Master Thesis

im Rahmen des

Universitätslehrganges „Geographical Information Science & Systems“
(UNIGIS MSc) am Zentrum für Geoinformatik (Z_GIS)
der Paris Lodron –Universität Salzburg

zum Thema

„Dynamische Rasterdatendienste“
Ausfallsicherheit, Architektur und Servicemanagement

vorgelegt von

Dipl.-Ing. (FH) Slaudo Marx
U1357, UNIGIS MSc Jahrgang 2007

Zur Erlangung des Grades
„Master of Science (Geographical Information Science & Systems) –
MSc(GIS)”

Gutachter:
Ao. Univ. Prof. Dr. Josef Strobl

Dresden, 23. Oktober 2009

Danksagung

An dieser Stelle möchte sich der Autor bei seinem Betreuer Günter Dörffel (ESRI Deutschland GmbH) für die Bereitstellung des Themas und der technischen Unterstützung sowie der Betreuung dieser Arbeit bedanken.

In besonderer Weise dankt der Autor seinen ständigen Wegbegleitern, Kollegen und vor allem seiner Familie für die aufmunternden Worte und für die herzliche Unterstützung während des gesamten Studiums und bei der Erstellung dieser Arbeit.

Eigenständigkeitserklärung

Ich versichere, diese Master Thesis ohne fremde Hilfe und ohne Verwendung anderer als der angeführten Quellen angefertigt zu haben und, dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen hat.

Alle Ausführungen der Arbeit, die wörtlich oder sinngemäß übernommen wurden, sind als solche gekennzeichnet.

Dresden, 23. Oktober 2009

_____

Slaudo Marx

Kurzfassung

Die vorliegende Arbeit befasst sich mit der Ausfallsicherung dynamischer Rasterdatendienste als Basisdienstleistung wertschöpfender Geschäftsprozesse im Geoinformationsbereich.

Ausgehend von rechtlichen, organisatorischen und technischen Rahmenbedingungen und Notwendigkeiten wird der Begriff der Compliance auf Rasterdatendienste und Servicedienstleistungen im Geoinformationsbereich angewandt.

Dementsprechend werden Service Level abgeleitet, die die Grundlage für spätere strategische Verhandlungen bilden können.

Auf Basis gängiger Servicemanagementprozesse und daraus ableitbarer Qualitätskriterien werden diesbezügliche Anforderungen, auch der Nutzer, mit Hilfe der Möglichkeiten des ArcGIS Image Servers verschnitten.

Schlüsselbegriffe: Compliance, IT-Sicherheit, Webservice, Servicequalität, Servicegüte, Servicemanagement, Servicekontinuität, ITIL, Rasterdatendienst, Verfügbarkeit, Cluster, Service Level Agreement, Service Level Requirement, Servicesicherheit, Risikomanagement, Businesskontinuität

Abstract

The paper deals with the failure prevention (failover) of dynamic raster data services as a basis for basic services for value-added businesses in the geographic information sector.

Based on legal, organizational and technical conditions and requirements, the concept of compliance is applied to raster data services and rendering support services in the geographic information sector. Accordingly, service levels are identified, which can form the basis for subsequent strategic negotiations.

On the basis of current service management processes and related requirements for quality criteria, demands, even by the users, are derived from them and are blended with the capabilities of the ArcGIS Image Server.

Keywords: compliance, IT-security, web service, quality of service, service level, service management, service continuity, ITIL, raster data service, availability, cluster, service level agreement, service level requirement, security of service, risk management, business continuity

Inhaltsverzeichnis

Abkürzungsverzeichnis

AEC	Availability Environment Classification
AktG	Aktiengesetz
AO	Abgabenordnung
AOI	Area Of Interest
API	Application Programming Interface
ARIS	Architektur integrierter Informationssysteme
BDSG	Bundesdatenschutzgesetz
BLA	Business Level Agreement
BLR	Business Level Requirements
BSI	British Standard Institute
BSI	Bundesamt für Sicherheit in der Informationstechnik
C4ISR	Command/Control/Communications/Computers Intelligence Surveillance and Reconnaissance
CC	Common Criteria
COM	Component Object Model
CORBA	Common Object Request Broker Architecture
COTS	commercial off-the-shelf
DCOM	Distributed Component Object Model
DCP	Distributed Computing Platform
DIGEST	Digital Geographic Exchange Standard
DoS	Denial-of-Service-Attacken
DSS	Decision Support System
DTED	Digital Terrain Elevation Data
E-Commerce	Electronic Commerce
E-Contracting	Electronic Contracting
E-Government	Electronic Government
ESRI	Environmental System Research Institute
E-Trading	Electronic Trading
ETM	Enhanced Thematic Mapper
FTA	Fault Tree Analysis
GDI	Geodateninfrastruktur
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen

GeoDRM	Digital Rights Management System
GeoXACML	Geospatial Extensible Access Control Markup Language
GeoZG	Geodatenzugangsgesetz
GG	Grundgesetz
GmbHG	Gesetz betreffend die Gesellschaft mit beschränkter Haftung
HGB	Handelsgesetzbuch
HLR	Home Location Register
IEC	International Electronic Commission
IEEE	Institute of Electrical and Electronics Engineering
ISO	International Organization for Standardization
IT	Informationstechnik
ITIL	IT Infrastructure Library
ITK	Informations- und Telekommunikationstechnologie
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
KML	Keyhole Markup Language
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KWG	Kreditwesengesetz
MTBF	Mean Time Between Failures
MTBSI	Mean Time Between System Incidents
MTTR	Mean Time to Repair
MTRS	Mean Time to Restore Service
NDVI	Normalized Differenced Vegetation Index
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Office of Government Commerce
OGC	Open Geospatial Consortium (Open GIS Consortium)
OLA	Operational Level Agreements
OPZ	Operationszentrale
PDCA	Plan-Do-Check-Act
REST	Representational State Transfer
RfC	Request for Change
ROI	Return of Investment

RPC	Remote Procedure Call
SigG	Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz)
SLA	Service Level Agreements
SLM	Service Level Management
SLR	Service Level Requirements
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	Server Object Container
SOM	Server Object Manager
SP	Service Provider
SPoF	Single Point of Failure
TC211	Technical Commitee 211 – Geographic Information/Geomatics
TDG	Gesetz zur Nutzung von Telediensten
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UC	Underpinning Contracts
UrhG	Urheberrechtsgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
W3C	World Wide Web Consortium
WAS	Web Authentification Services
WCPS	Web Coverage Processing Service
WCS	Web Coverage Service
WMS	Web Map Service
WpHG	Wertpapierhandelsgesetz
WPS	Web Processing Service
WS-I	Web Service Interoperability Organization
WSLA	Web Service Level Agreement
WSS	Web Security Service
XADef	XML Attribute Definition
XFDef	XML Form Definitions
XML	Extensible Markup Language

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

Rasterdatendienste stellen in der heutigen Zeit ein enormes Nutzungspotential dar. Die damit verbundene Servicedienstleistung ist von rechtlichen, organisatorischen und technischen Parametern bestimmt, um Dienstleistung zu definieren und die daraus hervorgehende Dienstleistungserbringung zu validieren.

1.1 Motivation

Die Ausprägung *Serviceorientierter Architekturen* findet zunehmend in Form von *Webservices* statt. Diese bilden heute die fundamentale Basis für die Abbildung von Geschäftslogik und diesbezüglichen Geschäftsprozessen. Der Geoinformationsmarkt bedient sich bereits solcher normierter Standarddienste innerhalb von *Geodateninfrastrukturen*. Ein Beispiel dafür sind *Rasterdatendienste*, die Konsumenten mittels offener Schnittstellen zur Verfügung gestellt werden. Es existiert bereits heute ein enormes Abhängigkeitsverhältnis zwischen Dienstanbieter und Konsumenten, die Ihrerseits Basisdienste für eigene *Geschäftsprozesse* verwenden.

Unter sicherheitstechnischen Aspekten sind Dienstanbieter vornehmlich an der Sicherung ihrer Daten interessiert. Dafür gibt es bereits umfangreiche und implementierte Zugriffsverfahren sowie Strategien zur Datensicherung. Offen sind derzeit Regelungen über garantierte Verfügbarkeiten der Dienste und damit der Funktionalitäten für Dritte.

Die Ausfallsicherung dynamischer WebServices spielt in der IT-Sicherheit eine enorme Rolle, da zum einen die Abhängigkeiten vom Nutzer zum Serviceanbieter und zum anderen die damit verbundenen Wechselwirkungen im Bereich der darauf aufbauenden Applikationen stetig gewachsen sind. Die massenhafte Versorgung und Verarbeitung von Rasterdaten in Applikationen mittels WebServices findet zudem zunehmend Anwendung in Geodateninfrastrukturen. Aufgrund dieser stetigen Wechselwirkungen macht eine Auseinandersetzung Sinn, mit welchen Verfahren solche WebServices gegen Ausfall gesichert werden, um den Forderungen von Nutzern nach stetig verfügbaren Diensten nachkommen zu können.

1.2 Zielsetzung und Aufgabenstellung

Die Arbeit befasst sich mit der Ausfallsicherung dynamischer WebServices am Beispiel von Rasterdatendiensten basierend auf ArcGIS Image Server. Auf der Grundlage technischer, rechtlicher und organisatorischer Anforderungen, werden verschiedene Service Level abgeleitet, die es im Folgenden ermöglichen sollen, eine Verhandlungsgrundlage für dementsprechende Service Level Agreements zu definieren. Ferner sollen Strategien der Integration, Anwendungsmöglichkeiten des Programmsystems sowie dessen mögliche Skalierungen am Beispiel von Rasterdatendiensten untersucht werden.

Mit der Arbeit sollen die folgenden Fragen beantwortet werden:

- welche Verfügbarkeitsansprüche an Rasterdatendienste aus Sicht der Konsumenten generell bestehen,
- wie sich diese Ansprüche formal technisch-organisatorisch definieren lassen und
- mit welchen Methoden und Verfahren sich ein entsprechender Servicebetrieb sicherstellen lässt.

Dazu sollen die technischen Möglichkeiten des ArcGIS Image Server untersucht werden, um ihn als zentralen Baustein in eine bestehende Geodateninfrastruktur integrieren zu können.

1.3 Methodik und Lösungsansatz

Die Arbeit basiert auf einem klassischen Top-down Entwurf. Ausgehend von der generell zu erfüllenden Compliance von Servicedienstleistungen werden allgemeine Dienstleistungseigenschaften organisatorisch, rechtlich und technisch im Rahmen von Servicevereinbarungen und vor dem Hintergrund des ITIL-Servicemanagementframeworks betrachtet.

Aus den entsprechenden Managementprozessen lassen sich die für den allgemeinen Servicebetrieb evident wichtigen Leistungs- und Qualitätsparameter gewinnen. Auf Basis dieser referenzierbaren Qualitätseigenschaften von Webservices in serviceorientierten Architekturen und deren möglicher Transformation zu Rasterdatendiensten, sind die Qualitätseigenschaften für Rasterdaten-

dienste adaptierbar. Da Rasterdatendienste und –dienstleistungen durch entsprechende Organisationen und deren Applikationen in Wert gesetzt werden, muss die Servicebereitstellung und deren Garantie auf rechtlicher, organisatorischer und technischer Ebene betrachtet werden.

Ausgehend von dieser Betrachtungsweise lassen sich die Ansprüche und damit verbundene Implementierungsstrategien gewinnen, um zum einen, aus bestehenden Applikationen und Applikationsumgebungen, Lösungen zu eruieren und zum anderen, falls diese nicht praktikabel oder nicht durchführbar sind, neue Methoden und Verfahren zu entwickeln.

1.4 Aufbau der Arbeit

Die Arbeit folgt in ihrem Aufbau der Methodik aus Kapitel 1.3 und ist vereinfacht in Abbildung 1 dargestellt. Sie führt zunächst mit den Kapiteln 1.1 bis 1.3 in die grundlegende Thematik und Problemstellung ein. Ausgehend von der allgemein zu gewährleistenden Compliance im IT-Servicebereich werden die Grundsätze und die Notwendigkeit von IT-Sicherheit in Kapitel 2.1 sowie die Verbindung zur Servicequalität und deren Umfeld in Kapitel 2.2 erläutert.

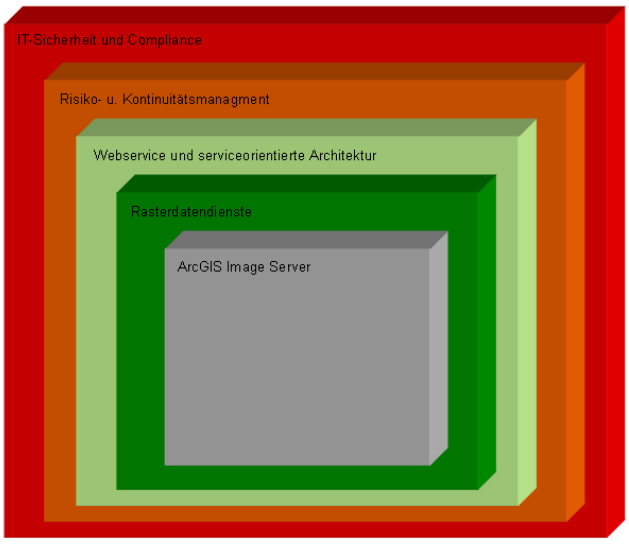

Abbildung 1 – Logik der Arbeit[1]

Da die Compliance und damit auch die Servicedienstleistung generellen Bedrohungen unterliegen, wird die allgemeine Bedrohungslage in Kapitel 2.3

[1] Quelle: eigene Darstellung

beschrieben. Das Kapitel 2.4 formuliert die daraus ableitbare rechtliche Notwendigkeit der Complianceerfüllung und damit der Leistungserbringung. Ausgehend von diesen rechtlichen Standards werden technische sowie organisatorische Standards in Kapitel 2.5 betrachtet.

Darauf aufbauend, verbindet Kapitel 2.6 die allgemeine Sicherheit der Dienstleistungserbringung mit dem übergeordneten Risikomanagement nicht nur für Servicedienstleistungen. Diese werden technologisch durch Webservices in Wert gesetzt und deshalb in Kapitel 2.7, neben deren Qualitätskennzahlen, näher beschrieben. Da Rasterdatendienste eine Erweiterung von Webservices darstellen, werden sie in Kapitel 2.8 betrachtet. Dort findet auch die Vorstellung des verwendeten Programmssystems statt.

Die Kapitel 4.1 und 4.2 setzen sich mit den variablen Nutzeranforderungen auseinander und bestimmen dienstleistungsbezogen entgegenstehende Risiken. Ferner wird in Abhängigkeit von Nutzeranforderung und Risiko der Grad der Servicegüte in Kapitel 4.3 eingegrenzt. Darauf aufbauend eine mögliche Formalisierungsform durch Kapitel 4.4 beschrieben. Das Kapitel 4.5 setzt sich mit dem Programmsystem selbst und seinen Möglichkeiten auseinander. Es folgt eine Beurteilung in Kapitel 5 sowie ein Ausblick in Kapitel 6.

1.5 Abgrenzung

Diese Arbeit beschäftigt sich zwar mit Wertschöpfung im Rahmen von Rasterdatendienstleistungen, es erfolgt jedoch keine betriebswirtschaftliche Betrachtung in Bezug auf ROI. Ferner wird zwar der Bezug zu E-Commerce im Rahmen von E-Contracting und E-Trading hergestellt, jedoch nicht weiter vertieft.

Diese Arbeit befasst sich weiterhin auch nicht mit der .NET- Entwicklungsumgebung oder deren Absicherung und behandelt auch keinerlei Aspekte zum Thema Betriebssystem- oder Netzwerksicherheit. Eine konkrete softwareseitige Programmierung und Implementierung von Lösungen bis hin zum produktiven Betrieb liegt ebenso außerhalb des Betrachtungsbereiches dieser Arbeit.

2 Theoretische Grundlagen

Die Modularisierung elementarer Geschäftsprozesse durch Dienste und die damit einhergehende autonome Verfügbarmachung bzw. Funktionalisierung von IT-Infrastruktur und IT-Technologie, ermöglicht die Flexibilisierung von Wertschöpfungsketten in der Wirtschaft.

Durch den stringenten Einsatz granularisierter Dienste in service-orientierten Architekturen lassen sich die sowohl steigende Risikobelastung, als auch der permanente Kostendruck verlagern und minimieren. Dadurch entstehende Ressourcen können reinvestiv in die Weiterentwicklung von bestehender Wertschöpfung und in der Schaffung neuer wertschöpfender Geschäftsprozesse, auch in der Geoinformationswirtschaft, genutzt werden.

2.1 Grundsätze von IT-Sicherheit

Vordringliches Ziel von IT-Sicherheit muss es sein, die vorhandenen Unternehmensdaten, darauf aufbauende Dienste sowie die verwendete Hard- und Software zu schützen, um die Risiken für den laufenden Geschäftsbetrieb zu minimieren.

Die funktionale Sicherheit der Geschäftsprozesse, und damit auch die Sicherheit der Dienstleistungserbringung, werden durch die allgemeine Betriebssicherheit (Safety) und die zu gewährleistende Angriffssicherheit (Security) definiert. Zusammen vereinen sie die klassischen Säulen der IT-Sicherheit. Rechtliche Rahmenbedingungen, daraus ableitbare technische Voraussetzungen und verpflichtende organisatorische Maßnahmen bilden das Grundgerüst der IT-Sicherheit.

Den praktischen Rahmen bilden in erster Linie Standards, Normen, rechtliche Vorgaben sowie vertragliche Regelungen aus denen sich formal-rechtlich Ansprüche und Schutzrechte ableiten lassen. Dies umfasst beispielhaft:

- das Durchsetzen von Ansprüchen,
- die Sanktionierung bei Verstößen,
- die Forderung auf Unterlassung,

- Forderung nach Schadenersatz bei Nichtbeachtung.

Aus den vorbenannten Rechten und Pflichten ergeben sich für Unternehmen dringend gebotene organisatorische Maßnahmen, um rechtliche Vorgaben und Bedingungen zu erreichen bzw. einzuhalten. Damit eng verbunden ist insbesondere die Bewertung möglicher interner und externer Bedrohungen aus Sicht des Unternehmens, der dazugehörigen Ableitung von Notfallplänen und der Verankerung von Verantwortung in unterschiedlichen Unternehmensbereichen auf verschiedenen Verantwortungsebenen.

Aus den rechtlichen Vorgaben und der Benennung möglicher Risiken[2] resultieren grundlegende, mindestumfänglich-technische Realisierungsmaßnahmen, um dem jeweils vom Gesetzgeber vorgegebenen Stand der Technik zu entsprechen und damit möglichen Haftungsrisiken und Imageschäden zu entgehen.

Sofern alle Maßnahmen getroffen wurden und damit die Normenkonformität des Unternehmens und der darin Beschäftigten bezüglich Recht, Organisation und Technik gewährleistet ist, spricht man in der Informationstechnik von Compliance. Diesen Zusammenhang verdeutlicht noch einmal Abbildung 2.

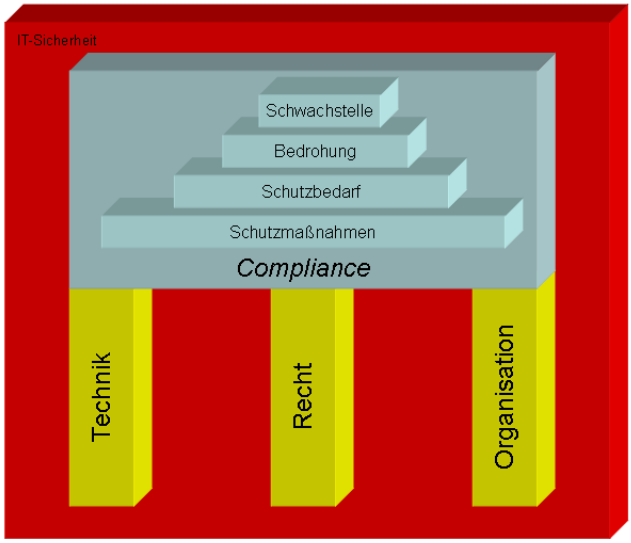

Abbildung 2 – Zusammenhang IT-Sicherheit und Compliance[3]

[2] Vgl. Kapitel 2.6 Servicesicherheit und Risikomanagement
[3] Quelle: eigene Darstellung

Der Schutzbedarf orientiert sich zum einen an einer Vielzahl möglicher systembedingter Bedrohungen und führt zum anderen, auf Grund der Verschiedenartigkeit der Systeme und der zu leistenden Aufgaben, zu unterschiedlichen Sicherheitszielen und damit gleichwohl zu unterschiedlichen Schutzmaßnahmen. Allerdings lassen sich die Anforderungen nach Verfügbarkeit, Vertraulichkeit, Integrität, Rechtsverbindlichkeit und Zurechenbarkeit[4] als die gemeinsamen und damit klassischen Sicherheitsziele definieren.

2.1.1 Verfügbarkeit

Unter der klassischen Verfügbarkeit versteht man das garantierte Bereitstehen eines Systems und damit von Prozessen, Diensten, Daten oder Informationen innerhalb eines bestimmten Zeitfensters, um den kontinuierlichen Geschäftsbetrieb uneingeschränkt fortsetzen zu können.

Die möglichen Gründe für den Ausfall von Systemen sind durchaus vielfältig und werden in Kapitel 2.3 beispielhaft erläutert. Damit eng verbunden ist die dementsprechende bzw. resultierende Ausfallzeit, die das System nicht zur Verfügung steht. Zu unterscheiden ist hierbei zwischen geplanten und ungeplanten Ausfallzeiten. Beide ergeben sich allgemein davon unabhängig aus dem Verhältnis von vereinbarter Servicezeit abzüglich Ausfallzeit zu Gesamtbetriebszeit und werden in Prozent angegeben.

Die folgende Tabelle 1 verdeutlicht den Zusammenhang von Verfügbarkeit, Ausfallzeit und verbleibender Restzeit an Hand von zwei möglichen Szenarien. *Szenario 24h x 365d* beschreibt einen vierundzwanzigstündigen Dauerbetrieb an allen Tagen eines Jahres.

Verfügbarkeit	minimale erwartete Betriebszeit [h]		maximal erlaubte Ausfallzeit [h]		Restzeit [h]	
	24h x 365d	12h x 5d x 52W	24h x 365d	12h x 5d x 52W	24h x 365d	12h x 5d x 52W
99%	8672	3089	88	31	0	5671
99.5%	8716	3104	44	16	0	5656
99.95%	8756	3118	4	2	0	5642
100%	8760	3120	0	0	0	5640

Tabelle 1 - Beispiel Betriebs- und Ausfallzeit[5]

[4] Auch als Nicht-Abstreitbarkeit bezeichnet.
[5] Quelle: eigene Darstellung, angelehnt an Weygant, P. (2001), S.15

Szenario 12h x 5d x 52W zeigt dementsprechende Werte für einen täglichen Betrieb von zwölf Stunden an fünf Tagen pro Woche und insgesamt zweiundfünfzig Wochen.

Interessant ist die dementsprechende Restzeit in beiden Szenarien. Bei Szenario 1 bleiben im Falle einer Verfügbarkeitsgarantie von 99,5 Prozent lediglich 44 Stunden übrig. Dies bedeutet 50 Minuten mögliche Ausfallzeit pro Woche.

Bedenkt man die zusätzlichen systemrelevanten Faktoren wie Wartbarkeit[6], Zuverlässigkeit und Reaktionszeit des Systems selbst, aber auch seiner Einzelkomponenten[7], müssen doch enorme software- und hardwaretechnische sowie organisatorische Anstrengungen[8] unternommen werden, um diese Verfügbarkeit garantieren zu können.

Fallen einzelne Komponenten aus und sind das System, die Dienste bzw. die assoziierten Daten dennoch für eine gewisse Zeit noch ohne Einschränkungen nutzbar, spricht man von Hochverfügbarkeit. Diese wird in der der Praxis u.a. nach Definition der *Harvard Research Group* klassifiziert und ist in Tabelle 2 dargestellt.

AEC	Beschreibung
0	Geschäftsbetrieb kann unterbrochen werden, die Verfügbarkeit von Daten ist nachrangig, Daten können verloren gehen, der Nutzer beendet unkontrolliert seine Arbeit
1	Geschäftsbetrieb kann unterbrochen werden, Daten sind verfügbar und liegen gesichert vor, Nutzer kann nicht weiterarbeiten, unvollständige Transaktionen lassen sich jedoch wiederherstellen
2	Geschäftsbetrieb mit minimalen Unterbrechungen, zeitlich konstant über den Tag, die Woche bzw. das Jahr gesehen, Nutzer kann unterbrochen werden, allerdings seine Arbeit schnell fortsetzen; es können Geschwindigkeitsverluste auftreten
3	Nahezu unterbrechungsfreier Geschäftsbetrieb, zeitlich konstant über den Tag, die Woche, das Jahr (Hauptgeschäftszeit); die Arbeit des Nutzers wird nicht unterbrochen in dieser Zeit; es können Geschwindigkeitsverluste auftreten

[6] Auch als Servicefähigkeit bezeichnet – sie enthält die vertragliche Zusicherung von Zeitfenstern an interne oder externe Dienstleister. Vgl. Kapitel 2.2.1 Service Level Agreements – OLA, UC. Zusätzlich wird diese mit Hilfe von MTTR als Durchschnittszeit zur Wiederherstellung des Service beschrieben.
[7] Vgl. Kapitel 2.5.1 ITSEC sowie Kapitel 2.5.2 Common Criteria
[8] Vgl. Kapitel 2.5.4 ISO/IEC20000/ITIL

4	unterbrechungsfreier Geschäftsbetrieb; keine Beeinträchtigung des Nutzers; keine Geschwindigkeitseinbußen; keine Transaktionsverluste; 24 x 7 Szenario

Tabelle 2 - AEC-Klassifikation[9]

AEC-1 fokussiert eindeutig auf die noch im folgenden Kapitel 2.1.2 zu behandelnde Datenintegrität, während *AEC-4* zusätzlich nur durch ein fehlertolerantes System bewerkstelligt werden kann.

Die Trennung zwischen einzelnen Komponenten und der Summe der Komponenten, die das Gesamtsystem zur Servicebildung benötigt, führt zur Klassifikation der Verfügbarkeit in Komponentenverfügbarkeit und Serviceverfügbarkeit.

Die Serviceverfügbarkeit lässt sich weiterhin unterscheiden nach der zugrundeliegenden Architektur der beteiligten Servicekomponenten. Liegen diese linear vor, spricht man von *serieller Verfügbarkeit*. Wird im Gegensatz dazu eine nicht-lineare Architektur gewählt, wird dies als *parallele Verfügbarkeit* bezeichnet. Diese ist, wie Abbildung 3 an einem konstruiertem Rechenbeispiel zeigt, bei gleicher Komponentenanzahl und identischer Komponentenverfügbarkeit höher, als die serielle Verfügbarkeit. Man spricht in diesem Zusammenhang auch von Parallelisierung.

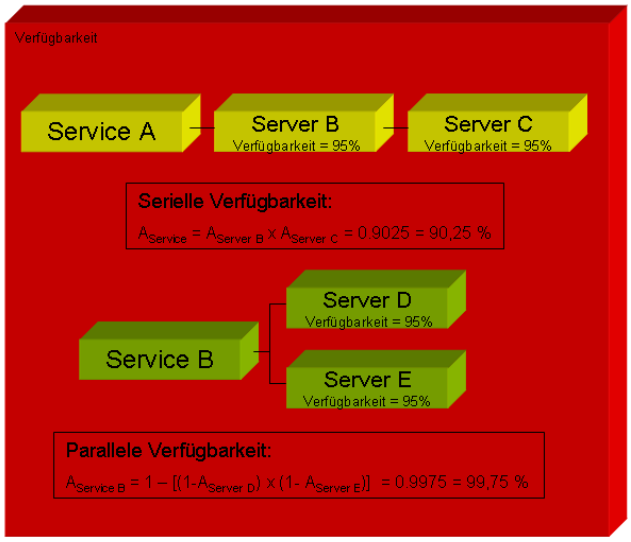

Abbildung 3 - Formen der Verfügbarkeit[10]

[9] Quelle: eigene Darstellung, angelehnt an Harvard Research Group (2001), S.4
[10] Quelle: eigene Darstellung, angelehnt an Ebel, N. (2008), S.257

Eine weitere Kennzahl für die Gütebeurteilung von Verfügbarkeit ist die Zuverlässigkeit. Diese kann jedoch unterschiedlich definiert werden. Zum einen als *Mean Time Between Service Incidents* (MTBSI) und damit über den Quotienten aus produktiver Servicezeit zur Anzahl der Serviceunterbrechungen, und zum anderen Seite aus *Mean Time Between Failure* (MTBF), dem Quotienten aus der um die Ausfallzeit bereinigten Servicezeit zur Anzahl der Serviceunterbrechungen. Beide Kennzahlen repräsentieren den Zuverlässigkeitsgrad eines Dienstes in Abhängigkeit seiner Unterbrechungen.

Für die Beurteilung der durchschnittlichen Zeit, die benötigt wird, um einen Service wieder verfügbar zu machen, existiert die *Mean Time to Restore Service* (MTRS) Kennzahl. Sie wird berechnet aus dem Quotienten von Ausfallzeit zur Anzahl der Serviceunterbrechungen.

Damit stehen Kennzahlen zur Verfügung, um die Verfügbarkeit eines Service kennzahlenseitig allgemein zu beschreiben. Diese Kennzahlen können in Form von *Service Level Agreements*[11] vertraglich fixiert werden. Die dementsprechende Auswahl obliegt den Vertragspartnern und ist nicht vorgeschrieben.

2.1.2 Integrität

Unter Integrität versteht man im Allgemeinen die Vollständigkeit und Unveränderbarkeit von Systemen oder Daten während oder nach Transaktionen. Das bedeutet, dass Daten, zeitlich unabhängig, sicher vor Manipulation sein müssen. Daher muss zum einen generell ausgeschlossen werden, dass Unbefugte das System, Daten oder Teile von Daten verändern können und zum anderen, dass technische Maßnahmen zur Integritätsprüfung getroffen werden müssen. Dies geschieht heute oftmals durch Rollen- und Rechtekonzepte, verbunden durch Authentifizierungsverfahren[12], mit deren Hilfe nur zugelassene Nutzerkeise Einblick zu bestimmte Daten bekommen. Zusätzlich werden etwaige Veränderungen protokolliert, softwareseitig auf Konsistenz geprüft und können bei einer möglichen Wiederherstellung des Systems als Wiederherstellungsgrundlage dienen.

