder Vereinbarungen zur Übertragbarkeit erfüllt.

Zuverlässigkeit: Kann die Software ein bestimmtes Leistungsniveau unter bestimmten Bedingungen über einen bestimmten Zeitraum aufrechterhalten? Fähigkeit der Software, ihr Leistungsniveau unter festgelegten Bedingungen über einen festgelegten Zeitraum zu bewahren.

- *Fehlertoleranz*: Fähigkeit, ein spezifiziertes Leistungsniveau bei Software-Fehlern oder Nicht-Einhaltung ihrer spezifizierten Schnittstelle zu bewahren.
- *Konformität*: Grad, in dem die Software Normen oder Vereinbarungen zur Zuverlässigkeit erfüllt.
- *Reife*: Geringe Versagenshäufigkeit durch Fehlerzustände.
- *Wiederherstellbarkeit*: Fähigkeit, bei einem Versagen das Leistungsniveau wiederherzustellen und die direkt betroffenen Daten wiederzugewinnen. Zu berücksichtigen sind die dafür benötigte Zeit und der benötigte Aufwand.

Können sich die Hersteller der Erfassungskomponenten hieran halten? Eine detaillierte Prüfung der Komponenten kann in dieser Arbeit nicht durchgeführt werden, da hierfür der Rahmen einer Masterarbeit nicht ausreicht. Ob die Software nach den Richtlinien entwickelt wurde, kann lediglich anhand einer expliziten Nachfrage bei den Herstellern erfolgen.

2. Qualität der Bereitstellung

Zur Qualität der Bereitstellung durch den IT-Betrieb geben die Anhaltspunkte aus 2.3 Technische Anforderungen (Sicherheitsaspekte) die notwendigen Informationen und Regularien.

3. Qualität der Daten

Wie könnte die Qualität der Daten und der Endnutzer bewertet werden? Dies stellt eine zentrale Frage dar, die in Zusammenhang mit den zuvor genannten Punkten einhergeht. In dem 4.3 „Qualitätssicherungsmaßnahmen“ soll diese Frage generell geklärt werden.

3.7 Teilnahme und Motivationsgründe der Erfasser

Anders als erwartet, muss dieser Punkt allgemein und auf bisher wissenschaftlichen Veröffentlichungen betrachtet werden. Goodchild & Li (2012) haben wesentliche Punkte dargestellt. So haben sie drei Ansätze zur Qualitätssicherung und zu Motivationsgründen von VGI ermittelt.

1. Crowd-Sourcing-Approach: Qualitätssicherung aufgrund Crowd-Sourcing. Sprich, die Motivation ist das Konzept und ich helfe um einen guten Datensatz zu erzeugen, bin aber kein Experte.
2. Social-Approach: Qualitätssicherung durch Hierarchie-Systeme. Sprich, ich habe das Interesse einem sozialen Faktor beizutragen, um eventuell Katastrophen entgegenzuwirken und bin eventuell Experte.
3. Geographic-Approach: Qualitätssicherung durch geografische Regeln (Abhängigkeiten, Zusammenhänge) dies bleibt jedoch weiterhin schwierig. Sprich, ich bin ein Experte und möchte allen Regeln der Geographie entsprechen.

Ein entscheidendes Problem von VGI ist, dass die Metadaten oft gar nicht, nicht vollständig oder inkorrekt erfasst werden. Dieser Umstand erschwert die Qualitätsbewertung der daraus resultierenden Daten. VGI wird manchmal als „behauptete Infos“ beschrieben, da sie teils keine Quellenangaben haben und sie jeder bearbeiten bzw. sogar mit Absicht Fehler einbauen kann. Dies sollte bei der Arbeit mit VGI immer mit beachtet werden.

3.8 Resultat

Resultierend aus diesem Kapitel soll sich die Forschungsfrage beantworten lassen, um diese abzusichern. Insbesondere liefern diese Erkenntnisse zu den untersuchenden Anwendungsfällen (siehe 1.4 „Strategie zur geplanten Umsetzung“) und damit eine quantitative und qualitative Bewertung. Im Vordergrund sollen hier die Erfassungssysteme und deren Methoden stehen. Vor allem ist folgend zu klären, mit welcher Qualität und Güte diese bereitgestellt und erfassen können. Einhergehend ist hier auch der Datenschutz zu untersuchen. Einen Unterschied zur Erfassung von Geodaten ist im ersten Moment nicht erkennbar. Wo genau liegen jedoch die Unterschiede? Dies soll im folgenden Kapitel genauer erläutert werden.

4 Ergebnisse und Diskussion

Fokus der Ergebnisse liegt in einer nachhaltigen Bewertung der verwendeten Softwaresysteme, sowie die dazugehörigen Prozesse zur Übernahme erfassten Daten mit einer Qualitätssicherung. Besonders beachtet wurden hierbei die Anforderungen nach BSI für die Bereitstellung solcher Systeme und außerdem die Standards, die für Datenerfassungen allgemein gelten. Daher werden die Ergebnisse in einer Mischung von unterschiedlichen Bewertungsstilen beantwortet.

4.1 Bewertung der VGI-Software

Bewertung der IT zu Survey123

Der IT-Grundschutz gibt eine hohe Messlatte an Anforderungen vor. Mit einer durchgeplanten Infrastruktur nach ESRI, können diese Forderungen umgesetzt werden. Das modulare System nach den Beschreibungen von ESRI gibt es her. Die Umgebung eines Enterprise-GIS setzt auf den „Named User“-bezogenen Ansatz. Unter anderem wird dies von der IT-Sicherheit und dem Schutzbedarf gefordert. Lediglich authentifizierte Anwender können die Angebote nutzen. Einer großen Palette von nicht authentifizierten Anwendern kann das Angebot ebenfalls zur Verfügung gestellt werden. Wobei sich hier die größte Vielfalt und zugleich Sicherheitslücke ergibt. Der Aufbau einer multiplen Server-Infrastruktur scheint gegeben zu sein, was wiederum für eine höhere Sicherheit spricht. Da das BKG bereits eine hochverfügbare Enterprise-GIS-Umgebung zur Verfügung stellt, wäre die zusätzliche Bereitstellung von Survey123 eine Ergänzung und würde sich insgesamt in die Infrastruktur einpassen. Größtes Manko ist, das mögliche Hochladen gefährdender Daten. Hierunter fallen vor allem Bild-, Video- und Audiodateien. Wie sieht es mit einem SQL-Injection aus? Es ist davon auszugehen, dass diese Sicherheitslücken technisch umgesetzt und damit unterbunden wurden. Eine weitere Frage beschäftigt sich mit der Containerisierung, um eine sichere und dynamische Plattform bereitzustellen. Können die Systeme von ESRI containerisiert werden? Und was sagt der IT-Grundschutz des BSI zu Containerisierungen? ESRI empfiehlt auf seinen Internetseiten eine Containerisierung mittels Kubernetes (*Einführung in ArcGIS Enterprise on Kubernetes—ArcGIS Enterprise on Kubernetes / Dokumentation, 2023*). Ist diese Containerisierung jedoch auch IT-Grundschutzkonform? Das BSI hat die unterschiedlichen Umgebungen von Containerisierungen erkannt und stellt zur allgemeinen Thematik eine Empfehlung zur Verfügung (Bundesamt für Sicherheit in der Informationstechnik, 2022c). Über eine Bereitstellung von IT-Systemen mittels Kubernetes geht das BSI sogar noch weiter. Siehe hierzu (Bundesamt für Sicherheit in der Informationstechnik, 2022b). Unter anderem wird hier beschrieben, dass eine Orchestrierung von Systemen mittels Kubernetes ein „Quasi-Standard“ ist. Mit der Orchestrierung ist das Bereitstellen einer Anwendung bezeichnet, die eine Zusammenstellung mehrerer Programme bedeutet und die gemeinsam eine Aufgabe erfüllen. In dieser Umgebung sind

mehrere einzelne Container miteinander, und nur für sich, verbunden und bilden damit ein gesamtes IT-System. Größte Sicherheitslücke bildet dabei eine mangelnde Authentisierung und Autorisierung zwischen den einzelnen Containern. Verbunden ist damit der Verlust eventueller, vertraulicher Daten und somit auch aller Daten, die innerhalb einer solchen Umgebung existieren.

Was ist zusätzlich zu beachten, wenn man die Abgrenzungen aus dem 2.4 Abgrenzungen betrachtet? Hier geht es um „Erfassung von situativen Ereignissen“, „Erfassung von Korrekturen von Bestandsprodukten“ und „Erfassung neuer Objektarten für Bestandsprodukte“ mit unterschiedlichen User-Konzepten. Bezogen auf diese Anwendungsfälle ist ein freier Zugang lediglich für die Erfassung von Korrekturen angedacht. Anwender/User müssen damit nicht registriert sein. Bei den anderen beiden Anwendungsfällen müssen User registriert sein. Ein registrierter Anwender, der aktiv an der ESRI-Umgebung angemeldet ist, nutzt gleichzeitig eine Lizenz. Eine genutzte Lizenz bedeutet gleichzeitig auch Kosten. Sofern nur einzelne (wenige) die Plattform bzw. Anwendung nutzen, sollte das keine Rolle spielen. Wie sieht es jedoch aus, wenn Adhoc viele Anwender zeitgleich auf die Plattform bzw. Anwendung zugreifen? Das stellt ein großes Lizenzierungsproblem dar, da eine Anzahl der Lizenzen endlich ist. Grundsätzlich stellt sich hiermit das Problem, dass eine Anzahl von Lizenzen nicht planbar, bzw. kalkulierbar, ist. Nutzen kann man auch eine ESRI-Authentifizierung, diese obliegt jedoch jedem einzelnen und den Datenschutzrichtlinien der Vereinigten Staaten. Ebenfalls eine Lokalisierung innerhalb einer Kartenanwendung problematisch, da eine vorgegebene Ortssuche über Online-Dienste von ESRI bereitgestellt wird. Diese leitet Anfragen an Server außerhalb der EU weiter und kann von weiteren dritten verarbeitet werden. Diese Informationen sind in den ESRI-eigenen Datenschutzinformationen enthalten (<https://trust.arcgis.com/de/privacy/privacy-tab-intro.htm>). Gerade den Passus „Esri erfasst personenbezogene Daten in minimalem Umfang, um Kunden die Nutzung von ArcGIS Online zu ermöglichen“ kritisieren die europäischen Datenschützer.

Bewertung der IT zu KoboToolbox

Bezogen auf die Anforderungen des IT-Grundschutzes kann nach der Abbildung 8 folgende Annahme getroffen werden. Sofern eine vollständige Composable Containerisierung umgesetzt wird, befindet sich jede einzelne Gesamtsystemkomponente in einem eigenen Docker-Container. Dies würde dann dem Prinzip des IT-Grundschutz entsprechen. Also ein Container, bzw. Server, für eine Aufgabe. Diese Annahme muss gegengeprüft werden. Auch das Prinzip des registrierten „Named-User“ scheint gegeben, muss jedoch geprüft werden. Allgemein scheint, dass sich dieses Konzept nicht nahtlos in die bestehende ESRI-Umgebung integrieren lässt. Ob das jedoch zwingend erforderlich ist, wird in diesem Kapitel noch geprüft. Nach wie vor ist das größte Problem das mögliche Hochladen gefährdender Daten. Wie bereits erwähnt, sind diese vor allem Bild-, Video- und Audiodateien. Auch SQL-Injection

muss geprüft werden. Und was sagt der IT-Grundschutz des BSI zu Containerisierungen mittels Docker? Entgegen Kubernetes, wird ein explizites Dokument zu Docker von dem BSI nicht zur Verfügung gestellt. In dem allgemeinen Dokument (Bundesamt für Sicherheit in der Informationstechnik, 2022c) steht ein wichtiger Teil. Hier heißt es:

„Mindestens die folgenden Zugangsdaten MÜSSEN sicher gespeichert werden: Passwörter jeglicher Accounts, API-Keys für von der Anwendung genutzte Dienste, Schlüssel für symmetrische Verschlüsselungen sowie private Schlüssel bei Public-Key-Authentisierung.“

Diese Punkte hat KoboToolbox auf ihrer Internetseite definiert. Somit ist davon auszugehen, dass KoboToolbox in diesem Bereich IT-Grundschutzkonform ist. Der BSI-Standard gibt zu Docker-Containerisierungen folgende unterstützende Links zur Prüfung von Docker-Containern.

1. CIS Benchmark Docker <https://www.cisecurity.org/benchmark/docker/>
2. SANS Checkliste <https://www.sans.org/reading-room/whitepapers/auditing/checklist-audit-dockercontainers-37437>
3. Docker Security Guide <https://docs.docker.com/engine/security/>

In dem Kapitel 2.4 „Abgrenzungen“ sind drei Bereiche der Erfassungen genannt: „Erfassung von situativen Ereignissen“, „Erfassung von Korrekturen von Bestandsprodukten“ und „Erfassung neuer Objektarten für Bestandsprodukte“. Ein freier Zugang zu der Anwendung ist grundsätzlich angedacht. Die Problematik der Anzahl von Lizenzen besteht bei KoboToolbox generell nicht, da der gesamte Bereich als Open-Source-Software umgesetzt ist. Lizenzrechtliche Probleme würden hier entgegenstehen.

Einen ganz wichtigen Hinweis zum Thema Datenschutz gibt KoboToolbox auf seiner Internetseite bekannt. Dort steht ins Deutsche übersetzt: „Wir halten uns vollständig an die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union.“. Mit dieser Aussage ist KoboToolbox dem Hersteller ESRI weit voraus.

Damit KoboToolbox genauer bewertet werden kann, wurde die Open-Source-Software exemplarisch auf einem virtuellen Server installiert. Das Serverbetriebssystem war Ubuntu 22.04.2 LTS mit der aktuellsten Docker und Docker Compose Version. KoboToolbox lässt sich mit dieser Basis relativ einfach installieren. Dokumentiert sind alle Schritte unter <https://github.com/kobotoolbox/kobo-install>. Während der Installation wird man durch einzelne Schritte per Kommandozeile geführt (siehe Anhang 1). Anhand dieser lokalen Installation konnte keine Überprüfung anderer Geräte im gleichen Netzwerk überprüft werden, da die Installationsroutine nur einen Echt- oder Testbetrieb vorsieht. Mit

dem Testbetrieb sind alle Zugriffe von Geräten im gleichen Netzwerk unterbunden. Dies unterstreicht die hohe Sicherheitsstufe von KoboToolbox. Abbildung 14 zeigt die Überprüfung der Container. Alle Container besitzen lediglich einen Port zur internen Kommunikation. Lediglich der Container, der das Gesamtsystem zur Verfügung stellt besitzt zwei Ports, „NGINX:1.21“. Einen für die Kommunikation nach extern und einen für die interne Kommunikation. Eine Kreuzverbindung zu einzelnen Systemen ist damit unterbunden.

```
[sudo] Passwort für user-adm:
CONTAINER ID   IMAGE                                COMMAND                  CREATED    STATUS    PORTS
889081dbdfcc  kobotoolbox/kpi:2.022.24           "/bin/bash -c 'exec ..." 6 months ago Up 3 minutes 8000/tcp
4ecd73136507  kobotoolbox/enketo-express-extra-widgets:3.0.5 "docker-entrypoint.s..." 6 months ago Up 3 minutes 8005/tcp
09ea433a4b9c  kobotoolbox/kobocat:2.022.24      "/bin/bash -c 'exec ..." 6 months ago Up 3 minutes 8000-8001/tcp
0d43cf875e6e  nginx:1.21                          "/docker-entrypoint..." 6 months ago Up 3 minutes 0.0.0.0:80->80/tcp, :::80->80
1e283dcd0703  postgres/postgis:9.5-2.5          "docker-entrypoint.s..." 6 months ago Up 3 minutes 5432/tcp
c727543a775d  mongo:3.4                          "docker-entrypoint.s..." 6 months ago Up 3 minutes 27017/tcp
0a11b5180659  redis:3.2                          "docker-entrypoint.s..." 6 months ago Up 3 minutes 6379/tcp
d056d21dd7d0  redis:3.2                          "docker-entrypoint.s..." 6 months ago Up 3 minutes 6379/tcp
user-adm@useradm-VirtualBox:~$
```

Abbildung 14: Installierte KoboToolbox Container

Auch die Anzahl der Docker-Container ist gleich der Systeme, die in Abbildung 14 zu sehen sind. Anhand dieser Tatsachen lässt sich generell feststellen, dass ein IT-Grundschutz nach den Richtlinien des BSI gewährleistet ist. Im Endeffekt muss jedoch ein ISB darüber entscheiden. Wobei, bei dieser Grundlage eine Gegenargumentation schwierig erscheint. Einzig bleibt jedoch das Thema mit dem Hochladen von Daten offen.