[11] Vgl. Kapitel 2.2.1 Service Level Agreements
[12] Eine unfangreiche Erläuterung dementsprechender Methoden und Verfahren findet sich in Bengel, G. (2004), S.406ff

2.1.3 Vertraulichkeit

Eng verbunden mit der im vorherigen Kapitel 2.1.2 beschriebenen Integrität von Systemen, Diensten und Daten, ist das Maß der Vertraulichkeit. Sie soll sicherstellen, dass nur vorher autorisierte Nutzer entsprechende Daten nutzen können. Es steht in diesem Zusammenhang nicht der Schutz der Transaktion im Vordergrund, sondern es geht vielmehr um den Schutz der Daten vor dem Zugriff Dritter vor und nach der Transaktion. Dies wird maßgeblich mit Hilfe von Verschlüsselungstechniken realisiert[13]. Die Vertraulichkeit wird zusätzlich von verbindlichen Rechtsnormen getragen. Dies betrifft insbesondere die Wahrung von Geheimnispflichten und den zu gewährleistenden Datenschutz[14].

2.1.4 Rechtsverbindlichkeit

Die Umsetzung von Rechtnormen ist die grundlegende Bedingung für den laufenden Geschäftsbetrieb. Generell müssen alle Authentifizierungs-, Authentisierungs-, Autorisierungs-, Transaktions- und Verschlüsselungsprozesse nachvollziehbar und durch entsprechende Maßnahmen beweisbar sein, um vertraglich zugesicherte Systemzustände, Dienst- bzw. Datenrepräsentationen zu bestimmten Zeiten belegen zu können. Dabei gilt es, die Einhaltung der unter Kapitel 2.1.3 aufgeführten Normative nachzuweisen.

2.1.5 Zurechenbarkeit

Zurechenbarkeit ist die eindeutige Zuordnung eines Nutzers zu einer gesicherten Transaktion. Dies umfasst neben der eigentlichen Sicherheit für die Transaktion selbst[15] und der Protokollierung der korrekten Transaktionsdurchführung, auch den dementsprechenden Authentizitätsnachweis. Ist dieser erbracht liegen die Voraussetzungen für die normative Beurteilung der Rechtsverbindlichkeit vor[16] und sind damit handhabbar.

[13] Eine unfangreiche Erläuterung dementsprechender Methoden und Verfahren findet sich in Bengel, G. (2004), S.395ff
[14] Vgl. Kapitel 2.4 Rechtliche Rahmenbedingungen
[15] Die, als solches auch als eigenständiger Service oder Teil eines Service ablaufen kann.
[16] Vgl. Kapitel 2.1.4 Rechtsverbindlichkeit

2.1.6 Interoperabilität

Unter Interoperabilität versteht man die notwendige Forderung nach Einhaltung von operationalisierten Standards, um den Informationsaustausch in heterogenen Systemen unter den o.a. Kriterien gewährleisten zu können. Dementsprechende Standards leiten sich aus den jeweils unterschiedlichen Implementierungsebenen ab.

- Die semantische Ebene formuliert Interoperabilität als die Fähigkeit, auf Basis von Beschreibungssprachen und Abbildungsmodellen systemübergreifend, inhaltlich gleichartige Aussagen abbilden zu können.

- Die technische Ebene definiert Interoperabilität als die standardisierte Interaktionsmöglichkeit von Diensten mittels einheitlich gestalteter Architekturen sowie dazugehöriger Schnittstellen und Protokolle[17] über Systemgrenzen hinweg.

- Die sicherheitstechnische Ebene definiert Interoperabilität als die Fähigkeit, Sicherheitsziele systemübergreifend und in beliebiger Schichttiefe in verteilten Systemen umzusetzen.

- Die geografische Ebene, die im Definitionsbereich geografischer Objekte und damit im vordergründigen Wirkungsbereich des Geoinformationswesens gleichsam versucht, realweltliche Phänomene in eineindeutiger Sichtweise global zu modellieren.

Interoperabilität führt nicht zuletzt in Summe der oben aufgeführten Interoperabilitätsformen zu neuen Möglichkeiten, mit Hilfe globaler Dienste, Informationen systemübergreifend verfügbar zu machen, um Entscheidungen transparent zu gestalten und nachvollziehen zu können[18].

Verfügbarkeit, Integrität, Vertraulichkeit, Rechtsverbindlichkeit, Zurechenbarkeit und Interoperabilität sind gerade unter dem Aspekt von verteilten Systemen und darauf aufbauenden Dienst und Dienstarchitekturen evident wichtig für eine funktionierende serviceorientierte Wirtschaft.

[17] Vgl. Kapitel 2.7 Webservices i.V.m. Kapitel 2.8 Rasterdatenservices
[18] Vgl. Kapitel 2.4 Rechtliche Rahmenbedingungen, INSPIRE

2.2 IT-Sicherheit und Servicequalität

Die Forderungen und Vorgaben für solche durch den Dienstleister und dessen System einzuhaltenden und damit für den Nutzer zu garantierenden Leistungen werden als Qualitätsmerkmale eines Service bezeichnet. Sie dienen im Bereich der allgemeinen IT-Dienstleistung ebenso, wie im Dienstleistungsbereich der Geoinformationswirtschaft als Grundlage für die umfassende Beurteilung der Leistungserbringung. Qualität ist dabei definiert durch den Grad der Erfüllung der Kunden- bzw. Nutzeranforderung, um aus einem Produkt, einem Service oder abstrahiert betrachtet, aus einem Prozess, eine vorher definierte Wertschöpfung zu erhalten.

Die vertragliche Fixierung von Serviceeigenschaften wird im IT-Dienstleistungsbereich durch Service Level Agreements festgehalten.

2.2.1 Service Level Agreements

Service Level Agreements sind rechtsverbindliche Vereinbarungen zwischen Dienstanbietern (Serviceprovider) und Nutzern (Servicerequestor). Sie dienen in erster Linie dem Abgleich komplexer Kundenanforderungen gegenüber dem Leistungsvermögen von Serviceprovidern (Business Level) und sind damit elementarer Bestandteil des Leistungs- aber auch des Risikomanagements[19].

SLA leiten sich aus den übergeordneten Service Level Requirements (SLR) ab. SLR stellen die zwischen den Vertragsparteien auszuhandelnden Serviceziele den allgemeinen Geschäftszielen, den Business Level Agreements (BLA) gegenüber und dienen als Grundlage für die Vereinbarung für die Verhandlung von Rahmenbedingungen für die Leistungserbringung von Services.

[19] Vgl. Kapitel 2.6 Servicesicherheit und Risikomanagement

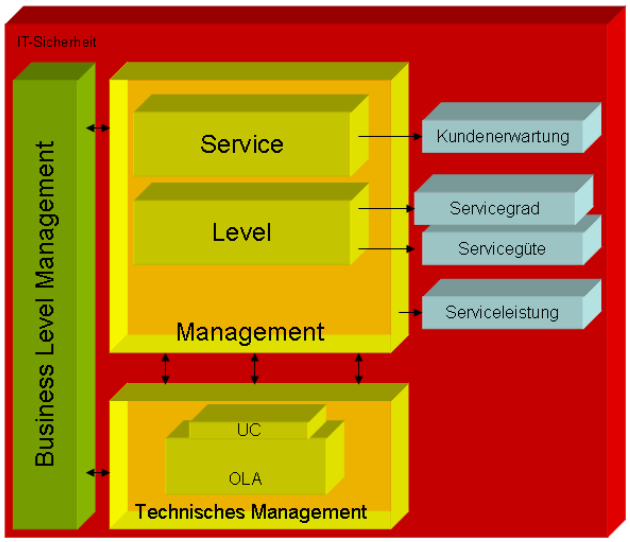

Abbildung 4 - Übersicht Service Level Agreement[20]

Dabei definiert der *Service*, wie in Abbildung 4 dargestellt, die generelle Anforderung des Kunden bzw. dessen Erwartung an den zu leistenden Service durch den Provider. Der *Level* beinhaltet im Anschluss die Ausprägung der Serviceleistung in Form komplexer Maß- und Kennzahlen[21]. Diese werden wiederum in einer vertraglichen Übereinkunft, dem *Agreement* fixiert, auf dessen gemeinschaftlicher Grundlage die Leistungserbringung, Überprüfung und Abrechnung erfolgt.

SLA lassen sich in drei wesentliche Kategorien unterteilen[22]:

- Servicebezogene-SLA (Service-based) werden universell für einzelne global-organisationsbezogene IT-Dienstleistungen, wie E-Mail-Dienste oder Speicherdienste definiert und in unterschiedlichen Qualitätsdimensionen vereinbart. Diese Qualitätsdimensionen lassen sich nach gängiger Praxis in Gold-, Silber- und Bronzedienste unterteilen. Für den Anspruch an Verfügbarkeit ließe sich hier der Grad der Verfügbarkeit je nach zu vereinbarenden Verfügbarkeitsniveaus für Rasterdatendienste klassifizieren.

- Kunden-SLA (Customer-based) fassen einzelne Nutzergruppen (business units) unter Berücksichtigung inhaltlich-thematischer bzw. busi-

[20] Quelle: eigene Darstellung
[21] Vgl. Tabelle 2 - AEC-Klassifikation
[22] Vgl. *OGC* (2007d), S.67f

nessbedingt-gleicher Forderungen zusammen. Eine dementsprechende Ausprägung könnte das Zusammenfassen aller Rasterdatendienste eines auf Geodaten spezialisierten Bereiches sein.

- Mehrdimensionale-SLA (Multi-level) bilden eine Kombination aus servicebezogenen-SLA und Kunden-SLA. Hierbei stehen die einzelnen SLA nicht unabhängig voneinander da, sondern werden hierarchisch, organisationsbezogen vereinbart, in dem die SLA den einzelnen Organisationsstufen und –einheiten angepasst werden. Mehrere Kunden, z.B. Behörden, möchten Rasterdaten auf unterschiedlichen Verfügbarkeitsniveaus anbieten können. Daraus ergibt sich formal die generelle Forderung nach Speicherplatz und in weiterer Folge für den Serviceprovider die Notwendigkeit des thematischen Zusammenfassens beispielsweise nach einer Servicekategorie „Rasterdaten für Behörden“.

Die Kategorisierung von SLA ist Aufgabe des Service Level Managements. Sie wird unterstützt durch die Vorgaben des Business Level Managements (Was soll im Zuge der Businessziele machbar sein?) und das technische Management in Form von Beratungsleistung bezüglich technischer Infrastruktur (Was ist praktisch machbar?).

SLA können sowohl für den internen Geschäftsbetrieb als auch für ausgelagerte Geschäftsprozesse oder Services definiert werden. Für interne betriebliche Vereinbarungen steht der Begriff *Operational Level Agreements* (OLA). Vereinbarungen mit externen Dienstleistern werden als Underpinning Contracts (UC) bezeichnet. Beide fokussieren jedoch auf die Definition von Zielen und Verantwortlichkeiten, um die in den SLA definierten Servicelevel zu erreichen[23].

2.2.2 Servicekatalog und Servicebeschreibung

Formal bestehen SLA, wie dies Abbildung 5 illustriert, aus Servicekatalogen und Servicebeschreibungen. Servicekataloge bieten einen ersten differenzierten Überblick über aktuell verfügbare Services bzw. Dienstleistungen in knapper Form und können je nach Unternehmensziel und Unternehmensausrich-

[23] Eine tiefgreifende Auseinandersetzung der Wechselbeziehung von SLA, OLA und UC findet in Tyurin, N. (2007) statt.

tung in weitere wesentliche Kategorien unterschieden bzw. zusammengefasst werden.

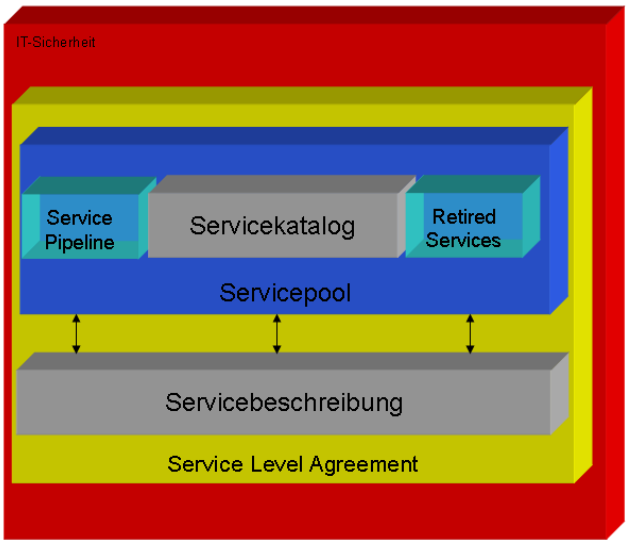

Abbildung 5 - Servicekatalog und Servicebeschreibung[24]

In der Praxis haben sich folgende Katalogtypen durchgesetzt[25]:

- Infrastruktur-Services
- Applikations-Services
- Individual-Services

Infrastruktur-Services umfassen die Etablierung und den Betrieb von IT-Infrastrukturen. Dazu gehören unter anderem der Server-, Netzwerk-, Email- und Druckbetrieb sowie die dementsprechende Überwachung. Zu den Applikationsdiensten zählen der gesamte Softwarebetrieb inklusive Datensicherung und Patchmanagement. Beide Dienstarten sind etabliert und ermöglichen die Konzentration des Unternehmens auf das eigentliche Kerngeschäft. Individualdienste können eine Mischung aus beiden vorbenannten Dienstarten oder aber auch völlig neue Dienste sein. Die Schwierigkeit hier liegt insbesondere in der unmöglichen Vorausplanung solcher Dienste[26].

Die Summe der verfügbaren Services bildet den Servicepool, der durch geplante Services (Service Pipeline) und durch nicht mehr zur Verfügung gestellte Services (Retired Services) vervollständigt wird. Ergänzt werden diese Ka-

[24] Quelle: eigene Darstellung
[25] Vgl. Elsener, M. (2005), S.126
[26] Dies bedeutet, dass der gesamte Zyklus eines Dienstes für die entsprechende Anwendung komplett neu erstellt bzw. aus vorhandenen Diensten zusammengesetzt werden muss.

taloge durch zusätzliche Servicebeschreibungen, die die wesentlichen Kennzahlen für die Güte des einzelnen Service dokumentieren.

2.2.3 Service Level Management

Die wissenschaftliche Auseinandersetzung im Bereich der Ausprägung und Formalisierung von SLA wurde durch verschiedene Standardisierungsgremien und durch verschiedene Forschergruppen geführt. Daraus entstandene Modelle und Methoden[27] wie *Service Quality Agreements* (ITU), *Policy-basiertes Service Level Management* (IETF), *Domänenübergreifendes Management* (Bhoj et al.), dem Konzept der *langfristigen Liefererbeziehungen* (Preuß) und der *Architektur für die elektronische Abwicklung und Verhandlung von Verträgen* (COSMOS) führen nicht zu der aus heutiger Sicht benötigten prozessorientierten Sichtweise und der Übertragung minimaler Managementfunktionen an den Nutzer[28].

Die geforderte prozessorientierte Beschreibung und Implementierung von IT-Servicedienstleistungen lässt sich daher am besten mit den heute verfügbaren und etablierten Dienstleistungsprozessen im Rahmen von Standardwerken wie ISO20000/ITIL[29] beschreiben.

Mit Hilfe eines normierten Servicemanagements, insbesondere Service Level Managements und daraus ableitbaren SLA, lassen sich damit die folgenden Punkte mindestumfänglich definieren und durch die Vertragsparteien vereinbaren:

- Vertragspartner/Ansprechpartner
- Vertragslaufzeit/Servicezeit
- Servicebeschreibung/Zweck
- Freigabeinformationen/Nutzungsbeschränkungen
- Leistungsbeschreibung/Kennzahlenwerk
    - Leistungsumfang
    - Änderungsmanagement/Aktualisierung der Leistungsbeschreibung
    - Qualität

[27] Vgl. Schmidt, H. (2005), S.39ff
[28] Vgl. ebd., S.50
[29] Vgl. Kapitel 2.5.4 ISO/IEC20000/ITIL

        - Verfügbarkeit
        - Performance
        - Zuverlässigkeit
        - Sicherheit
        - Erreichbarkeit
    - Notfallmanagement/Eskalationsstufen
- Leistungsverrechnung (Verrechnungsmethode)
- Qualitätssicherung
    - Reportingverfahren
    - Zeitpunkte für Leistungsabgleich (Leistungsreview)
- Unterschriften
- Begriffsdefinitionen/Rollen

Die Qualitäts- und Qualitätssicherungsmerkmale müssen dabei eindeutig definiert, messbar, von beiden Vertragsparteien als realistisch akzeptiert und zu spezifizierten Zeitpunkten überprüfbar sein[30].

Damit erleichtern SLA den Vergleich zwischen verschiedenen oder gleichartigen Prozessen bezogen auf die Kosten und die Risikobelastung. Sie sind damit nicht nur vertragliches Gestaltungsmittel und Grundlage für die rechtliche Durchsetzung von Haftungs- und Gewährleistungsansprüchen[31], sondern sind auch ein wichtiges Instrument zur Steuerung der Servicekontinuität. Dies trägt nicht zuletzt zu einer verbesserten Unternehmenskultur sowie zu einer dauerhaften Kundenzufriedenheit bei.

[30] Es handelt sich hier um Kriterien aus der qualitativen und quantitativen Beurteilung von Zielvereinbarungen (SMART).
[31] Vgl. Kapitel 2.4 Rechtliche Rahmenbedingungen

2.3 Informationstechnische Bedrohungslage

Der technische Fortschritt ermöglichte in den vergangenen Jahren eine zunehmende Vernetzung von Rechnersystemen. Ausgehend von verteilten Systemen über Grid Computing bis hin zu kaskadierenden Diensten und Dienstearchitekturen bietet sich eine Vielzahl an modernen Interaktionsmöglichkeiten. Global wie lokal operierende Unternehmen sind in der Lage, vierundzwanzige Stunden über ihre Kommunikationssysteme am weltweiten Marktgeschehen teilzuhaben. Via Internet und Satellitenverbindung bekommen Mitarbeiter von überall auf der Welt Zugriff auf Dienste und Systeme, um Transaktionen durchzuführen und marktwirtschaftlichen Erfolg zugenerieren.

Was auf der einen Seite Chance und Möglichkeit bietet, birgt gleichzeitig aber auch potentielle Gefahren. Was passiert, wenn einzelne Dienste nicht verfügbar oder essentielle Server nicht erreichbar sind? Oder aber Dienste auf Grund von Manipulationen falsche Ergebnisse liefern?

Was ein Ausfall zweier Zentralrechner anrichten kann, zeigte eindrucksvoll der diesjährige und bisher einzigartige Netzausfall bei T-Mobile am 21. April[32]. Für die Kunden war das T-Mobile-Netz vorübergehend aufgrund zweier nicht funktionierender Home-Location-Register-Server (HLR) nicht mehr zu erreichen. Diese sind für die Zuordnung der Mobilfunknummer und der dazugehörigen SIM-Karte im Mobilfunknetz verantwortlich. Fallen diese Server aus, kann sich das Mobiltelefon nicht mehr im Netz anmelden. Für den konkreten Fall war das Netz für etwa drei Stunden nicht verfügbar. Über die Schadenhöhe für den Mobilfunkbetreiber sowie für die Kunden lässt sich nichts beziffern.

Der Ausfall eines der Mobilfunknetze war jedoch bei weitem nicht so gravierend wie die Folgen des Elbehochwassers im August 2002. Damit verbunden waren Unterbrechungen in der Stromversorgung, ebenso wie der sporadische Totalausfall der Mobilfunk- und der Festnetze. Diverse Rechenzentren von IT-Dienstleistern und öffentlichen Dienststellen wurden überflutet und waren damit ebenso wie die dazugehörigen Dienste nicht mehr operabel.

[32] Vgl. Der Tagesspiegel (2009)

Als letztes und für den Bewusstseinswandel charakteristisches Beispiel ist der gezielte Angriff auf die Lufthansa-Webseite mittels Denial-of-Service-Attacken (DoS) durch Protestgruppen am 20. Juni 2001 während der Aktionärshauptversammlung. Mit diesem Angriff sollte die Internetseite der Lufthansa blockiert und das IT-System in die Knie gezwungen werden. Damit wollten die Initiatoren gegen die Abschiebung von Asylbewerbern mit Hilfe von Lufthansamaschinen demonstrieren[33].

Die genannten Beispiele sind leider nur Auszüge aus dem breiten Spektrum möglicher Bedrohungen. Die Tabelle 3 zeigt die Ergebnisse der KES-Umfrage aus dem Jahr 2008 zum Thema Gefahrenbereiche. Daran ist zu erkennen, dass Unternehmen einer Vielzahl von Bedrohungen ausgesetzt sind. Generell kann in folgende Gefahrenbereiche zusammenfassend unterschieden werden:

- Höhere Gewalt (Überschwemmung, Streik)
- Technisches Versagen (Hardwaremängel, Softwaremängel)
- Organisatorische Mängel (Mitarbeiter, Mängel in der Dokumentation)
- Fahrlässigkeit (Mitarbeiter, Fehler von Externen)
- Vorsatz (Malware, Manipulation, Bereicherung, Informationsdiebstahl, Sabotage)[34]

Der Bedeutung von Malware[35] wird von den Unternehmen der höchste Stellenwert zugewiesen, dicht gefolgt von den Gefahren, die von den eigenen Mitarbeitern ausgehen.

[33] Vgl. Silberschmidt, R. (2001), S.1f
[34] Dazu zählen insbesondere auch DoS, Hacking, Spoofing und Chipping (Einsatz schadhafter Computerchips).
[35] Zur Gruppe der Schadsoftware gehören Computerviren, -würmer, Trojanische Pferde, Backdoors, Spy- und Adware.

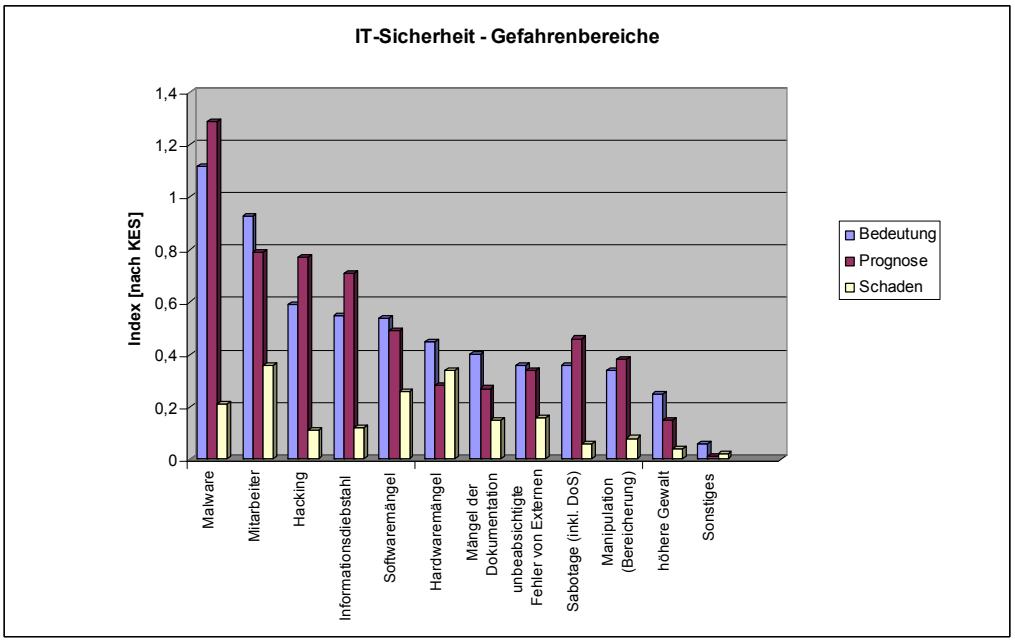

Tabelle 3 - Gefahrenbereiche der IT-Sicherheit[36]

Für die Zukunft wird ein eher gegenläufiger Trend erwartet und mit einem höheren Einfluss von aktiven Angriffen in Form von Hacking, Informationsdiebstahl und Sabotage gerechnet. Dennoch verursachen vor allem Mitarbeiterfehler und Hardwaremängel wirtschaftlich gesehen, immer noch die größten Schäden.

Es ist nicht schwer sich vorzustellen, welche dramatischen Folgen von solcherlei Gefahren auch für die Geoinfomationswirtschaft ausgehen. Der Ausfall von Rechenzentren, die Nichtverfügbarkeit von Geobasisdiensten, Manipulationen an Diensten, Veränderung von Geodaten bzw. das Löschen von Geodaten und die damit möglicherweise einhergehenden Informationsverluste zeigen mögliche Szenarien auch für diesen Wirtschaftsbereich.

Daher ist es unbedingt notwendig, regulativ, mit Hilfe rechtlicher Rahmenbedingungen, einzugreifen, um den Wertschöpfungsprozess auch der Geoinformationswirtschaft zu schützen.

[36] Quelle: eigene Darstellung, angelehnt an Luckardt, N. (2008), S.11

2.4 Rechtliche Rahmenbedingungen

Der Großteil der Geschäftsprozesse basiert heute auf IT-Lösungen. Ziel von IT-Sicherheit muss daher sein, das Risiko von massiven wirtschaftlichen Schäden für ein Unternehmen zu minimieren. Dabei ist es nicht nur vordergründiges Ziel und Aufgabe des Unternehmers sich selbst und damit die eigene Unternehmensexistenz sowie Unternehmensdaten zu schützen, sondern auch, geltende Normative anzuwenden und einzuhalten, um überlassene Daten Dritter zu schützen.

Aus der KES-Studie von 2006 ist zu entnehmen, dass bei weitem nicht alle existierenden internationalen, europäischen und nationalen Gesetze oder Bestimmungen im Bewusstsein der jeweiligen Verantwortlichen angekommen sind.

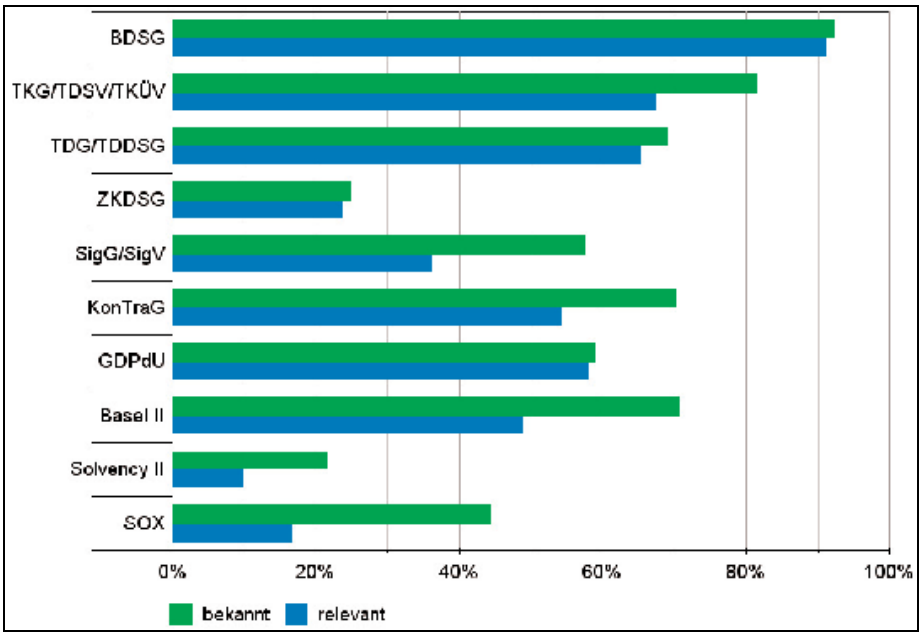

Abbildung 6 - Bekanntheit und Relevanz von Gesetzen und Regularien[37]

Aus Abbildung 4 geht hervor, das mehr als neunzig Prozent der Befragten das Bundesdatenschutzgesetz kennen und es als relevant für ihren Unternehmensbereich einstufen. Die größte Diskrepanz zwischen Bekanntheit und

[37] Quelle: Luckardt, N. (2006), S.13

Relevanz besteht für Deutsches Recht in Bezug auf das Signaturgesetz bzw. die Signaturverordnung.

2.4.1 Sorgfaltspflicht

Das Deutsche Recht bietet kein eigenständiges Regelwerk für die Einhaltung und Ausführung von IT-Sicherheit. Eine Vielzahl von Gesetzen, Verordnungen, Ausführungsbestimmungen und Richtlinien greifen vielmehr ineinander. Den allgemeinen Zusammenhang verdeutlicht zunächst Abbildung 7.

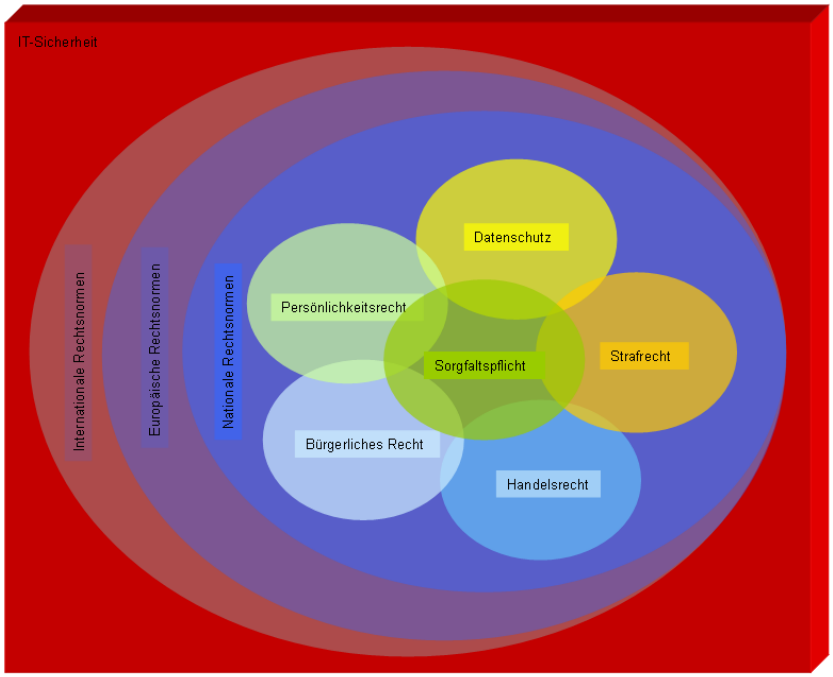

Abbildung 7 - Überblick zusammenhängender Rechtsnormen[38]

Eine einheitliche Grundlage bildet jedoch die gesetzlich bestimmte Sorgfaltspflicht. Bereits das GmbH-Gesetz verpflichtet den oder die Geschäftsführer „die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden“[39] und macht ihn gleichzeitig im Falle einer Verletzung „haftbar“[40]. Ähnliches kann man im Aktiengesetz nachlesen. Dort heißt es, dass für die Vorstandsmitglieder bei der „Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden“[41] ist. Des Weiteren muss ein Überwachungssystem eingerichtet werden, damit für den „Fortbestand der Gesellschaft ge-

[38] Quelle: eigene Darstellung
[39] §43 Abs. 1 GmbHG
[40] §43 Abs. 2 GmbHG
[41] §93 Abs. 1 AktG

fährdende Entwicklungen früh erkannt werden“[42] können. Daneben muss der Abschlussprüfer für eine börsennotierte Aktiengesellschaft im Rahmen seiner Prüfung beurteilen, „ob das einzurichtende Überwachungssystem seine Aufgaben erfüllen kann“[43]. Beide Maßnahmen wurden über das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ergänzt und modifiziert. Zusätzlich gilt für die Beschäftigten eines Unternehmens, die Pflicht zur Wahrung des Geschäfts- und Betriebsgeheimnisses[44].

Daneben existieren verschiedene weitere Gesetze, die durch den jeweiligen Anwenderkreis bzw. durch die zugrunde liegenden Tätigkeitsbereiche adressiert sind. Darunter fallen unter anderem das Gesetz zur Nutzung von Telediensten (TDG), das Telekommunikationsgesetz (TKG) sowie das Telemediengesetz (TMG), die maßgeblich auf den Verbraucherschutz ausgerichtet sind. Weiterhin bestehen umfangreiche Regelwerke aus den Bereichen der Kreditwirtschat (KWG), des Wertpapierhandels (WpHG), des Urheberrechtes (UrhG), des Verwaltungsrechtes (GDPdU) und des Steuerrechtes (AO).

2.4.2 Datenschutz

Einen Schwerpunkt in der rechtlichen Würdigung erfährt der Datenschutz. Ziel der Datenschutzgesetze ist der Schutz von personenbezogenen Daten eines Einzelnen zur Wahrung seiner Persönlichkeitsrechte[45]. Es umfasst ist die Erfassung, Verarbeitung und Weitergabe von diesbezüglichen Informationen und verpflichtet Unternehmen außerdem, die dementsprechende Daten automatisiert verarbeiten, „einen Datenschutzbeauftragten schriftlich zu bestellen“[46] und räumt diesem Kontrollrechte ein[47]. Zudem verpflichtet das Gesetz in der Datenverarbeitung beschäftigte Personen zur Geheimhaltung[48].

Besonders deutlich zeichnet sich der Zusammenhang zwischen Datenschutz und Geoinformationen aus, bei dem sich „kollektive Offenlegungsinteressen“[49] von Staat und Wirtschaft „individuellen Interessen an Geheimhaltung bzw.

[42] §92 Abs. 2 AktG
[43] §317 Abs. 4 HGB
[44] Vgl. §17 UWG
[45] Vgl. §1 Abs. 1 BDSG i.V.m. Art. 1 Abs. 1 GG und Art. 2 Abs. 1 GG
[46] §4f Abs. BDSG
[47] Vgl. §4 Abs. 1 BDSG
[48] Vgl. §5 Satz 2 BDSG
[49] Karg, M.; Weichert, T. (2007), S.9

Zweckbindung“[50] des Einzelnen gegenüberstehen. Es besteht Konsens in dem Willen, politische Entscheidungen auf Basis transparenter und für jedermann zugänglichen (Geo-)Informationen öffentlich zu treffen und zu gestalten. Jedoch stehen auch hier den wirtschaftlich-politischen Interessen von Staat (Refinanzierung) sowie unternehmerischen Interessen (Partizipation) die individuellen Persönlichkeitsrechte des Einzelnen gegenüber[51]. Aktuelles Beispiel für die kontroverse Diskussion um Geoinformation und Datenschutz zeigt die Debatte um die Aufnahme und anschließende Nutzung von Google Street View-Daten in Deutschland, bei denen Datenschützer die Persönlichkeitsrechte enorm beeinträchtigt sahen und das Unternehmen zwangen, dementsprechende Schutzmaßnahmen einzurichten. Nachdem bereits Kennzeichen und Gesichter aus den Aufnahmen entfernt wurden, reagierte Google und schaltete ein Formular online, womit der Nutzung einzelnen Bildern widersprochen und die Löschung veranlasst werden kann. Allerdings liegt die Zahl entsprechender Einwände im Promillebereich[52].

In Deutschland gibt es für die Nutzung von Satellitenbilddaten und der Etablierung von kommerziellen Anbietern zur Gewinnung von Satellitenbildern hoher Auflösung des deutschen Staatsgebietes eine zusätzliche Beschränkung durch das Satellitendatensicherheitsgesetz[53].

Verletzungen der hier aufgeführten Gesetze können umfangreich geahndet werden. Verstöße gegen den Datenschutz beispielsweise, werden bei Vorsatz bzw. Fahrlässigkeit mit Bußgeldern[54] bzw. mit Freiheitsstrafen[55] sanktioniert. Außerdem besteht für den Geschädigten die Möglichkeit, Schadenersatzansprüche geltend zu machen[56].

Zusätzliche Sanktionierungsmöglichkeiten ergeben sich außerdem bei einem schuldhaften Verstoß gegen bestehende allgemein-zivilrechtliche Sicherungspflichten und gegen die einleitend erwähnten Sorgfaltspflichten[57]. Zu Verkehrspflichten, auch als außervertragliche Pflichten bezeichnet, eines Unter-

[50] Vgl. Karg, M.; Weichert, T. (2007), S.9
[51] Karg, M.; Weichert, T. (2007), S.5
[52] Vgl. Financial Times Deutschland (2009)
[53] Vgl. §§3,4,11, 12 SatDSigG
[54] Vgl. §43 BDSG
[55] Vgl. §44 BDSG i.V.m. §43 Abs. 2 BDSG
[56] Vgl. §§7,8 BDSG
[57] Vgl. §280 Abs. 1 BGB i.V.m. §241 Abs. 2 BGB

nehmens gehört beispielsweise der zu erwartende und technisch wie wirtschaftlich zumutbare Einsatz[58] eines Virenscanners mit aktuellen Virensignaturen ebenso wie der adäquate Einsatz einer Firewall. Verstößt ein Unternehmen gegen Verkehrspflichten tritt Haftung und die Verpflichtung zum Schadenersatz ein[59]. Zusätzlich besteht ein Beseitigungs- und Unterlassungsanspruch für den Geschädigten[60].

Besondere Verstöße, die nicht durch die bisher erwähnten zivilrechtlichen Maßnahmen geahndet wurden, finden ihre Würdigung im materiellen Strafrecht[61], insbesondere im Strafgesetzbuch. Unter ausdrücklicher Strafe stehen Delikte wie das (Vorbereiten und) Ausspähen oder Abfangen von Daten[62], die Verletzung von Privat-, Betriebs-, Geschäfts- sowie von Fernmeldegeheimnissen[63], die Verletzung des Lebensbereiches durch Bildaufnahmen[64], Computerbetrug[65], Urkundenfälschung und Fälschung technischer Aufzeichnungen und beweiserheblicher Daten[66], Datenveränderung und Computersabotage[67].

IT-Sicherheit ist im Zuge von Globalisierung nicht ausschließlich an nationalstaatliches Recht gebunden, sondern orientiert und unterwirft sich zusätzlich internationalen und europäischen Rechtsnormen sowie Verordnungen.

Insesondere dem Datenschutz wurde ein hoher Stellenwert innerhalb der Europäischen Union zugewiesen. Dies zeigt sich in den Richtlinien 95/46/EG und 2002/58/EG zum „Schutz der Privatsphäre in der elektronischen Kommunikation“[68] und bei der „Verabeitung personenbezogener Daten im freien Datenverkehr“ [69].

Parallel zu den hier aufgeführten Datenschutzrichtlinien profitiert auch die Geoinformationsbranche im Rahmen des europäischen Normgebungsverfahrens von der für die evident wichtigen Richtlinie

[58] Und damit dem Stand der Technik vergleichbar.
[59] Vgl. §823ff BGB
[60] Vgl. §1004 Abs. 1 Satz 2 BGB und §97 UrhG
[61] Zum materiellen Strafrecht gehören u.a. AO, BDSG und HGB.
[62] Vgl. §§202 a, b, c StGB
[63] Vgl. §§203, 204, 206, §353b StGB
[64] Vgl. §201a StGB
[65] Vgl. §263a StGB
[66] Vgl. §§267, 268, 269 StGB
[67] Vgl. §§303a, b StGB
[68] 2002/58/EG (2002), S.1
[69] 95/46/EG (1995), S.1

2007/2/EG, der sog. INSPIRE-Richtlinie, zur Umsetzung bzw. Schaffung einer Geodateninfrastruktur innnerhalb der Europäischen Gemeinschaft. Diese Richtlinie wird in Deutschland mit Hilfe des Geodatenzugangsgetzes in Wert gesetzt[70]. Sie verpflichtet die Europäsichen Staaten, Geodaten und Geodatendienste im Zuge der behördlichen Vorhaltung innerhalb von Geodateninfrastrukturen grenzüberschreitend standardisiert auszutauschen[71].

[70] Vgl. §§ 1, 2 GeoZG
[71] Vgl. 2007/2/EG, Abs. 3ff

2.5 Allgemeine Sicherheitsstandards

Ziel einer jeden Standardisierung ist die Vereinheitlichung von Vorgängen und Regelungen bezüglich eines Dienstleistungs- oder Warenobjektes. Dies ist insofern nötig, als das am Markt operierenden Unternehmen nicht nur die Möglichkeit der technischen Handhabbarkeit eröffnet wird und damit eine mögliche Partizipation am Marktgeschehen stattfinden kann, sondern auch gleichzeitig die rechtliche Handhabbarkeit und Würdigung gegenüber Unternehmen stattfinden kann, die sich an bestehende Normen und Standards gesetzlich wie vertraglich binden.

Ähnlich wie in Kapitel 2.4 zeigt sich auch hier eine sehr heterogen gewachsene Landschaft an Standards und Normen. Allen gemein ist das Ziel und die Bestrebung, IT-Sicherheit in seinen unterschiedlichen Ausprägungen zu harmonisieren und handhabbar zu gestalten[72]. Dies geschieht auf der einen Seite durch historisch gewachsene, stark national ausgeprägte Sicherheitsinteressen und auf der anderen Seite, bedingt durch die Effekte globaler Märkte, durch internationale Interessens- und Wirtschaftsgemeinschaften und deren dementsprechenden Sicherheitsbedürfnisse.

Institutionen wie das British Standard Institute, das US-amerikanische National Institute of Standard und das Bundesamt für Sicherheit in der Informationstechnik bestimmen in Ihrem Verantwortungsbereich den unter nationalen Sicherheitsaspekten mindestumfänglich zu erzielenden Stand der Technik als Maßstab für die rechtliche Würdigung.

Ergänzt und adaptiert werden diese Regelungen von Organisationen, Initiativen und Normgebungsverfahren auf europäischer und internationaler Ebene. Hier spielen Organisationen wie ISO, IEC, IEEE, ITU, das britische *OGC* und OASIS eine maßgeblich bestimmende Rolle[73].

Die folgende Abbildung zeigt einen Überblick zusammenhängender Sicherheitsstandards und deren Herkunft.

[72] IT-Sicherheit bezieht sich dabei nicht nur auf die Sicherheit des Gesamtsystems, sondern besteht aus der kumulativen Sicherheit seiner Teilkomponenten.
[73] ITU und IEC werden unter dem Dach der ISO vereint.

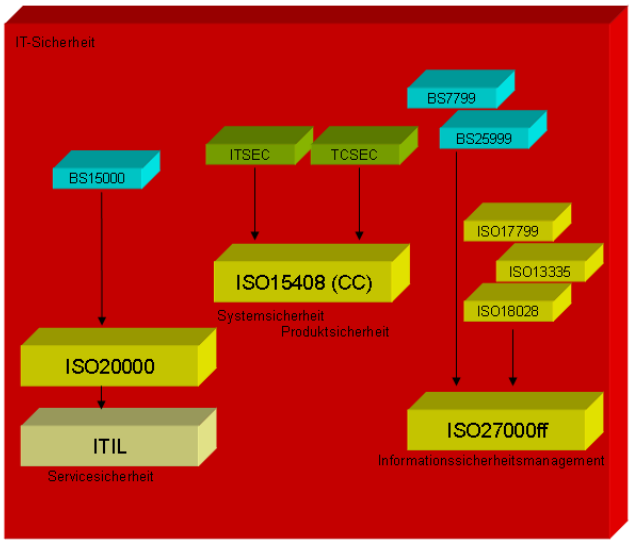

Abbildung 8 - Übersicht Sicherheitsstandards[74]

2.5.1 ITSEC

Erste Harmonisierungsbestrebungen wurden im europäischen Bereich zwischen Deutschland, Frankreich, Großbritannien und den Niederlanden mittels ITSEC im Jahre 1991 umgesetzt. Sie dient der Zertifizierung von Systemen oder Produkten und bewertet diese im Wesentlichen nach den Kriterien von Funktionalität und Vertrauenswürdigkeit. Letzteres erfährt einer weiteren Unterscheidung nach Wirksamkeit und Korrektheit.

Die Tabelle 4 zeigt die zehn Funktionalitätsklassen im Überblick. Die Klassen FC-1 bis FB-3 sind dabei hierarchisch geordnet. Diese fünf Klassen wurden um die Belange der Integrität, der Verfügbarkeit und der Datenübertragung im Zuge der Harmonisierung mit anderen Sicherheitsrichtlinien ergänzt[75].

F-Klasse	Funktion	Bedeutung
F-C1	Funktionalität	einfache Zugriffskontrolle
F-C2		Nutzeridentifizierung, einfache Protokollierung, Trennung von Betriebsmitteln
F-B1		Regelbasierte Zugriffskontrolle
F-B2		Referenz-Monitor-Konzept, umfangreiche Protokollierung
F-B3		Erweiterung um Admin-Rollen, detaillierte Protokollauswertung, Nachvollziehbarkeit der Bedrohung

[74] Quelle: eigene Darstellung
[75] Vgl. ITSEC (1991), S.121

F-IN	Integrität	Datenkonsistenz
F-AV	Verfügbarkeit	Fehlerüberbrückung, Ausfallwahrscheinlichkeit
F-DI	Datenübertragung	Integrität der übertragenen Information (Fehlererkennung und Behebung)
F-DC		Vertraulichkeit der übertragenen Information (Verschlüsselung)
F-DX		Sicherheit bei der Übertragung innerhalb von Netzwerken

Tabelle 4 - ITSEC - Funktionsklassen[76]

Das Maß der Wirksamkeit kann in Form der Möglichkeit der Abwehr von Gefahren beschrieben werden und wird nach ITSEC in *niedrig*, *mittel* und *hoch* unterschieden[77]. Die zusätzlich mögliche Bewertung der Korrektheit erfolgt bei ITSEC durch sieben Evaluationsstufen, die in Tabelle 5 zusammengefasst wurden.

F-Klasse	Bedeutung
E0	Unzureichend
E1	Sicherheitsvorgaben, funktionale Tests
E2	zusätzlich informelle Beschreibung des Feinentwurfes
E3	zusätzlich Bewertung von Quellcode und Hardwarekonfiguration
E4	zusätzlich formales Sicherheitsmodell, semiformale Notation
E5	Konsistenz zwischen Quellcode, Konfiguration und Feinentwurf
E6	formale Spezifikation entspricht formalen Sicherheitsvorgaben

Tabelle 5 - ITSEC - Evaluationsstufen[78]

Die von der ITSEC aufgestellten Sicherheitskriterien wurden 2006 in einer weiteren Harmonisierungsstufe mit den amerikanischen und kanadischen Kri-

[76] Quelle: eigene Darstellung, angelehnt ITSEC (1991), S.122ff
[77] Vgl. ITSEC (1991), S.36
[78] Quelle: eigene Darstellung, angelehnt an ITSEC (1991), S.45f

terien zur *Common Criteria* vereinigt[79]. Eine Zertifizierung nach ITSEC ist dennoch weiterhin mit Blick auf den Europäischen Wirtschaftraum möglich.

2.5.2 Common Criteria

Die Common Criteria für Information Technology Security Evaluation liegen als internationaler Standard ISO/IEC15408 in Version 3.1 seit 1999 vor. Die CC verfolgen das Ziel einer einheitlichen Zertifizierung von Informationssicherheit bei der Verarbeitung von Daten in Computersystemen. Im Wesentlichen besteht CC aus drei Teilen[80]:

- Einführung und allgemeines Modell
- Funktionale Sicherheitsanforderungen
- Anforderungen an die Vertrauenswürdigkeit

Ebenso wie in ITSEC und TCSEC wird zunächst der generelle Sicherheitsbedarf festgestellt und dementsprechende Sicherheitsvorgaben deklariert. Daraus lassen sich im Anschluss funktionale Sicherheitsanforderungen ableiten und zu komponentenübergreifenden bzw. korrespondierenden Funktionalitätsklassen zusammenfassen. Tabelle 6 zeigt die dementsprechenden Klassen.

F-Klasse	Beschreibung
FAU	Sicherheitsprotokollierung
FCO	Kommunikation
FCS	Kryptographische Unterstützung
FDP	Schutz der Benutzerdaten
FIA	Identifikation und Authentisierung
FMT	Sicherheitsmanagement
FÜR	Privatsphäre
FPT	Schutz der Sicherheitsfunktionen
FRU	Betriebsmittelnutzung
FTA	Schnittstelle
FTP	vertrauenswürdiger Pfad/Kanal

Tabelle 6 – CC - Funktionalitätsklassen[81]

Die Funktionalitätsklassen werden in Sicherheitsprofilen für die verschiedenen Komponenten eines IT-Systems organisiert. Diese Komponenten können wie-

[79] Vgl. BSI (2001), S.1
[80] Vgl ISO/IEC (2006a), S.3
[81] Quelle: eigene Darstellung, angelehnt an ISO/IEC (2006b), S.29ff

derum in einer dementsprechenden Prüftiefe von eins bis sieben evaluiert werden. Eine Übersicht kann Tabelle 7 entnommen werden.

EAL-Klasse	Bedeutung
EAL1	funktionell getestet
EAL2	strukturell getestet
EAL3	methodisch getestet und geprüft
EAL4	methodisch entwickelt, getestet und geprüft
EAL5	semiformal entwickelt und getestet
EAL6	semiformal überprüfter und getesteter Entwurf
EAL7	formal überprüfter und getesteter Entwurf

Tabelle 7 – CC- Evaluierungsgrade[82]

In einem weiteren unabhängigen Teil werden die Zertifizierungsmechanismen und –methoden beschrieben, die die Basis für eine Evaluierung unter CC bilden.

2.5.3 ISO/IEC27000ff

Die Familie der ISO-Norm 27000ff besteht im Wesentlichen aus zehn Normen und beschäftigt sich mit der organisationsübergreifenden Implementierung und Evaluierung von IT-Sicherheit auf Basis eines Informationssicherheitsmanagementsystems. Einen Überblick über relevant-verfügbare Normen bietet Tabelle 8.

Norm	Bezeichnung	Referenz
ISO/IEC 27000	Grundlagen und Begriffe	
ISO/IEC 27001	Informationssicherheitsmanagementsystem (ISMS), Grundlagen und Voraussetzungen	BS 7799:2:2005
ISO/IEC 27002	Kontrollmechanismen für IT-Sicherheit	ISO/IEC 17799:2005
ISO/IEC 27003	ISMS – Implementierungsrichtlinien	
ISO/IEC 27004	ISMS – Kennzahlen	
ISO/IEC 27005	Informationssicherheitsrisikomanagementsystem (ISRMS)	ISO/IEC 13335:2
ISO/IEC 27006	Grundlagen für Auditierung und Zertifizierung von ISRMS	
ISO/IEC 27031	Betriebliches Kontinuitätsmanagement (Business Continuity)	BS 25999
ISO/IEC 27033	Richtlinien für Netzwerksicherheit (Design, Risiken, Kontrolle)	ISO 18028
ISO/IEC 27034	Richtlinien für Applikationssicherheit	

Tabelle 8 - ISO27000ff - Überblick[83]

[82] Quelle: eigene Darstellung, angelehnt an ISO/IEC (2006c), S.31

Das Informationssicherheitsmanagementsystem ist die elementare Voraussetzung, um nicht nur in heterogenen Systemlandschaften, Sicherheit für das IT-System und die zu verarbeitender Informationen zu erzielen, sondern frühzeitig Sicherheit in die allgemeinen Managementprozesse eines Unternehmens zu integrieren, um eine dauerhafte betriebliche Existenz gewährleisten zu können[84].

Die Ableitung von Sicherheitsstrategien aus den für das Unternehmen elementaren Sicherheitszielen wird mit Hilfe von ISMS gewährleistet. Gleichfalls werden die Grundlagen für die Implementierung und Überwachung definiert. Die Überwachung von Sicherheitsrisiken bzw. Sicherheitsgefahren[85], wird durch das Informationssicherheitsrisikomanagementsystem gewährleistet. Dementsprechende Vorgaben für Komponenten von IT-Systemen, zu Gewährleistung von Sicherheitsvorgaben[86], werden beispielweise für Applikationen und Netzwerke in Einzelstandards vereinbart.

Wesentlich ist die Definition des Vorgehensmodells bzw. des Standardverfahrens für die kontinuierliche Überprüfung und Validierung der implementierten Sicherheitsarchitektur nach dem PDCA-Zyklus[87]. Nach entsprechender Risikoanalyse und veränderter Sicherheitslage müssen neue oder geänderte Sicherheitsrisiken im ISMS geplant (Plan), umgesetzt (Do), überprüft (Check) und nach einer erneuten Überprüfung (Act) in Wert gesetzt werden.

2.5.4 ISO/IEC20000/ITIL

Der aktuelle ITIL-Standard[88] in der Version drei, mit Stand von Juni 2007, befasst sich in mehreren Büchern mit IT-Service Management. Ihm zu Grunde liegen die wesentlichen Erfahrungen des britischen *OGC* für „die wirtschaftliche und zweckmäßige Erbringung von IT-Dienstleistungen“[89]. ITIL zeichnet sich durch seine Kompatibilität zum ISO 20000 Standard aus, der als wesent-

[83] Quelle: eigene Darstellung, angelehnt an Andenmatten, M. (2008), S.434
[84] Vgl. Kapitel 2.4 Rechtliche Rahmenbedingungen
[85] Vgl. Kapitel 2.3 Informationstechnische Bedrohungslage
[86] Vgl. Kapitel 2.5.2 Common Criteria
[87] Vgl. Kapitel 2.5.4.4 Servicebetrieb und Serviceverbesserung
[88] Gemein wird dieser Standard als „Best Practice“ - Referenzmodell bezeichnet.
[89] Vgl. Böttcher, R. (2008), S.1

liche Basis für Zertifizierungen im Bereich des IT-Service Managements gilt[90]. Formal geht die ISO 20000 auf den alten British Standard 15000 zurück, der im Jahr 2005 überführt wurde.

Im Blickpunkt von ITIL steht, wie Abbildung 1 zeigt, der Lebenszyklus von Services auf Basis einer *Servicestrategie*, des daraus resultierenden *Serviceentwurfes*, der anschließenden *Serviceüberführung* und des finalen *Servicebetriebes*. Alle Kernprozesse[91] werden einem *kontinuierlichen Verbesserungsprozess* auf Basis von Messungen und Beurteilungen unterworfen. Dies führt letztlich zur Lebenszyklusbildung von IT-Services.

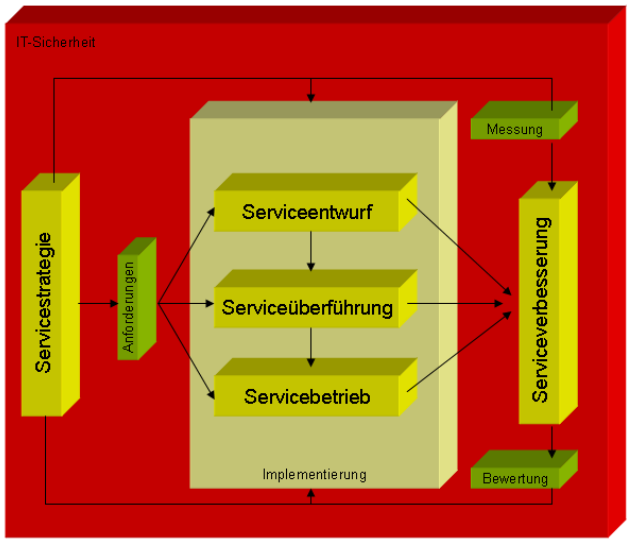

Abbildung 9 - Lebenszyklus von IT-Services[92]

2.5.4.1 Servicestrategie

Die *Servicestrategie* ist eng mit der Geschäfts- und Unternehmensstrategie verbunden. Sie vereint Zweckmäßigkeits- und Gebrauchstauglichkeitsbewertung eines Service und führt zu dem für das Unternehmen resultierenden strategischen Nutzwert[93]. Eng verbunden sind damit Prozesse wie das Service Portfolio Management[94] und das Financial Management[95].

[90] Vgl. ebd. S.164f
[91] Die Kernprozesse sind gem. ITIL in gleichlautenden Kernpublikationen veröffentlicht.
[92] Quelle: eigene Darstellung, angelehnt Glenfis AG (Hg.) (2009)
[93] Vgl. Böttcher, R. (2008), S.16
[94] Vgl. Kapitel 2.2.1 Service Level Agreements
[95] Vgl. *OGC* (2007e), S.98

2.5.4.2 Serviceentwurf

Aus der Servicestrategie kann unmittelbar der *Serviceentwurf* entwickelt bzw. abgeleitet werden. Es handelt sich bei dem Entwurf um eine Sammlung von formalen Managementprozessen, die wie folgt zusammengefasst werden können[96]:

- Servicekatalogmanagement
- Servicelevelmanagement
- Kapazitätsmanagement
- Verfügbarkeitsmanagement
- Kontinuitätsmanagment
- Informationssicherheitsmanagement
- Unterstützungsmanagement

Das Katalogmanagement übernimmt die Festschreibung des Leistungsspektrums aller verfügbaren Services[97]. Das Servicelevelmanagement stellt dieses Leistungsvermögen den Kundenanforderungen gegenüber und setzt es vertraglich in Wert. Außerdem definiert es qualitativ messbare Serviceleistungsparameter sowie die dazugehörige Erfassungsmethodik[98].

Mit Hilfe des Kapazitätsmanagements lassen sich ressourcenbedingte bzw. serviceimmanente Leistungsengpässe sowie Leistungsressourcen bei der Erbringung von IT-Services überwachen, in dem die zuvor definierten und ermittelten Serviceleistungsparameter den Leistungsparametern aus den Kundenanforderungen gegenübergestellt werden. Auftretende Abweichungen lassen sich formal-analytisch bestimmen und können damit wiederum Grundlage für die Minimierung oder Erweiterung von Kapazitäten bzw. von Effizienzsteigerung sein.

Generell ist die Bereitstellung von Services nicht ausschließlich von verfügbaren Kapazitäten abhängig, sondern wird, wie bereits in Kapitel 2.1.1 beschrieben, durch die Kennzahlen des Verfügbarkeitsmanagements definiert und beinhaltet nicht nur Angaben zu Verfügbarkeit, sondern auch zu Zuverlässig-

[96] Vgl. *OGC* (2007d), S.19
[97] Vgl. Kapitel 2.2.2 Servicekatalog und Servicebeschreibung
[98] Dies wird auch als Service Level Reporting bezeichnet.

keit, Wartbarkeit und Servicefähigkeit sowie zu dementsprechenden Auswirkungsanalysen.

Für den Fall von extremen Störungen des Geschäftsbetriebes, zum Beispiel durch eine Naturkatastrophe, ist das Kontinuitätsmanagement und die daraus abzuleitende Strategie für die Wiederherstellung[99] der für den Service benötigten IT-Infrastruktur verantwortlich. Eng damit verbunden ist das Informationssicherheitsmanagement[100], welches zum Ziel hat, nach bestimmten Vorgehensmustern, die Grundsätze der IT-Sicherheit auch im Servicemanagement umzusetzen[101].

2.5.4.3 Serviceübertragung

Unter Beachtung des zuvor erwähnten Entwurfes, werden Services im Anschluss finalisiert und dem operativen Geschäft übergeben. Diese *Serviceübertragung* ist elementar verbunden mit der kontinuierlichen Leistungsbewertung bezüglich zuvor definierter SLR und SLA und auf ständigen Abgleich zwischen beiden fokussiert. Unter dem Aspekt der dauerhaften Minimierung von Einflussfaktoren auf den laufenden Geschäftsbetrieb vereint der Prozess der Serviceübertragung Methoden des Qualitäts-, Risiko- und Projektmanagements. Zu den kritischen Bereichen zählen insbesondere das Veränderungsmanagement, das Releasemanagement[102], das Konfigurationsmanagement und die Servicevalidierung.

Das Veränderungsmanagement umfasst die von Nutzern gestellten Veränderungsanfragen[103] einschließlich aller Komponenten, fasst diese zusammen, bewertet, koordiniert dementsprechende Implementierungen und bildet die Basis für die Lebenszyklusorientierung von Services[104]. Veränderungsanfragen bedingen oftmals auch infrastrukturelle Veränderungen bzw. Maßnahmen. Daher ist es in diesem Zusammenhang nötig, die vorhandene bzw. resultierende Infrastruktur zu erfassen und zu optimieren. Dies geschieht im Rahmen des Konfigurationsmanagements, da nur an einer vernünftig dokumentierten IT-Infrastruktur kontrollierte und nachhaltige Veränderungen statt-

[99] Als Synonym dient in diesem Zusammenhang der Begriff *Recovery.*
[100] Vgl. 2.5.3 Kapitel ISO/IEC27000ff
[101] Vgl. Kapitel 2.6 Servicesicherheit und Risikomanagement
[102] Vgl. *OGC* (2007a), S.62
[103] Diese werden als *Request for Change* (RfC) bezeichnet.
[104] Vgl. Abbildung 9 - Lebenszyklus von IT-Services

finden und dementsprechende Auswirkungen untersucht werden können. Die Umsetzung solcher Veränderungen erfolgt zu einem, im Rahmen des Übertragungsmanagements zu terminierenden Zeitfenster; in Form von Releases nach speziellen Richtlinien. Diese umfassen zusammengehörige hardware- und/oder softwareseitige Veränderungsmaßnahmen. Im Anschluss werden die Veränderungen unter Berücksichtigung bestehender SLR und SLA validiert.