4.1.1 Vergleich der technischen Fähigkeiten

Der erste operative Teilschritt aus 1.3 „Forschungsziel und Gliederung“ wird in diesem Abschnitt beantwortet. Hier dreht es sich gezielt um die technischen Fähigkeiten beider Systeme, die untersucht wurden. Aus den gewonnenen Erkenntnissen werden folgende Fragen zum Vergleich beider Systeme herangezogen, um das nachhaltige Ziel bewerten zu können:

1. Gibt es Unterschiede in der Art und Weise der Bereitstellung?
2. Sind Unterschiede in Lizenzierungen vorhanden?
3. Wie können Erfassungsumfragen erstellt werden und wie ist ein „Customizing“ möglich?
4. Ist der Standard aus Kapitel „Standard der Erfassungskomponenten“ gleichwertig umgesetzt?

Zu Frage 1:

In Kapitel „Standard der Erfassungskomponenten“ wurde festgehalten, dass beide Systeme auf dem gleichen Standard beruhen. Die Art ist damit ident. Lediglich Nuancen der Bereitstellungsweise können identifiziert werden. Die zugrundeliegende IT unterscheiden die Systeme. ESRI Plattformen können auf

Linux- und Windows-Basis bereitgestellt werden. Dies geschieht containerisiert oder gewöhnlich per Setup. KoboToolbox scheint nur anhand von Linux und Docker-Containerisierung möglich zu sein.

Fazit: Diese Frage kann in dieser Form neutral bewertet werden. Insgesamt muss diesen Punkt der ISB und der IT-Betrieb der Organisation festlegen.

Zu Frage 2:

Die Beantwortung dieser Frage erscheint recht einfach. ESRI, als kommerzieller Anbieter verfolgt stets ein Lizenzmodell, dass mit zusätzlichen Kosten verbunden ist. Wenn gleich Erfassungsumfragen frei und für Jedermann zur Verfügung gestellt werden können, muss mindestens derjenige, der Umfragen erstellt, eine Lizenz nutzen. KoboToolbox ist Open-Source-Software und verfolgt den Ansatz mittels beauftragtem „Customizing“ finanzielle Mittel zu erwirtschaften. Diesen Ansatz hat ESRI zusätzlich.

Fazit: Dieser Punkt geht vordergründig an KoboToolbox wegen der transparenten Preisgestaltung, da die Kosten bei ESRI zum derzeitigen Zeitpunkt nicht kalkulierbar wären. Sicherlich kann eine detaillierte Wirtschaftlichkeitsbetrachtung einen genauen Aufschluss geben.

Zu Frage 3:

Grundsätzlich ähneln sich beide Systeme. Anhand eines WYSIWYG-Editors können in beiden Plattformen Erfassungsumfragen erstellt werden. Unterschiede liegen im Detail. ESRI bietet von Haus aus eine sehr komfortable Umgebung an, in der u. a. farblich gestalterische Feinheiten eingestellt werden können. KoboToolbox enthält dagegen nur einen Layout-Style. Dieser Style kann über Umwege jedoch angepasst werden. Ebenso sieht es mit den Karten bei der Lokalisierung aus. ESRI lässt sich einfach verändern, während KoboToolbox ein „Customizing“ nur im Quellcode zulässt. Einen weiteren Unterschied zeigt das Anwenden bzw. das Nutzen der XLSForms. In KoboToolbox lassen sich diese Formulare ganz einfach in dem WYSIWYG-Editor importieren. Dies hat ESRI nicht in dem WYSIWYG-Editor implementiert. Bei ESRI muss man eine zusätzliche Applikation, Survey123 Connect, auf einem Client installieren, um XLSForms interoperabel nutzen zu können.

Fazit: Intuitiv sind beide Systeme. Bezogen auf eine zusätzliche ESRI-Software für den Client fällt eine Entscheidung eher auf KoboToolbox. Diese Entscheidung neutralisiert sich jedoch, aufgrund des „Customizing“ der Karten und der farblichen Gestaltungsmittel.

Zu Frage 4:

Beide Systeme haben die XLSForms aus den Anhängen 2 bis 4 gleichermaßen umgesetzt. Es gab keine Fehler bei dem Importieren und bei der Bereitstellung.

Fazit: Auch diese Frage kann in dieser Form neutral bewertet werden.

4.1.2 Benutzerführung und Usability

Aus der zuvor dargestellten Erhebung wurden zwei Anwendungen erstellt und bereitgestellt. Eine der beiden beinhaltete die explizite Zustimmung der Datenschutzrichtlinien. Sprich, bei einer Nicht-Zustimmung erhielt der Nutzer eine Anzeige, dass eine Zustimmung notwendig ist. Bei der anderen Variante wurden die Datenschutzrichtlinien bei dem Weiterklicken alternativlos akzeptiert. Die erst genannte Variante entsprach einem einzelnen Formular, so dass alle Fragen auf einer Seite dargestellt wurden. Die zweite Variante beinhaltete die gleichen Fragestellungen. Der Unterschied war, dass jede einzelne Frage der Erhebung auf einer einzelnen Seite abgefragt wurde.

Beide Varianten wurden von ausgewählten Mitarbeitenden des BKG getestet, um den zweiten operativen Teilschritt beantworten zu können. Die ausgewählten Mitarbeitenden wurden aus unterschiedlichen Bereichen/Referaten eingeladen. Dieser Zweck diente einer unabhängigen und möglichst nicht abgesprochenen Beurteilung. Eine anschließende Beurteilung wurde ebenfalls mittels KoboToolbox anhand einer weiteren Befragung der Teilnehmenden vollzogen. Die Fragen waren gezielt auf die Usability der Erhebungsalternativen und entsprechend einfach gehalten. Eine zusätzlich unterschiedliche Betrachtung beider Systeme erschien nicht notwendig, da der Ablauf einer formularbasierten Erhebung gleich ist.

Die Befragung enthielt folgende drei Fragen:

1. Welche Version hat besser gefallen?
2. Warum hast du dich für die Version entschieden?
3. Hast du sonst noch Kommentare oder ergänzende Wünsche?

Von 14 Teilnehmenden des BKG ergaben sich folgende Antworten.



Abbildung 15: Frage 1 zur Variante

Die Frage zur Variante ist relativ eindeutig (Abbildung 15). Das „Endlosformular“ (One-Pager) scheint den Teilnehmenden besser zu gefallen. Doch was sagen die nachfolgenden Begründungen? Einzelne Antworten müssen im Kontext dieser ersten Frage gesichtet und bewertet werden. Grundsätzlich finden sich die Antworten auch in der ersten Beantwortung wider (siehe Abbildung 16).

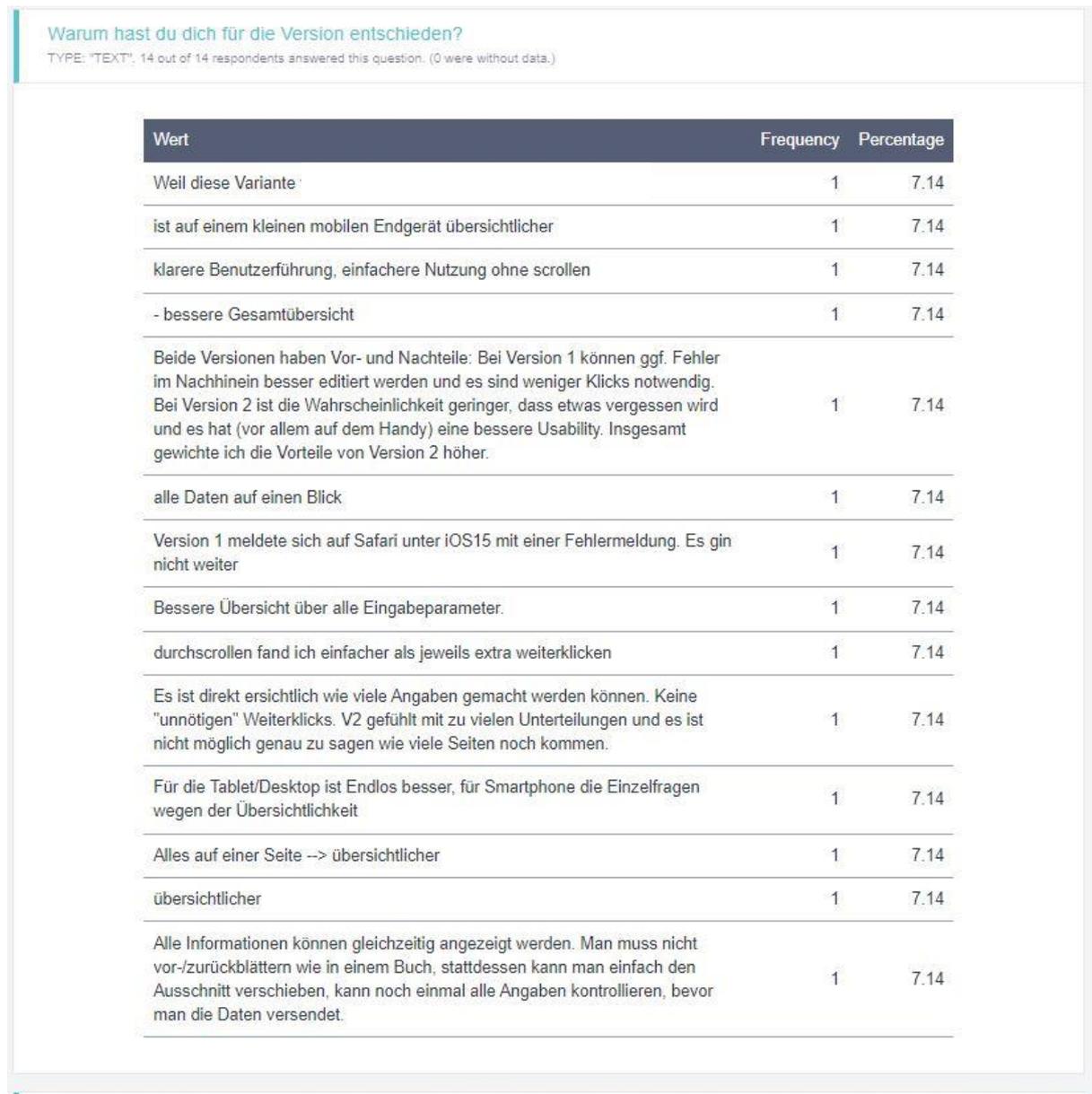


Abbildung 16: Frage 2 zur Variante

Anhand der Erklärungen wird es deutlicher. So kann man allgemein feststellen, dass ein Endlosformular (One-Pager) auf einem Desktop-PC besser geeignet erscheint. Trotz alle dem, gibt es Teilnehmende, die diese Variante allgemein besser empfinden. Zusätzlich gibt aber jedoch wenige, die die Alternative „Eine Frage=eine Seite“ (Multi-Pager) besser empfinden. Ausreißer gibt es einen, der mit seinem Betriebssystem Schwierigkeiten hatte.

Die dritte Frage klärt weitere allgemeine Punkte (siehe Abbildung 17).

Hast du sonst noch Kommentare oder ergänzende Wünsche?
TYPE: "TEXT". 12 out of 14 respondents answered this question. (2 were without data.)

Wert	Frequency	Percentage
Es fehlt noch: Frage x von y und eine Dankeseite	1	7.14
es wäre nützlich, wenn bei der Version 2 angezeigt werden würde, wie weit man bei der Datenerfassung ist (z.B. 5 von 7)	1	7.14
Bitte Beispiele der Attribute in Bildform, Material oder Typ des Gullideckel ist nicht einfach ersichtlich, spricht auch für Version 2, da hier gut erklärende Beispiele eingebunden werden könnten	1	7.14
- Typo in der Landing-Page: "Mit dieser mobile Anwendung ..." - Failed to execute 'transaction' on 'IDBDatabase': The database connection ist closing -> nach Submit auf dem Handy (iPhone) - Bei Bildupload können auch z.B. .csv Dateien hochgeladen werden	1	7.14
Version 2 landet bei 0° L und 0° B. Das heißt man sieht nur blau, auch beim Rauszoomen. Man konnte einen Punkt setzen, aber weiter ging es nicht. Unter der Karte gab es nur noch die Mülltonne. Weiter kam dort nichts. Wahrscheinlich sollte das ganze viel mehr können...	1	7.14
Kartenfenster könnte etwas größer sein.	1	7.14
Bei Version 2 wurden die Eingaben bei accuracy und Höhe nicht angenommen? Kann auch mein Fehler sein!? Bei der ersten Version wurden fehlende Eingaben eingefordert, bei Version 2 war das nicht der Fall!?	1	7.14
Zoomlevel nicht groß genug um die Position präzise manuell am Smartphone zu setzen.	1	7.14
Bei der Erfassung mehrerer Kanaldeckel sollte nur einmal die Begrüßungsseite kommen	1	7.14
V1: - Next-Button deaktivieren bei fehlendem Einverständnis - Nach Submit wieder auf Erfassungsseite springen, nicht auf Start V2: - Automatische Zustimmung ohne extra Checkbox - ist das denn noch erlaubt?	1	7.14
- beide Versionen auf Smartphone: Karte lädt nur, wenn man draufklickt, nicht in der Übersicht (Firefox Android) - Vorschlag: verschiedene Hintergrundkarten einbinden, z.B. Luftbilder	1	7.14
Das "Burger"-Menü erfüllt in der Enlos-Version keinen Zweck mehr, da hier nur Verlinkungen auf die einzelnen Abschnitte aufgeführt werden. Diese sind aber sowieso schon schnell über die Scrollfunktion erreichbar. Nach der Übermittlung des Datensatzes springt die App auf die Einwilligungsseite zurück. Diese sollte nur einmal anfangs angezeigt werden.	1	7.14

Abbildung 17: Frage 3 zur Variante

Allgemein lässt sich festhalten und bestätigen, dass das Endlosformular (One-Pager) die bessere Variante darstellt. Wertet man die Antworten weiter aus, so ist es ersichtlich, dass eine wiederkehrende Abfrage des Datenschutzes unerwünscht ist. Die wiederkehrende Frage nach dem Datenschutz obliegt der Technologie und dem formularbasierten Ansatz der Erfassung. Auch die Kartendarstellung scheint wenig zu gefallen. Dies sind jedoch Dinge, die wenig zu beeinflussen sind. Da die Teilnehmenden Mitarbeitende des BKG sind, ist die Erwartungshaltung hier erfahrungsgemäß hoch und können somit als „Nice To Have“ eingestuft werden.

Lösungsansatz zur besseren Benutzerführung

Aus den Bewertungen können Veränderungsmaßnahmen für den Ablauf erzielt werden. Bei der Multi-Pager-Variante möchte der Nutzer darüber informiert werden, in welchem Schritt er sich bei einer Erhebung befindet. Allgemein kann festgestellt werden, dass die Lokalisierung und das Kartenfenster intuitiver gestaltet werden sollte. Dies lässt sich mit den gegebenen Erfassungskomponenten nicht so einfach lösen. Hierzu bedürfte es einer individuellen Lösung. Betrachten muss man hierzu jedoch den Teilnehmerkreis, der aus GIS-Experten bestand und die Ansprüche somit sehr hoch liegen. Wichtigste Erkenntnis aller Meinungen ist, dass die Datenschutzeinverständniserklärung nicht ständig akzeptiert werden soll. Dies ist verständlich, liegt jedoch in der Natur der formularbasierten Erfassung. Hierauf basierend kann ein Workaround erstellt werden. Pro Erfassungsthema kann eine Einstiegserhebung (Anwendung 1) erstellt werden. Mit einer solchen Einstiegserhebung wird kurz das Thema beschrieben und den Datenschutzerklärungen zugestimmt. An dem Ende dieser Einstiegserhebung werden Hyperlinks zu den eigentlichen Erhebungen (Anwendung 2 + 3) bereitgestellt. Hierdurch können die thematischen Erhebungen sich auf das eigentliche Thema beschränken und fokussieren. Abbildung 18 zeigt einen solchen Workflow auf.