2.5.4.4 Servicebetrieb und Serviceverbesserung

Für den finalen und damit operationellen Betrieb ist es nötig, von Kunden geforderte IT-Services sowie deren zugrunde liegende Ressourcen zu beobachten. Dafür existiert das Eventmanagement. Auf Basis von Statusinformationen von ausgewählten IT-Komponenten kann die Servicefähigkeit beurteilt werden. Sofern Ereignisse[105] vorliegen, die den operationellen Betrieb beeinträchtigen könnten oder sogar verhindern[106], wird mit Hilfe des *Incident Managements*, unter Zuhilfenahme spezieller Szenarien und daraus abgeleiteter Modelle, versucht, die Beeinträchtigung innerhalb vereinbarter Zeitfenster zu beseitigen. Sofern das nicht möglich ist, wird dieser Incident dem *Problemmanagement* übergeben[107] und versucht, der noch unbekannten Ursache anhand von systematischen Lösungsmustern zu begegnen[108]. Bleibt der für den laufenden Betrieb von IT-Services zu überwachende Zugriffschutz und die Rechteverwaltung, welche beide vom Zugriffsmanagement übernommen werden.

[105] Vgl. *OGC* (2007d), S.298 – vergleichbar mit dem Begriff „Events“
[106] Vgl. ebd. S.298, analog dem Begriff „Incidents“
[107] Vgl. *OGC* (2007b), S.128
[108] Vgl. *OGC* (2007c), S.60

2.6 Servicesicherheit und Risikomanagement

Grundlegendes Ziel von IT-Sicherheit ist es, den laufenden Geschäftsbetrieb mit den zur Verfügung stehenden Regelwerken, Frameworks und *Best-Practice-Methoden* aufrecht zu erhalten, um einer vertraglichen Verantwortung, der Bereitstellung von Services, Rechnung zu tragen[109]. Dafür ist es nötig, die in Kapitel 2.1 beschriebenen Sicherheitsziele stringent durch eine dementsprechende Sicherheitspolitik umzusetzen. Für den Fall, dass diese Ziele gefährdet sind, müssen etwaige Sicherheitsrisiken identifiziert, ihre Auswirkung beurteilt[110] und entsprechende Gegenmaßnahmen definiert und eingeleitet werden. Abstrahiert betrachtet, ist das die Aufgabe des Risikomanagements. Den Zusammenhang verdeutlicht Abbildung 10 – Risikomanagementprozess schematisch.

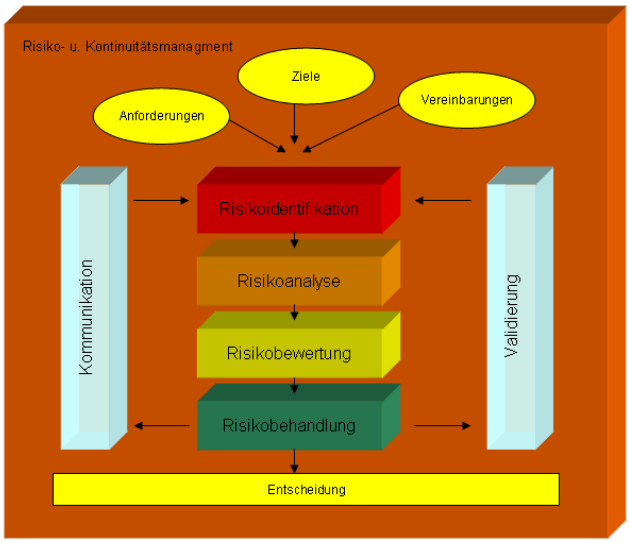

Abbildung 10 – Risikomanagementprozess[111]

Für den Gesamtprozess ist es wichtig, dass die Ergebnisse dauerhaft kommuniziert, in betriebliche Abläufe integriert und in einem kontinuierlichen Prozess auf ihre Gültigkeit überprüft werden[112].

[109] In diesem Fall spricht man von Business Continuity. Vgl. Kapitel 2 Theoretische Grundlagen
[110] In diesem Zusammenhang spricht man auch von Verletzlichkeit eines Systems (Vulnerabilität).
[111] Quelle: eigene Darstellung, angelehnt an Witt, B.(2006), S.100
[112] In Analogie zum Lebenszyklus von IT-Services, siehe Abbildung 9 - Lebenszyklus von IT-Services

2.6.1 Risikoidentifikation und Analyse

Die umfassende Identifikation von Risiken ist die Grundlage für einen kontinuierlichen Servicebetrieb- und damit auch für den Geschäftsbetrieb. Risiken können dabei definiert werden „aus der potentiellen Möglichkeit, dass eine Bedrohung die Schwachstelle(n) eines oder mehrerer schutzbedürftiger Wertobjekte (Assets) bzw. Schutzobjekte ausnutzt, sodass ein materieller oder immaterieller Schaden entsteht.“[113]. Dementsprechende Risikofaktoren betreffen demnach alle Komponenten eines Systems und lassen sich in der Praxis qualitativ und quantitativ bestimmen durch:

- Technische, rechtliche und wirtschaftliche Analysen
- Mitarbeiterbefragungen
- Marktbeobachtungen
- Kundenbefragungen

Mitarbeiterbefragungen liefern Ergebnisse von Beteiligten am eigentlichen Wertschöpfungsprozess. Marktbeobachtungen dienen der Analyse technischer, rechtlicher und/oder wirtschaftlicher Marktaspekte und bilden die Grundlage für vertiefende technische Analysen des vorhandenen Systems[114], rechtlicher Analysen des bestehenden Vertragswerkes[115] und wirtschaftlicher Analysen in Bezug auf das Wertschöpfungspotential. Die diesbezügliche Risikoanalyse fasst die Ergebnisse aus den verschiedenen Teilbereichen des Service Managements zusammen und leitet diese an das übergeordnete Risikomanagement weiter. Für die einzelnen Teilbereiche sind das im Wesentlichen:

- Verfügbarkeitsanalyse
- Servicelevelanalyse
- Kapazitätsanalyse
- Veränderungsanalyse
- Kontinuitätsanalyse

[113] Vgl. Müller, K.-R. (2008), S.29
[114] Vgl. Kapitel 2.5.4 ISO/IEC20000/ITIL
[115] Vgl. Kapitel 2.4 Rechtliche Rahmenbedingungen

Für die technischen Analysen stehen verschiedene, etablierte Verfahren zur Verfügung, die der Identifikation von Schwachstellen dienen. Tabelle 9 zeigt dazu einen Überblick.

Methode	Quantitativ	Qualitativ
Bottom-up	Ereignisbaumanalyse	Szenario-Analyse
	Fehler-Effekt- und Ausfallanalyse	Prozessrisiko-Analyse
	Simulationsmodell	Expertenbefragung
Top-down	Fehlerbaum-Analyse	Key-Performance-Indikatoren
	Risiko-Datenbank	Key-Control-Indikator
	Zufallsverteilungen	Key-Risk-Indikator
	Extremwert-Theorie	Nutzwert-Analyse

Tabelle 9 – Risikoanalyseverfahren[116]

Bei der *Fehlerbaumanalyse* (FTA) werden ausgehend von einem Schadereignis alle zu Grunde liegenden, gleichzeitig auftretenden, unabhängigen Ereignisse, die zum Eintreten des Schadens geführt haben, betrachtet. Für das Schadereignis kann dann die Eintrittswahrscheinlichkeit aus der Summe aller Produkte unabhängiger Ereignisse bestimmt werden. Führt nur ein einziges Ereignis zu einem Schaden, spricht man von einem *Single Point of Failure* (SPoF)[117]. Ziel in einem weiteren Verfahren ist es, diese SPoF (zum Beispiel durch Redundanz) zu minimieren.

Die *Ereignisbaumanalyse* verkehrt das Prinzip der Fehlerbaumanalyse indem hier ein einzelnes Ereignis die Grundlage für die Betrachtung ist und analysiert wird, welche Folgen dieses Ereignis im Restsystem auslöst[118].

In der Anwendungsentwicklung existiert noch ein weit verbreitetes Analyseverfahren zur Bedrohungsmodellierung mit dem Namen *STRIDE*. Ziel von STRIDE ist es, ein vorhandenes System in seine einzelnen Komponenten zu zerlegen und diese auf die in Tabelle 10 bezeichneten Bedrohungen zu testen. Damit soll sichergestellt werden, das das Gesamtsystem (und damit die Summe aller Komponenten), die in Kapitel 2.1 beschriebenen Sicherheitsanforderungen (Sicherheitseigenschaften) entspricht. Das ideal geschützte Sys-

[116] Quelle: eigene Darstellung, angelehnt an Königs, H.-P. (2006), S.37
[117] Vgl. Königs, H.-P. (2006), S.176ff
[118] Vgl. ebd. S.184

tem ist geschaffen, wenn alle Komponenten alle Sicherheitseigenschaften besitzen.

Bedrohung	Sicherheitseigenschaft
Spoofing (Verschleierung)	Authentifizierung
Tempering (Datenmanipulation)	Integrität
Repudiation (Nichtanerkennung)	Nichtabstreitbarkeit
Information Disclosure (Veröffentlichen von Informationen)	Vertraulichkeit
Denial of Service (Dienstverweigerung)	Verfügbarkeit
Elevation of Privilege (Rechteerweiterungen)	Autorisierung

Tabelle 10 - Risikoanalyse nach STRIDE[119]

2.6.2 Risikobewertung und Behandlung

Die Risikobewertung wird auf Grund der in der Risikoanalyse berechneten, geschätzten oder simulierten Eintrittswahrscheinlichkeiten von Schadereignissen abgeleitet. Oftmals existieren für verschiedene Anwendungsbereiche Datenbanken mit entsprechenden Kennzahlensystemen, um das Risiko eines Schadensereignisses bestimmen zu können. Beispiele dafür sind:

- Common Weakness Enumeration (CWE)[120]
- Open Web Application Security Project (OWASP)[121]
- Common Vulnerability Scoring System (CVSS)[122]

Das Ergebnis ist in Auswertung der Kennzahlen eine Risikolandkarte (Risk Map) oder Risikomatrix, bei der die Schadensereignisse den Servicelevels gegenübergestellt werden. Daraus wiederum lassen sich Aussagen zur Servicefähigkeit und letztlich zur Geschäftsfähigkeit eines Unternehmens treffen. Entsprechende Wertungen müssen kommuniziert und mit den Verantwortlichen in den unterschiedlichen Servicemanagements abgestimmt werden. Von dort aus werden die nötigen Veränderungen in den jeweiligen Bereichen (Sicherheit, Verfügbarkeit, Kapazität, Support, Servicelevel) durchgeführt und evaluiert.

[119] Quelle: eigene Darstellung, angelehnt an Hernan, S. et al. (2006)
[120] Vgl. http://cwe.mitre.org/, zuletzt geprüft am:20.5.2009
[121] Vgl. http://www.owasp.org, zuletzt geprüft am 20.5.2009
[122] Vgl. http://www.first.org/cvss, zuletzt geprüft am 20.5.2009

Teilweise lassen sich allerdings für bestimmte Kriterien keine Kennzahlen gewinnen. Image- bzw. Reputationsverluste sind häufig nicht messbar, sondern spiegeln sich erst später in der allgemeinen Auftragslage des Unternehmens wider. Haftungsansprüche aus nicht erbrachten Leistungen ziehen oftmals eine spätere Kürzung von Versicherungsleistungen nach sich oder gehen mit veränderten Liquiditätseinschätzungen des Unternehmens einher.

Damit wird das Risikomanagement von IT-Services zur Grundvoraussetzung für das gesamtbetriebliche Kontinuitätsmanagement.

2.7 Webservices

Die vorangegangenen Kapitel beschäftigten sich mit der Klassifikation und Normierung von allgemeinen IT-Servicedienstleistungen als Basis für den kontinuierlichen Geschäftsbetrieb. Diese Serviceleistungen müssen nun im Folgenden technisch in Wert gesetzt werden.

Die grundlegende Idee serviceorientierter Architekturen (SOA) war es, in einem verteilten System, autonom Services zu suchen, anzubieten und zu nutzen. Autonom bedeutet in diesem Zusammenhang, dass diese Services lose voneinander gekoppelt sind und hinter den Diensten stehende Applikationen zu einem beliebigen Zeitpunkt auf diese Dienste zurückgreifen können. Mit diesem Zugriff werden komplexe Funktionalitäten durch Dienste granularisiert.

Allgemein versteht man unter einer SOA „eine Systemarchitektur, die vielfältige, verschiedene und eventuell inkompatible Methoden oder Applikationen als wieder verwendbare und offen zugreifbare Dienste repräsentiert und dadurch eine plattform- und sprachenunabhängige Nutzung und Wiederverwendung findet.“[123]

Serviceorientierte Architekturen können in verschiedenen Formen technisch ausgeprägt werden. Eine spezifizierte Ausprägungsform von SOA, neben COM/DCOM und CORBA, ist der Webservice[124].

2.7.1 Rollenkonzept von Webservices

Eine grundlegende Definition von Webservices liefert das W3C:

„A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, using HTTP with an XML serialization in conjunction with other Web-related standards.“[125]

[123] Melzer, I. (2008), S.13
[124] Vgl. Melzer, I. (2008), S.66
[125] W3C (2004), S.7

Damit ist ein Webservice spezifiziert durch:

- den Austausch von Informationen zwischen Diensten mit Hilfe des Simple Object Protocol (SOAP),
- die Beschreibung von Metadaten eines Dienstes durch die Web Service Description Language (WSDL),
- die Vermittlung und den Transport von SOAP über das Hyper Text Transfer Protocol (HTTP).

SOAP und WSDL sind XML-basiert und erfüllen damit die Forderung nach maschinenlesbarer Interaktion, sowohl als Nachrichtenformat wie auch als Beschreibungssprache. Der Verzeichnisdienst UDDI, für den Zugriff auf Verzeichnisse sowie die Struktur für Webservices mit Hilfe Universal Description, Discovery and Integration Protocol (UDDI) verantwortlich, geht nicht unmittelbar aus der Definition hervor, sondern wurde getrennt vom W3C durch OASIS spezifiziert[126].

Mit Hilfe des Kommunikationsprotokolls, der Beschreibungssprache und des Verzeichnisdienstes lassen sich nun die drei wesentlichen Rollen einer serviceorientierten Architektur mit Hilfe eines Webservice wie in Abbildung 11 darstellen.

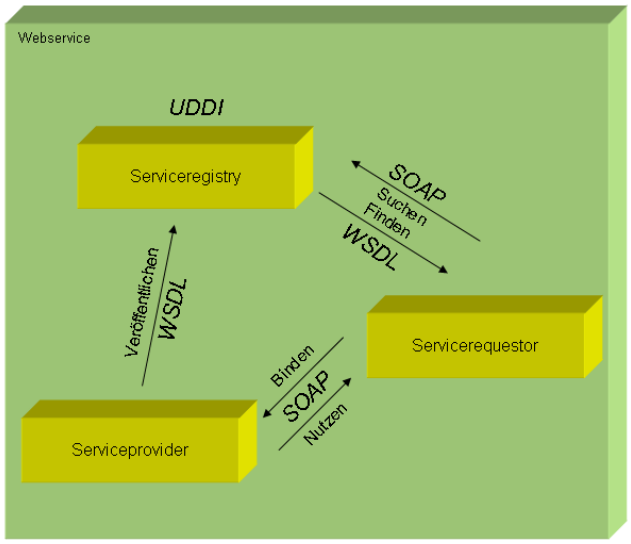

Abbildung 11 – Webservice - Architektur[127]

[126] Vgl. Gaulke, W. (2006), S.9
[127] Quelle: eigene Darstellung, angelehnt an Dustdar, S. (2003), S.114

Der Serviceprovider (Dienstanbieter) veröffentlicht eine Beschreibung seines Dienstes in einer Serviceregistry (Dienstverzeichnis) und stellt diesen zur Verfügung. In dieser Registry kann der Servicerequestor (Dienstnutzer) nach entsprechenden Services (Diensten) suchen. Wird ein dementsprechender Service gefunden, wird der Servicerequestor mit dem Serviceprovider verbunden und kann im Anschluss die Funktionalitäten des angebotenen Services nutzen. Sofern der Servicerequestor seinen Serviceprovider und dessen Services kennt, kann auf eine Serviceregistry (UDDI) verzichtet werden.

Architektonisch lassen sich diese Kommunikationsbeziehungen auf die technologische Ausprägung von Komponenten verteilter Systeme anwenden. Der Serviceprovider wird durch das Verfügbarhalten und Bereitstellen von Diensten und damit von Funktionalitäten bzw. von Daten zum Server, der Servicerequestor zu einem dementsprechend korrespondierend nachfragenden Clienten. Allein die Mächtigkeit der jeweiligen Ressourcen von Client bzw. Server entscheidet über die Repräsentationsart verteilter Systeme. Die klassische Ausprägung findet zweischichtig zwischen einem Clienten und einem Datenserver statt und kann mit zunehmender Komplexität und Art der zu bewältigenden Anfragen der Clienten bzw. korrelierend-nachgefragter Daten, um dementsprechende Applikationsserver bzw. Webserver erweitert werden.

2.7.2 Schichtenmodell von Webservices

Die in der Definition des Webservice enthaltenen Spezifikationen und Technologien lassen sich mit Hilfe des dazugehörigen Schichtenmodells darstellen.

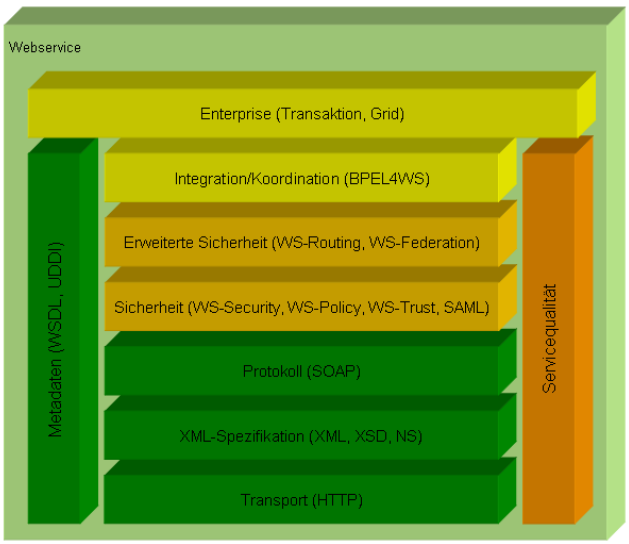

Abbildung 12 - Webservice – Schichtenmodell[128]

Wie Abbildung 12 zeigt, definiert die unterste Schicht die Transportschicht. Darauf folgt die XML-Spezifikation als Grundlage für die Definition der Datenstruktur, der eigentlichen Nachricht und des dazugehörigen Nachrichtenprotokolls. Die darauf folgenden Schichten dienen der Sicherheit, insbesondere im Bereich von Authentisierung und Autorisierung auf Basis von XML, der unabhängigen Integration und Koordination von Webservices und in der obersten Schicht, der dezentralen Steuerung und interaktiven sowie autonomen Nutzung von Webservices über Systemgrenzen hinweg.

Flankiert werden die horizontalen Schichten auf der einen Seite durch Metadatenelemente mit Informationen zur Servicebeschreibung und Serviceverzeichnis[129] und auf der anderen Seite durch Parameter, die die Qualität von Services beschreiben.

Zu diesen Qualitätsparametern gehören Verfügbarkeit, Zugänglichkeit, Integrität, Geschwindigkeit, Zuverlässigkeit, Kapazität, Sicherheit und Interoperabilität. Solche Parameter finden sich nicht nur als Einzeldefinitionen zur Qualität von Webservices durch das W3C[130] oder IBM[131] definiert, sondern auch in einem wesentlich übergeordneterem und auf deutliche Verzahnung zum Ser-

[128] Quelle: eigene Darstellung, angelehnt an Melzer, I. (2008), S.58
[129] Vgl. Kapitel 2.2.2 Servicekatalog und Servicebeschreibung
[130] Vgl. W3C (2003), S.1f
[131] Vgl. Mani, A.; Nagarajan A. (2002), S.1f

vicemanagement ausgerichtetem *Quality Model for Web Services* (WSQM)[132] von OASIS wieder.

2.7.3 Qualität von Webservices

Die im vorangegangenen Kapitel beschriebenen Qualitätsparameter sind deckungsgleich mit den Definitionen der Sicherheitseigenschaften aus dem Kapitel 2.1 und erweitern diese auf spezielle Webservice-zentrierte Eigenschaften und Metriken. Das zugehörige Qualitätsmodell orientiert sich außerordentlich stark an den Prozessen, Definitionen und Rollen der ISO20000 und damit am allgemeinen IT-Servicemanagement nach ITIL[133]. Es definiert die aufeinander aufbauenden Schichten von Qualität im Folgenden als[134]:

- Business Value Quality
- Service Level Measurement Quality
- Interoperability Quality
- Business Processing Quality
- Manageability Quality
- Security Quality

Die *Business Value Quality* beschreibt die Qualität der Geschäftswerte. Dies bedeutet nichts anderes als eine Bewertung, wann ein Webservice als Service überhaupt ausgeprägt werden sollte. Dabei geht es im Wesentlichen um eine Bedarfsanalyse, die Überprüfung des Bedarfs auf Übereinstimmung mit den Geschäftszielen und den Markteffekten, die eine Serviceausprägung mit sich bringen würde[135].

Die *Service Level Measurement Quality* definiert die Leistungskriterien für den zu erbringenden Service. Dabei wird für den Dienstnutzer nach Geschwindigkeits- und Stabilitätskriterien unterschieden. Erstere fokussiert auf zeitabhängige Kriterien wie Antwortzeit eines Dienstes und den maximalen Durchfluss von Nutzeranfragen[136]. Als Stabilitätskriterien werden Verfügbarkeit und Zugänglichkeit festgelegt. Hinzu kommt die Definition für Zuverlässigkeit aus

[132] Vgl. Eunju, K.; Youngkon, L. (2005), S.1f
[133] Vgl. Kapitel 2.5.4 ISO/IEC20000/ITIL
[134] Vgl. Eunju, K.; Youngkon, L. (2005), S.15f
[135] Vgl. Kapitel 2.5.4 ISO/IEC20000/ITIL, Servicestrategie
[136] Vgl. Eunju, K.; Youngkon, L. (2005), S.18

dem Quotienten der Nachfrageanzahl und der resultierenden Anzahl gültiger Antworten[137]. Als Form für die vertragliche Fixierung dieser Qualitätskriterien werden BLA und SLA[138] vorgeschlagen[139].

Service Level Measurement Quality und Business Value Quality repräsentieren die Wirkung eines Dienstes nach außen und damit auf den Markt und auf den Nutzer. Sie sind damit essentiell für die Gütebeurteilung eines Dienstes und somit unverzichtbare Grundlage für die Definition von SLA.

Die darunterliegende Schicht bildet die Interoperabilitätsschicht ab und umfasst die *Interoperability Quality* und die *Business Processing Quality*. Als interoperable Qualitätskriterien gelten die spezifikationsgetreue Verwendung von SOAP, WSDL und UDDI[140] sowie die Einhaltung von Interoperabilitätsprofilen, die durch Web Service Interoperability Organization (WS-I)[141] vereinbart werden. Business Processing Quality-Kriterien sind für die korrekte Abbildung von Businessprozessen durch Webservices verantwortlich. Dazu zählen eine zuverlässige Nachrichtenübermittlung und eine gesicherte Transaktionalität (ACID)[142] für die zuverlässige Implementierung von Geschäftprozessen[143].

Als letztes existiert die Systemschicht. Sie vereint Manageability Quality und Security Quality. *Manageability Quality* unterscheidet zwischen zu koordinierenden Webservices und dem dazugehörigen Managementgrad im Zuge der Qualitätssicherung. *Die Security Quality* besteht aus zwei Ebenen. Zum einen aus den bereits benannten Sicherheitseigenschaften wie Vertraulichkeit, Integrität, Interoperabilität und Zurechenbarkeit und zum anderen aus den diesbezüglichen Erweiterungen auf Transport- und Nachrichtenebene zuzüglich möglicher technischer Realisierungen[144].

[137] Vgl. Eunju, K.; Youngkon, L. (2005), S.19
[138] Vgl. Kapitel 2.2.1 Service Level Agreements
[139] Vgl. Eunju, K.; Youngkon, L. (2005), S.20
[140] Vgl. Kapitel 2.7.1 Rollenkonzept von Webservices
[141] WS-I ist eine Organisation, die versucht, Interoperabilitätsprofile plattformneutral, betriebssystemübergreifend und programmiersprachenunabhängig für Webdienste zu etablieren.
[142] ACID – ist ein Akronym und steht für Atomarität, Konsistenz, Isolation (keine gegenseitige Beeinflussung) und Dauerhaftigkeit (des Ergebnisses) als wesentliche Eigenschaften von Transaktionen in verteilten Systemen.
[143] Vgl. Eunju, K.; Youngkon, L. (2005), S.25f
[144] Vgl. ebd. S.34f

Dies ist evident, denn dementsprechende Risiken verteilen sich auf allen Ebenen und allem Komponenten der Webservicearchitektur[145]. Dementsprechend werden Sicherheitsprofile mit abfallenden Abstraktionsgraden für beide Ebenen definiert.

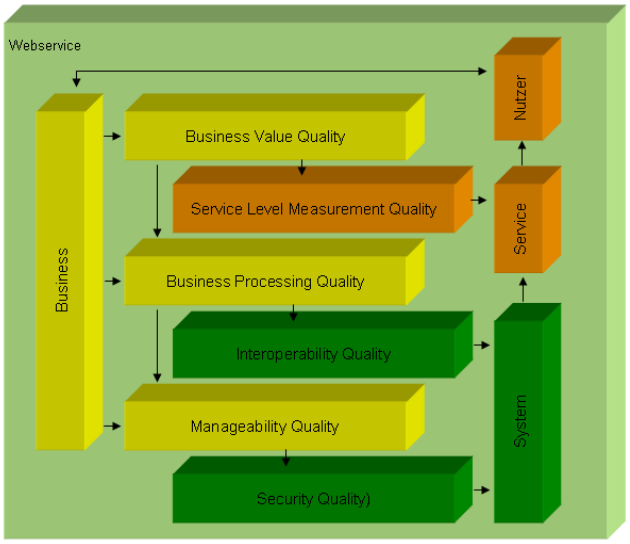

Abbildung 13 - Qualitätsmodell von Webservices[146]

Den Gesamtzusammenhang der verschiedenen Schichten des Modells zeigt Abbildung 13 noch einmal anschaulich. Daraus geht die eindeutige Verzahnung der abstrakten Businessanforderungen und der daraus erwachsenden Gütekriterien einher mit den operativen System- bzw. Servicekennzahlen.

[145] Vgl. Kapitel 2.1 Grundsätze von IT-Sicherheit
[146] Quelle: eigene Darstellung, angelehnt an Eunju, K.; Youngkon, L. (2005), S.10

Die dazugehörigen Kennzahlen für die Beurteilung von Services fasst Tabelle 11 noch einmal zusammen.

Qualitätsmerkmal		Bedeutung
OASIS WSQM	Geschwindigkeit	Durchschnittliche Antwortzeit eines Dienstes auf eine Serviceanfrage
	Kapazität / Skalierbarkeit	Anzahl gleichzeitig konkurrierender Dienstnutzer
	Verfügbarkeit	Verhältnis von vereinbarter Servicezeit zu Ausfallzeit
	Zuverlässigkeit	Verhältnis aus erfolgreichen abgearbeiteten Serviceanfragen zu nicht erfolgreich abgearbeiteten Anfragen
	Zugänglichkeit/Erreichbarkeit	Verhältnis aus formalen Serviceverfügbarkeitsanfragen zu Serviceanfragen
	Regelkonformität	Güte der Einhaltung von Standards für Webservices für SOAP, WSDL und UDDI
	Interoperabilität	Grad der Einhaltung der in WS-I definierten Interoperabilitätsprofile
	Sicherheit	Grad der Sicherheit in Abhängigkeit der definierten Sicherheitsstufe und der damit verbundenen Technologien (bzgl. Autorisierung, Authentifizierung, Zurechenbarkeit, Verschlüsselung)

Tabelle 11 - Kennzahlen von Webservices[147]

Die Aufzählung kann durch dementsprechende Gütekriterien noch erweitert bzw. durch andere Bedeutungsdefinitionen gerade auch im Zusammenhang von Geoinformation-publizierenden Dienstarchitekturen ergänzt[148] und auf den jeweiligen Deutungsspielraum hin erweitert werden.

[147] Quelle: eigene Darstellung
[148] Vgl. Donaubauer, A. J. (2004), S.87ff

2.8 Rasterdatenservices

Rasterdatendienste stellen eine Erweiterung der bisher hier erwähnten Webservices dar und dienen dem Austausch von rasterbasierten Geoinformationen in verteilten Systemen (Distributed Computing).

Die Verbreitung und Nutzung von Rasterdaten hat in den letzten Jahren sprunghaft zugenommen. Nicht nur durch den technologischen Fortschritt in der Speicherindustrie und der einhergehenden Vergrößerung von Kapazitäten, dem zusätzlich durchschlagenden Erfolg der Normierungen seitens des *Open Geospatial Consortium* (OGC) im Bereich des Geoinformationswesens, sondern auch durch die konsequent-marktorientierten Ziele und Umsetzungen seitens der Großkonzerne Google und Microsoft, Geoinformationen im Internet verfügbar zu machen, verdanken Rasterdatendienste im Allgemeinen ihre gestiegene Popularität.

Durch den Beitritt von Google und Microsoft zum OGC kann auf längere Sicht mit einer Beflügelung des Geoinformationsmarktes gerechnet werden. Insbesondere durch die Bereitstellung von Kartendiensten mit weltweit nahezu flächendeckenden hochauflösenden Satelliten- und Luftbildern wird die Integration und Interaktion mit Businessapplikationen weiter voranschreiten.

2.8.1 Rasterdatenmodell

Rasterdatendiensten liegen Rasterdaten mit entsprechenden Rastermodellen zu Grunde. Diese lassen sich durch Rasterzellen beschreiben. Rasterzellen wiederum sind als gleich große und als regelmäßig angeordnete Matrizen homogenen Inhaltes definiert. Sie werden in Anlehnung an die die zweidimensionale Bildverarbeitung mit Zeilen- und Spaltendefinition als Pixel bezeichnet[149]. Homogenität bedeutet in diesem Zusammenhang die explizite Verwendung eines einheitlichen Abbildungsmodells in Bezug auf Georeferenzierung und sensoraler bzw. daraus abgeleiteter thematischer Information.