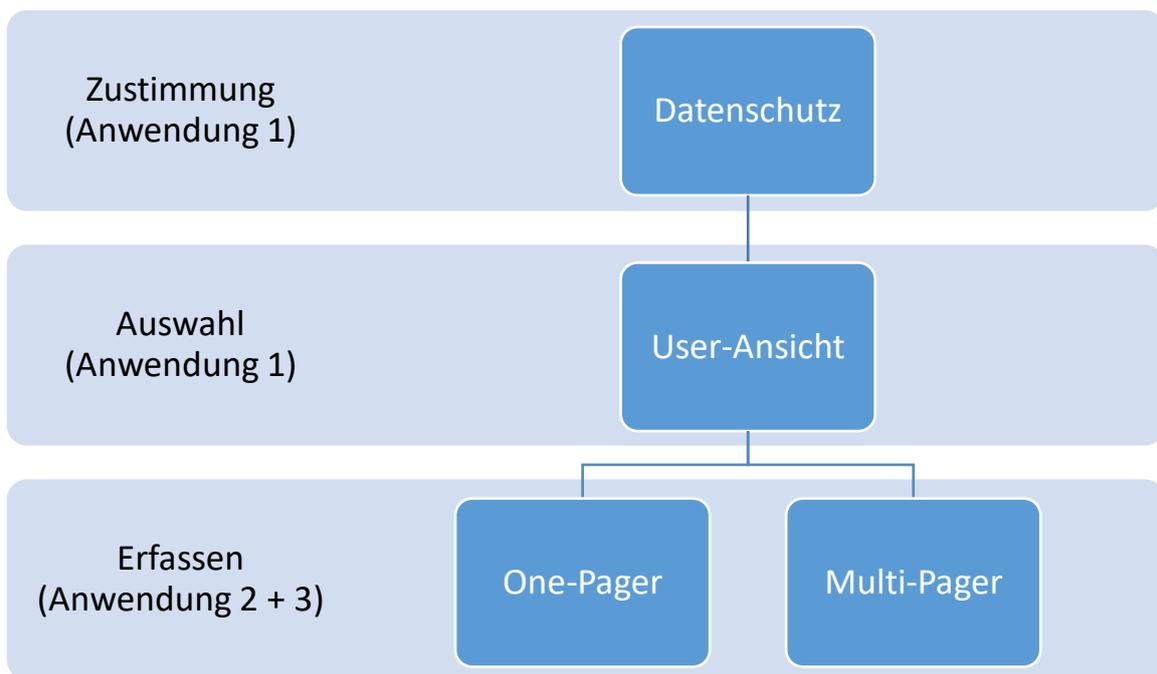


Abbildung 18: Möglicher Workflow der Benutzerführung

4.1.3 Sensorgenauigkeiten

Auf Grundlage der beschriebenen Methodik in Kapitel „3.3 Digitale Erfassungssensoren“ ist eine gesonderte Bewertung von Sensoren in dieser Arbeit nicht erforderlich und kann zur Beantwortung des dritten operativen Teilschrittes herangezogen werden.

Die Erfassungskomponenten (Survey123 und KoboToolbox) bieten von Haus aus jedoch die Möglichkeit, Genauigkeitsinformationen der mobilen Endgeräte bei einer Erfassung zu speichern. Um eventuelle Ausreißer erfassen zu können, sollte diese Funktionalität aktiviert bleiben. Dies unterstützt auch die Qualitätskontrolle der erfassten Geodaten.

4.1.4 Bereitstellung von Erfassungsumfragen

Eine Bereitstellung von Erfassungsumfragen ist Bestandteil des ersten operativen Teilschrittes. Auf Basis der bereits erhaltenen Erfahrungswerte können Umfragen erfolgreich bereitgestellt werden. Der allgemeine Ablauf einer Erfassungsumfrage wurde bereits in Kapitel 3.1.1 „Standard der Erfassungskomponenten“ definiert und exemplarisch in der Abbildung 6 festgehalten. Eine Erfassung mittels beider Systeme ist gleich und formularbasiert. Formularbasiert bedeutet, dass eine Erhebung über das Ausfüllen aller Fragen einer Umfrage erfasst wird. Mit anderen Worten, es wird ein Formular ausgefüllt, gespeichert und versendet. Das entspricht dann einem einzelnen Datensatz, bzw. Tupel in einer Datenbank. Nach einer Erfassung muss jeder Datensatz gegenkontrolliert werden. Der genauere Workflow wird in Kapitel „4.3 Qualitätssicherungsmaßnahmen“ beschrieben.

Nach der Strategie einer geplanten Umsetzung, aus Kapitel 1.4 Strategie zur geplanten Umsetzung, sollen drei unterschiedliche Anwendungsfälle und Erfassungsmöglichkeiten bereitgestellt werden. Diese finden sich in den anderen Kapiteln dieser Arbeit stets wieder. Anhand der Erkenntnisse der Benutzerführung und der Usability (siehe Kapitel Benutzerführung und Usability) wurden die drei Anwendungsfälle exemplarisch umgesetzt.

Die Abläufe dieser Arbeit wurden nach der „Business Process Model and Notation (BPMN 2.0)“ erstellt. BPMN ist eine visuelle Umsetzungssprache aus der Informationstechnologie und bildet Prozessabläufe dar. Mit vereinheitlichten Symbolen können Fach-, Methoden- und Informatikspezialisten Geschäftsprozesse und Arbeitsabläufe interpretieren.

Folgende Beispiele sollen für die Anwendungsfälle gelten und werden mit KoboToolbox dargestellt:

1. Erfassung von situativen Ereignissen

Exemplarisch soll mit dieser Erfassungsmethode die Erfassung von Wald- oder sonstigen Flächenbränden ermöglicht werden. Die Erfassung erfolgt als registrierter Benutzer (Named User).

Genereller Ablauf soll für das Erstellen der Erfassung gelten:

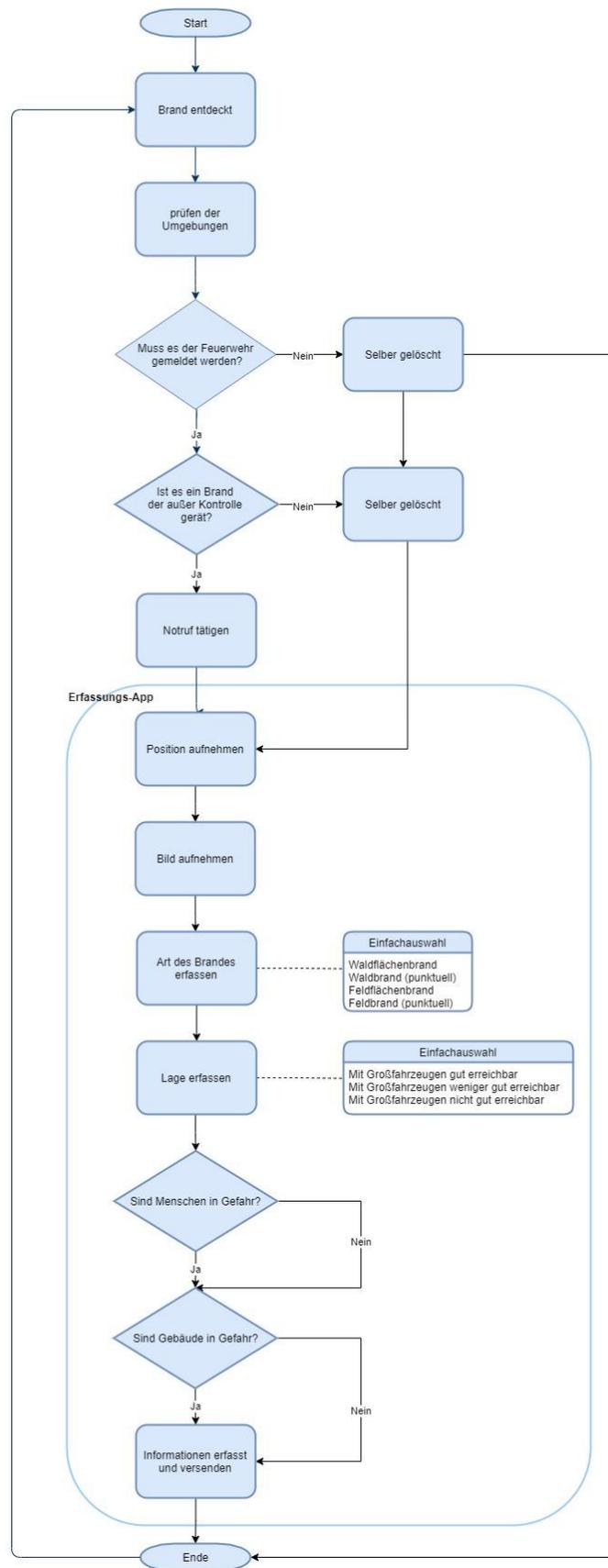


Abbildung 19: Beispielhafter Ablauf „Aufnahme situativer Ereignisse“

Anhang 2 zeigt das Excel Formular das sich aus dem Ablauf (Use Case) ergibt. Geprüft wurde die Erfassung auf einem mobilen Endgerät (siehe Abbildung 20 bis 23 auf iOS).

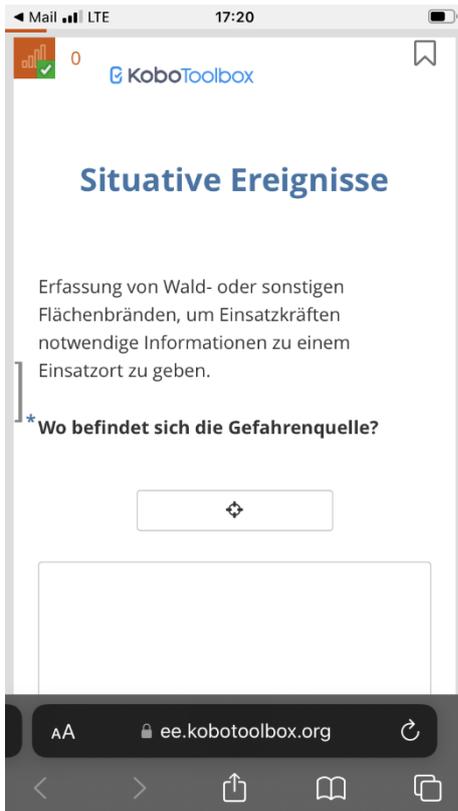


Abbildung 20: Anwendung 1 – Screen 1

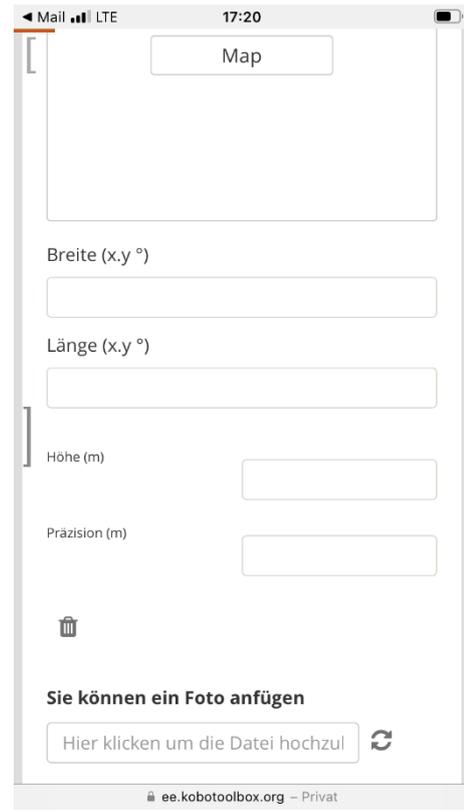


Abbildung 21: Anwendung 1 – Screen 2



Abbildung 22: Anwendung 1 – Screen 3

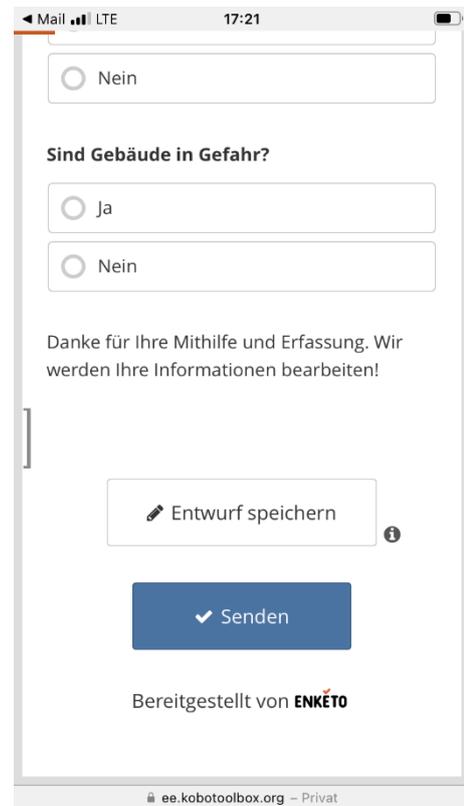


Abbildung 23: Anwendung 1 – Screen 4

2. Erfassung von Korrekturen von Bestandsprodukten:

Mit dieser Erfassungsmethode soll die Erfassung genereller Korrekturvorschläge von Bestandsprodukten ermöglicht werden, hier BKG-Produkte. Die Erfassung erfolgt grundsätzlich als nicht registrierter Benutzer. Dem Benutzer wird freigestellt, ob er über den Bearbeitungsstatus informiert bleiben will.