[149] Vgl. Bartelme, N. (2000), S.115

Eine mögliche Kategorisierung von Rasterdaten ergibt sich aus der ISO 19121, deren Kategorisierungsebenen in Tabelle 12 nach DIGEST definiert wurden.

Bildkategorie	Bezeichnung	Bildkategorie	Bezeichnung
VIS	Visible Imagery	SAR	Synthetic Aperture Radar
SL	Side Looking Radar	SARIQ	SAR Radio Hologram
TI	Thermal Infrared	IR	Infrared
FL	Forward Looking Infrared	MS	Multispectral
RD	Radar	MAP	Raster Maps
EO	Electro-Optical	LEG	Legends
OP	Optical	PAT	Colour Patch
HR	High Resolution Radar	DTEM	Matrix Data (DGM)
HS	Hyperspectral	MATR	Matrix Data (other)
CP	Colour Photography	LOCG	Location Grid
BP	Black/White Photography		

Tabelle 12 - Rasterdatenkategorien (DIGEST)[150]

Diesbezügliche Beispiele sind Fernerkundungsdaten unterschiedlicher Sensoren mit unterschiedlicher spektraler Auflösung bzw. Ausrichtung, digitale Gelände- oder Oberflächenmodelle mit unterschiedlichen Höhenauflösungen oder im einfachsten Fall digital verfügbare oder durch Digitalisierung digital verfügbar gemachte statische Karten.

Neben dem klassischen pixelbasierten Ansatz existieren auch andere geordnete Datenstrukturen, die keine Pixelbilder sind[151], sondern sich durch n-zusätzliche Attributdimensionen definieren lassen. Sollen diese Attributdimensionen in einem räumlich-funktionalen Zusammenhang dargestellt werden, spricht man im Gegensatz zum klassischen pixelbasierten Ansatz von einem *Coverage*. Beispiele dafür sind 3D-Zeitreihen, Klimamodelle, Ozeanographische Modelle, Schadstoffmodelle und Mehrkanalfarbraster.

2.8.2 Ausprägung von Rasterdatendiensten

Für die Ausprägung von Rasterdatendiensten gibt es eine Vielzahl an Möglichkeiten. Durch das ansteigende Aufkommen an rasterbasierten Basisdaten und der gleichzeitigen Forderung, diese Daten zur Verfügung zu stellen, sind Mechanismen gefordert, um zum einen extrem große bzw. extrem vielschichtige Rasterdatenbestände verwalten zu können und zum anderen, um Ausfall-

[150] Quelle: eigene Darstellung, angelehnt an ISO 19121 (2000), S.6
[151] Vgl. Korduan, P.; Zehner, M. L. (2008), S.70

zeiten von Diensten zu minimieren, damit die innerhalb von SLR und SLA geforderte Bereitstellungs- und Verfügbarkeitszeiten einhaltbar sind[152].

Generell gilt es, zwischen statischen und interaktiven Rasterkarten zu unterscheiden. Formal statische Rasterkarten sind vorprozessiert und werden üblicherweise von einem Server ausgeliefert. Google verfährt mit seinen Daten dementsprechend und hat auf Basis von topographischen Analysen, wie z.B. Landmassenberechnungen und Wasserbedeckungsgraden sowie durch die Festlegung auf lediglich drei wesentliche darzustellende Kartentypen in 18 Auflösungsstufen – Satellite, Map und die hybride Überlagerung, den zu prozessierenden Datenumfang auf geschätzte 33 Terrabytes[153] eingrenzen können.

Demgegenüber steht die interaktive Bereitstellung von Rasterdaten, bei dem ein Client einen individuellen Kartenausschnitt anfordert und von einem Server ein dementsprechend georeferenziertes Rasterbild geliefert bekommt. Die Rasterbilder sind dabei standardisiert. Etabliert für den Datenaustausch haben sich Portable Network Graphics (PNG), Joint Photographic Experts Group (JPEG), Graphic Interchange Format (GIF) und Tag Image File Format (TIF).
Neben der Normierung von Rasterbildern sind auch die dementsprechenden Dienste für die Veröffentlichung von Geoinformationen normiert worden. Eine maßgebende Rolle dabei spielen Organisationen wie OGC und ISO (TC211) und deren Interoperabilitätsbestrebungen für Services und Servicearchitekturen. Dazu zählen Darstellungsdienste wie der Web Map Service (WMS), Datendienste wie der Web Coverage Service (WCS) und Prozessierungsdienste wie der Web Processing Service (WPS).

Diese normierten bzw. standardisierten Geodatendienste dienen dem interoperablen Austausch von Geodaten in verteilten Systemen[154]. Geodaten werden somit über Geodatendienste recherchierbar, darstellbar, modifizierbar und in einem weiteren Entwicklungsschritt analysierbar, kombinierbar, prozessierbar und ergebnisbezogen verschmelzbar. Aus der Zentrierung von normierten Geodatendienste über Geodaten in verteilten Systemen lässt sich somit der Begriff Geodateninfrastruktur (GDI) ableiten. Damit kann, sofern alle notwen-

[152] Vgl. Kapitel 2.2.1 Service Level Agreements
[153] Vgl. Gibson, R. (2006), S.66
[154] Vgl. Kapitel 2.1.6 Interoperabilität

digen Geo-Prozesse in Geo-Diensten oder Geodatendiensten formulier- und abbildbar sind, die Verbindung zu einer geo-serviceorientierten Architektur[155] weitestgehend hergestellt werden.

2.8.3 OGC-Webservices

Die bisherigen Implementierungen durch das OGC bezüglich der Darstellung, Verarbeitung und Analyse von Rasterdaten zeigt im Überblick Abbildung 14.

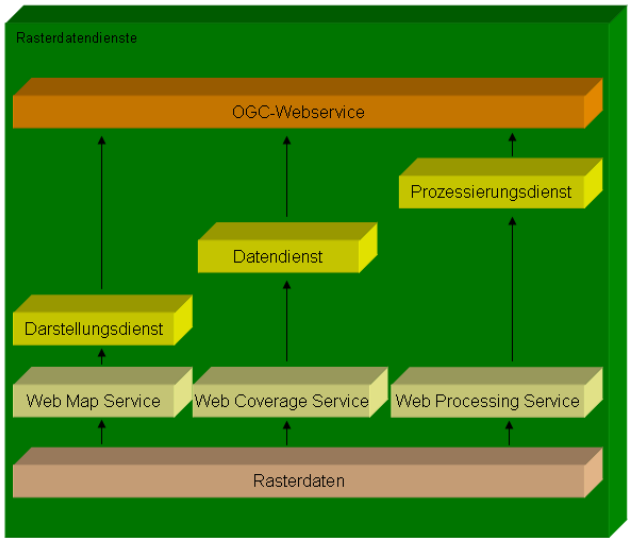

Abbildung 14 - OGC-Webservices[156]

Der OGC-Webservice bildet die abstrakte Grundlage für die Ausprägung der unterschiedlichen Diensttypen. Er besitzt eine eigene Schnittstelle (*Capabilities*), um sich selbst zu beschreiben. Abgeleitete Dienste wie WMS, WCS und WPS erben diese Metadatenschnittstelle und erweitern diesen um eigene Schnittstellen. Die Schnittstellenparameter werden als *Request* von einem Client an den Server geschickt und als *Response* von diesem wieder beantwortet[157]. Der Server tritt damit an die Stelle des Serviceproviders, der Client an die Stelle des Servicerequestors[158].

[155] Vgl. Kapitel 2.7 Webservices
[156] Quelle: eigene Darstellung. Aus Gründen der Übersichtlichkeit wurde auf die Darstellung des Web Coverage Processing Service (WCPS) verzichtet.
[157] Vgl. ISO 19119 (2001), S.22
[158] Vgl. Kapitel 2.7.1 Rollenkonzept von Webservices

2.8.3.1 WMS

Der WMS-Dienst dient ausschließlich der vereinfachten und standardisierten Übertragung grafischer Darstellungen in Form von georeferenzierten Karten über das HTTP-Protokoll. Er besitzt insgesamt zwei zusätzliche Schnittstellen, die ihn im Weiteren in einen einfachen und in einen abfragbaren WMS differenzieren lassen[159]. Außerdem ist es möglich, in einem bestehenden WMS einen anderen WMS aufzurufen und dessen grafische Repräsentation zu nutzen[160]. Durch die zusätzliche Möglichkeit, einzelne Kartenebenen transparent zu schalten, sind die Überlagerung und damit die Kombination von unterschiedlichen Inhalten aus verteilten Systemen möglich.

2.8.3.2 WCS

Der WCS-Dienst unterstützt die Ausgabe von Rasterobjekten und damit wiederum von regelmäßig angeordneten Rasterdaten. Im Gegensatz zu den dynamisch erzeugten aber statischen Karten des WMS liefert der WCS räumlich-funktional zusammenhängende Informationen zu n-dimensionalen Merkmalsräumen zurück. Dementsprechend unterstützte Ausgabeformate sind GeoTIFF, HDF-EOS, NITF bzw. CF-NetCDF[161].

2.8.3.3 WPS

Der WPS-Dienst ist in dieser Arbeit der Vollständigkeit halber mit aufgenommen worden, da er die elementare Grundlage für den Web Coverage Processing Service (WCPS) bildet. WPS dient der Definition von abstrakten Verarbeitungsprozessen von Geodaten in verteilten Systemen. Er spezifiziert generelle Eingangs-, Ausgangs- und Verankerungsmodalitäten von Prozessen zur Geoverarbeitung ohne die konkreten Verarbeitungsprozesse im Einzelnen zu beschreiben[162]. Der WCPS definiert auf Basis des WPS-Frameworks mögliche Algorithmen für die Verarbeitung bzw. Prozessierung von Rasterdaten[163].

[159] Vgl. OGC (2004), S.1 i.V.m. S.34
[160] Allgemein wird dies als Dienstkaskade bezeichnet.
[161] Vgl. OGC (2008), S.38
[162] Vgl. OGC (2007f), S.1
[163] Vgl. OGC (2009), S.1

2.8.4 Image Services

Die Bereitstellung OGC-konformer Dienste durch Web Mapping Applikationen ist allerdings nur ein möglicher Weg Geodaten (interoperabel) zu verarbeiten und auszutauschen. Der Normierung von Rasterdatendiensten stehen kommerzielle Industrielösungen gegenüber. Diese unterstützen durchaus in Endkonsequenz die Ausprägung von OGC-konformen Diensten auf der einen Seite, nutzen jedoch auf der anderen Seite unterhalb der Interoperabilitätsebene, jedoch standardisiert für dementsprechende Clienten, eigene anwendungsbezogene Beschreibungs- und Abfragesprachen, um im Kern, Rasterdaten hochperformant zu Verfügung zu stellen. Dabei reduziert sich die Funktionalität nicht nur auf das reine Darstellen von Rasterdaten selbst, sondern fügt grundsätzliche Rasterdatenprozessfunktionalitäten, wie das Verwalten Rasterdaten sowie das geometrische und radiometrische Prozessieren von Bilddaten, hinzu. Beispiele hierfür sind insbesondere Client-Server-Applikationen, die dazu geeignet sind, unternehmensweite Strukturen im Bereich der Rasterdatenverwaltung und der Rasterdatenverarbeitung aufzubauen.

Eine unvollständige Auswahl von derzeit am Markt verfügbaren Produkten kann der folgenden Tabelle 13 entnommen werden. Eine generelle Aussage zur Marktverteilung kann an dieser Stelle jedoch nicht getroffen werden.

Firma	Enterpriselösung	Rasterdatenlösung
ESRI	ArcGIS Server	Image Server
ERDAS	APOLLO	Image Web Server
INTERGRAPH	TerraShare Server	TerraShare Raster
RASDAMAN	rasgeo	rasdaman
GOOGLE	Google Earth Server	Google Earth Fusion

Tabelle 13 - Rasterdatenlösungen[164]

Der Einsatz von speziellen Applikationen zur Bereitstellung von Rasterdatendiensten macht außerordentlich Sinn, weil in diesem Bereich zum einen eine enorme Datenvielfalt bezüglich spezifischer Aufnahmesensoren vorherrscht[165], die dementsprechende Formate in verschiedensten geometrischen und spektralen Auflösungen, Überlappungsgraden und Farbtiefen abbilden und zum anderen, weil Rasterdaten durch ein dementsprechendes

[164] Quelle: eigene Darstellung
[165] Vgl. Tabelle 12 - Rasterdatenkategorien (DIGEST)

Überangebot auf dem derzeitigen Markt relativ preiswert, in Abhängigkeit zu deren Aktualität, zu beschaffen sind.

Im Zentrum dieser Arbeit steht der ArcGIS Image Server von ESRI. Dieser dient der schnellen Bereitstellung von Rasterdaten- und Rasterdatendiensten an beliebige Clienten im Umfeld verteilter Geodaten.

2.8.5 ArcGIS Image Server

Der ArcGIS Image Server positioniert sich im Wesentlichen durch die serverbasierte, dynamische Mosaikierung und Prozessierung verteilter Rasterdatenbestände. Die Wertschöpfung erfolgt dabei nicht nur ausschließlich durch die schnelle Mosaikierung und effiziente Bereitstellung großer Datenbestände selbst, sondern durch die zusätzliche Möglichkeit, dynamische Service- und Rasterprozesse in den Bereitstellungsprozess mit einfließen und durch die jeweiligen Clienten interaktiv beeinflussen zu lassen. Dadurch können dynamisch generierte Inhalte zur interaktiven Darstellung von Rasterobjekten durch Rasterdatendienste gekapselt und veröffentlicht werden.

Prozessual zu unterscheiden sind radiometrische von geometrischen Prozessen sowie verschiedene Mosaikierungsverfahren. Eine Übersicht kann Tabelle 14 entnommen werden. Hintergrund für die Etablierung ist die dynamische zur Verfügungstellung beliebiger, unabhängiger Prozesse und Methoden zur individuellen Interpretation und Produktableitung aus einem redundanzfreien Rasterdatenbestand.

Vergleichbar sind diese Prozesse im übergeordneten Sinn mit beliebigen, noch zu etablierenden Diensten und Funktionalitäten im Rahmen von WPS und im Speziellen, unter Nutzung der vorhandenen Algebra, mit WCPS[166].

[166] Vgl. Kapitel 2.8.3 OGC-Webservices

Prozesse		Mosaikierungsmethoden
radiometrisch	***geometrisch***	
Extract/Stack Bands	Affine	Closest to center
Image Algebra / NDVI	Projective	By attribute
Spectral Matrix	Polynomial	Lock image
Greyscale	Warp grid	Most nadir
Stretch	Orthorectification*	Closest to viewpoint
Convolution Filter		Most northwest
Pan-sharpen		Seamline*
Trend		
Classify		
Colormap		
Elevation visualization		
Histogram		

Tabelle 14 - Rasterdatenprozesse[167]

Damit stehen den Nutzern von Rasterdatendiensten in Abhängigkeit der Ihnen durch den Serviceanbieter zur Verfügung gestellten Funktionalitäten, Prozesse und Methoden zur Seite, die es beispielsweise ermöglichen, vollautomatisch Geländehöhen (Elevation visualization), Vegetationsindizes (NDVI) und Schärfungs- sowie Verschneidungsprozesse (Pan-sharpen, Convolution filter) auf den Ausgangsdatenbestand dynamisch anzuwenden. Die gleichzeitige geometrische Transformation in beliebige Systeme kann dabei ebenso frei gewählt werden wie das auf die Ausgangsdaten anzuwendende Mosaikierungsverfahren. Als Beispiel sei hier die Methode *Closest to center* erwähnt, bei der gewichtet, in Abhängigkeit der Entfernung zum Bildzentrum, die beteiligten Einzelraster dynamisch mosaikiert und an den jeweiligen Clienten übergeben werden. Dabei ist das wichtigste Kriterium, dass die Überlappungsbereiche im Gegensatz zum statischen Mosaikieren erhalten bleiben.

2.8.5.1 Architektur

ArcGIS Image Server reiht sich nahtlos in die Architektur bestehender ESRI-Produkte ein. Er kann als Erweiterung[168] von ArcGIS Server eingesetzt oder aber, mit Unterstützung einer ArcGIS Desktop-Umgebung, als Erstellungswerkzeug für Rasterdatendienste, isoliert von ArcGIS Server betrieben wer-

[167] Quelle: eigene Darstellung; die Funktionalitäten Orthorectification und Seamline benötigen eine gesonderte Lizenzierung.
[168] Erweiterungen werden bei ESRI als Extension bezeichnet.

den[169]. Eine vereinfachte Darstellung für die verwendete Konfiguration zeigt Abbildung 15.

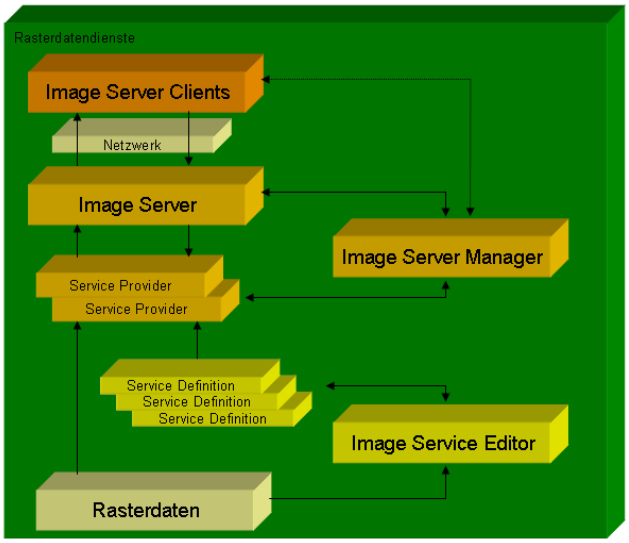

Abbildung 15 - ArcGIS Image Server, schematisch[170]

Zu den wesentlichen Komponenten des Image Servers zählen Image Service Editor, Service Provider, Image Server und Image Server Manager. Der finalisierte Rasterdatendienst setzt sich aus der Service Definition und den zu verarbeitenden Rasterdaten zusammen.

Mit Hilfe des Image Service Editors (ArcMap) werden die Service Definitionen erstellt. Die Service Definition selbst besteht aus der ISDef (Image Service Definition Datei, XML-basiert), welche die dienstspezifischen Eigenschaften des Rasterdatendienstes beschreibt, einem Footprint der beteiligten Rasterdaten, der daraus resultierenden Servicegrenze (Boundary) und den RPDefs (Raster Process Definition Dateien, XML-basiert) mit den Informationen zu den auf die Ausgangsdaten anzuwendenden geometrischen und radiometrischen Prozesse sowie zu Einstellungen für die Orthorektifizierung und Mosaikierung. Der Rasterdatendienst kann weiterverwendet werden, wenn der Service Editor die ISDef erfolgreich in die ISCDef (Image Service Compiled Definition) kompilieren konnte

[169] Vgl. Kapitel 3 Vorgehen und Methode.
[170] Quelle: eigene Darstellung

Der Service Provider übernimmt die Rasterdatendienste und registriert diese beim Image Server. Außerdem geht er die Kommunikation mit den Clienten ein und liefert die dementsprechend nachgefragten Rasterdaten.

Der Image Server publiziert die über den Service Provider registrierten Dienste sowie die dazugehörige Metadaten. Er führt die Zugriffskontrolle durch und überwacht protokollarisch die Kommunikation zwischen den Clienten und den Service Providern. Damit fungiert der Image Server als dementsprechender Broker für Serviceanfragen der Serviceprovider. Sofern mehrere Service Provider für einen Dienst zur Verfügung stehen, steuert er die Lastverteilung und stellt den Clienten dementsprechende Verbindungsparameter zur Verfügung.

Ein Rasterdatendienst kann mit den aufgezeigten Komponenten damit nach dem klassischen *Public-Serve-Use-Verfahren* mit folgendem Workflow erstellt, veröffentlicht und genutzt werden:

- Mit Hilfe des Image Service Editor (ArcMap) werden Servicedefinitionen (Service Definition) erstellt, verwaltet und am Ende kompiliert.
- Der Image Server instanziert einen oder mehrere Service Provider zur Abarbeitung von Clientenanfragen.
- Die finalisierten, kompilierten Servicedefinitionen werden einem oder mehreren Service Providern zugewiesen.
- Die Clienten melden sich beim Image Server an, werden authentifiziert und bekommen Zugriff auf das Rasterdatendienstverzeichnis.
- Nach Auswahl des Dienstes weist der Image Server den Clienten die Verbindungsparameter zu den entsprechenden Service Providern zu.
- Die Clienten greifen auf die Rasterdatendienste zu und können, entsprechend der Service Definition, änderbare Serviceeigenschaften modifizieren.

Damit steht der Rasterdatendienst zur weiteren Verwendung (Consuming). Im Folgenden gilt es die Kommunikation der Architekturkomponenten darzustellen.

2.8.5.2 Kommunikationsmodell

Für die Kommunikation zwischen den beteiligten Komponenten gilt es Direct Clients von Web Clients zu unterscheiden. Direct Clients kommunizieren über XML-basierte Remote Procedure Calls (RPC), also über entfernte Prozeduraufrufe mittels in XML-gefasster Parameter[171]. Diese Form von verteilter Verarbeitung findet auf prozeduraler Ebene verdeckt aus der Applikation heraus statt, ähnelt dem Client-Server-Verfahren und ist als Vorgänger des in Kapitel 2.7 beschriebenen SOAP-Protokolls anzusehen. Die Applikation ruft eine ausschließlich ihr bekannte Prozedur auf und wird damit zum Client[172]. Der Aufruf wird nach einem ebenso bekannten Verfahren kodiert und an einen Prozedurinhaber, den Server in diesem Fall, übertragen und dort dekodiert. Durch die definierten Prozeduren werden die Funktionalitäten bzw. Daten parametrisiert verarbeitet, das Ergebnis kodiert und an den Prozeduraufrufer weitergeleitet. Dieser dekodiert das entsprechende Ergebnis und setzt das zurückgelieferte Ergebnis in der jeweiligen Applikation um[173].

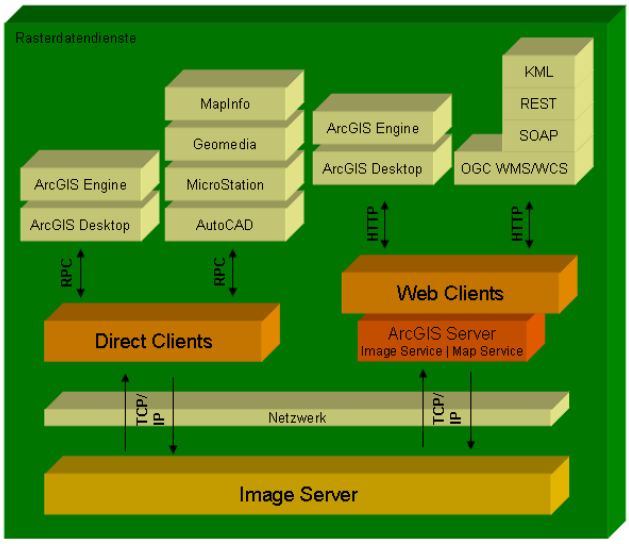

Abbildung 16 – Kommunikationsmodell, schematisch[174]

Zu den RPC-Aufrufern zählen alle ArcGIS Desktop Clienten sowie weitere in Abbildung 16 Dargestellte. Die Web Clients werden vornehmlich über den

[171] Vgl. Kapitel 2.8.5.4 Automation
[172] Vgl. Abbildung 11 – Webservice - Architektur. Die Bekanntheit der Prozedur ist einer Veröffentlichung (Public/Find) gleichzusetzen. Die dementsprechende Bindung (Binding) erfolgt durch die Übergabe der Prozedurparameter.
[173] Weiterführende Informationen zur Programmierung und Ablaufsteuerung von RPC in verteilten Systemen enthält Bengel, G. (2004), S.149ff
[174] Quelle: eigene Darstellung

ArcGIS Server instanziert, der über HTTP und dementsprechende API angesprochen wird und diesbezügliche Rasterdaten über ebenfalls in Abbildung 16 dargestellte Schnittstellen übermitteln kann. Dafür muss der Image Server als Erweiterung beim ArcGIS Server registriert worden sein. Die Registrierung erfolgt durch die Bekanntmachung des Image Servers und seiner korrespondierenden Serviceprovider beim Server Object Manager (SOM) des ArcGIS Server. Werden Rasterdatendienste durch die entsprechenden Clienten nachgefragt, leitet der SOM die Anfragen nicht wie üblich an seine Server Object Container (SOC) weiter, sondern übergibt die Anfrage an den Image Server und dieser wiederum an die Service Provider. Damit tritt der ArcGIS Server als klassischer Broker gegenüber den nach Rasterdatendiensten nachfragenden Clienten auf.

2.8.5.3 Dienstklassifikation

Mit Hilfe des Image Servers lassen sich beliebige Rasterdatendienste dynamisch in Wert setzen. Ausgangspunkt für die Bereitstellung solcher Dienste ist das Vorhandensein von dementsprechenden Rasterdaten in den verschiedensten Ausprägungen. Differenziert muss hier insbesondere nicht nur zwischen verarbeitbaren Rasterdaten selbst, sondern auch zwischen den Fähigkeiten der verwendeten Applikationen werden.

Mit Hilfe des ArcGIS Servers und der dementsprechenden Image Server Erweiterung lassen sich Rasterdaten in vielfältiger Weise mit Hilfe von Diensten bereitstellen bzw. veröffentlichen. Dazu zählen unter anderem, wie in Abbildung 16 dargestellt, die durch das OGC spezifizierten und für die Geoinformationswirtschaft elementaren WMS- und WCS-Dienste[175].

Mit der Unterstützung von SOAP[176] und REST eröffnet sich zusätzlich der Weg, dynamische Rasterdaten in Enterprise Architekturen (SOAP) oder Hypermedia-Informationssysteme[177] (REST) einzuführen und zu publizieren. Nicht zuletzt können Rasterdatendienste mit Hilfe von KML in Google Earth Anwendungen eingebunden werden.

[175] Vgl. Kapitel 2.8.3 OGC-Webservices
[176] Vgl. Kapitel 2.7 Webservices
[177] Dementsprechende, API-gesteuerte, zusammensetzbare Webinhalte werden auch als „mashup“ bezeichnet.

Die Verwendung des Image Servers als eigenständige Lösung und damit ohne die dementsprechende Korrespondenz zum ArcGIS Server beschränkt die Ausprägung von Rasterdatendiensten bzw. den Zugang auf direkte Clienten über das RPC-Protokoll. Damit stehen SOAP, REST, KML sowie WMS und WCS bei alleiniger Verwendung des Image Servers nicht zur Verfügung. Mit entsprechender Anpassung ist es jedoch möglich, WMS-fähigen Clienten den nativen Zugang, zu den über den Image Server veröffentlichten Rasterdatendiensten bzw. Rasterdaten, zu ermöglichen[178].

2.8.5.4 Automation

Die Erstellung und Verwaltung von Rasterdatendiensten durch den Image Server kann teilweise automatisiert und autonom von Service Editor und Server Manager erfolgen. Dazu bietet der Image Server Kommandozeilenoperationen und -programme an. Zum einen existiert der Console Client und zum anderen der Kommandozeilenaufruf zum Befehlsinterpreter ISCommand. Beide fungieren ebenfalls als Direct Clients und werden in Abbildung 17 dargestellt. Der Console Client verfügt über eine einfache Oberfläche zum Absetzen bereits vordefinierter Befehlssequenzen aber auch eigener oder fremder vorab bearbeiteter Befehlsstapel für die Abarbeitung komplexerer Aufgaben. Er kann primär für die Simulation beliebiger Clientanfragen genutzt werden und eignet sich vor allem für den Test der unterschiedlichen Ein- und Ausgabeparameter für die individuelle Rasterdatenrückgabe durch den Image Server.

[178] Vgl. ESRI (2008b)

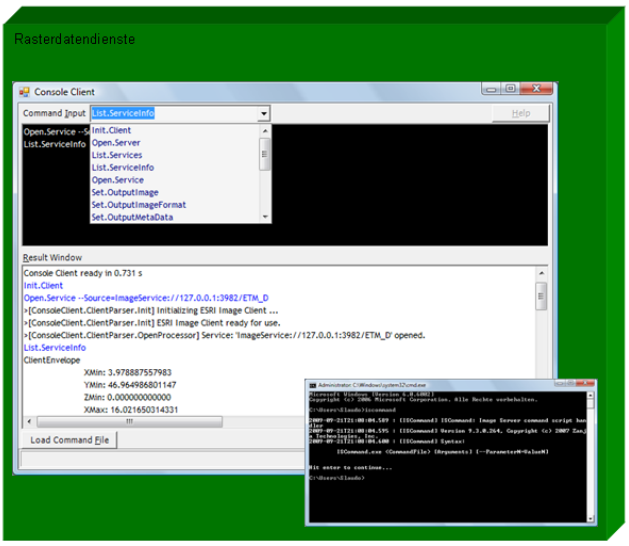

Abbildung 17 – Console Client (l) und Befehlszeile (r)[179]

Über den Kommandozeilenbefehlsinterpreter lassen sich die Funktionalitäten des Service Editors, des Server Managers und der Direct Clients automatisiert und ohne die jeweilige grafische Benutzeroberfläche absetzen. Es steht ein umfangreicher Befehlssatz zur Verfügung, um gängige Serviceoperationen zu komplexen Serviceabläufen zu verschachteln und diese im Anschluss automatisiert ablaufen zu lassen.

Damit wird es möglich, den Lebenszyklus von Rasterdatendiensten auf technischer Ebene[180] von der Erstellung, dem Betrieb bis zur kontinuierlichen Verbesserung komplett zu steuern.

[179] Quelle: eigene Darstellung
[180] Vgl. Kapitel 2.5.4.4 Servicebetrieb und Serviceverbesserung

Der parametrisierte Aufruf von Prozeduren[181], die Konfiguration des Image Servers, respektive der Serviceprovider, die Kommunikation des Servers, der Serviceprovider mit den Clienten, die Speicherung von Eigenschaften von Rasterdatendiensten sowie von Rasterdaten bzw. die Abarbeitung erfolgt dabei auf Basis von ArcGIS Image Server XML.

Abbildung 18 - Image Server XML

Der Vorteil darin besteht in der unmittelbaren Lesbarkeit und Veränderbarkeit von Inhalten und Parametern. Dementsprechende Arbeitsformulare können auf Basis vorgegebener Schemadefinitionen erstellt werden. Gesteuert wird dieser Prozess durch die Verwendung von XADef und XFDef. Die Struktur und Eigenschaften von Knoten werden über die Verwendung von XADef beeinflusst. Mit Hilfe von XFDef ist es möglich, die dementsprechenden Formulare nach Aussehen und Anordnung der Parameter dynamisch zu erzeugen.