Der Ablauf sollte für das Erstellen der Erfassung folgendermaßen gestaltet werden:

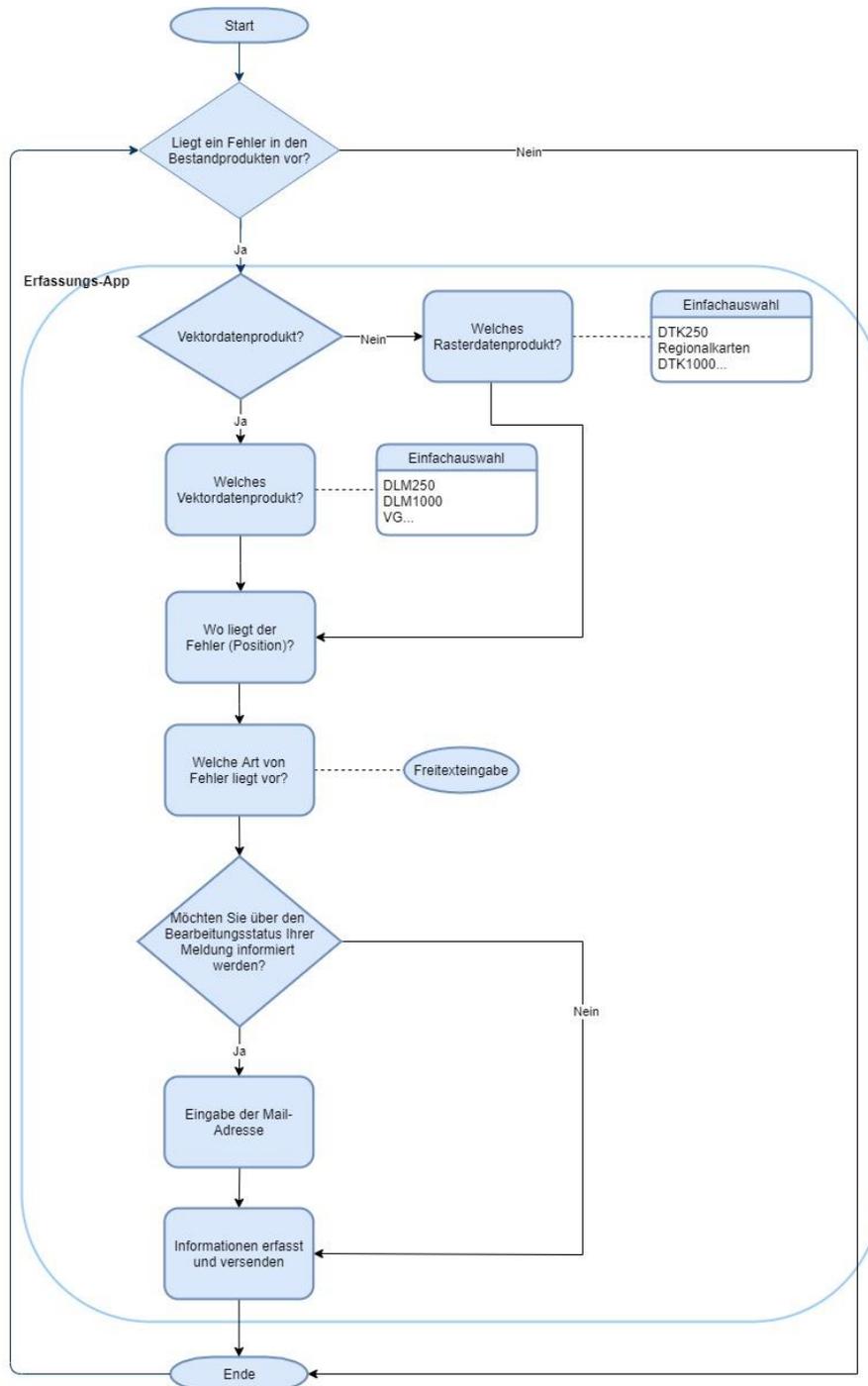


Abbildung 24: Beispielhafter Ablauf „Korrekturen von Bestandsprodukten“

Anhang 3 zeigt das Excel Formular, welches sich aus dem Ablauf (Use Case) für die Anwendung 2 ergibt. Geprüft wurde die Erfassung auf einem mobilen Endgerät (siehe Abbildung 25 bis 27 auf iOS).

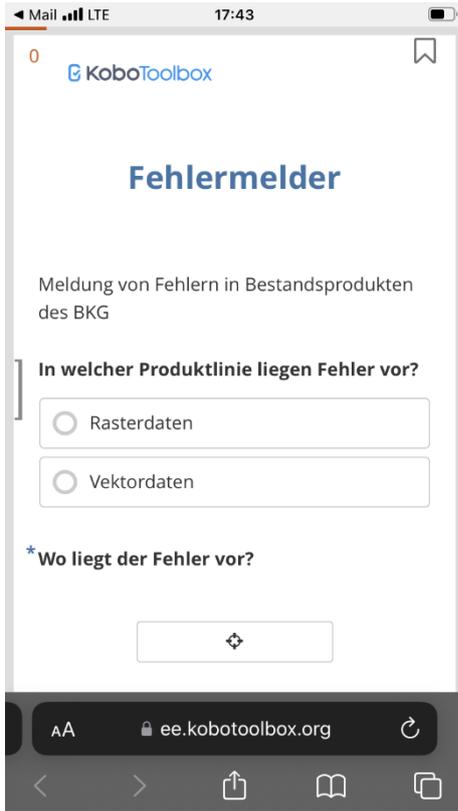


Abbildung 25: Anwendung 2 – Screen 1

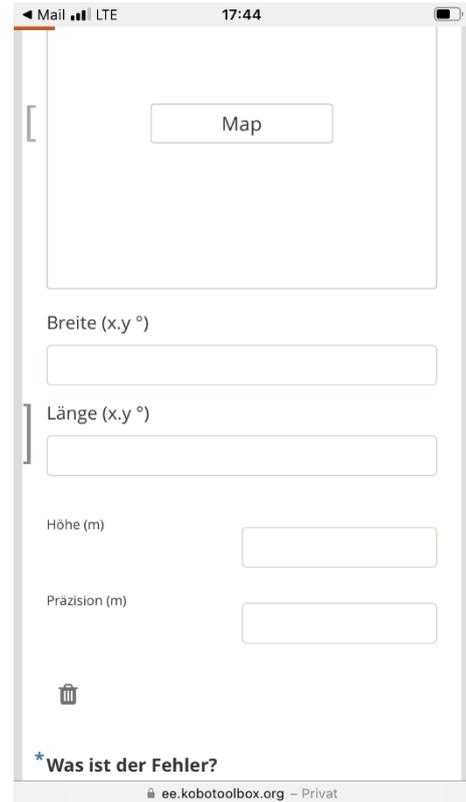


Abbildung 26: Anwendung 2 – Screen 2

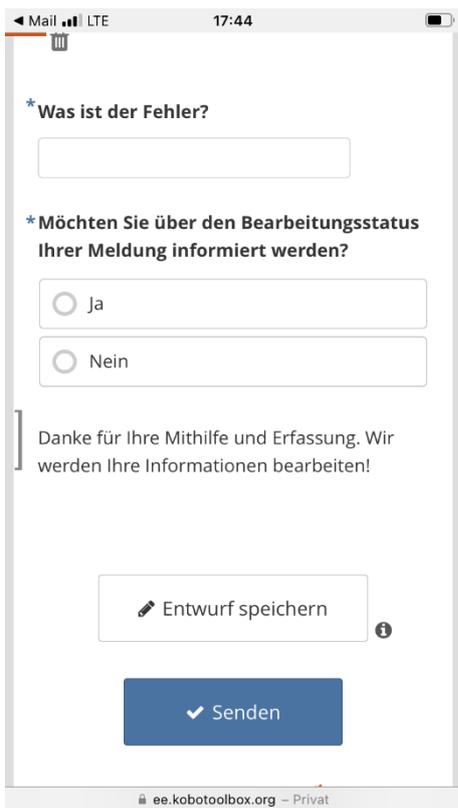


Abbildung 27: Anwendung 2 – Screen 3

3. Erfassung neuer Objektarten für Bestandsprodukte:

Eine neue Objektart soll dem DLM oder einem POI-Produkt hinzugefügt werden. Am Beispiel der Erfassung von „Freiwilligen Feuerwehren“ soll der nachfolgende Workflow gelten. Es gilt, dass die Erfassung als registrierter Benutzer (Named User) getätigt wird.

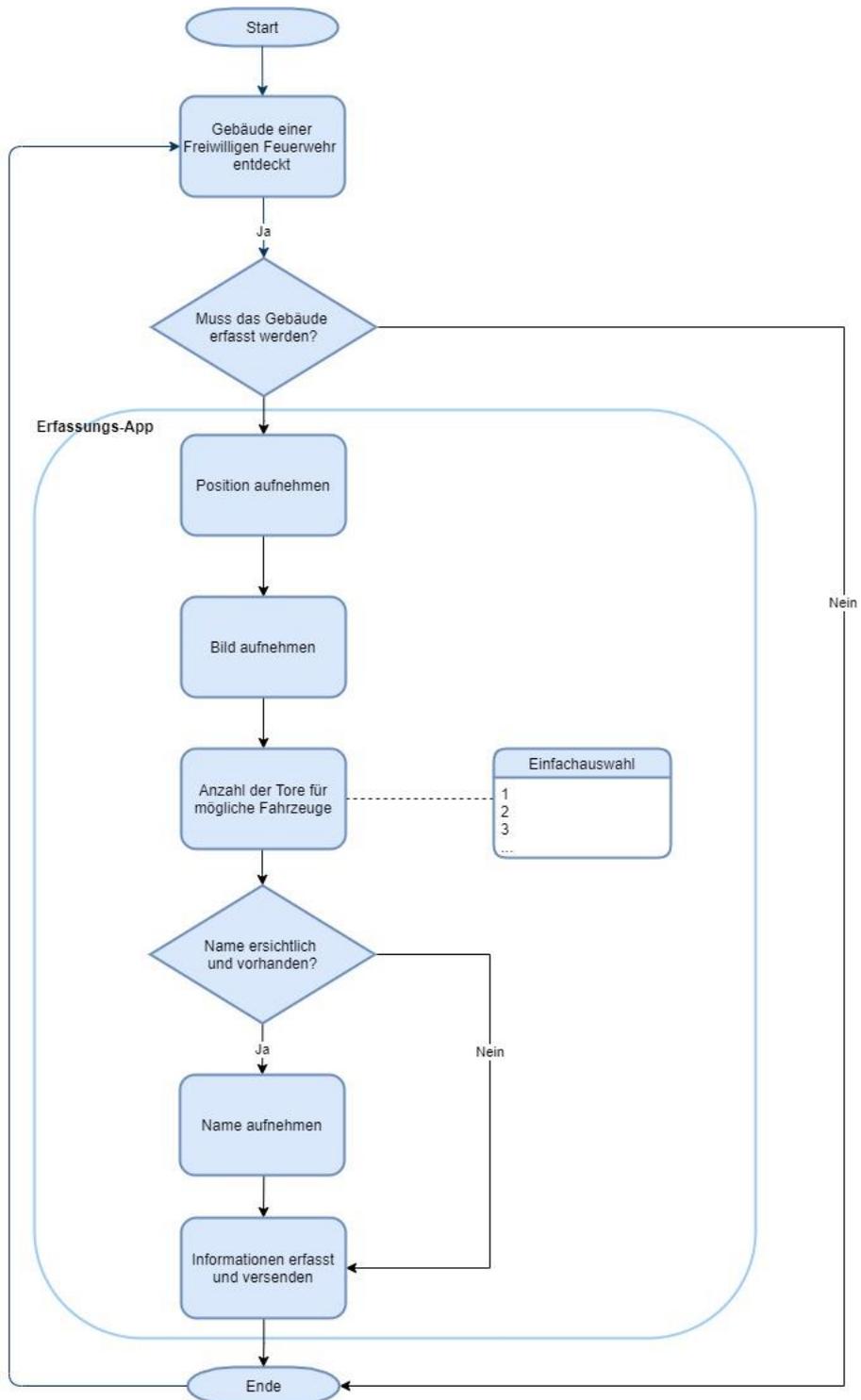


Abbildung 28: Beispielhafter Ablauf „Aufnahme neue Objektart“

Im Anhang 4 befindet sich das Excel Formular für die dritte Anwendung des Ablaufs (Use Case). Gegengeprüft wurde die Erfassung auf einem mobilen Endgerät (siehe Abbildung 29 bis 31 auf iOS).

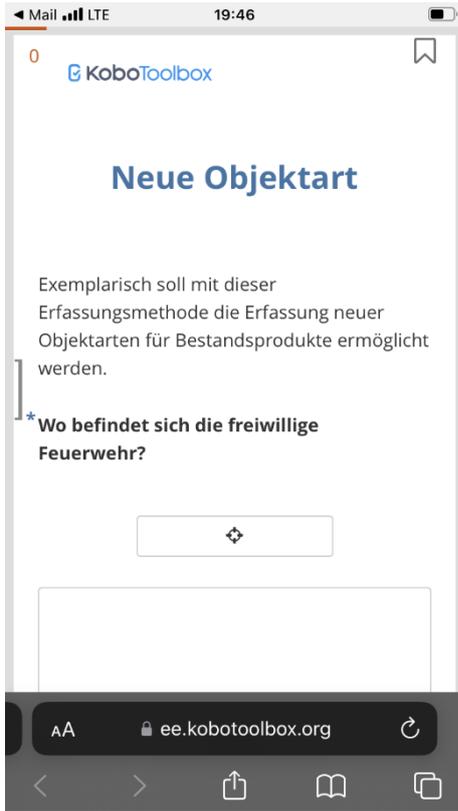


Abbildung 29: Anwendung 3 – Screen 1

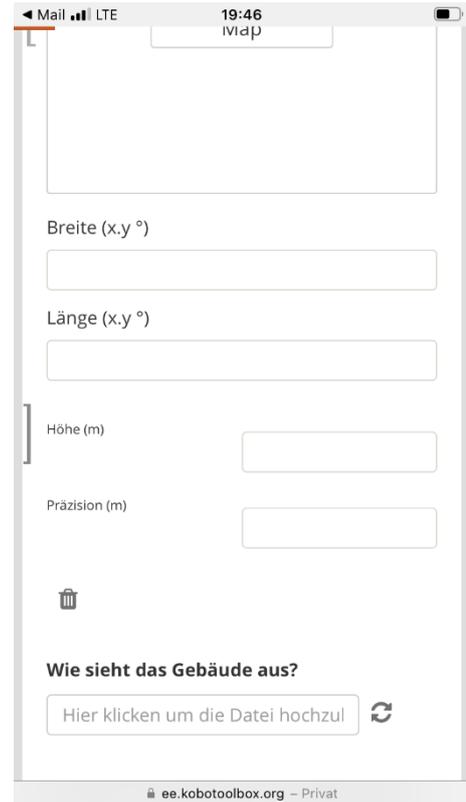


Abbildung 30: Anwendung 3 – Screen 2

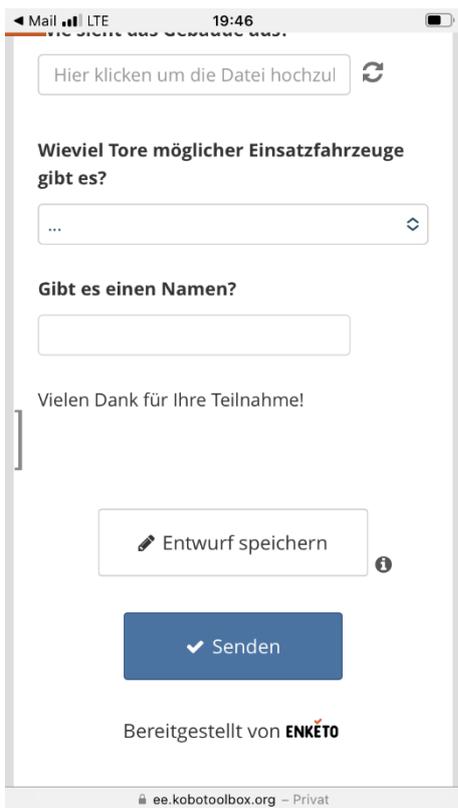


Abbildung 31: Anwendung 3 – Screen 3

4.2 Erfasser und Verantwortlichkeiten

Auf Grundlage der methodischen Beschreibungen in den Kapiteln 3.4 Sammlereigenschaften und 3.5 Verantwortlichkeiten sind die Teilschritte 4 und 5 nachfolgend zu beantworten.

Gruppierung der Erfasser

In Kapitel 3.2 Benutzerführung wurde eine Gruppe von Erfassern beschrieben. In dieser Arbeit konnte die Gruppe nicht erweitert werden. Grund hierfür war unter anderem die Zeit. Aber auch eine mangelnde Bereitstellung der Erfassungskomponenten. Die Problematik der Bereitstellung wurde in Kapitel Anforderungen beschrieben. Dennoch wurden Erfassungen einer kleineren Gruppe bereitgestellt und getestet. Eine klare Gruppierung unterschiedlicher Nutzer konnte nicht identifiziert und zugeordnet werden. Die Gruppe entsprach Anwendern, die mit Geodaten und Erfassungsmethoden vertraut sind.

Anhand der Beurteilungen aus dem Kapitel „Benutzerführung und Usability“ können Erkenntnisse gewonnen werden. Diese entsprechen einem Expertenwissen und können somit nicht detailliert ausgewertet bzw. verglichen werden. Grundsätzlich gelten die Gruppierungen nach Goodchild (2007) als aktuell und können in der vorliegenden Arbeit nicht weiter untersucht werden.

Verantwortlichkeiten

Die Aufnahme bzw. Ausarbeitung aus dem Kapitel 3.5 Verantwortlichkeiten“ beruht auf vorgegebenen Standards und Richtlinien des BSI. Aus diesem Grund lässt sich hier wenig bis gar nichts neu regulieren. Größte Erkenntnis ist jedoch, dass übergeordnete Organisationszuordnungen nach den IT-Grundschutz Dokumenten fest definiert sind. Das stellt sich zwar als starr dar, ist aber diskret und allgemein für jede Organisation umsetzbar.