[181] Vgl. Kapitel 2.8.5.2 Kommunikationsmodell

3 Vorgehen und Methode

Die Verfügbarmachung von Rasterdaten oder Rasterinformationen durch die konsequente Nutzung dienstleistungsorientierter bzw. dienstorientierter Architekturen als Basis wertschöpfender Geschäftsprozesse besitzt in der Geoinformationswirtschaft einen nicht zu unterschätzenden Stellenwert.

Die rechtliche, organisatorische und technische Korrelation der verschiednen Prozesse im Zuge der rasterbasierten Dienstleistungserbringung ist durch die steigenden Bedürfnisse der Anwender und die nahezu symbiotischen Abhängigkeiten anderer Geschäftsprozesse und potentieller Geschäftsmodelle im Umfeld von Rasterdaten enorm. In der Vergangenheit waren die Nutzer zufrieden, heterogene, statische Rasterdaten auf beliebigen Wegen in ihre eigenen Systeme mit sehr viel Aufwand zu transformieren und vor Ort verfügbar zu machen.

Mit Voranschreiten kontinuierlicher Standardisierungen, nicht nur im Bereich der Geoinformatik, sondern auch im Bereich der Entwicklung und Implementierung von serviceorientierten Architekturen und dementsprechender Technologien, stehen Rasterdaten nicht mehr nur ausschließlich im Fokus wissenschaftlicher oder fachspezifischer Anwender, sondern erschließen sich zusätzlichen Zugang zu Enterpriseanwendungen für professionelle Nutzer oder gänzlich neuer Nutzergruppen bis hin zum Privatanwender. Die dementsprechende schnelle, sichere und garantierte Bereitstellung von Rasterdaten bzw. rasterdatenbasierten Dienstleistungen als Ausgangsbasis für weitere wertschöpfende Prozesse, gilt es rechtlich, organisatorisch und technologisch bereits in Geoinformationsbereich abzusichern.

- Dazu ist es nötig, in einem ersten Schritt die verschiedenen technischen und rechtlichen Anforderungen an Rasterdatendienste und mögliche assoziierte Nutzergruppen überhaupt zu klassifizieren, um die dementsprechend umfänglichen Ansprüche an Dienste formal-inhaltlich zu definieren.

- Diese Ansprüche stehen den allgemeinen technischen und organisatorischen Risiken gegenüber, die einer Bereitstellung von Diensten, insbesondere Rasterdatendiensten entgegenstehen, die es in weiteren Schritt zu bestimmen gilt.

- In Folgenden ist es unumgänglich, die gewonnen Anforderungen unter Maßgabe eines real existierenden Servicemanagementframeworks (ITIL, V3) bereits in den organisatorischen Ablauf der Dienstgestaltung und Diensterstellung durch den Einsatz und die Gewinnung von bereits bekannten oder neu zu definierender Kennzahlen mit einzubeziehen.

- Darauf aufbauend ist die technologische Möglichkeit am konkreten Programmsystem zu bewerten, um im Anschluss Empfehlungen für den Einsatz in Produktivumgebungen geben zu können.

Die dementsprechenden Hardware- und Softwarekomponenten sowie die Testdatensätze bilden den Rahmen für die Erstellung und den Betrieb von Rasterdatendiensten.

Hardware

Zum Einsatz kommt ein handelsüblicher Laptop der Marke Samsung, Modell R560, mit Doppelkern-Prozessor (2,4 GHz) und drei Gigabyte Arbeitsspeicher.

Software

Für die Ausprägung von Rasterdatendiensten wird der ArcGIS Image Server in der Version 9.3.0.264 als stand alone Variante im Zusammenspiel mit ArcGIS Desktop in der Version 9.3 Build 1770 auf einer Windows Vista Home Premium Plattform, Servicepack 2 genutzt[182]. Zusätzlich wurde das Developer Kit des ArcGIS Image Server installiert.

Als Clienten dienen zum einen ArcMap selbst, der Image Server Viewer und der Console Client.

[182] Die erforderlichen Systemvoraussetzungen können der Anlage 1 und Anlage 2 entnommen werden.

Testdaten

Für die Evaluierung von Diensten werden zum einen deutschlandweite dreikanalige Landsat ETM (RGB) Szenen aus dem Jahr 2006 und zum anderen europaweit vorliegende DTED(Level 0)-Höhendaten verwendet, um entsprechende Referenzdienste erzeugen zu können. Abbildung 19 illustriert die dementsprechenden Abdeckungsbereiche.

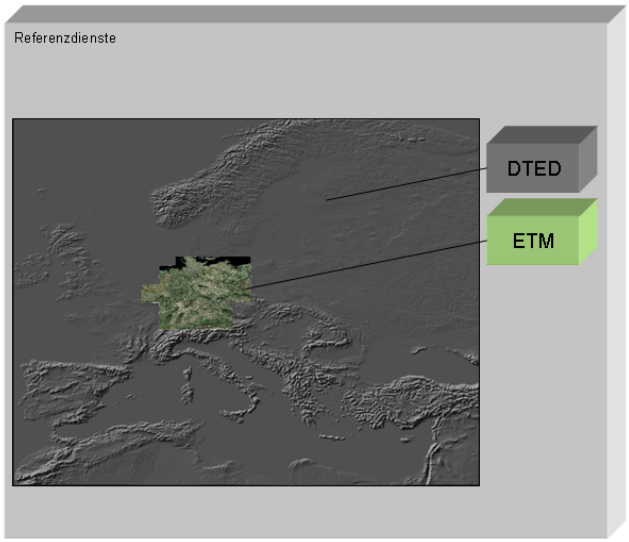

Abbildung 19 - Abdeckung Referenzdienste

4 Umsetzung

Die Spezialisierung auf Wertschöpfung im rasterbasierten Dienstleistungsbereich ist ein nicht zu unterschätzender Wirtschaftsfaktor. Durch die allgemein gestiegene Verfügbarkeit an digitalen Informationen in Form von Rasterdaten, der gleichzeitigen Erweiterung und Standardisierung vorhandener bzw. neuer Technologien im Sinne der Verfügbarmachung sowie der rechtlichen Vorgabe und damit der gesetzlichen Verpflichtung, Daten in bestimmter thematischer Tiefe und Umfang veröffentlichen zu müssen, besteht der natürliche Anspruch, diese Informationen durch die dementsprechenden Nutzergruppen technisch zu verwerten.

4.1 Erusion der Nutzeranforderungen

Die Klassifikation der einzelnen Nutzergruppen und Anforderungen ist nicht trivial und nur interdisziplinär zu beantworten. Durch die vorliegende Diversifikation von Rasterdaten lassen sich zunächst dementsprechende Kategorien von Rasterdaten auf Basis ihres sensoralen Erfassungsursprunges zusammenfassen[183].

Die entsprechende sensorale Klassifikation lässt eine weitere Aufschlüsselung unter räumlichen, spektralen, radiometrischen, optischen und vor allem zeitlichen Aspekten zu. Die räumliche Auflösung ist entscheidend für die Locationsgenauigkeit von Objekten, die mit Hilfe von spektraler, radiometrischer und zeitlicher Auflösung zusätzlich interpretier- und analysierbar sind. Die räumliche, spektrale und radiometrische Auflösung sind gleichzeitig verantwortlich für den aus den gewonnenen Daten resultierenden Speicherbedarf, wobei die spektrale Auflösung die Anzahl möglicher Beobachtungskanäle, die radiometrische Auflösung die Farbtiefe und damit die Informationstiefe der verwendeten Kanäle und die optische Auflösung, die verwendete physikalische Bandbreite der Kanäle, beschreibt.

Ein nicht zu vernachlässigender Aspekt ist die temporale Auflösung von Rasterdaten. Damit ist primär der Zeitunterschied zwischen aufeinanderfolgenden Aufnahmen eines Sensors zu verstehen. Die Abbildung 20 zeigt die Affinität

[183] Vgl. Kapitel 2.8.1 Rasterdatenmodell

der Beteiligten Komponenten eines auf Rasterdaten ausgerichteten Wertschöpfungsprozesses.

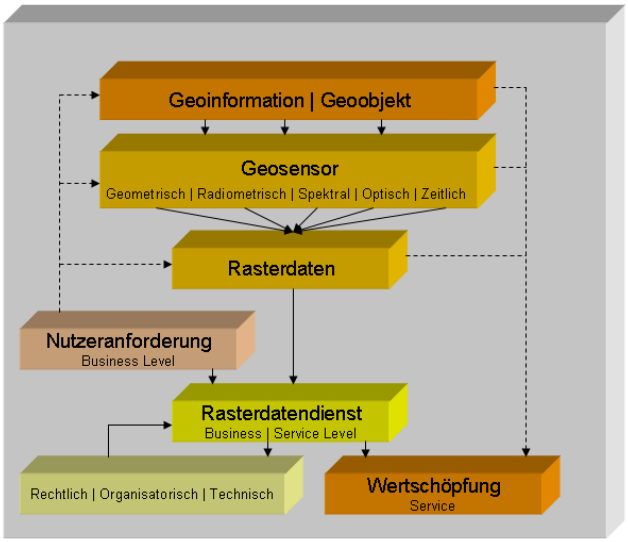

Abbildung 20 – Wertschöpfungskette[184]

Aus den damit zu Grunde liegenden Eigenschaften ergeben sich nicht minder unterschiedliche Nutzungsformen und -potentiale von Rasterdaten und deren abgeleiteten Diensten. Damit leitet sich die Anforderung an den Dienst unmittelbar aus der beabsichtigten Nutzung und damit aus dem Grad der Abhängigkeit ab.

Dementsprechende Abhängigkeiten formulieren sich auf diese Weise rein aus den Nutzeranforderungen. Diese ergeben sich hauptsächlich aus rechtlichen, organisatorischen und technischen Bedingungen für den jeweiligen Wertschöpfungsprozess.

4.1.1 Rechtliche Anforderungen

Rechtliche Anforderungen ergeben sich zunächst aus der grundlegenden Pflicht der Leistungserfüllung durch eine dementsprechende Rasterdatendiensterbringung im Rahmen der zu gewährleistenden Compliance[185].

[184] Quelle: eigene Darstellung
[185] Vgl. Kapitel 2.1 Grundsätze von IT-Sicherheit

Die Fixierung zugesicherter Leistungen, im Sinne der Bereitstellung von Rasterdatendiensten, muss durch dementsprechende Vereinbarungen erfolgen, um den Grad der Leistungserfüllung mess- und bewertbar zu bestimmen[186] und damit die Leistung rechtlich sowohl verwertbar[187] als auch technisch handhabbar zu gestalten. Stehen die vereinbarten Rasterdatendienste in der zugesicherten Form nicht zur Verfügung, kann der Dienstanbieter zivilrechtlich zur Verantwortung gezogen werden.

Auch die zur Verfügung gestellten Rasterdatendienste unterliegen generell der gesetzlich definierten Sorgfaltspflicht[188], dem Datenschutz[189] und dem Urheberrecht[190]. Dementsprechende Dienste müssen demnach den Forderungen entsprechen, auf der einen Seite gewissenhaft betrieben zu werden und auf der anderen Seite den gängigen Datenschutzrichtlinien zu entsprechen. Ein Verweis auf den jeweiligen Quelldatenanbieter ist, im Sinne der Definition von Sorgfaltspflicht und des Datenschutzes, nicht ausreichend. Zu dem bestehen Haftungsrisiken für bzw. durch die Verwendung von Rasterdatendiensten im Zuge der Wertschöpfungsprozesse. Hier gilt es formal zwischen organisationsinterner und externer Dienstbereitstellung zu unterscheiden. Organisationsinterne Dienste dienen der hausinternen Nutzung und Ableitung von Informationen und Produkten sind vom Haftungsrisiko relativ niedrig einzustufen, da die abgeleiteten Produkte zunächst internen Revisionskontrollen unterliegen. Auf extern abgeleitete Produkte oder Informationen besitz der Dienstprovider meist keinen Zugriff mehr, so dass hier nicht nur das Haftungs- sondern auch das allgemeine Nutzungs- bzw. Weiternutzungsrisiko als hoch eingestuft werden muss[191].

Außerdem existieren zusätzliche gesetzliche Einschränkungen durch das SatDSigG. Damit ist es für Rasterdatendienste im Sinne dieses Gesetzes unerlässlich, Rasterdaten auch auf ihre Publikationserlaubnis hin für die Verwendung in Diensten zu überprüfen[192].

[186] Vgl. Kapitel 2.2.1 Service Level Agreements
[187] Vgl. Kapitel 2.1.5 Zurechenbarkeit
[188] Vgl. Kapitel 2.4.1 Sorgfaltspflicht
[189] Vgl. Kapitel 2.4.2 Datenschutz
[190] Vgl. Kapitel 2.4.1 Sorgfaltspflicht
[191] Im Sinne der vertraglich zugesicherten Leistung.
[192] In diesem Zusammenhang gilt es, vor allem UC aber auch OLA im Rahmen von kaskadierenden rechtlichen (innerbetrieblichen) Vertragswerken (Vereinbarungen) abzusichern.

Rechtliche Anforderungen liegen bereits aber auch in Form von gesetzlichen Verpflichtungen vor, unter anderem durch INSPIRE[193] begründet, Geodaten technologisch auch durch Rasterdatendienste in Wert zu setzen, um politische Entscheidungen für den einzelnen Bürger transparent, mit Hilfe räumlicher Informationen, nachvollziehbar zu gestalten und ihn im Rahmen des zukünftig elektronisch unterstützen Demokratieprozesses (E-Demokratie) eine dementsprechende Partizipationsmöglichkeit einzuräumen (E-Government).

4.1.2 Technische Anforderungen

Die technischen Anforderungen lassen sich nicht immer aus den allgemein gehaltenen rechtlichen Rahmenbedingungen ableiten, sondern werden zu großen Teilen aus marktspezifischen Anforderungen gewonnen.

Marktwirtschaftliche Anforderungen werden als solches selbst durch den Geoinformationsmarkt, insbesondere durch Angebot und Nachfrage von Rasterdatendiensten bestimmt. Durch das mannigfache Vorhandensein von Rasterdaten, das hohe Entwicklungsstadium der verfügbaren Software und dem Fortschreiten der Standardisierung innerhalb der Softwareprodukte, lassen sich in enormer Geschwindigkeit frei-definierbare Rasterdatendienste in extrem kurzer Produktionszeit in Wert setzen.

Allein aus marktwirtschaftlicher Sicht ist es verständlich, dass dementsprechende Anbieter von Rasterdatendiensten aber auch die assoziierten Nutzer selten verbindliche Zahlen zu den Diensten offenlegen oder festschreiben bzw. sofern Zahlen vorliegen, dementsprechende Berechnungsgrundlagen oder Metriken nicht veröffentlicht werden, da dies nicht nur eine rechtlich-handhabbare Haftungsgrundlage darstellt[194], sondern als Bestandteil vertraglicher Vereinbarungen der Geheimhaltung unterliegt[195]. Auf der anderen Seite sind sich Nutzer oder Nachfrager der Dienste teilweise nicht bewusst, was aus technischer Sicht zum einen zu fordern ist und zum anderen, welche Investitionen teilweise diesbezüglich Forderungen nach sich ziehen und wie diese folgerichtig die Preisbildung bei einem Serviceanbieter beeinflussen.

[193] Vgl. Kapitel 2.4 Rechtliche Rahmenbedingungen
[194] Vgl. Kapitel 2.4.2 Datenschutz
[195] Vgl. Forsythe, Jennifer. <jennifor@microsoft.com> “Bing: SLA”. Persönliche Email. 24.09.2009. 24.09.2009.

Konkretere technische Forderungen lassen sich aus dem taktisch-operativen Einsatz von Rasterdatendiensten ableiten. Aus der definierten Notwendigkeit heraus, mit Hilfe von Rasterdatendiensten zum Beispiel hoheitliche Aufgaben in Bereichen wie innere Sicherheit, Katastrophenschutz, Umweltschutz, Militär und Nachrichtendienst durchzuführen und dementsprechende Rasterinformationen unbedingt und nahezu verzögerungsfrei im geforderten Rahmen und Umfang zur Verfügung zu stellen bzw. gestellt zu bekommen[196].

Den theoretischen Größen der im Kapitel 2.1.1 gemachten Angaben zur Verfügbarkeit von Komponenten, Diensten oder Daten können aktuelle Beispiele von Verfügbarkeiten von Rasterdatendiensten kommerzieller Anbieter gegenübergestellt werden[197]. Die Werte wurden für verschiedene Anbieter eruiert und sind in Tabelle 15 aufgelistet.

Anbieter	Service	Verfügbarkeit	Version
Google	Google Maps	99.9 % / 24x7	Premium API[198]
Microsoft	Bing Maps	99.9 % / 24x7	Bing Maps for Enterprise[199]
ESRI	ArcGIS Online Maps	99.9 % / 24x7	Standard/Premium[200]

Tabelle 15 - Verfügbarkeit von Diensten[201]

Erkennbar ist deren zahlenwertige Homogenität trotz völlig verschiedener Vertragswerke und dem Einsatz grundverschiedener Technologien zur Bereitstellung von statischen Rasterdatendiensten sowie dem breiten Spektrum weltweit in Wert gesetzter und damit verfügbarer Rasterdaten. Die finale Aussage liegt in der minimalen Zusicherung der Verfügbarkeit der Dienste von 99.9 Prozent für ein ganzes Jahr. Eine potentielle Einschränkung auf bestimmte Servicezeiten liegt allgemein nicht vor. Damit kann von einer jährlich erlaubten maximalen Ausfallzeit von unter acht Stunden und fünfundvierzig Minuten ausgegangen werden[202].

Da es sich um die markt-dominierenden Dienstanbieter handelt, lässt sich daraus indirekt ein referenzierbarer, marktspezifischer Standard für die Mindestverfügbarkeit jetziger kommerzieller Rasterdatendienste definieren und

[196] Vgl. Kapitel 4.1.1 Rechtliche Anforderungen - Interne und externe Dienstnutzung
[197] Vgl. Kapitel 2.6.1 Risikoidentifikation und Analyse
[198] Vgl. Google (2009)
[199] Vgl. Microsoft (2009)
[200] Vgl. ESRI (2009)
[201] Quelle: eigene Darstellung
[202] Vgl. Tabelle 16 - Verfügbarkeit von Rasterdatendiensten

als am Stand der Technik orientierte Mindestanforderung durch die Nutzer vereinbaren. Die Betonung liegt dabei auf Mindestverfügbarkeit, da kommerzielle Dienste durch den Einsatz zusätzlicher, vertraglich vereinbarter, technischer und damit kostenintensiver Mittel in der Verfügbarkeit gesteigert werden können[203].

Damit angesprochen sind insbesondere taktisch-operative Bereiche bei denen eine Ausfallzeit von mehreren Stunden im Zuge unmittelbarer Reaktionen auf unvorhergesehene Ereignisse nicht hinnehmbar ist. Dies betrifft insbesondere die Einsatzbereiche von Polizei, Feuerwehr, Katastrophenschutz und Militär bei denen Rasterdatendienste hochverfügbar[204] gehalten werden müssen. Dementsprechende Ausfallzeiten bewegen sich in nächsthöheren Spektren, gegenüber den zuvor erwähnten kommerziellen Rasterdatendiensten, zwischen 99,99 und 99,999 Prozent. Die daraus resultierenden Ausfallzeiten sind in Tabelle 16 dargestellt.

Verfügbarkeit	Minimale erwartete Betriebszeit [h] pro Jahr	maximal erlaubte Ausfallzeit [h] pro Jahr	maximal erlaubte Ausfallzeit pro Woche
	24h x 365d	24h x 365d	24h x 365d
99%	8672,40	87,60	1h 41'
99,9%	8751,24	8,76	10'
99,99%	8759,12	0,88	1'
99,999%	8759,91	0,09	6"
100%	8760,00	0	0"

Tabelle 16 - Verfügbarkeit von Rasterdatendiensten[205]

Auf der anderen Seite existieren, wie die Spezifikation der Darstellungsdienste von INSPIRE belegt, auch publizierbare niedrigere Forderungen. Hier insbesondere besteht der Anspruch einer Verfügbarkeit von 99 Prozent[206].

Der Verfügbarkeit stehen nicht minder Forderungen bzw. Anforderungen an Kapazität, Geschwindigkeit, Sicherheit und Interoperabilität[207] sowie Skalierbarkeit, Parallelisierbarkeit und Automatisierbarkeit gegenüber. Die Verfügbarkeit eines Dienstes allein zur Gütebeurteilung reicht nicht aus, weil damit

[203] Dies obliegt der Auseinandersetzung in konkreten vertraglichen Verhandlungen zu Service Level Agreements. Vgl. Kapitel 2.2.3 Service Level Management
[204] Vgl. Kapitel 2.1.1 Verfügbarkeit
[205] Quelle: eigene Darstellung
[206] Vgl. Network Services Drafting Team (2009), S. 27
[207] Vgl. Tabelle 11 - Kennzahlen von Webservices

nichts darüber ausgesagt wird, welche Last der Dienst in welcher Zeit und mit welchem Erfolg bewerkstelligen kann.

Darüber hinaus gilt es die generelle technische und sicherheitstechnische Ebene und damit den Grad der technischen als auch der sicherheitstechnischen Interoperabilität zu definieren, in dessen Umfeld der Dienst interagieren muss. Handelt es sich zum Beispiel um Rasterdatendienste, die als reine Webservices[208] zur Verfügung gestellt werden oder gilt es OGC-konforme Dienste[209] bereitzustellen. Erst auf dieser technischen Vereinbarung lassen sich dann zusätzliche technische und vor allem aber auch sicherheitstechnische Eigenschaften definieren und umsetzen[210].

4.1.3 Organisatorische Anforderungen

In Summe ergibt sich eine Vielzahl von nutzerspezifischen Anforderungen, die es bereits im Rahmen von Service Strategien im Sinne der Betrachtung der jeweiligen Businessanforderungen und in der darauffolgenden Serviceausprägung im Rahmen von zu staffelnden Service Levels auszuhandeln und im laufenden Betrieb zu überprüfen gilt[211]. Eine enge Bindung an bestehende Servicemanagement- und Servicesicherheitsstrategien ist, auch im Zuge der vertraglichen Gewährleistung und im Zuge der Sicherung der Compliance unumgänglich[212]. Möglichkeiten der Erweiterung oder der Veränderung bestehender Rasterdatendienste sind im Rahmen weiterer Serviceleistungsparameter in SLA einzubringen bzw. kontinuierlich zu ergänzen. Das betrifft nicht nur explizit die Verfügbarkeit, sondern auch deren Variabilität und zusätzlich zu vereinbarender Leistungsparameter[213]. Des Weiteren gilt es die in Kapitel 4.2 beschriebenen Risiken durch dementsprechende Strategien abzusichern[214].

[208] Vgl. Kapitel 2.7 Webservices
[209] Vgl. Kapitel 2.8.3 OGC-Webservices
[210] Zum Beispiel für Webservices: WS-Security, WS-Trust, WS-Policy, SAML und für OGC-Services: Geo Digital Rights Management (GeoDRM), Web Authentification Services (WAS), Web Security Service (WSS), Geospatial Extensible Access Control Markup Language (GeoXACML).
[211] Vgl. Kapitel 2.5.4.1 Servicestrategie
[212] Vgl. Kapitel 2.5.3 ISO/IEC27000ff und 2.5.4ISO/IEC20000/ITIL
[213] Vgl. Kapitel 2.2.3 Service Level Management
[214] Vgl. Kapitel 2.5.4.4 Servicebetrieb und Serviceverbesserung

4.2 Risikobestimmung

Das vorangegangene Kapitel beschäftigte sich mit individuell möglichen Nutzeransprüchen gegenüber der Bereitstellung von Rasterdatendiensten. Diesen stehen potentielle Risiken gegenüber, die es im jeweiligen Systemumfeld zu betrachten gilt. Generelle Risiken wurden bereits in den Kapiteln 2.3 und 4.1.1 beschrieben. Das Hauptrisiko eines Rasterdatendienstes besteht in dessen Nichtverfügbarkeit als Ganzes sowohl für den Nutzer als auch für den Dienstanbieter. Betroffen davon sind alle Komponenten des Systems[215] sowie die assoziierten Servicemanagementbereiche. Die Architektur und das Kommunikationsmodell des Image Servers wurden bereits im Kapitel 2.8.5 vorgestellt. Die dementsprechende Konfiguration lässt sich aus Kapitel 3 eruieren. Die erforderlichen Parameter zur Risikobestimmung sind in Kapitel 2.6.1 zusammengefasst.

4.2.1 Technische Risiken

Allgemein lässt sich zunächst feststellen, dass die in Kapitel 2.6.2 vorgestellten Datenbanken keinerlei Gefahrenklassifikation und damit verbundene Risikoklassen für die verwendete Konfiguration des Programmsystems abbilden. Services, insbesondere die hier verwendeten Rasterdatenservices, sind nicht durch dementsprechende Kennzahlen repräsentiert[216]. Formal muss ebenso festgestellt werden, dass die hier verwendeten Komponenten des ArcGIS-Image Server sowie dessen hardwareseitige Umgebung nicht nach ITSEC oder Common Criteria zertifiziert sind[217] und damit sicherheitstechnisch in diesem Rahmen nicht beschreibbar sind. Dadurch kann eine entsprechende Einordnung in diesem Rahmen nicht stattfinden.

Wie in Kapitel 2.1.1 beschrieben, ist das Zusammenspiel aller Komponenten ausschlaggebend für einen funktionierenden Dienst und dessen mögliche Ausfallsicherung. Dementsprechende marktspezifische Anforderungen wurden in Kapitel 4.1.2 beleuchtet. In der vorliegenden Architektur beschränken sich daher die komponententechnischen Risiken auf die Daten selbst, die Art der Datenspeicherung, das Netzwerk, das Betriebssystem, die Serverapplika-

[215] Vgl. Kapitel 2.6.1 Risikoidentifikation und Analyse
[216] Vgl. Tabelle 9 – Risikoanalyseverfahren
[217] Vgl. Kapitel 2.5.1 ITSEC und Kapitel 2.5.2 Common Criteria

tion und die Clientapplikation. Die zusammenhängende Wirkungsweise dafür ist in Abbildung 21 zur Übersicht dargestellt[218].

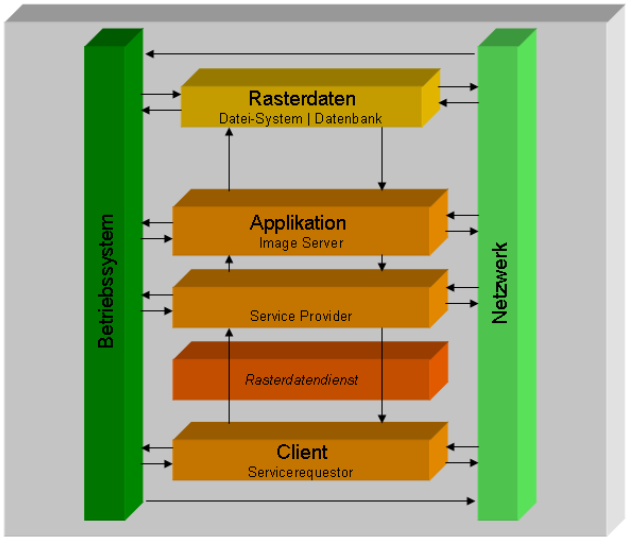

Abbildung 21 - Systemkomponenten[219]

Bei der Form der Datenspeicherung gilt es zwischen dem Vorhandensein der Rasterdaten im Dateisystem bzw. in einer Datenbank zu unterscheiden. Die Speicherung von Rasterdaten im Dateisystem ist die eigentliche Domäne des Image Servers. Das primäre Risiko für den Dienst besteht in der Nichtverfügbarkeit der Daten bzw. der Änderung oder Veränderung der Daten. Für den Zugriff auf die Daten bzw. die Datenbank ist das Netzwerk entscheidend. Ohne eine dementsprechende Verbindung kann sowohl die Kommunikation zwischen Serviceanbieter (Provider) und Servicenutzer (Client), als auch der generelle Zugriff auf die Daten nicht erfolgen.

Als weiteres Risiko lässt sich die Applikation selbst definieren. Hier spielt insbesondere die Schnelligkeit, die Robustheit und die Skalierbarkeit der Serverapplikation und damit des Dienstes eine entscheidende Rolle. Das bedeutet in diesem Zusammenhang zum einen, wie reagiert die Applikation auf Veränderungen von zugrundeliegenden Daten, und auf der anderen Seite, wie verhält sich das System bei Lastwechseln. Veränderungen an Daten können zwangsläufig zu Fehlern in dementsprechend assoziierten Rasterdatendiensten führen. Ebenso können signifikante Veränderungen von Nutzerzahlen zu einer

[218] Vgl. Kapitel 2.6.1 Risikoidentifikation und Analyse
[219] Quelle: eigene Darstellung

Destabilisierung des Rasterdatendienstes beitragen[220]. Zu dem besteht ein Risiko in der Frage, wie schnell können Daten durch Dienste überhaupt repräsentiert, in Wert gesetzt oder aktualisiert werden. Eine unsichere Applikation birgt ebenso, wie ein unsicheres Betriebssystem die grundsätzliche Gefahr eines nicht-kontinuierlichen Servicebetriebes. Das Risiko des unautorisierten Zugriffs auf Quelldaten, Dienst, Programm- und Betriebssystem und damit die eigentliche Servicesicherheit[221] gilt es ebenso nicht zu vernachlässigen, um damit ungewollte Manipulationen an hier genannten Rasterdatendiensten oder ungewollte Ressourcenzugriffe zu vermeiden.

Aus technisch-organisatorischer Sicht gilt es zusätzlich die betriebliche Infrastruktur im Zuge einer klar zu garantierenden Betriebssicherheit zu betrachten. Die Betriebssicherheit[222] selbst darf für einen dienstleistungsorientierten, dienstzentrierten Wertschöpfungsprozess kein Risiko darstellen.

4.2.2 Organisatorische Risiken

Die organisatorischen Risiken bestehen prinzipiell in der Nichtverwirklichung organisatorisch-technischer und rechtlich relevanter Anforderungen[223]. Der dementsprechende Ausfall von Rasterdatendiensten auf Basis organisatorischer Defizite ist im Zuge heutiger serviceorientierter Dienstleistung nicht hinzunehmen. Daher bestehen die größten Risiken in der fehlenden oder mangelhaften Orientierung bzw. Umsetzung von Servicemanagement-, Qualitätsmanagement- und Sicherheitsmanagementframeworks und deren mehr oder weniger umfangreichen Kennzahlensysteme. Sofern dies nicht gegeben ist, können auch daraus ableitbare rechtliche verbriefte Dienst- bzw. Dienstleistungsvereinbarungen in Form von SLA nicht umfassend in Vertragswerke aufgenommen und damit Dienste auf deren Grundlage nicht in Wert gesetzt werden.