4.3 Qualitätssicherungsmaßnahmen

Qualität der Erhebungen

Es gibt unterschiedliche Herangehensweisen, wie die Qualität von Daten bewertet werden können. Der Zugang zu Geodaten hat sich in den letzten Jahren verändert, einerseits gibt es noch ganz klassische Unternehmen, die Geodaten kommerziell vermarkten. Gleichzeitig gibt es verschiedene Crowd-Sourcing-Plattformen, die in kollaborativer Methode Geodaten sammeln, bearbeiten und kostenlos zur Verfügung stellen (Goodchild & Li, 2012).

Damit der sechste operative Teilschritt beantwortet werden kann, stellt sich die Frage, wie qualitativ hochwertig solche VGI-Daten sind bzw. sein können, wenn sie ohne jegliche Qualitätskontrolle zur Verfügung gestellt werden und jede Person auch ohne kartografische Vorkenntnisse an Karten wie

zum Beispiel bei OSM mitarbeiten kann. Ein Ansatz ist es, zwei Datensätze (VGI- und kommerzielle-Daten) so aufzubereiten, dass sie miteinander vergleichbar sind. Um anschließend die Vollständigkeit und Genauigkeit des VGI-Datensatzes (extern erhobene Daten) mit einem etablierten Geodatenatz vergleichen zu können. Inspirierend ist hier die Arbeit von Wang et al., welche eine Analyse bereits 2013 anhand des Straßennetzes in Wuhan durchgeführt haben (Wang et al., 2013). Die Vorgehensweise war ein relativ umfangreicher Workflow:

1. Datenvorbereitung,
2. Datenverarbeitung und
3. Datenbereinigung.

Erst nach diesen Schritten ist es möglich die Datensätze zu vergleichen. Wang et al. haben zwei Methoden zum Datenvergleich angewandt. Einerseits die Berechnung der „Lenght Completeness“ und andererseits die „Positional Accuraccy“. Dieser grundsätzliche Workflow kann allgemein für die Erhebung neuer Objektarten angewandt werden, um die neu erfassten Geodaten zu überprüfen. Der genannte Workflow stellt lediglich einen wissenschaftlichen und exemplarischen Ablauf dar und muss für jeden Einzelfall individuell angepasst werden.

Welcher Workflow eignet sich jedoch für die anderen beiden Erfassungsmethoden? Im Sinne der Meldung von etwaigen Korrekturen in Bestandsprodukten könnte dieser Ansatz hilfreich sein, muss aber dennoch manuell überprüft werden. Meldungen über Korrekturvorschläge von Bestandsprodukten stellen eine Information allgemeiner Art dar. Andere Vergleichsprodukte können eine unterstützende und manuelle Hilfe darstellen. Für beide Erhebungsmethoden wäre eine Qualitätsüberprüfung in Form einer inversen Adressgeokodierung denkbar. Eine inverse Adressgeokodierung muss jedoch mit dem DSB abgesprochen werden, da es sich hier um personenbezogene Daten handeln kann.

Muss für die dritte Erfassungsmethode eine Qualitätsüberprüfung stattfinden? Im Fall situativer Ereignisse sollten keine weiteren Maßnahmen zur Kontrolle herangezogen werden. Grund hierfür ist, dass eine situative Momentaufnahme einen Vergleich nicht zulässt. Es entscheidet immer eine manuelle Sichtprüfung der Daten. Als Beispiel sei hier die Katastrophenlage des Ahrtals genannt.

Nachdem die Daten eingeordnet werden können, stellt sich jedoch eine weitere Frage zur Qualität der Erhebungen. Wie können Geodaten erhoben werden, die qualitativ sinnvoll erscheinen? Damit eine höhere Anzahl von Datenerhebungen gut eingestuft werden kann, muss die Erfassungskomponente entsprechend entwickelt sein. Sofern sich ein Erfasser quasi „austoben“ kann, stellt eine zügige Übernahme der erfassten Daten eine größere Hürde dar. Unterbinden lässt sich dies nicht. Wohl aber wie der Erfasser die Daten eingeben kann. Zwei wichtige Aspekte sind hier „Quality by Design“ und

“Security by Design”. Beide können unterstützen. “Quality by Design“ bedeutet, dass der Erfasser möglichst keinen Freitext erfassen kann, so dass eine weitestgehend automatisierte Überführung der Information erfolgen kann. Es gilt hierbei, je mehr individueller Freitext eingegeben werden kann, desto mehr manuelle Arbeit zur Auswertung ist notwendig. Das entspricht also einer Auswahl von vordefinierten Angaben. Je mehr man diesen Ansatz verfolgen kann, desto mehr verfolgt man auch dem anderen Aspekt, nämlich “Security by Design”. Mit standardisierten und vorgegebenen Angaben können individuelle Überprüfungen der erfassten Daten umgangen werden. Das sog. SQL-Injection in Freitextfelder wird damit ausgeschlossen. Folglich stellen diese Daten keine größere Gefährdung dar und entsprechen einer Kombination eines vorgegebenen Rasters.

Arbeitsabläufe zur Integration

Allgemein stellt sich die Frage, wie ein genereller Workflow aussehen kann und wie sich dieser in die Sicherheitsaspekte integrieren lässt. Hierbei müssen unterschiedliche Sichtweisen betrachtet werden. Wie steht es um die IT-Sicherheit und wie kann es vor einer Übernahme eine „Qualitäts-“ Kontrolle geben, damit die Daten vorab geprüft sind?

Die Arbeitsabläufe zur Integration der erfassten Daten stellt eine große Herausforderung dar. Dies muss aus drei Sichten geschehen. Einmal aus Sicht des Datenschutzes, der IT-Sicherheit und zum anderen aus der Sicht des Auftraggebers (siehe Kapitel 3.5 3.5 Verantwortlichkeiten“). Der Auftraggeber ist derjenige, der mit den erfassten Daten arbeiten möchte. Eine Rangfolge des ISB und DSB kann nicht definiert werden. Beide sind auf Grund ihrer Existenz gleichrangig zu bewerten. Der Auftraggeber befindet sich in der Hierarchie eine Ebene tiefer, da DSB und ISB eine Freigabe geben müssen. Aus diesem Grund bietet es sich an, die drei Erfassungsmethoden zunächst separat zu betrachten, um anschließend ein Gesamtbild zu erzeugen. Die Sicherheitsaspekte des DSB und ISB wurden bereits in „Anforderungen“ betrachtet. Deswegen müssen an dieser Stelle keine weiteren Betrachtungen stattfinden.

1. Erfassung von situativen Ereignissen:

Dadurch, dass die erhobene Daten nicht in eine interne IT-Infrastruktur überführt werden müssen, ist der Datenschutz in der Hand anderer Behörden (siehe Kapitel 2.4 „2.4 Abgrenzungen“). Auch um die Überführung dieser erhobenen Daten muss sich keinerlei weitere Gedanken gemacht werden. So könnte man es auslegen. Was passiert aber, wenn die Daten dennoch vom BKG übernommen werden sollen? In jedem Fall zählt, dass der Betreiber bzw. Anbieter einer solchen Kollaborationsplattform das BKG ist und somit ein Sicherheitskonzept vorlegen muss (siehe Kapitel „2.3 Technische Anforderungen (Sicherheitsaspekte“). Also muss die Sicherheit stimmen. Im Fall einer internen Datenübernahme muss auch der DSB eingebunden werden. In Anbetracht dieser Erfassungsmethode muss es sicherlich umfangreicher hinterleuchtet werden. Generell gilt, für alle Methoden die richtigen

Stakeholder an „einen Tisch“ zu bekommen. Gemäß dem 3.5 „Verantwortlichkeiten“ wären die Stakeholder hierfür:

- Fachverfahrensverantwortliche
- ISB
- DSB
- IT-Abteilung
- Auftraggeber

2. Erfassung von Korrekturen von Bestandsprodukten:

Basierend auf die zuvor genannte Erfassungsmethode kann für diese Methode etwas ausgedünnt werden. Grund hierfür ist unter anderem, dass der Inhalt laut Kapitel „Bereitstellung von Erfassungsumfragen“ weitaus dünner ist. Festhalten lässt sich auch, dass die Daten nicht in eine interne Infrastruktur überführt werden müssen (siehe „2.4 Abgrenzungen“). Daraus ergibt sich ein insgesamt kleinerer Workflow. Auch der Auftraggeber, als Stakeholder, ist nicht notwendig. Folgende Stakeholder bleiben:

- Fachverfahrensverantwortliche
- ISB
- DSB
- IT-Abteilung

3. Erfassung neuer Objektarten für Bestandsprodukte:

Diese Erfassungsmethode ähnelt der ersten. Der Unterschied ist, dass der Datenschutz in eigener Hand liegt. Somit sind die Erhebungsfragen auch in eigener Regie und können gemäß dem Ansatz von „Quality by Design“ und „Security by Design“ gesteuert werden. Hiermit entstehen auch weniger Sicherheitslücken. Die Stakeholder lauten:

- Fachverfahrensverantwortliche
- ISB
- DSB
- IT-Abteilung
- Auftraggeber

Mit diesen Grundlagen kann der generische Prozess zur Integration bzw. Übernahme der Daten erarbeitet werden. Betrachtet werden explizit nur die Systemkomponenten, die für die Erfassungen

notwendig sind. Da beide Systeme den gleichen Ansatz und Standard verfolgen, lässt sich ein vereinheitlichter Prozess erarbeiten, der für beide Systeme gelten kann. Für die erfassten Daten ist *zunächst der Erfasser/Sammler selber verantwortlich* und prüft im Optimalfall die eigene Erhebung. Das Mehraugenprinzip haben viele wissenschaftliche Veröffentlichungen als zuverlässig bestätigt. Dabei sollen in diesem *Schritt die Erfasser/Sammler zur Validierung und Korrektur* von möglichen Fehlern anderer Erfasser herangezogen werden. Das dieses Prinzip funktioniert, haben unter anderem Goodchild & Li (2012) erforscht und folgen einem intrinsischen Ansatz. Ein *dritter Schritt wäre optional* und sollte lediglich bei der Erfassung neuer Objektarten nutzbar sein. Wie sich dieser Prozess in den Gesamtprozess integrieren lassen kann, muss separat untersucht werden. Denkbar ist jedoch auch ein extrinsischer Ansatz über eine Gegenkontrolle der Daten mit anderen Referenzdatensätzen. Helbich et al. (2012) untersuchen anhand vergleichender räumlicher Analysemethoden die Positionsgenauigkeit von OSM und proprietären Geodaten. Als Ergebnis der damaligen Untersuchung kam heraus, dass OSM-Daten eine akzeptable Genauigkeit haben. Heute, im Jahr 2023, kann davon ausgegangen werden, dass OSM-Daten weiter an Qualität gewonnen haben. Mit den ohsome quality analyst (OQT) der HeiGIT lassen sich unterschiedliche Qualitätsaussagen generieren. Auch können OSM-Daten mit Referenzdaten kontrolliert werden. In dem Fall einer Erhebung neuer Objektarten könnte man den Spieß umdrehen. Das heißt, man nimmt die OSM-Daten als Referenzdatensatz. Sofern der erhobene Datensatz in OSM vorhanden wäre, wäre dieser qualitätsgeprüft. Wäre er in den OSM-Daten nicht vorhanden, könnte man diesen als aktiven Beitrag der OSM-Community bereitstellen. Das wäre eine Win-Win-Situation. Schritt vier wäre eine manuelle Sichtkontrolle der erfassten Daten. Bei einer manuellen Sichtkontrolle tritt der Auftraggeber und/oder Fachverantwortliche in Aktion. Diese Personen entscheiden darüber, ob die erfassten Daten in eine interne IT-Infrastruktur überführt werden können. In den ersten drei Schritten bleiben die erfassten Daten in den jeweiligen Umgebungen der Erfassungskomponenten. Diesen genannten Workflow bildet die Abbildung 32 ab.

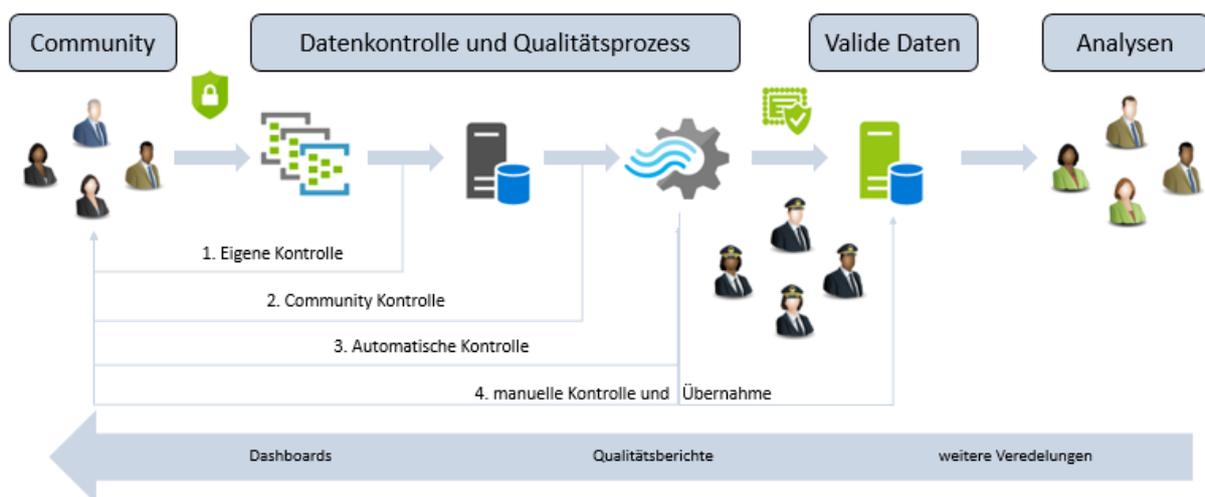


Abbildung 32: Generischer Prozess zur Integration bzw. Übernahme

In Bezug auf sicherheitsrelevante IT-Aspekte gibt die Abbildung 32 nicht genügend Informationen her. Gerade der Prozess der Übernahme der Daten von einer externen Plattform - dem Internet frei zugänglich - in die internen Netze muss genauer beschrieben werden. Aus betrieblichen Gründen wird hier ein allgemein gültiger Prozess beschrieben, der individuell verfeinert werden muss.

Wie können also extern erhobene Daten, die in einer externen Umgebung geführt werden, in eine interne Umgebung überführt werden? Warum ist das überhaupt notwendig? Man könnte die Daten eigentlich dort belassen, wo sie sich befinden. Wie bereits dokumentiert ist eine Überführung der Daten der zweiten Methode nicht notwendig. Exemplarisch könnte bei einer Fehlermeldung von Bestandsdaten eine Mail an ein Ticketsystem generiert werden, damit bereits etablierte Verfahren weiterhin genutzt werden können. Das Ticketsystem leitet die Meldung anschließend an die zuständige Stelle weiter. Anders sieht es bei den anderen beiden Methoden aus. Daten der ersten Methode könnten intern überführt werden, dies ist aber nicht fest geregelt. Bei den erhobenen Daten der dritten Methode sollen die Daten jedoch überführt werden. Grund hierfür ist, dass mittels dieser Methode die Daten des BKG angereichert bzw. veredelt werden sollen. Daten der ersten Methode scheinen potentiell ebenfalls dafür geeignet, müssen aber auf die individuellen Ereignisse geprüft und vereinbart werden. Die Übernahme ist somit unerlässlich, um Doppelarbeit zu vermeiden. Wie könnte nun eine solche Überführung sicherheitstechnisch aussehen? Der Begriff „Datenschleuse“ wird sich hierzu fest etablieren. Die Zeiten, dass Daten ungesehen zwischen zwei oder mehr Sicherheitsbereichen transportiert werden, sind Vergangenheit. Wie eingangs erwähnt spielen mittlerweile weitreichende Anforderungen eine große Rolle. Die Idee sieht folgendes vor. Eine Erfassungskomponente bleibt ein in sich geschlossenes System. Mittels eines weiteren externen Clients werden die Daten, per Get-Methode, von dem Erfassungssystem heruntergeladen und umfangreich anhand von Virenscannern geprüft. Auf diesem externen Client erfolgt zusätzlich eine Integritätsprüfung des generischen Datensatzes über die MD5-Checksumme. Die MD5-Checksumme ist ein Sicherheitsfeature. Sie bildet bei Dateien eine sog. Prüfsumme. Bei einem Austausch von Dateien kann im Anschluss eine Zahlenkette miteinander verglichen werden, um die Echtheit der Daten zu verifizieren. Sind Checksummen identisch, ist der Austausch fehlerfrei und die Datei unverändert. Sind die Checksummen ermittelt und ident, kann ein externer Client die Daten mittels Push-Prinzip in die nächste Ebene transportieren. In dieser Ebene stehen ebenfalls Virenscanner zur Verfügung. Außerdem muss erneut die Checksumme verglichen werden. In dieser Ebene sind die Daten nach wie vor noch nicht in einer internen Umgebung. Erst jetzt können wiederum über ein Get-Prinzip und weitere Virenscanner von einem internen Client die Daten in die interne Infrastruktur durchgeschleust werden. Nach diesem Schritt stehen die Rohdaten einer weiteren internen Verwendung zur Verfügung. Abbildung 33 zeigt den Ablauf.

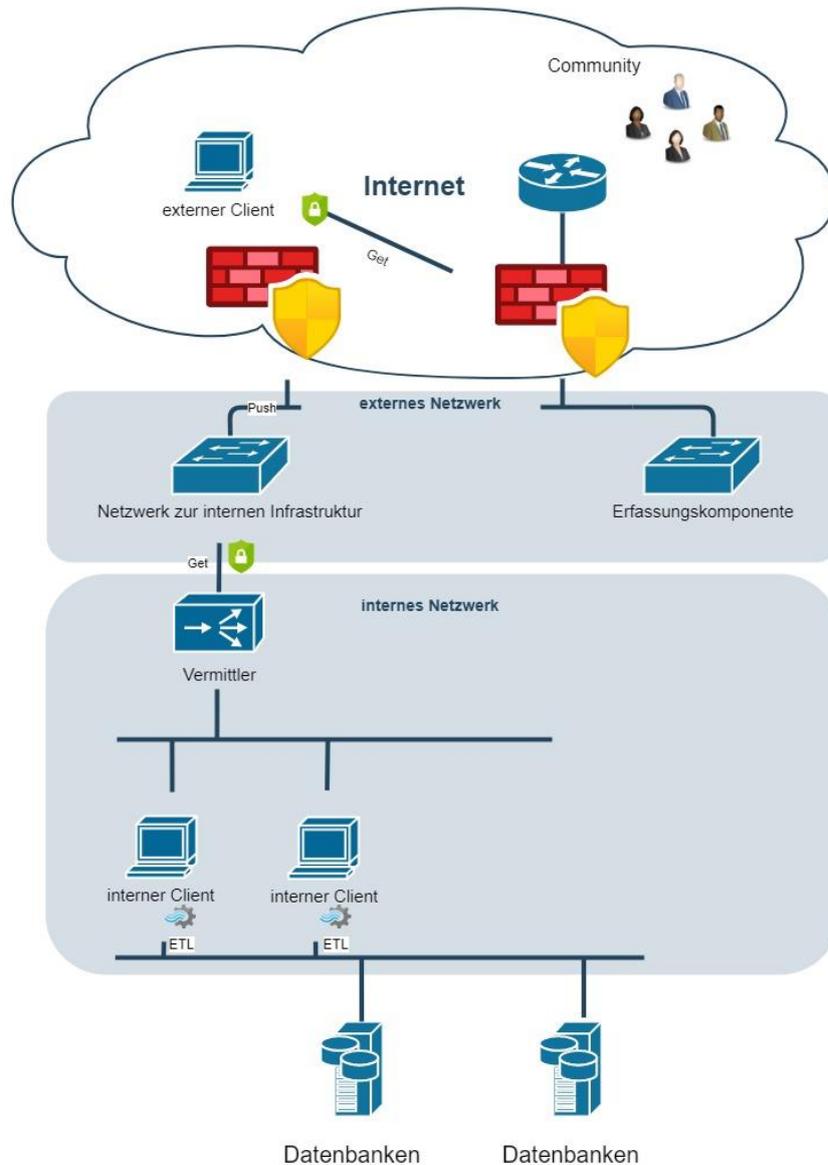


Abbildung 33: Datenschleuse

Nachdem die Rohdaten mittels eines sicheren Verfahrens in das interne Netzwerk übernommen werden konnten, können diese anhand von Extract-Transform-Load (ETL) Prozessen in eine sichere Datenbank überführt werden. Anschließend kann die weitere Analyse, Verarbeitung und Veredelung anderer Daten erfolgen.

Monitoring (Dashboards) der Erhebungen

Ein Monitoring der erhobenen Daten einer Community kann durchweg durch die Systeme der Erfassungskomponenten erfolgen. ESRI bietet hierzu eine zusätzliche „Dashboard“-Methode an. Diese sind jedoch nicht zwingend erforderlich. Erfasste Daten können ebenfalls Jedermann zur Verfügung gestellt werden. Anhand eines Benutzer-Rechtekonzeptes wird dies von beiden Systemen ermöglicht.

Daten können in diesem Berichtswesen analysiert, kontrolliert, verändert und exportiert werden. Nachfolgende Abbildungen zeigen das Berichtswesen/Dashboard in KoboToolbox.

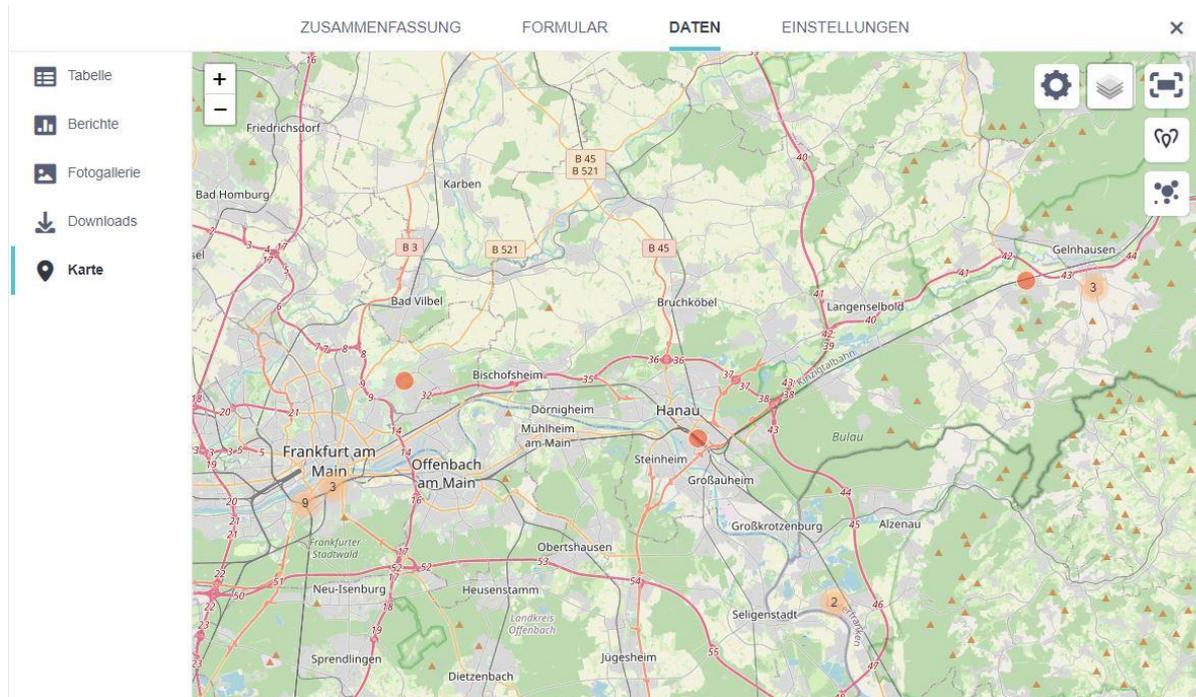


Abbildung 34: Berichtswesen – Allgemeine Kartenansicht

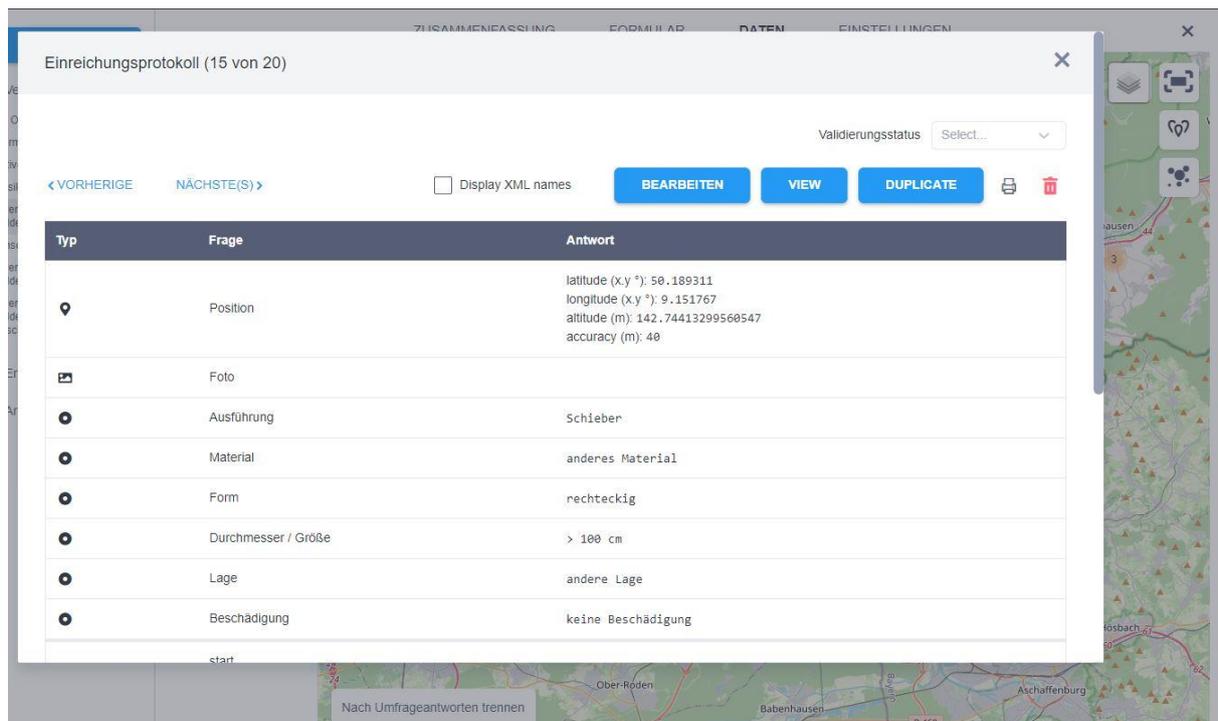


Abbildung 35: Berichtswesen – Informationen einer Erhebung

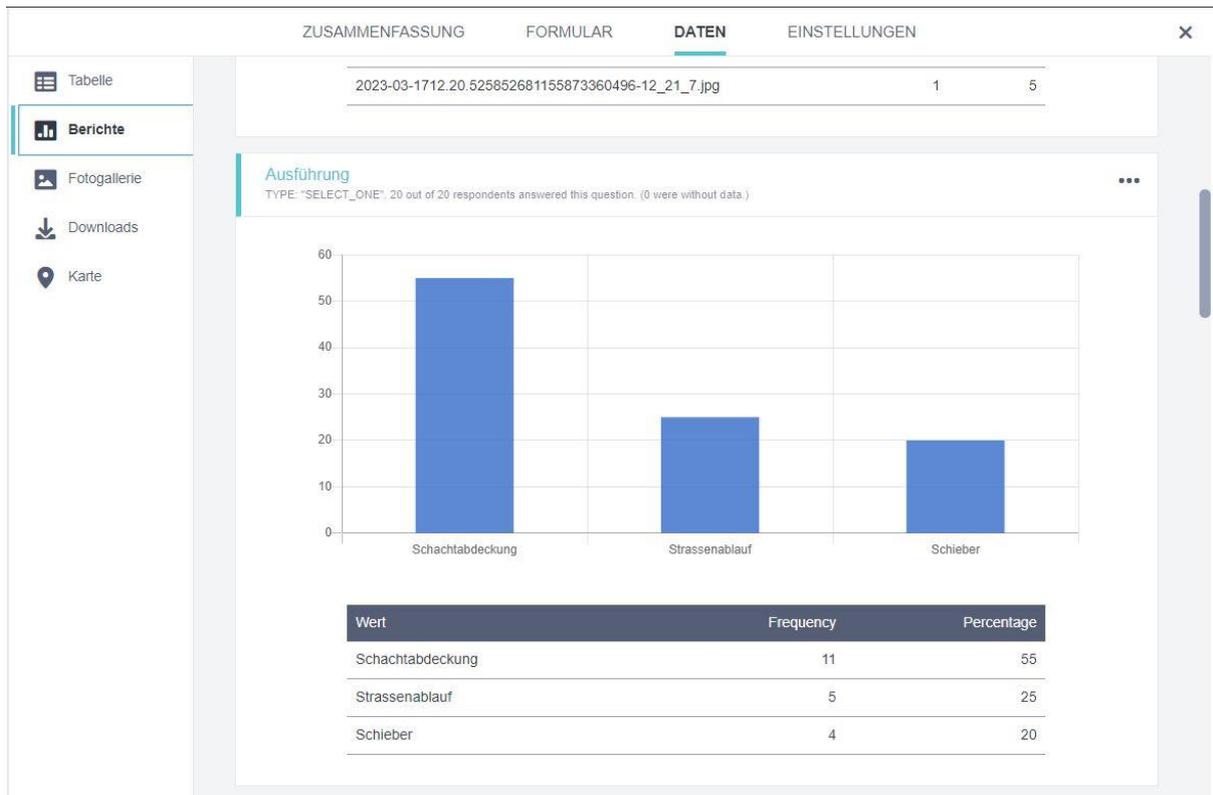


Abbildung 36: Berichtswesen – Auswertung aller Erhebungen

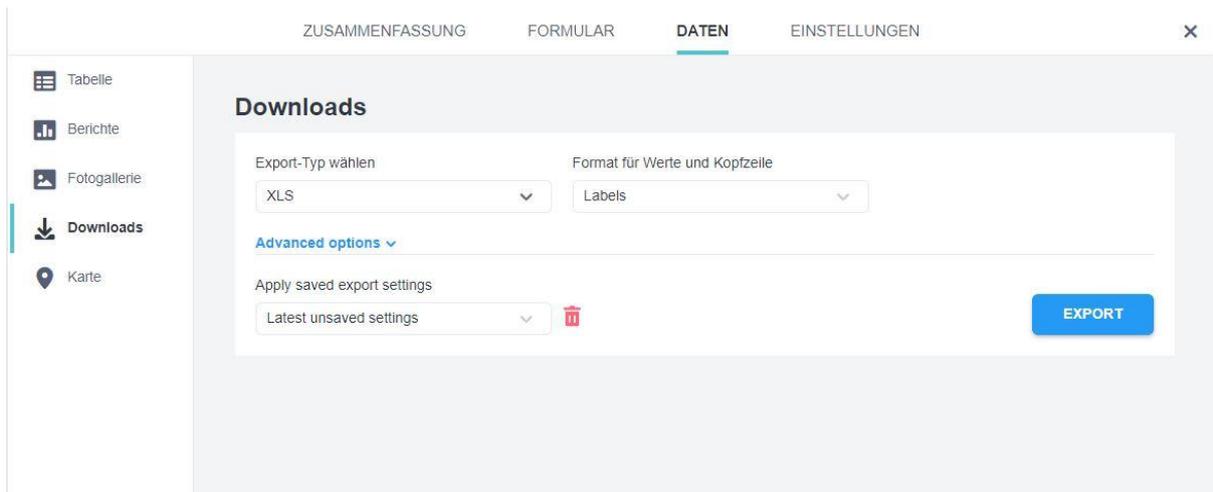


Abbildung 37: Berichtswesen – Exportfunktion der erhobenen Daten

4.4 Motivationsgründe

Zum letzten Teilschritt kann allgemein festgehalten werden, dass eine Community umsorgt werden muss und will. Dieser Punkt stellt sich aus meiner Sichtweise nicht einfach dar, da es zunächst eine Community geben muss. Damit verbunden bedarf es einer richtigen Umsetzung und guten Idee, um eine „weitere“ App bzw. Erfassungskomponente fest zu etablieren.