Existiert eine diesbezügliches Bindung an dementsprechende Managementframeworks nicht, ist davon auszugehen, dass die damit verbundenen Managementprozesse wie Servicelevelmanagement, Verfügbarkeitsmanagement, Kapazitätsmanagement, Veränderungsmanagement und Kontinuitätsmana-

[220] Vgl. Tabelle 11 - Kennzahlen von Webservices
[221] Vgl. Kapitel 2.1 Grundsätze von IT-Sicherheit, Security
[222] Vgl. Kapitel 2.1 Grundsätze von IT-Sicherheit, Safety
[223] Vgl. Kapitel 4.1 Erusion der Nutzeranforderungen

gement sowie Problemmanagement nicht oder nur rudimentär umgesetzt worden sind, eine Lebenszyklusorientierung an und von Diensten als Dienstleistung nicht gewährleistet und die Dienstleistung als solches potenziell gefährdet ist. Die damit einhergehenden Risiken für die Servicepolitik lassen sich daraus weiter ableiten.

Auf Basis von Nutzerforderungen oder Marktbeobachtungen werden Dienst- und Dienstleistungsansprüche nicht immer in entsprechende SLR in formale SLA kanalisiert. Durch die querschnittliche, auf die Nutzung von SLA fokussierte Interaktion des Servicelevelmanagements mit den allen anderen Managementdisziplinen, gehen Informationen im Zuge der Dienstleistungserbringung unter. Diesen Zusammenhang verdeutlicht Abbildung 22.

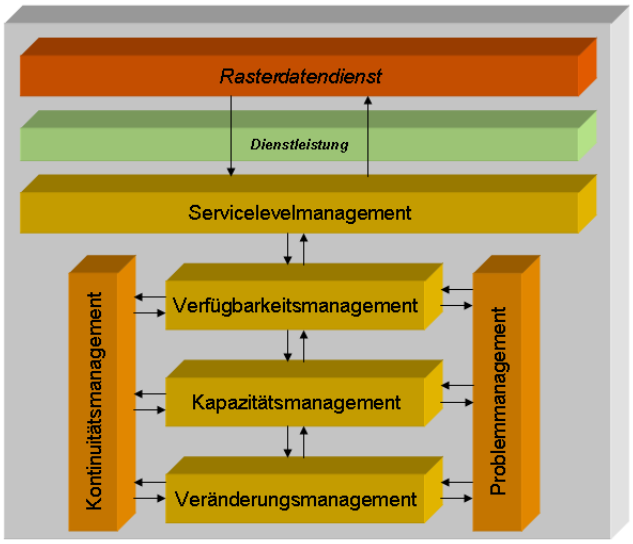

Abbildung 22 – Managementdisziplinen

Die verschiedenen Services werden nicht aus einer entsprechenden Servicestrategie, basierend auf konkreten Nutzerforderungen oder Marktumfragen, gewonnen und in SLA-Vereinbarungen festgehalten. Die darauf aufbauenden Managementprozesse können dann dementsprechend nicht mit den benötigten Parametern versorgt werden. Daraus folgt wiederum, dass die Dienstleistungserbringung als solche gefährdet ist, da das Servicelevelmanagement die Basis für die qualitative und quantitative Beschreibung des Rasterdatendienstes durch die Einbeziehung von Verfügbarkeits-, Kapazitäts- und Veränderungsmanagement legt. Daneben regulieren SLA, respektive SLR, den Umfang des Dienstes sowie die kontinuierliche Dienst- und Dienstleistungsver-

besserung durch die Hinzunahme von Ausnahme- und Problemlösungsstrategien. Ist dieser Kreislauf an Managementprozessen in diesem minimalquerschnittlichen Umfang dienstleistungs- und organisationsbezogen nicht etabliert, ist die Wertschöpfung bzw. das Wertschöpfungspotenzial eines Rasterdatendienstes stark risikobehaftet.

4.3 Ableitung von Service Levels

Service Levels dienen der grundlegenden Granularisierung der Qualität von zu erbringenden Rasterdatendienstleistungen. Eine diesbezügliche Ausprägung ist in allererster Linie abhängig von den in Kapitel 4.1 eruierten Anforderungen und entsprechend entgegenwirkenden Risiken aus Kapitel 4.2. Die Umsetzung der Businessziele (BLA) auf operativer Ebene durch entsprechende Serviceziele (SLA) im Rahmen ökonomischer Anforderungen und Bedingungen (BLR) ist vordringliches Ziel einer Servicedienstleistung auf Basis von Rasterdatendiensten. Eine davon abhängige Differenzierung der Servicegüte und damit Servicequalität erfolgt durch Dienstanbieter und Nachfrager sowie durch den damit verbundenen (Geoinformations-)Markt für Rasterdatendienste und deren marktüblichen Vereinbarungen, gleichzeitig basierend auf dem derzeitigen Stand der Technik.

Aus rechtlicher Sicht geht es, primär und unabhängig von der Servicegüte, immer um die vollständige Erfüllung des Vertrages und um die Gewährleistung der Rasterdatendienstleistung[224]. Daher gilt es, innerhalb des organisatorischen Rahmens, technische Maßnahmen im erforderlichen Umfang umzusetzen. Den Grad der Umsetzung bestimmt dann die mit dem Nutzer individuell zu verhandelnde Servicegüte.

Die Kapitel 2.1.1, 2.5.4.4, 2.7.3 sowie 4.1.2 zeigten bereits die Notwendigkeit der Verwendung unterschiedlicher dienst- und damit gütebeschreibender Kennzahlen im organisatorisch-technischen Rahmen von Rasterdatendiensten. Es ist jedoch anzumerken, dass keine allgemeinverbindlichen Richtlinien für die jeweilige Festschreibung von Kennzahlen und Metriken zu SLA im Bereich von Rasterdatendiensten existieren. In diesem Zusammenhang ist es wichtig, dass entsprechende SLA dynamisch gestaltet bzw. gehalten werden

[224] Vgl. Kapitel 2.1 Grundsätze von IT-Sicherheit

und vertraglich die Möglichkeit besteht, nach zu vereinbarenden Leistungsreviews sowohl auf Anbieter- als auch auf Nachfragerseite, diesbezügliche Anpassungen in allen Bereichen vornehmen zu können, da sich Nutzungsverhalten und Nutzungsaufkommen jederzeit ändern können[225]. Evident wichtig ist ebenso die die Festschreibung, in welchen Intervallen diese Änderungen, die zum Teil immense technische und organisatorische Veränderungen für den Dienstanbieter haben, stattfinden können. Für den Servicenachfrager spiegeln sich diesen Angaben nur in konkret zu verhandelnden SLA wider, wohingegen der Dienstanbieter weiterführende kritische technische und organisatorische sowie zum Teil infrastrukturelle Maßnahmen umsetzen muss[226].

Von daher verstehen sich die hier vorgeschlagenen Kennzahlenwerte als Näherungswerte, da sie sich zum einen in steter Korrelation zueinander befinden und zum anderen in einer unüberschaubaren Vielzahl auftreten können sowie anwendungsbezogen validiert werden müssen.

Besonders in diesem Zusammenhang ist die Verfügbarkeit von der Hochverfügbarkeit eines Dienstes als erster Differenzierungsgrad zu unterscheiden. Dabei kann die Ausfallsicherheit aus der Verfügbarkeit definiert werden. Rasterdatendienste lassen sich aus den Anforderungen und aus gängiger Praxis damit in entsprechenden Umgebungen in verschiedene Grade klassifizieren. Die Tabelle 17 zeigt ein dementsprechend mögliche Aufteilung sowie eruierte Beispielanwendungen.

Verfügbarkeit [%]	Beschreibung	Beispielimplementierung
99	einfache Verfügbarkeit	INSPIRE
99.9	erhöhte Verfügbarkeit	Google Maps
99.99	gesteigerte Verfügbarkeit	Katastrophenschutz (DSS)
99.999	Hochverfügbarkeit	Einsatzleitsysteme (OPZ)

Tabelle 17 - Verfügbarkeitslevel

Dabei sind zusätzlich eindeutige Aussagen zu den in Kapitel 2.1.1 getroffenen Verfügbarkeitskennzahlen, nötig. Das betrifft insbesondere Angaben zu MTBF und MTBSI. MTBSI stellt die direkte Verbindung zum Kontinuitäts- bzw. Incidentmanagement her bzw. fokussiert eindeutig auf die nicht zu vernachlässigende Servicezuverlässigkeit. Darauf aufbauend müssen dementsprechende

[225] Vgl. Abbildung 22 – Managementdisziplinen
[226] Vgl. Kapitel 4.5.2 Programmspezifische Möglichkeiten und 4.5.3 Optionale Möglichkeiten

Klassifikationen vereinbart werden, die einen Incident als solchen beschreiben. Davon ausgehend wird teilweise in der Praxis die Anzahl der maximal auftretenden Serviceunterbrechungen festgelegt, für den ein entsprechender Support durch den Serviceprovider geleistet wird[227]. Diese Werte lassen sich allerdings schwer bestimmen, sofern nicht dementsprechende Erfahrungswerte bestehen bzw. sind zunächst operativ zu ermitteln und in darauffolgenden SLA-Verhandlungen konkret mit Zahlenwerten zu belegen[228].

Neben der generellen Verfügbarkeit und Zuverlässigkeit für Rasterdatendienste wirkt sich die Geschwindigkeit der durch die Dienste bereitgestellten Rasterdaten als dritte Kennzahl wesentlich auf einen zu definierenden Servicegrad aus. Hierfür ist insbesondere der Nutzungsgrad bzw. das Nutzungspotenzial und der Grad der Abhängigkeit in korrelierten Produktivsystemen entscheidend[229]. Während reine, webbasierte Informativsysteme mit regulären Antwortzeiten von in der Regel nicht mehr als zehn Sekunden auskommen, sind entscheidungsrelevante Systeme mit Antwortzeiten besser fünf Sekunden durch die assoziierten Dienste zu versorgen. Sofern diese Übertragungszeiten nicht eingehalten werden, ist mit entsprechenden Verzögerungen in den jeweiligen Entscheidungssystemen bzw. Produktionsumgebungen zu rechnen.

Damit verbunden ist gleichzeitig die Fähigkeit der Skalierung, d.h. der Bewältigung komplexer Serviceanfragen in Form von gleichzeitig konkurrierenden Zugriffen. Nicht zu vernachlässigen ist dabei insbesondere das Volumen der zu übertragenden Daten[230] sowie die damit verbundenen Sicherheitsstufen für Zugriff und Übertragung der Dienstinhalte in Abhängigkeit zur technischen Realisierung und zum geforderten Interoperabilitätsniveau. Im übergeordneten Rahmen ist auf eine Fixierung der Servicekontinuität zu achten. Dies bedeutet, dass entsprechende Notfallpläne zur Problembewältigung im interagierenden Rahmen mit allen anderen Servicemanagementprozessen implementiert,

[227] Vgl. Forsythe, Jennifer. <jennifor@microsoft.com> “Bing: SLA”. Persönliche Email. 24.09.2009. 24.09.2009.
[228] Dies setzt die Vereinbarung von Service Reviews innerhalb von SLA voraus. Vgl. Kapitel 2.2.3 Service Level Management
[229] Dementsprechende OLA und UC im Zuge interner und externer Dienst- und Dienstleistungsbereitstellung sind hierfür nicht zu vernachlässigen.
[230] Bei Rasterdatendiensten sind entsprechende Größen zu definieren. Ein typisches Ausgaberaster für den Webbereich hat dabei eine Größe von 800x600 Pixeln und ist bei entsprechender Farbtiefe von 8 bit etwa 800 Kilobyte groß.

abgeglichen und auch in SLA fixiert sein müssen. Die Zusicherung einer Verfügbarkeit eines Rasterdatendienstes von 99.9 Prozent macht keinen Sinn, wenn dementsprechende Ansprechpartner und diesbezügliche Eskalationsstrategien nicht erreicht und nicht definiert worden sind.

4.4 Formalisierung

Die Anforderungen an Rasterdatendienste müssen, um rechtlich, organisatorisch und technisch verwertbar zu sein, in entsprechende Vertragswerke überführt werden. Ein erster Schritt ist dabei die schriftliche Fixierung der vereinbarten Kennzahlen und Metriken[231]. Im Zuge der voranschreitenden Automatisierung sind Wege zu suchen, diese Bedingungen in maschinenlesbarer Form interagierenden Vertragspartnern zur Verfügung zu stellen und zukünftig darauf aufbauende Verträge automatisiert auszuhandeln. Grundlegende Möglichkeiten ergeben sich zum einen aus formalisierten SLA und zum anderen aus deren Implementierung in Produktivsysteme. Entsprechende Serviceparameter können je nach Serviceart und Implementierung in unterschiedlichen Bereichen fixiert werden. Für Webservices[232] ergeben sich bereits zwei Möglichkeiten, auf Basis von UDDI und WSDL, SLA-Parameter entsprechend zu fixieren und zumindest auslesbar zu gestalten. Für RPC und die hier in Verbindung stehenden Rasterdatendienste auf Basis des Image Servers ergeben sich diese Möglichkeiten auf dieser Ebene leider nicht. Generell besteht allerdings die Möglichkeit, SLA als Metainformationen außerhalb des Programmsystems in Form zusätzlicher Parameterdateien zur Verfügung zu stellen. Diese können mit Hilfe von Formalisierungssprachen wie WSLA normiert werden. Die Anlage 3 enthält ein vereinfachtes Beispiel für ein WSLA-Dokument. In ihr wird die Kapazität der Rasterdatenservicedienstleistung zwischen zwei Vertragspartnern auf Basis einer Mittelwertberechnung mit dem Regelwert 1000 als SLA-Parameter vereinbart[233].

Mit Hilfe der Formalisierung wird der Weg zur automatisierten Verhandlung zwischen Vertragsparteien im Rahmen von E-Business und damit verbunde-

[231] Vgl. Kapitel 2.2.3 Service Level Management
[232] Vgl. Kapitel 2.7 Webservices
[233] Die Kapazität (SLA-Kennzahl) wird mit dem Sollwert 1000 (SLA-Bedingung) und dem arithmetischen Mittel, d.h. die Anzahl aller tatsächlich pro Stunde eingehenden Requests(SLA-Metrik), verglichen.

nem E-Contracting und E-Trading frei[234]. Dementsprechenden Implementierungsaufwand gilt es auch im Bereich von Rasterdatendiensten im Geoinformationsbereich umzusetzen, um die Servicequalität hinreichend voranzutreiben und vor allem zu sichern.

4.5 Umsetzung im Programmsystem

Die rechtlichen Rahmenvorgaben sind auf der Grundlage vertraglicher Gestaltungsmittel und organisatorischer Rahmenprozesse auf Basis von ITIL[235] auch für Rasterdatendienste technisch realisierbar. Im Vordergrund steht vor allem das in SLA zu fixierende Verfügbarkeits- und Servicekontinuitätsniveau als Basis für die Sicherung der zu erbringenden Dienstleistung.

4.5.1 Allgemeiner Betrieb

Generell lässt sich zunächst sagen, dass es sich bei dem verwendeten Programmsystem um eine sehr zuverlässige Dienstumgebung handelt. Während der gesamten Beobachtungsdauer gab es keinerlei Dienstausfälle. Die beiden betriebenen Services[236] waren ohne Einschränkungen über die Clienten mit gleichbleibender Performance erreichbar. Die Anlaufzeiten für die Inbetriebnahme bzw. für die Diensterstellung können Anlage 4 entnommen und als performant bezeichnet werden. Alle Komponenten, Image Server, Serviceprovider und Clienten wurden dabei auf einer Recheneinheit betrieben.

Bei dem in dieser Konfiguration betriebenen System handelt es sich unschwer um ein SPOF-System[237]. Fällt eine Komponente aus, ist der Service nicht verfügbar[238]. In Verbindung mit Abbildung 21 müssen die zusammenwirkenden Komponenten getrennt voneinander betrachtet werden. Die Rasterdaten und dementsprechend assoziierte Daten liegen im Dateisystem vor[239]. Ein Trennen der Daten von der Applikation führt unweigerlich zur Nichtverfügbarkeit

[234] E-Contracting und E-Trading bezeichnen die Vertragsschließung und den diesbezüglichen Handel auf elektronischer Basis. E-Contracting hat einen wesentlichen Einfluss auf den Realisierungsgrad von E-Government und damit unter anderem auch auf den Bereich des heutigen, behördlichen Geoinformationswesens bzw. der Geoinformationswirtschaft.
[235] Vgl. Kapitel 2.5.4 ISO/IEC20000/ITIL
[236] Vgl. Kapitel 3 Vorgehen und Methode
[237] Vgl. Kapitel 2.6.2 Risikobewertung und Behandlung
[238] Nach der Definition exkludiert dies die Clientapplikation. Fällt der Client aus, ist der Service dennoch erreichbar. Ausschlaggebend in diesem Zusammenhang ist, ob die Clientapplikation Bestandteil der SLA-Vereinbarungen gewesen ist.
[239] Dies umfasst sämtliche Servicedateien, die für den kontinuierlichen Betrieb des Service verantwortlich sind. Vgl. Kapitel 2.8.5.1 Architektur

des Rasterdatendienstes. Ist die Applikation als solche nicht präsent, können die Rasterdaten ebenfalls nicht als Service zur Verfügung gestellt werden. Änderungen an den Rasterbasisdaten im Zuge von Aktualisierungen führen zunächst nicht zu einer Veränderung des Services[240].

4.5.2 Programmspezifische Möglichkeiten

Es gilt festzuhalten, dass das technische Risiko des Ausfall eines Dienstes bereits im Rahmen des Programmsystems selbst minimiert werden kann, indem die verwendeten Komponenten auf verschiedenen Recheneinheiten implementiert und betrieben werden.

Im Zuge heutiger, leistungsfähiger COTS-Hardware ist diese schlichte Variante in Produktivsystemen bevorzugt umzusetzen. Die Anzahl der Image Server ist dabei abhängig von der Anzahl vorhandener Lizenzen, wohingegen die Zahl korrespondierender Serviceprovider unbegrenzt ist. Im Fall der verteilten Anlage von Servicekomponenten verfügt der Image Server mit Hilfe des Server Managers über eine Zugangskontrolle. Damit lassen sich unter einfachen sicherheitstechnischen Gesichtspunkten die Nutzer für Server Manager, Service Provider und Service Editor in einfacher Weise einschränken[241].

Die Abbildung 23 zeigt eine dementsprechende Konfiguration sowie deren Erweiterung. Hierfür gibt es mehrere Varianten. Eine erste Möglichkeit besteht darin, dass ein Image Server auf mehrere Service Provider zurückgreifen kann. Eine erste Form der Absicherung kann, wie beschrieben, in Form der Verteilung von Serviceprovidern auf verschiedene Hostrechner erfolgen.

Eine weitere Möglichkeit besteht in der zusätzlichen Etablierung eines Image Servers auf einem weiteren Hostrechner. Dieser kann für einen dritten Fall, mit weiteren, wieder unabhängigen Service Providern verbunden werden. Der Prozess lässt sich beliebig fortsetzen und geht mit der steigenden Redundanz von Komponenten einher, was die Grundlage für eine daraus abzuleitende Verfügbarkeit bildet[242]. Durch die Möglichkeit der Verteilung der Softwarekomponenten auf verschiedene Recheneinheiten zeichnet sich das betrachtete System durch eine hohe Parallelisierbarkeit aus.

[240] Die umfasst das Entfernen und Hinzufügen von Rasterdaten.
[241] Vgl. Kapitel 2.1 Grundsätze von IT-Sicherheit
[242] Vgl. Kapitel 2.1.1 Verfügbarkeit

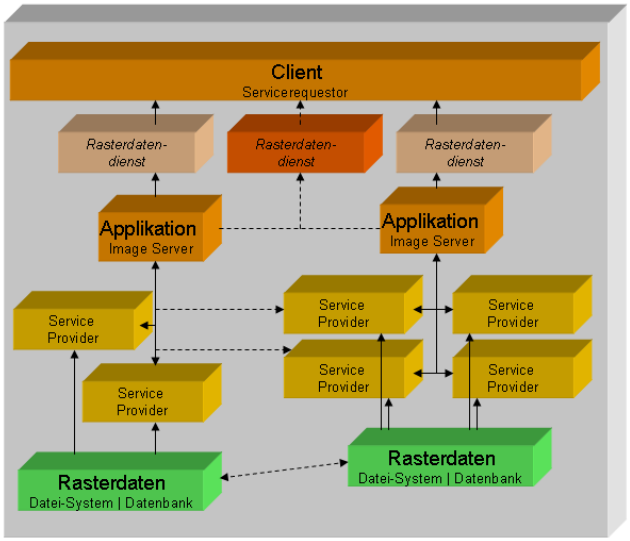

Abbildung 23 - Konfigurationsmöglichkeiten[243]

Die Multiplikation von Komponenten kann mit einer gleichzeitigen Multiplikation entsprechend referenzierter Rasterdatendienste verbunden werden. Fallen einzelne Dienste aus, kann deren Ausfall durch parallelen Betrieb auf anderen Instanzen wiederum kompensiert werden. Entsprechend parallelisierbare Dienstanlagemöglichkeiten tragen zur Ausfallsicherung und Verfügbarkeitssteigerung bei.

In Bezug auf die Skalierbarkeit des Programmsystems, ferner auf eine mögliche Dienstauslastung durch Nutzeranfragen, gilt es festzuhalten, dass der Image Server selbstständig in Abhängigkeit der vorhandenen Verbindungen und der Anzahl der Service Provider deren Auslastung skaliert. Diese können mit Hilfe des Server Managers zusätzlich gewichtet werden[244]. Dies ist insbesondere bei der Ausprägung mehrer Rasterdatendienste von Vorteil, um auf Geschwindigkeitsanforderungen der Nutzer direkt reagieren zu können. Zusätzlich besteht dadurch die Möglichkeit, in verteilten Systemen, Services zu priorisieren und bevorzugt in Abhängigkeit zur Last zur Verarbeitung zu bringen.

Die Ergebnisse des Lasttests in Tabelle 18 zeigen die gute Skalierbarkeit des Image Servers bei gleichzeitiger Steigerung der parallelen Verbindungen für

[243] Quelle: eigene Darstellung
[244] Die Gewichtung wird als Power Rating bezeichnet.

beide Dienste[245]. Getestet wurden beide Dienste mit Hilfe zufällig verteilter Interessengebiete bei gleichzeitig redundanten Messungen. Eine entsprechende Aufstellung kann der Anlage 5 und Anlage 6 entnommen werden. Etwa 60000 Requests trugen zum Ergebnis in Tabelle 18 bei. Der zahlenwertige Unterschied zwischen dem ETM- und dem DTED-Dienst ist durch die spezifizierte Aufteilung und die daraus resultierende große Anzahl von DTED-Kacheln bedingt[246].

Anzahl der Service Provider	connections	duration [s]	AOI	Service	Requests	average request time [s]	max process time [s]	request per second
1	10+40	300	1+2	ETM	3916	0.19	1.81	13.05
2	10+40	300	1+2	ETM	3918	0.32	2.54	13.06
4	10+40	300	1+2	ETM	3962	0.67	3.91	13.21
1	10+40	300	1+2	DTED	960	0.70	3.31	3.20
2	10+40	300	1+3	DTED	975	1.24	4.70	3.25
4	10+40	300	1+4	DTED	983	2.31	8.08	3.28

Tabelle 18 - Lasttest (vereinfacht)[247]

Als evident wichtig für das Betreiben von Rasterdatendiensten gestaltet sich das Monitoring laufender Dienste. Der ArcGIS Image Server verfügt durch das Frontend des Image Server Managers und über die ISCommand-Umgebung über die Möglichkeit, den Status der vorhandenen Dienste anzuzeigen und zu verändern.

Mit Hilfe der ISCommand-Umgebung kann dies ohne umfangreichen programmatischen Aufwand geschehen. Für das notwendige, automatisierte Monitoring von Diensten eignet sich die Möglichkeit, bestehende Dienste mit Hilfe einer zeitgesteuerten Batchdatei in bestimmten Intervallen zu stoppen und gleichzeitig die Dienste im umgekehrten Verfahren wieder zu starten. Für diesen sehr einfachen Weg der Realisierung stehen ISCommand-Befehle zur

[245] Die Anlage 7 enthält die komplette Übersicht der Ergebnisse.
[246] Dementsprechend groß ist die Zeit, die für den Zugriff benötigt wird. Vgl. Anlage 4.
[247] Quelle: eigene Darstellung. Serviceparameter waren Bilineare Interpolation, Closest-to-Center Mosaikierungsverfahren und JPEG-Kompression.

Verfügung[248]. Diese werden in Tabelle 19 dienstbezogen beispielhaft dargestellt.

Funktion	ISCommand
Servicestart	ISCommand ServerManager --Action=**StartService** --ServerHost=<Host> --Endpoint=<Port> --ServiceName=<ServiceName> --ISPList=<ListOfISP>
Servicestop	ISCommand ServerManager --Action=**StopService** --ServerHost=<Host> --Endpoint=<Port> --ServiceName=<ServiceName> --ISPList=<ListOfISP>
Synchronize	ISCommand ServerManager --Action=**Synchronize** --ServerHost=<Host> --Endpoint=<Port> --ServiceName=<ServiceName>

Tabelle 19 – ISCommand[249]

Gleichzeitig steht mit der ISCommand-Umgebung auch ein Kommando zur Verfügung, um für Dienste nach Aktualisierungen von Rasterbasisdaten die Synchronität zwischen den Service Providern und den jeweiligen Diensten herzustellen. Dies umfasst das Laden bzw. das erneute Laden eines Dienstes sowie das Entfernen des Dienstes, sofern er nicht mehr in im Dienstverzeichnis aufgeführt wird[250]. Diese Funktion kann auch automatisiert für die Service Provider im Rahmen der Einstellungen des Image Server Managers konfiguriert werden. Der Vorteil besteht darin, dass sich dynamisch ändernde Rasterdaten über spezifische Service Provider selbst aktualisieren können.

Die Aktualisierung von Diensten ist ein nicht zu vernachlässigender Aspekt, da in Produktiv- aber insbesondere in Einsatzumgebungen ein Widerspruch zwischen einem Produkt bzw. einer Planungsgrundlage und den aktuellen Daten existiert. Dieser Widerspruch tritt deshalb auf, weil das Produkt bzw. die Entscheidung zu einem fixierten Zeitpunkt aus dem assoziierten Dienst abgleitet wird. Sofern Rasterdaten vorliegen, die die Entscheidung oder das Produkt nachhaltig beeinflussen oder verändern können, muss dementsprechend eine Aktualisierung erfolgen. Problematisch ist hier die Entscheidung über die Nachhaltigkeit. Daher gilt es hier zusätzliche Regeln oder Prozesse zu vereinbaren, wann der Dienst aktualisiert wird. Denkbar wäre, die Rasterdatenverzeichnisse zu überwachen und bei Veränderungen automatisch neue Dienste zu erzeugen. Allerdings muss in diesem konkreten Fall zwischen hinzukom-

[248] Vgl. Tabelle 19 – ISCommand, Servicestart und Servicestop
[249] Quelle: eigene Darstellung
[250] Vgl. Tabelle 19 - ISCommand, Synchronize

menden und gelöschten Daten unterschieden werden, da gelöschte Daten nicht mehr zur Diensterstellung genutzt werden können. Dieses Problem kann mit der Speicherung und Versionierung von Rasterdaten umgangen werden[251].

4.5.3 Optionale Möglichkeiten

Wie im vorangegangenen Kapitel bereits beschrieben, kann neben einer Multiplikation von Diensten, Applikationen und Komponenten auch das Gesamtsystem redundant gehalten werden. Dies wird als Systemcluster bezeichnet und ist in abstrahierter Form in Abbildung 24 dargestellt.

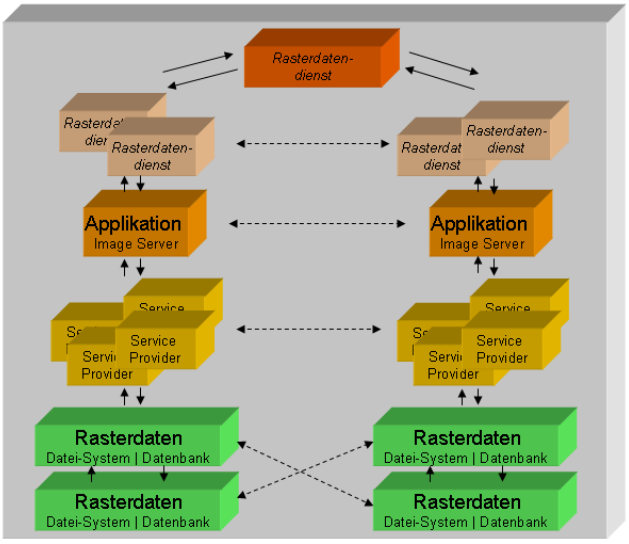

Abbildung 24 - Cluster, einfach

Bei einer dementsprechenden Multiplizität des Systems im Zuge einer Clusterbildung spricht man auch von Clusterverfügbarkeit[252]. Fallen einzelne Knoten aus, wird deren Information bzw. Aufgabe durch eine dementsprechend gespiegelte Komponente im Parallelsystem übernommen. Dies kann ebenso für Dienste erfolgen.

Die Abbildung 24 zeigt jedoch nur eine einfache Variante. Grundsätzlich lassen sich solche Systeme technisch beliebig weiter kaskadieren. Zu unterscheiden ist hier insbesondere nach dem Status der beteiligten Systeme, ob diese aktiven oder passiven Status besitzen. Sind beide Knoten aktiv wird dies

[251] Vgl. Kapitel 4.5.3 Optionale Möglichkeiten
[252] Als Clusterverfügbarkeit wird eine Verfügbarkeit von 99.99 Prozent bezeichnet.

als synchroner Modus bezeichnet, wohingegen die Passivität eines einzelnen Knotens zur Asynchronität des Knotenverbundes führt.