4.5 Zusammenfassung

Aus den Ergebnissen dieses Kapitels fällt der Vergleich für meine Fragestellung sehr ähnlich aus. Aus meiner Sicht kann ich festhalten, dass sich beide Systeme für eine Bereitstellung der Anwendungsfälle eignen. Lediglich Nuancen unterscheiden beide Systeme. Bei der Umsetzung wurde zunächst auf ein Erstellungsstandard geachtet. Sprich, wie können demnach Erfassungen erstellt und bereitgestellt werden? Mit dem sogenannten Formularstandard XLSForm (EXCEL) könne beide Systeme richtig umgehen. Beide Systeme können gemäß den Richtlinien des BSI implementiert bzw. aufgesetzt werden. Eine Ortssuche anhand einer Karte funktioniert bei beiden, genauso wie die Positionierung über die Sensoren von mobilen Endgeräten. Folglich lassen sich die Erhebungen mit beiden Systemen auch auf mobilen Endgeräten umsetzen und können auch in einem Offline-Modus erfasst werden. Die Unterschiede fangen mit der Nutzerverwaltung an. Während KoboToolbox diese direkt in ihrem System beinhaltet, ist es bei ESRI nur über das weitere Enterprise-GIS Portal möglich. Mit anonymen Usern können beide Systeme umgehen. Hiermit fallen bei ESRI also weitere Named-User Lizenzkosten an. Aber auch für Open-Source Lösungen können Kosten entstehen, die genauer untersucht werden müssen. Aus Sicht des Datenschutzes ist es ebenfalls differenzierter. Bei KoboToolbox steht ganz klar die Transparenz zur europäischen DSGVO. Bei ESRI muss man weiter schauen und oftmals das Kleingedruckte lesen. Die Ortssuche bei ESRI wird nämlich auf direktem Wege an Server in die USA weitergeleitet, um die Anfrage zu bearbeiten. Dies kritisieren europäische Datenschützer zu Recht. Abschließende Matrix soll den Unterschied beider Systeme darstellen, um das allgemeine Fazit dieser Arbeit bilden zu können.

Tabelle 7: Bewertungsmatrix der Systeme

	KoboToolbox	Survey123
Umsetzung Standard	✓	✓
Umsetzung nach BSI	✓	✓
Positionseingabe	GNSS/Ortssuche/Karte	GNSS/Ortssuche/Karte
Alle Endgerät bedienbar	✓	✓
Offlineeingabe möglich	✓	✓
Nutzerverwaltung	✓ (jeder einzeln)	✓ (über weiteres Portal)
Lizenzierung	OpenSource	ESRI
EU DSGVO	✓	(✓)

5 Fazit/Ausblick

In Bezug zur BKG-internen Infrastruktur erscheint eine Erweiterung, um Survey123, relativ simpel. Ein frei zugängliches Portal wird bereits betrieben. Dieses Portal beinhaltet jedoch nur eine Bereitstellung von Geodaten und –diensten. Folgende Fragen bleiben damit offen. Wie kann eine neue Erfassungskomponente in das Angebot des BKG und damit in die IT-Infrastruktur überführt werden? Wie sieht es mit dem Datenschutz und der Sicherheit aus? Wie in Kapitel „Survey123“ und „Vergleich der technischen Fähigkeiten“ beschrieben fügt sich die Erfassungskomponente Survey123 von ESRI in die Kernkonzepte einer GDI am besten ein. Über einheitliche GDI gibt es viele Lektüren. Eine der bekanntesten deutschen Lektüren stammt von dem Wichmann Verlag und trägt den Titel „Geodateninfrastruktur – Grundlagen und Anwendungen“ (Bernard/Fitzke/Wagner, 2004). In dem Beitrag „Geodateninfrastrukturen – ein Überblick“ von Bernhard, Cromptoets und Fitzke werden Gründe für eine einheitliche GDI genannt. Unter anderem wurde über einen verbesserten Datenaustausch und eine effiziente Datennutzung geschrieben. Sofern also die Portal-Umgebung von ESRI umgesetzt werden kann und Survey123 vollumfänglich in dieser Umgebung verfügbar ist, wäre eine Integration der Daten sofort vorhanden. Die erhobenen Daten stünden in Datenbanken, in denen gleichzeitig diverse andere Fachdaten verfügbar wären. Die Kombination vieler Geodaten wäre also denkbar einfach.

Bei KoboToolbox sieht das anders aus. KoboToolbox stellt ein in sich gekapseltes System dar, mit dem Daten erhoben werden und einer Plattformformumgebung zugänglich sind. Eine Integration der erfassten Daten muss stets in andere Umgebungen überführt werden, um Synergien zu erzeugen. Grundsätzlich entspricht der Ansatz einer GDI, jedoch nicht einer in sich geschlossenen Gesamtinfrastruktur.

Eine Gesamtinfrastruktur muss bekanntlich vielen Anforderungen entsprechen (siehe u.a. 2.3 Technische Anforderungen (Sicherheitsaspekte)). Aufgrund der Sicherheitsaspekte eines IT-Betriebes wäre auch die Lösung von ESRI eingekapselt. So viel ist aus dieser Arbeit klar geworden. Wie sieht eine Empfehlung auf Basis dieser Arbeit aus?

Allgemein lässt sich auf Basis dieser Arbeit festhalten, dass sich die Geoinformatik und die allgemeine Informatik in den letzten zwei Jahrzehnten enorm weiterentwickelt haben. Sicherlich nicht zum Vorteil der Geoinformatiker, da die Erwartungshaltung eines Geoinformatiker eine andere geworden ist, als die eines reinen Informatikers. Die Geoinformatiker hatten oftmals eine „Spielwiese“, die heute einfach nicht mehr existent ist. Dennoch stellt der Geoinformatiker eine Schlüsselposition zwischen der IT und einem Endanwender dar, auch wenn der Geoinformatiker keine detaillierten Informationen von IT-Zusammenhängen hat.

5.1 Empfehlung für das BKG

Aus der Sichtweise des BKG konnten viele theoretische Informationen in dieser Arbeit zusammengetragen werden, um eine Empfehlung auszusprechen. Vielleicht auch nicht alle und auch nicht in einer Tiefe zu den einzelnen Details. Es geht jedoch hervor, dass eine Erfassungskomponente (Sammel-App) nicht ohne weiteres erstellt werden kann. Hierzu gibt es hinreichende Argumente. Vor allem steht die IT-Sicherheit, die bei einem Hochladen von Daten immer kritisch begutachtet werden muss. Aus diesem Grund wären beide untersuchten Systeme immer von integrierten Systemen abgekapselt.

Wenn man sich diese Sicht verinnerlicht, dann wäre es also folglich egal, mit welchem der Systeme eine BKG-Sammel-App veröffentlicht wird. Basierend auf dieser Information sollte eine Wirtschaftlichkeitsbetrachtung erfolgen. Dies kann kurzgehalten werden. Da beide Systeme grundsätzlich auf dem gleichen Standard beruhen, nämlich XLSForms, und der eine Hersteller Lizenzkosten veranschlagt (siehe 4.1 Bewertung der VGI-Software“), fällt die Wahl auf den Hersteller, der gleiches ohne weitere Kosten anbietet. Dennoch muss eine Wirtschaftlichkeitsbetrachtung durchgeführt werden. Grund hierfür ist, dass auch Open Source Software Kosten verursachen. Sicherlich nicht im Bereich von Lizensierungen, wohl jedoch im Gebrauch. Sprich das Customizing, die Wartung und der Veröffentlichung.

Nachdem eine Wahl getroffen wurde, stellt sich nun die Frage, wie die Plattform bereitgestellt werden kann. Nach den Ausführungen der vorhergehenden Kapitel muss die Bereitstellung der Plattform grundsätzlich durch den IT-Betrieb (IT-Abteilung) erfolgen. Da es sich hier jedoch um ein neues Fachverfahren handelt und man nicht weiß, ob es sich fest etablieren kann, muss man weiter darüber nachdenken. Strategisch gedacht kann eine „Lift and Shift“ Methodik angewendet werden. „Lift and Shift“ ist einer von vielen Ansätzen für die Migration von Applikationen in die Cloud. Dabei werden eine Applikation und die zugehörigen Daten auf eine Cloud-Plattform verschoben. Die Methodik wird angewandt, um kurzfristige Kosteneinsparungen und schnelle Migrationen herbeizuführen. Es verschafft einem internen IT-Betrieb ebenfalls Zeit, um sich auf neue Anforderungen vorzubereiten. Es erhöht auch die interne Sicherheit und damit die betriebliche Ausfallsicherheit.

Aus diesen Gründen empfiehlt es sich eine Erfassungskomponente zunächst in einer extern betriebenen Cloud zu realisieren. Einen der zahlreichen Anbieter muss das BKG durch die IT-Abteilung, den ISB und DSB definieren. Schlussendlich muss durch den Fachverantwortlichen ein Customizing, z.B. in Form von BKG-Logo für das sog. Favoriten-Icon, betrieben werden. Es besteht jedoch auch die Möglichkeit, einen kompletten Service einzukaufen. Dies würde die Installation, das Betreiben der

Grundinfrastruktur und ein mögliches „Customizing“ beinhalten. Die Verantwortlichkeit der Zugriffsmöglichkeiten müsste bei diesem Modell aber bei dem BKG verbleiben.

Tabellenverzeichnis

Tabelle 1: Fragenkatalog zu OPS_1_1_2.....	- 19 -
Tabelle 2: Fragenkatalog zu OPS_1_1_3.....	- 19 -
Tabelle 3: Fragenkatalog zu SYS_1_1	- 20 -
Tabelle 4: Fragenkatalog zu SYS_1_2_3	- 21 -
Tabelle 5: Fragenkatalog zu APP_3_1.....	- 21 -
Tabelle 6: Fragenkatalog zu APP_3_2.....	- 22 -
Tabelle 7: Bewertungsmatrix der Systeme	- 73 -

Abbildungsverzeichnis

Abbildung 1: Gliederung der Arbeit.....	- 7 -
Abbildung 2: IT-Grundschutz-Bausteine (Quelle: BSI)	- 15 -
Abbildung 3: Ablaufschema Einführung neuer Fachverfahren	- 17 -
Abbildung 4: Beispiel XLSForm (Quelle: https://xlsform.org/)	- 26 -
Abbildung 5: Beispiel WYSIWYG-Editor von KoboToolbox	- 26 -
Abbildung 6: Ablaufzyklus der Erfassungskomponenten	- 28 -
Abbildung 7: Architektur ESRI Survey123 (nach: ESRI)	- 30 -
Abbildung 8: Architektur KoboToolbox (Quelle: https://support.kobotoolbox.org/software_architecture.html)	- 33 -
Abbildung 9: Ablauf eines Testszenarios	- 35 -
Abbildung 10: Interne BKG-Stakeholder.....	- 37 -
Abbildung 11: Aufbau der Organisation (nach: BSI-IT-Grundschutz).....	- 39 -
Abbildung 12: Qualitätsaspekte (Bernard/Fitzke/Wagner, 2004)	- 42 -
Abbildung 13: Softwarequalitätsmerkmale (nach ISO 9126).....	- 43 -
Abbildung 14: Installierte KoboToolbox Container.....	- 50 -
Abbildung 15: Frage 1 zur Variante	- 53 -
Abbildung 16: Frage 2 zur Variante	- 54 -
Abbildung 17: Frage 3 zur Variante	- 55 -
Abbildung 18: Möglicher Workflow der Benutzerführung	- 56 -
Abbildung 19: Beispielhafter Ablauf „Aufnahme situativer Ereignisse“	- 58 -
Abbildung 20: Anwendung 1 – Screen 1.....	- 59 -
Abbildung 21: Anwendung 1 – Screen 2.....	- 59 -
Abbildung 22: Anwendung 1 – Screen 3.....	- 59 -
Abbildung 23: Anwendung 1 – Screen 4.....	- 59 -
Abbildung 24: Beispielhafter Ablauf „Korrekturen von Bestandsprodukten“	- 60 -
Abbildung 25: Anwendung 2 – Screen 1.....	- 61 -
Abbildung 26: Anwendung 2 – Screen 2.....	- 61 -
Abbildung 27: Anwendung 2 – Screen 3.....	- 61 -
Abbildung 28: Beispielhafter Ablauf „Aufnahme neue Objektart“	- 62 -
Abbildung 29: Anwendung 3 – Screen 1.....	- 63 -
Abbildung 30: Anwendung 3 – Screen 2.....	- 63 -
Abbildung 31: Anwendung 3 – Screen 3.....	- 63 -
Abbildung 32: Generischer Prozess zur Integration bzw. Übernahme	- 68 -

Abbildung 33: Datenschleuse	- 70 -
Abbildung 34: Berichtswesen – Allgemeine Kartenansicht	- 71 -
Abbildung 35: Berichtswesen – Informationen einer Erhebung.....	- 71 -
Abbildung 36: Berichtswesen – Auswertung aller Erhebungen	- 72 -
Abbildung 37: Berichtswesen – Exportfunktion der erhobenen Daten	- 72 -


```
||  
||  
|| Where are the files located locally? It can be absolute or  
|| relative to the directory of `kobo-docker`.  
||  
|| Leave empty if you do not need to overload the repository.  
||  
||
```

KoBoCat files location? []:

KPI files location? []:

Enable DEBUG?

- 1) Yes
- 2) No

[2]:

How do you want to run `npm`?

- 1) From within the container
- 2) Locally

[1]:

KoBoCat PostgreSQL database name?

[kobocat]:

KPI PostgreSQL database name?

[koboform]:

PostgreSQL user's username?

[kobo]:

PostgreSQL user's password?

[09AiIdeONCLTpYZQdBID]: ++++++

Do you want to tweak PostgreSQL settings?

- 1) Yes
- 2) No

[2]:

MongoDB root's username?

ANHANG

[root]:

MongoDB root's password?

[J6yFsed23XuDDt3hUXV5]: ++++++

MongoDB user's username?

[kobo]:

MongoDB user's password?

[6gE93il2obTCpXvAbrZO]: ++++++

Do you want to run the Redis containers from this server?

1) Yes

2) No

[1]:

Redis password?

[xCSJHSGoZnqwbY3Pq76D]: ++++++

Max memory (MB) for Redis cache container?

Leave empty for no limits

[]): 20

Do you want to expose back-end container ports (`PostgreSQL`, `MongoDB`, `Redis`)?

1) Yes

2) No

[2]:

Do you want to customize the application secret keys?

1) Yes

2) No

[2]:

Do you want to use AWS S3 storage?

1) Yes

2) No

[2]:

Google Analytics Identifier []:

Google API Key []:

Do you want to use Sentry?

Anhang 2

Hauptfragen:

	A	B	C	D	E	F
1	type	name	label	required	parameters	appearance
2	start	start				
3	end	end				
4	note	Erfassung_von_Wald_Einsatzort_zu_geben	Erfassung von Wald- oder sonstigen Flächenbränden, um Einsatzkräften notwendige Informationen zu einem Einsatzort zu geben.	false		
5	geopoint	Wo_befindet_sich_die_Gefahrenquelle	Wo befindet sich die Gefahrenquelle?	true		placement-map
6	image	Sie_können_ein_Foto_anfügen	Sie können ein Foto anfügen	false	max-pixels=1024	
7	select_one brandart	Um_welche_Art_des_Brandherdes_handelt_es_sich	Um welche Art des Brandherdes handelt es sich?	false		minimal
8	select_one lage	Wie_ist_die_Lage_mit_Großfahrzeugen_zu_erreichen	Wie ist die Lage mit Großfahrzeugen zu erreichen?	false		
9	select_one janein	Sind_Menschen_in_Gefahr	Sind Menschen in Gefahr?	false		
10	select_one janein	Sind_Gebäude_in_Gefahr	Sind Gebäude in Gefahr?	false		
11	note	Danke_für_Ihre_Mithilfe_und_Erfassung_Wir_werden_Ihre_Informationen_bearbeiten	Danke für Ihre Mithilfe und Erfassung. Wir werden Ihre Informationen bearbeiten!	false		
12						

Optionen:

	A	B	C	D
1	list_name	name	label	
2	brandart	waldflächenbrand	Waldflächenbrand	
3	brandart	waldbrand_klein_und_punktuell	Waldbrand (klein und punktuell)	
4	brandart	feldflächenbrand	Feldflächenbrand	
5	brandart	feldbrand_klein_und_punktuell	Feldbrand (klein und punktuell)	
6	brandart	böschungsbrand	Böschungsbrand	
7	brandart	böschungsbrand_klein_und_punktuell	Böschungsbrand (klein und punktuell)	
8	brandart	grünstreifenbrand	Grünstreifenbrand	
9	brandart	grünstreifenbrand_klein_und_punktuell	Grünstreifenbrand (klein und punktuell)	
10	lage	gut_erreichbar	gut erreichbar	
11	lage	weniger_gut_erreichbar	weniger gut erreichbar	
12	lage	nicht_gut_erreichbar	nicht gut erreichbar	
13	janein	ja	Ja	
14	janein	nein	Nein	
15				

Anhang 3

Hauptfragen:

	A	B	C	D	E	F	G
1	type	name	label	required	relevant	appearance	
2	start	start					
3	end	end					
4	note	Meldung_von_Fehlern_ndsprodukten_des_BKG	Meldung von Fehlern in Bestandsprodukten des BKG	false			
5	select_one prodfamil	In_welcher_Produktlinie_liegen	In welcher Produktlinie liegen Fehler vor?	false			
6	begin_group	group_xq3hv67	Group		\$(In_welcher_Produktlinie_liegen) = 'rasterdaten'		
7	select_one raster	Um_welches_Produkt_handelt_es_sich	Um welches Produkt handelt es sich?	false		minimal	
8	end_group						
9	begin_group	group_zv4au47	Group		\$(In_welcher_Produktlinie_liegen) = 'vektordaten'		
10	select_one vektor	Um_welches_Produkt_handelt_es_sich_001	Um welches Produkt handelt es sich?	false		minimal	
11	end_group						
12	geopoint	Wo_liegt_der_Fehler_vor	Wo liegt der Fehler vor?	true		placement-map	
13	text	Was_ist_der_Fehler	Was ist der Fehler?	true			
14	select_one janein	M_chten_Sie_ber_den_Stand_informiert_bl	Möchten Sie über den Bearbeitungsstatus Ihrer Meldung informiert werden?	true			
15	begin_group	group_xq3hv68	Group		\$(M_chten_Sie_ber_den_Stand_informiert_bl) = 'ja'		
16	text	Geben_Sie_Ihre_EMail_ein	Bitte geben Sie Ihre E-Mail ein. Wir informieren Sie.	false			
17	end_group						
18	note	Danke_f_r_Ihre_Mithilfe_und_Erfassung_Wir_werden_Ihre_Informationen_bearbeiten	Danke für Ihre Mithilfe und Erfassung. Wir werden Ihre Informationen bearbeiten!				
19							

Optionen:

	A	B	C	D
1	list_name	name	label	order
2	prodfamilie	rasterdaten	Rasterdaten	
3	prodfamilie	vektordaten	Vektordaten	
4	raster	dtk250	DTK250	
5	raster	dtk500	DTK500	
6	raster	dtk1000	DTK1000	
7	raster	regionalkarten	Regionalkarten	
8	raster	topplus	TopPlus	
9	vektor	d1m250	DLM250	
10	vektor	d1m1000	DLM1000	
11	vektor	vg250	VG250	
12	vektor	vg1000	VG1000	
13	vektor	vg5000	VG5000	
14	vektor	gn250	GN250	
15	vektor	dgm5	DGM5	
16	vektor	dgm10	DGM10	
17	janein	ja	Ja	
18	janein	nein	Nein	
19				

Anhang 4

Hauptfragen:

	A	B	C	D	E	F
1	type	name	label	required	appearance	
2	start	start				
3	end	end				
4	note	Exemplarisch soll mi te erm glicht werden	Exemplarisch soll mit dieser Erfassungsmethode die Erfassung neuer Objektarten für Bestandsprodukte ermöglicht werden.	false		
5	geopoint	Wo_befindet_sich_die_reiwillige_Feuerwehr	Wo befindet sich die freiwillige Feuerwehr?	true	placement-map	
6	image	Wie_sieht_das_Geb_ude_aus	Wie sieht das Gebäude aus?	false		
7	select_one anztore	Wieviel_Tore_m_glich_atzfahrzeuge_gibt_es	Wieviel Tore möglicher Einsatzfahrzeuge gibt es?	false	minimal	
8	text	Gibt_es_einen_Namen	Gibt es einen Namen?	false		
9	note	Vielen_Dank_f_r_Ihre_Teilnahme	Vielen Dank für Ihre Teilnahme!	false		
10						
11						

Optionen:

	A	B	C	D
1	list_name	name	label	
2	anztore	1	1	
3	anztore	2	2	
4	anztore	3	3	
5	anztore	4	4	
6	anztore	5	5	
7	anztore	6	6	
8	anztore	7	7	
9	anztore	8	8	
10	anztore	9	9	
11	anztore	10	10	
12				

Literaturverzeichnis

Bernard/Fitzke/Wagner. (2004). *Geodateninfrastruktur*. Wichmann.

Brunette, W., & Hartung, C. (2023). The Open Data Kit Project. In T. Madon, A. J. Gadgil, R. Anderson, L. Casaburi, K. Lee, & A. Rezaee (Hrsg.), *Introduction to Development Engineering: A Framework with Applications from the Field* (S. 613–637). Springer International Publishing.
https://doi.org/10.1007/978-3-030-86065-3_23

Bundesamt für Sicherheit in der Informationstechnik. (2008). *BSI-Standard 100-4 Notfallmanagement*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2017a). *BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2

Bundesamt für Sicherheit in der Informationstechnik. (2017b). *BSI-Standard 200-2 IT-Grundschutz-Methodik*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2

Bundesamt für Sicherheit in der Informationstechnik. (2017c). *BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2

Bundesamt für Sicherheit in der Informationstechnik. (2020). *Definition der Schutzbedarfskategorien*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/A21_Definition_Schutzbedarfskategorien.pdf?__blob=publicationFile&v=5

Bundesamt für Sicherheit in der Informationstechnik. (2021a). *APP.3.2 Webserver*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2022/06_APP_Anwendungen/APP_3_2_Webserver_Edition_2022.pdf?__blob=publicationFile&v=3

Bundesamt für Sicherheit in der Informationstechnik. (2021b). *OPS.1.1.2 Ordnungsgemäße IT-*

Administration. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2022/04_OPS_Betrieb/OPS_1_1_2_Ordnungsgemaesse_IT_Administration_Edition_2022.pdf?__blob=publicationFile&v=3)

[Kompodium_Einzel_PDFs_2022/04_OPS_Betrieb/OPS_1_1_2_Ordnungsgemaesse_IT_Administration_Edition_2022.pdf?__blob=publicationFile&v=3](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2022/04_OPS_Betrieb/OPS_1_1_2_Ordnungsgemaesse_IT_Administration_Edition_2022.pdf?__blob=publicationFile&v=3)

Bundesamt für Sicherheit in der Informationstechnik. (2021c). *OPS.1.1.3 Patch- und*

Änderungsmanagement.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2022/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2022.pdf?__blob=publicationFile&v=3

Bundesamt für Sicherheit in der Informationstechnik. (2022a). *APP.3.1 Webanwendungen und*

Webservices. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2022/06_APP_Anwendungen/APP_3_1_Webanwendungen_und_Webservices_Edition_2022.pdf?__blob=publicationFile&v=4

Bundesamt für Sicherheit in der Informationstechnik. (2022b). *APP.4.4 Kubernetes*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2022/06_APP_Anwendungen/APP_4_4_Kubernetes_Edition_2022.pdf?__blob=publicationFile&v=3

Bundesamt für Sicherheit in der Informationstechnik. (2022c). *SYS.1.6 Containerisierung*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2022/07_SYS_IT_Systeme/SYS_1_6_Containerisierung_Edition_2022.pdf?__blob=publicationFile&v=3

LITERATUR

Bundesamt für Sicherheit in der Informationstechnik. (2022d). *SYS.1.1 Allgemeiner Server*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Drafts/Final_Draft/SYS_1_1_Allgemeiner_Server_2023.pdf?__blob=publicationFile&v=1

Bundesamt für Sicherheit in der Informationstechnik. (2022e). *SYS.1.2.3 Windows Server*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Drafts/Final_Draft/SYS_1_2_3_Windows_Server_2023.pdf?__blob=publicationFile&v=1

Bundesamt für Sicherheit in der Informationstechnik. (2023). *IT-Grundschutz-Kompodium*.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/IT_Grundschutz_Kompodium_Edition2023.pdf?__blob=publicationFile&v=4#download=1

CON.8: Software-Entwicklung. (2021).

Dr. Klaus Brand, GI Geoinformatik GmbH, & Prof. Dr. Matthäus Schilcher, Runder Tisch GIS e.V.

(Hrsg.). (2014). *Leitfaden—Mobile GIS-Hardware, Software, IT-Sicherheit (Version 2.0)*.

Runder Tisch GIS e.V.

https://rundertischgis.de/images/9_documents/downloads/Leitfaden_Mobile_GIS_V20.pdf

Dunkel, A., Löchner, M., & Burghardt, D. (2020). Privacy-Aware Visualization of Volunteered

Geographic Information (VGI) to Analyze Spatial Activity: A Benchmark Implementation.

ISPRS International Journal of Geo-Information, 9(10), Art. 10.

<https://doi.org/10.3390/ijgi9100607>

Einführung in ArcGIS Enterprise on Kubernetes—ArcGIS Enterprise on Kubernetes | Dokumentation.

(o. J.). Abgerufen 22. Februar 2023, von <https://enterprise->

[k8s.arcgis.com/de/latest/introduction/what-is-arcgis-enterprise-kubernetes.htm](https://enterprise-k8s.arcgis.com/de/latest/introduction/what-is-arcgis-enterprise-kubernetes.htm)

Goodchild, M. F. (2007). Citizens as sensors: The world of volunteered geography. *GeoJournal*, 69(4),

211–221. <https://doi.org/10.1007/s10708-007-9111-y>

Goodchild, M. F., & Li, L. (2012). Assuring the quality of volunteered geographic information. *Spatial*

Statistics, 1, 110–120. <https://doi.org/10.1016/j.spasta.2012.03.002>

- Grönroos, C. (1993). A Service Quality Model and Its Marketing Implications. *European Journal of Marketing*, 18, 36–44. <https://doi.org/10.1108/EUM0000000004784>
- Guinez-Molinos, S., Gonzalez Diaz, J., Barahona Ponce, C., & Lorenzo Bermejo, J. (2022). Development of an Application for Electronic Retrieval of Patient and Sample Information in Latin American Regions with a High Incidence of Gallbladder Cancer. *Journal of Personalized Medicine*, 12(9), Art. 9. <https://doi.org/10.3390/jpm12091476>
- Hammon, L., & Hippner, H. (2012). Crowdsourcing. *Business & Information Systems Engineering*, 4(3), 163–166. <https://doi.org/10.1007/s12599-012-0215-7>
- Helbich, M., Amelunxen, C., Neis, P., & Zipf, A. (o. J.). *Comparative Spatial Analysis of Positional Accuracy of OpenStreetMap and Proprietary Geodata*.
- Hennig, S., Abad, L., Hölbling, D., & Tiede, D. (2020). Implementing Geo Citizen Science Solutions: Experiences from the citizenMorph Project. *GI_Forum*, 1, 3–14. https://doi.org/10.1553/giscience2020_01_s3
- Höferlin, M. (2021). *Deutscher Bundestag / 19. WP / Sitzung 225 / Tagesordnungspunkt 37 (Sicherheit informationstechnischer Systeme)*. <https://de.openparliament.tv/media/DE-0190225055?documentID=4152&sort=topic-asc>
- Howe, J. (2006). The Rise of Crowdsourcing. *Wired Magazine*, 14, 5. http://www.wired.com/wired/archive/14.06/crowds_pr.html
- Huang, J., Guo, Y., Li, X., Zhang, N., Jiang, J., & Wang, G. (2022). Evaluation of Positioning Accuracy of Smartphones under Different Canopy Openness. *Forests*, 13(10), Art. 10. <https://doi.org/10.3390/f13101591>
- IMAGI, I. A. für G. (Hrsg.). (2019). *Handlungsoptionen zum Umgang mit Crowdsourcing-Geodaten zur Nutzung innerhalb der Bundesverwaltung*. Bundesministerium des Innern, für Bau und Heimat. https://www.imagi.de/SharedDocs/downloads/Webs/IMAGI/DE/Veroeffentlichungen/handlungsoptionen-crowdsourcing-geodaten.pdf?__blob=publicationFile&v=4

LITERATUR

- ISO/IEC JTC 1/SC 7 Software and systems engineering. (o. J.). *ISO/IEC 9126-1:2001*. ISO. Abgerufen 19. März 2023, von <https://www.iso.org/standard/22749.html>
- ISO/TC 211 Geographic information/Geomatics. (o. J.). *ISO 19157:2013*. ISO. Abgerufen 19. März 2023, von <https://www.iso.org/standard/32575.html>
- Loola Bokonda, P., Ouazzani-Touhami, K., & Souissi, N. (2020). A Practical Analysis of Mobile Data Collection Apps. *International Journal of Interactive Mobile Technologies (IJIM)*, 14(13), 19. <https://doi.org/10.3991/ijim.v14i13.13483>
- Matheus, A. (2018). *Sicherheitsaspekte und Best Practices in Geodateninfrastrukturen für den Einsatz in Smart Cities*. 38. Wissenschaftlich-Technische Jahrestagung der DGPF und PFGK, München. https://www.dgpf.de/src/tagung/jt2018/proceedings/proceedings/papers/66_PFGK18_Matheus.pdf
- Mocnik, F.-B., Mobasheri, A., & Zipf, A. (2018). Open source data mining infrastructure for exploring and analysing OpenStreetMap. *Open Geospatial Data, Software and Standards*, 3(1), 7. <https://doi.org/10.1186/s40965-018-0047-6>
- Pinheiro, M. B., & Davis, C. A. (2018). ThemeRise: A theme-oriented framework for volunteered geographic information applications. *Open Geospatial Data, Software and Standards*, 3(1), 9. <https://doi.org/10.1186/s40965-018-0049-4>
- Senagi, K., & Tonnang, H. E. Z. (2022). A Novel Tightly Coupled Information System for Research Data Management. *Electronics*, 11(19), Art. 19. <https://doi.org/10.3390/electronics11193196>
- Shapiro, C., & Varian, H. R. (1999). The Art of Standards Wars. *California Management Review*, 41(2), 8–32. <https://doi.org/10.2307/41165984>
- Tobler, W. R. (1970). *A computer movie simulating urban growth in the Detroit region* (Bd. 46).
- Wang, Y., Ouillon, G., Woessner, J., Sornette, D., & Husen, S. (2013). Automatic reconstruction of fault networks from seismicity catalogs including location uncertainty: RECONSTRUCTION OF FAULT NETWORKS. *Journal of Geophysical Research: Solid Earth*, 118(11), 5956–5975. <https://doi.org/10.1002/2013JB010164>

LITERATUR

Yeon, Y.-K. (2021). KMapper: A Field Geological Survey System. *ISPRS International Journal of Geo-Information*, 10(6), Art. 6. <https://doi.org/10.3390/ijgi10060405>