Die Abbildung 24 zeigt gleichfalls zwei einfache Clusterknoten, die in dieser Grundkonfiguration wohl am meisten verwendet werden können. Im Sinne einer gesteigerten Betriebssicherheit sind diese Knoten an geografisch unterschiedlichen Orten zu positionieren, um das zusätzliche, gleichzeitig auf beide Orte auswirkende Risiko von Stromausfällen oder Naturkatastrophen auf ein Minimum zu reduzieren[253]. Die Abbildung 25 illustriert diese Variante der Verfügbarkeitssteigerung. Zusätzlich denkbare wäre der Einsatz aller Clusterknoten in Verbindung mit einem LOAD-Balancing System. Das bedeutet, dass die Last der nachgefragten Dienste zusätzlich eine Kontrolle erfährt[254] und in Abhängigkeit davon, der Request an das jeweilige System im entsprechenden Cluster weitergeleitet wird.

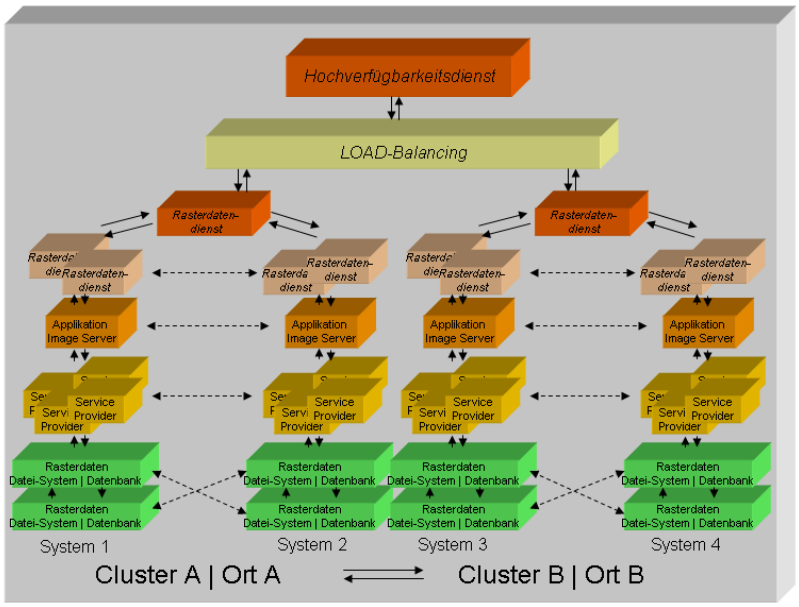

Abbildung 25 - Hochverfügbarkeitsfall[255]

Für Hochverfügbarkeitsdienste im Geoinformationsbereich sind sicherlich beide Varianten einsetzbar. Der Vorteil der einseitig aktiven Knoten liegt in der

[253] Vgl. Kapitel 2.3 Informationstechnische Bedrohungslage
[254] So wie es bei der Lastverteilung des Image Servers bereits bei der Einzellastverteilung der Service Provider der Fall ist.
[255] Quelle: eigene Darstellung

möglichen Wartbarkeit solcher Systeme[256]. Dies ist im Rahmen des Verfügbarkeits-, Kapazitäts- und Kontinuitätsmanagements individuell zu bestimmen.

In Kapitel 4.5.2 wurde bereits die Möglichkeit des Einsatzes von Datenbanken erwähnt, um das Problem der Versionierung von Rasterdaten zu beheben. ESRI bietet dazu durch den möglichen Zugriff auf Enterprise-Datenbanken via ArcSDE[257] entsprechende Versionierungsmöglichkeiten bereits an. Der zusätzliche Vorteil, der sich durch die Nutzung von Datenbanken bietet, liegt in der erhöhten Sicherheit des Zugriffs bzw. der zusätzlichen Möglichkeit, den Zugriff auf die Daten zu beschränken und mittels Replikationsverfahren, Rasterdatendaten automatisiert zwischen verteilten Instanzen abzugleichen. Allerdings gilt es mit dieser Lösung die Frage zu beantworten, ob es sinnvoll ist, die Daten redundant zu halten, da diese dann im Dateisystem und in der Datenbank vorliegen würden und zusätzlicher Arbeitsaufwand[258] entstünde, die Daten in die Datenbank zu überführen. Ein nicht zu unterschätzender Aspekt bei der Verwendung von ArcSDE ist die zusätzliche Authentifizierungsmöglichkeit für den Zugriff auf die Rasterdaten und die gleichzeitig mögliche Beschränkung auf zu spezifizierende Rasterdatensätze.

4.5.4 Integration in Geodateninfrastrukturen

Die applikationsseitige Skalierbarkeit des Image Servers und die dementsprechenden Lösungsvorschläge aus den Kapiteln 4.5.2 und 4.5.3 haben die generelle Möglichkeit gezeigt, Dienste gegen Ausfall abzusichern. Durch die zusätzlichen Möglichkeiten, Rasterdaten dynamisch zu prozessieren und dem Nutzer performant und ohne Redundanz zur Verfügung zu stellen, leistet der Image Server einen entscheidenden Beitrag in der Wertschöpfungskette.

Rasterdaten sind elementarer Bestandteil heutiger Geoinformationssysteme und damit Arbeits- sowie Entscheidungsgrundlage geoinformationszentrierter Geschäftsprozesse[259]. Es besteht daher ein erhöhter Bedarf, mit Hilfe von Rasterdaten Rasterdatendienste zur Verfügung zu stellen. Die vorliegende

[256] Vgl. Kapitel 2.1.1 Verfügbarkeit
[257] Nach der Definition eine Middleware, die den Zugriff auf Enterprise-Datenbanken, wie etwa Oracle oder SQL-Server erlaubt.
[258] Nicht zu vernachlässigen ist an dieser Stelle auch das Risiko zusätzlicher Fehler beim Übertragen der Daten in die Datenbank.
[259] Vgl. Kapitel 2.8 Rasterdatenservices

Konfiguration erlaubt, diesbezügliche Dienste bereitzustellen und Mehrwert durch die zusätzliche Dynamisierung von Inhalt zu generieren.

Um diese Dienste zu erzeugen, ist allerdings ein Service Editor in Ausprägung eines ArcGIS-Desktop Clienten notwendig[260]. Dies kann auf der einen Seite gut für Infrastrukturen sein, in denen ArcGIS ohnehin bereits verfügbar ist bzw. verwendet wird, führt allerdings auf der anderen Seite zu zusätzlichen Kosten. Daneben ist der Image Server zunächst in seiner Kommunikation auf RPC ausgerichtet und ist mit derzeitigem Stand, nur mit Hilfe des ArcGIS Servers in der Lage, gängige Protokolle in Geodateninfrastrukturen zu unterstützen. Generell kann diese Lösung als die zu bevorzugende Lösung angesehen werden, da entsprechende Freiheitsgrade durch zusätzlich zur Verfügung stehende Funktionalitäten und die zusätzlich unterstützten Protokolle erreicht werden. Dazu zählen insbesondere die Unterstützung des SOAP-Protokolls für die Partizipation von Rasterdatendiensten in Enterprisesystemen, die Unterstützung gängiger OGC-Webservices sowie von KML[261].

Die Verwendung des Image Servers ermöglicht daneben die Minimierung von Produktionsprozessen oder von Prozessen, in denen zusätzliche prozessuale Weiterverarbeitungsschritte nötig sind[262], da diese Ergebnisse durch den Dienst mit bereitgestellt werden können und sich dadurch zusätzliche Ressourcen bzw. Kapazitäten nicht nur organisations- oder unternehmensbezogen, sondern auch innerhalb von Geodateninfrastrukturen gewinnen lassen. Letztlich ist eine betriebswirtschaftliche Gesamtrechnung unabdingbar, die die Größe der möglichen Einsparungen erhebt und die mögliche Anschaffung des Programmsystems indizieren kann.

Die technischen Anforderungen bzw. die Systemanforderungen[263] des ArcGIS Image Servers und seiner Komponenten können zumindest als minimal und von handelsüblichen Rechnersystemen als erfüllbar bezeichnet werden.

[260] Vgl. Kapitel 2.8.5.1 Architektur sowie Anlage 2 – Komponenten und Produkte
[261] Vgl. Kapitel 2.8.5.3 Dienstklassifikation
[262] Vgl. Tabelle 14 - Rasterdatenprozesse
[263] Vgl. Anlage 1 - Systemvoraussetzung

5 Analyse und Beurteilung

Die Rasterdatendiensterstellung mit Hilfe des ArcGIS Image Servers kann als sehr praktikabel und nutzerfreundlich charakterisiert werden. Die Inwertsetzung von Rasterdaten erfolgt sehr performant, ressourcenschonend und bedarf wenig Systemleistung.

Generell ist diese technische Inwertsetzung an rechtliche und organisatorische Rahmenbedingungen geknüpft. Ausgehend von den über ITIL identifizierten Managementprozessen zur konsequenten und durchgreifenden Planung, Erstellung, Überführung, zum Betrieb und zur Verbesserung von Servicedienstleistungen können diese auf den Dienstleistungsprozess der dynamischen Rasterdatenbereitstellung über Rasterdatendienste im Bereich des Geoinformationswesens angewendet werden.

Darauf aufbauend lassen sich die Nutzeransprüche definieren. Allerdings sind diese sehr vielfältig, oftmals durch die Vorgaben der Serviceanbieter bestimmt oder erst im konkreten Servicebetrieb messbar. Unterschiedliche Anwendungsspektren bedingen sehr heterogene Ansprüche an die Verfügbarkeit, Kapazität, Geschwindigkeit, Zuverlässigkeit und Sicherheit sowie an die zusätzlich durchzuführenden Maßnahmen im Bereich der Eskalationsstrategien. Daher ist es unumgänglich, dementsprechende Graduierungen, vergleichbar der Granularisierung von Diensten, zwischen Dienstnutzer und Dienstanbieter teilweise individuell und mit den Erfahrungen eines umfassenden Testbetriebes zu vereinbaren.

Die Arbeit hat gezeigt, dass im Bereich heutiger Rasterdatendienste mit Grundverfügbarkeiten von 99 Prozent zu rechnen und dies für die Masse der Anwender ausreichend ist. In entscheidungstragenden Systemen liegt die Forderung dementsprechend höher und ist von der Ebene und der Konsequenz der jeweiligen Entscheidung abhängig.

Die Arbeit zeigt ebenfalls, dass Rasterdatendienste als wertschöpfende Prozesse von Servicemanagementframeworks wie ITIL partizipieren können. Dabei haben sich die gängigen Managementprozesse nahtlos auch für den ras-

terbasierten Dienstleistungsbereich der Geoinformationswirtschaft verwenden lassen. Fragestellungen, insbesondere des Verfügbarkeits-, Kapazitäts-, des Veränderungs- und Kontinuitätsmanagementes lassen sich auch für Rasterdatendienste in konkrete Forderungen in Form von SLA umsetzen. In der Arbeit konnten entsprechende Mindestanforderungen beschrieben werden. Die dafür benötigten Parameter wurden aus der Korrelation zwischen Rasterdatendiensten, Webservices und Servicemanagementframework eruiert.

Ferner konnte beispielhaft die Formalisierung einer konkreten Kennzahl am Beispiel von WSDL demonstriert werden. Formalisierung kann die Grundlage für zukünftige automatisiert verhandelbare Servicedienstleistungen auch im rasterbasierten Dienstleistungsbereich bilden. Damit eröffnet sich für den Geoinformationsbereich die Möglichkeit, ad hoc verhandelbare Dienstleistungen zur Verfügung zu stellen, ohne in zusätzliche Verhandlungen mit den Servicenehmern treten zu müssen und dennoch rechtlich abgesicherte Dienstleistungen zu erbringen.

Die Absicherung der Dienstleistung und damit die Sicherung der Servicekontinuität ist die Grundlage der technischen Betrachtung zum ArcGIS Image Server. Es konnte gezeigt werden, dass die Applikation bereits implementierte Möglichkeiten zur Serviceüberwachung, Skalierung und Sicherung besitzt. Darüber hinaus wurde die Sicherung der Verfügbarkeit mit ausgewählten Beispielen der Parallelisierung und der Möglichkeit der Clusterbildung veranschaulicht. Weiterhin wurde die Möglichkeit der Nutzung von Geodatenbanken diskutiert und mögliche Integrationsoptionen und Erweiterungsmöglichkeiten auf Basis des ArcGIS Servers betrachtet, um die Integration und den Einsatz in vorhandene Geodateninfrastrukturen aber eben auch in andere, nicht-geoinformationszentrierte Servicelandschaften zu eröffnen. Dafür bleibt festzustellen, dass der ArcGIS Image Server erst im kombinierten Einsatz mit dem ArcGIS Server seine volle horizontale Wertschöpfung, in Bezug auf die Verwendung unterschiedlicher Serviceprotokolle und damit auf die diversen Möglichkeiten Services zu publizieren, entfaltet.

Final bleibt allerdings auch festzustellen, dass das zugrundeliegende ITIL-Servicemanagementframework nicht frei von Schwächen ist. Mit den darin enthaltenen Kennzahlen fehlen aus Sicht des Autors dementsprechende Met-

riken zur Bestimmung der dort veröffentlichten Kennzahlen. ITIL geht im Einzelnen nicht auf Spezifika von bestimmten Dienstleistungen ein, sondern beschreibt nur in einem sehr allgemeinen Rahmen die zu etablierenden und zu verifizierenden Dienstleistungsprozesse. Außerdem ist ITIL in der Version 3 zu einem sehr mächtigen Regelwerk herangewachsen, die es, nach der Bewertung des Autors, in seiner Fülle, zu einem sehr unübersichtlichen Gesamtwerk machen.

Ähnliche Kritik lässt sich auch zu den Fehlerdatenbanken aus Kapitel 2.6 formulieren. Rasterbasierte Dienstleistungen bzw. Rasterdatendienste liegen offensichtlich nicht im Betrachtungsschwerpunkt solcher Sammlungen an konkreten Bedrohungen, deren Klassifikation und dementsprechenden Optionen zu weiteren Handlungs- und Verfahrensabläufen.

Zusammenfassend kann jedoch festgehalten werden, dass mit dieser Arbeit ein wichtiger Schritt in Richtung Sicherung von Servicekontinuität vollzogen wurde, indem auf Basis der Lebenszyklusorientierung von Rasterdatendiensten, Möglichkeiten aufgezeigt wurden, Forderungen der Nutzer in SLA umzusetzen, damit dementsprechende SLA kontinuierlich zu verbessern, vorhandene Ressourcen effektiv zu nutzen, dadurch entsprechende Kosten einzusparen und letzen Endes, die beabsichtigte Wertschöpfung im Geoinformationsbereich zu erzielen und weiter auszubauen.

6 Ausblick

Das Thema der dynamischen Rasterdatendienste hat sich als ein sehr komplexes und vielfältiges Themengebiet erwiesen. Ausgehend von der generell zu gewährleistenden Compliance auch und unmittelbar im Bereich rasterbasierter Geoinformationsdienste im Zuge verteilter Architekturen sowie unter dem Aspekt rechtlicher, organisatorsicher und technischer Rahmenbedingungen, lassen sich eine Vielzahl möglicher zusätzlicher Forschungsschwerpunkte identifizieren.

Die Arbeit hat gezeigt, dass bei der Betrachtung von dynamischen Rasterdatendiensten ein breites Spektrum an zu beantwortenden Fragestellungen aufgeworfen werden kann und eine immense Anzahl an zusätzlichen Themenbereichen in das Betrachtungsfeld mit einbezogen werden musste. Der Autor erhebt daher mit dieser Arbeit keinesfalls den Anspruch auf Vollständigkeit, sondern wollte vielmehr zeigen, welche wesentlichen Bereiche bei der rasterbasierten Servicedienstleistung interagieren.

Auf Basis des hier involvierten Serviceframeworks kann und muss die Betrachtung der Servicedienstleistung im Geoinformationsbereich zusätzlichen Strategien entsprechender Enterpriseframeworks unterworfen werden, da Servicedesign und Servicestrategie evident wichtig für zukünftige Architektur von Enterprisesystemen und daraus resultierenden Enterprisediensten sowie Enterprisedienstleistungen sind. Qualitätsaspekte von Rasterdatendiensten werden nicht allein erst durch konkrete Vertragsverhandlungen mit Kunden im Sinne von SLA festgelegt, sondern werden maßgeblich durch die technischen, organisatorischen und rechtlichen Weiterentwicklungen in diesem Bereich genährt.

Daher macht eine spätere Auseinandersetzung mit entsprechenden Enterprisesystemen wie C4ISR, GERAM oder ARIS Sinn, um die Ansprüche von Geoinformationssystemen aber eben auch darauf aufbauender Geoinformationsdienstleistungen, frühzeitig in die Entwicklung mit einzubeziehen und daraus ableitbare qualitativ hochwertige Dienstleistungsumgebungen sowie Dienst-

leistungsparameter zu gewinnen, da diese die zukünftige Grundlage für die Ausprägung auch von rasterdienstbasierten Technologien sind.

Durch die Fokussierung auf SOAP kann ein weiterer Schwerpunkt in der Implementierung dieses Protokolls und der damit verbundenen Rasterdatendienste im Bereich von E-Government und E-Trading definiert werden, um auch dort im rasterbasierten Dienstleistungsbereich der Geoinformationswirtschaft zukünftig dauerhafte und gesicherte Wertschöpfung zu erzielen.

Gleichzeitig stehen die Sicherung der Dienstleistungsqualität und damit die Sicherung der benannten Wertschöpfung im Fokus zukünftiger Zertifizierungsbemühungen verschiedener Serviceanbieter. Es macht daher außerordentlichen Sinn, Geodatendienste unter dem Aspekt der Zertifizierung nach ISO 20000 zu betrachten.

Für die Zukunft wird es spannend und herausfordernd zugleich sein, wie sich Dienste, ob nun rasterbasiert oder anderweitig geoinformationszentriert, nicht nur mit Hilfe des SOAP-Protokolls weiter in allgemeine Geschäftprozesse und Businessapplikationen integrieren, sondern sich in dieser stetig verändernden Lage mit Hilfe von Qualitätsparametern und Servicemanagementframeworks beschreiben und sichern lassen. Die Sicherung eines Dienstes in einer Cloud-Umgebung hat sicherlich nichts mehr mit der klassischen Sicherung eines Dienstes im heutigen Sinne gemein.

Literatur und Quellenverzeichnis

95/46/EG (1995):

RICHTLINIE 95/46/EG - DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION, *Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. In der Fassung vom 24.10.1995. Online verfügbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html, zuletzt geprüft am 18.06.2009

2002/58/EG (2002):

RICHTLINIE 2002/58/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES, *Datenschutzrichtlinie für elektronische Kommunikation*, in der Fassung vom 12.07.2002. Online verfügbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:DE:PDF, zuletzt geprüft am 18.06.2009

2007/2/EG (2007):

RICHTLINIE 2007/2/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES, *Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft.* INSPIRE, in der Fassung vom 14. März 2007. Online verfügbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:108:0001:0014:DE:PDF, zuletzt geprüft am 18.06.2009

Andenmatten, M. (2008):

Andenmatten, M. (2008), *ISO 20000.* Praxishandbuch für Servicemanagement und IT-Governance. 1. Aufl. Düsseldorf: Symposion.

Bartelme, N. (2000):

Bartelme, N. (2000), *Geoinformatik.* Modelle, Strukturen, Funktionen. Berlin, Heidelberg: Springer.

BDSG:

Bundesdatenschutzgesetz. BDSG, in der Fassung vom 14. Januar 2003.

Bengel, G. (2004):

Bengel, G. (2004), *Grundkurs Verteilte Systeme.* Grundlagen und Praxis des Client-Server-Computing ; inklusive aktueller Technologien wie Web-Services u.a. ; für Studenten und Praktiker. 3., verb. und erw. Aufl. Wiesbaden: Vieweg (Aus dem IT erfolgreich lernen).

BGB:

Bürgerliches Gesetzbuch. BGB, in der Fassung vom 2.1.2002.

Böttcher, R. (2008):

Böttcher, R. (2008), *IT-Servicemanagement mit ITIL V3.* Einführung, Zusammenfassung und Übersicht der elementaren Empfehlungen. Hannover: Heise-Zeitschriften-Verl.

BSI (2001):

Bundesamt für Sicherheit in der Informationstechnik (2001), *IT Sicherheit auf Basis der Common Criteria - ein Leitfaden.* Herausgegeben von BSI. Online verfügbar unter http://www.bsi.de/cc/cc_leitf.pdf, zuletzt aktualisiert am 18.05.2001, zuletzt geprüft am 08.07.2009.

Der Tagesspiegel (2009):

Der Tagesspiegel (Hg.) (2009), *Bundesweite Störung.* Netzausfall bei T-Mobile trifft Millionen Handykunden. Online verfügbar unter http://www.tagesspiegel.de/wirtschaft/Unternehmen-Telekom-Netzausfall-T-Mobile;art129,2779354, zuletzt geprüft am 27.05.2009.

Donaubauer, A. J. (2004):

Donaubauer, A. J. (2004), *Interoperable Nutzung verteilter Geodatenbanken mittels standardisierter Geo Web Services.* Dissertation an der TU München. Online verfügbar unter http://tumb1.biblio.tu-muenchen.de/publ/diss/bv/2004/donaubauer.html, zuletzt geprüft am 18.08.2009.

Dustdar, S. (2003):

Dustdar, S. (2003), *Software-Architekturen für Verteilte Systeme.* Prinzipien, Bausteine und Standardarchitekturen für moderne Software mit 22 Tabellen. Unter Mitarbeit von Harald Gall und Manfred Hauswirth. Berlin, Heidelberg: Springer.

Ebel, N. (2008):

Ebel, N. (2008), *ITIL V3 Basis-Zertifizierung.* Grundlagenwissen und Zertifizierungsvorbereitung für die ITIL® Foundation-Prüfung. München: Addison-Wesley.

Elsener, M. (2005):

Elsener, M. (2005), *Kostenmanagement in der IT.* [Leistungssteigerung und Kostenoptimierung, Kostentreiber erkennen und eliminieren, Total Cost of Ownership, Outsourcing, Service Level Agreements, Benchmarking, Methoden zur Kostensenkung und Effizienzsteigerung]. Bonn: mitp-Verl.

ESRI (2008a):

ESRI (Hg.) (2008), *ArcGIS Image Server Help.* Version 9.3.

ESRI (2008b):

ESRI (Hg.) (2008), *ArcGIS Image Server Developer Guide.* Version 9.3.

ESRI (2009):

ESRI (Hg.) (2009), *About ArcGIS Online.* System Infrastructure. Online verfügbar unter http://resources.esri.com/help/9.3/arcgisonline/about/content/infrastructure.htm, zuletzt aktualisiert am 27.10.2008, zuletzt geprüft am 07.07.2009.

Eunju, K.; Youngkon, L. (2005):

Eunju, K.; Youngkon, L. (2005), *Quality Model for Web Services.* Herausgegeben von OASIS. Online verfügbar unter http://www.oasis-open.org/committees/download.php/15910/WSQM-ver-2.0.doc, zuletzt geprüft am 02.04.2009.

Financial Times Deutschland (2009):

Financial Times Deutschland (2009), *Datenschutz.* Google lässt Einspruch bei Street View zu. Herausgegeben von FTD.de. Online verfügbar unter http://www.ftd.de/technik/medien_internet/:Datenschutz-Google-l%E4sst-Einspruch-bei-Street-View-zu/505914.html, zuletzt geprüft am 12.06.2009.

Gaulke, W. (2006):

Gaulke, W. (2006), *Ausarbeitung WSDL und UDDI.* Online verfügbar unter http://www.gaulke.net/werner/arbeiten/Ausarbeitung_WSDL_UDDI.pdf, zuletzt aktualisiert am 17.12.2006, zuletzt geprüft am 25.08.2009.

GeoZG:

Gesetz über den Zugang zu digitalen Geodaten. GeoZG, in der Fassung vom 10.2.2009.

GG:

Grundgesetz für die Bundesrepublik Deutschland. GG, in der Fassung vom 29.07.2009

GmbHG:

Gesetz betreffend die Gesellschaften mit beschränkter Haftung. GmbHG, in der Fassung vom 31.07.2009

Gibson, R. (2006):

Gibson, R. (2006), *Google maps hacks.* [tips & tools for geographic searching and remixing]. Unter Mitarbeit von Schuyler Erle. Beijing, Köln: O'Reilly.

Google (2009):

Google (Hg.) (2009), *Google Maps API Premier.* FAQs. Online verfügbar unter http://www.google.com/enterprise/maps/faq.html, zuletzt aktualisiert am 20.08.2009, zuletzt geprüft am 20.08.2009.

Harvard Research Group (2001):

Harvard Research Group Inc. (Hg.) (2001), *HIGHLY AVAILABLE SERVERS MARKET ASSUMPTIONS.* Online verfügbar unter http://www.hrgresearch.com/pdf/HAS%20Forecast%20rpt%20082301%20p.pdf, zuletzt geprüft am 29.06.2009.

Hernan, S. et al. (2006):

Hernan, S.; Lambert, S.; Ostwald, T.; Shostack, A. (2006), *Threat Modeling.* Aufdecken von Fehlern im Sicherheitsentwurf mithilfe des STRIDE-

Ansatzes. Online verfügbar unter http://msdn.microsoft.com/de-de/magazine/cc163519.aspx, zuletzt geprüft am 20.05.2009.

HGB:

Handelsgesetzbuch. HGB, in der Fassung vom 17.12.2008.

ISO 19119 (2001):

ISO 19119 (2001), Geographic information — Services, vom 07.12.2001

ISO 19121 (2000):

ISO 19121 (2000), *Geographic information - Imagery and gridded data*, vom 03.04.2000

ISO/IEC (2006a):

ISO/IEC (Hg.) (2006): *Common Criteria for Information Technology Security Evaluation.* Part 1: Introduction and general model. Online verfügbar unter http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf, zuletzt geprüft am 07.07.2009.

ISO/IEC (2006b):

ISO/IEC (Hg.) (2006), *Common Criteria for Information Technology Security Evaluation.* Part 2: Security functional components. Online verfügbar unter http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf, zuletzt geprüft am 05.08.2009.

ISO/IEC (2006c):

ISO/IEC (Hg.) (2006): *Common Criteria for Information Technology Security Evaluation.* Part 3: Security assurance components. Online verfügbar unter http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf, zuletzt geprüft am 05.08.2009.

ITSEC (1991):

ITSEC. Version 1.2 (1991), Online verfügbar unter http://www.bsi.bund.de/zertifiz/itkrit/itsec-dt.pdf, zuletzt geprüft am 07.07.2009.

Karg, M.; Weichert, T. (2007):

Karg, M.; Weichert, T. (2007), *Datenschutz und Geoinformation.* Herausgegeben von Bundesministerium für Wirtschaft und Technologie. (11/07). Online verfügbar unter http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/geoinformationswirtschaft-datenschutzstudie,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf, zuletzt geprüft am 10.06.2009.

Königs, H.-P. (2006):

Königs, H.-P. (2006), *IT-Risiko-Management mit System.* Von den Grundlagen bis zur Realisierung ; ein praxisorientierter Leitfaden ; mit Online-Service zum Buch. 2., korrigierte Aufl. Wiesbaden: Vieweg.

Korduan, P.; Zehner, M. L. (2008):

Korduan, P.; Zehner, M. L. (2008), *Geoinformation im Internet.* Technologien zur Nutzung raumbezogener Informationen im WWW. Unter Mitarbeit von Marco L. Zehner. Heidelberg: Wichmann.

Luckardt, N. (2006):

Luckardt, N. (2006), *Sonderdruck aus <kes> – Die Zeitschrift für Informations-Sicherheit Nr. 2006#4, 2006#5 und 2006#6.* Herausgegeben von <kes> –Die Zeitschrift für Informations-Sicherheit. Online verfügbar unter http://www.kes.info/archiv/material/studie2006/kes-Microsoft-Studie%202006%20(Sonderdruck).pdf, zuletzt geprüft am 09.06.2009.

Luckardt, N. (2008):

Luckardt, N. (2008), *Die <kes>/Microsoft-Sicherheitsstudie2008.* Herausgegeben von <kes> –Die Zeitschrift für Informations-Sicherheit. Online verfügbar unter http://www.it-sa.de/fileadmin/itsa_files/Handouts/2008/RO_Di_16_30_Luckhardt.pdf?PHPSESSID=onmousedown%3Dreturn, zuletzt geprüft am 09.06.2009.

Mani, A.; Nagarajan A. (2002):

Mani, A.; Nagarajan A. (2002), *Understanding quality of service for Web Services.* Improving the performance of your Web services. Online verfügbar unter ibm.com_developerworks_library_ws-quality.html, zuletzt aktualisiert am 25.08.2009, zuletzt geprüft am 25.08.2009.

Masuhr, J. (2008):

Masuhr, J. (2008), *Google.* Der Plan X. Google verschenkt seine Dienste – und wird damit immer reicher: So tickt die Suchmaschinenaktie. Online verfügbar unter http://www.focus.de/finanzen/boerse/google-der-plan-x_aid_333719.html, zuletzt geprüft am 20.04.2009.

Melzer, I. (2008):

Melzer, I. (2008), *Service-orientierte Architekturen mit Web Services.* Konzepte - Standards - Praxis. Heidelberg: Spektrum Akad. Verl.

Microsoft (2009):

Microsoft (Hg.) (2009), *Bing Maps for Enterprise from Microsoft.* Licensing And Pricing Options. Online verfügbar unter http://www.microsoft.com/maps/product/licensing.aspx, zuletzt geprüft am 15.07.2009.

Müller, K.-R. (2008):

Müller, K.-R. (2008): *IT-Sicherheit mit System.* Sicherheitspyramide, Sicherheits-, Kontinuitäts- und Risikomanagement, Normen und Practices, SOA und Softwareentwicklung. Wiesbaden: Vieweg.

Network Services Drafting Team (2009):

Network Services Drafting Team (Hg.) (2009), *Technical Guidance to implement INSPIRE View Services.* Online verfügbar unter http://inspire.jrc.ec.europa.eu/documents/Network_Services/Technical%20Guidance%20View%20Services%20v%202.0.pdf, zuletzt geprüft am 30.07.2009.

OGC (2004):

OGC (2004), *Web Map Service.* Version 1.3.0. Herausgegeben von OGC. Online verfügbar unter http://portal.opengeospatial.org/files/?artifact_id=4756, zuletzt aktualisiert am 26.01.2004, zuletzt geprüft am 09.08.2009.

***OGC* (2007a):**

OGC (2007),*Service Tansition, ITIL.* London: TSO (The Stationery Office).

***OGC* (2007b):**

OGC (2007), *Service Oeration.* ITIL. London: TSO (The Stationery Office).

***OGC* (2007c):**

OGC (2007), *Continual Service Improvement.* ITIL. London: TSO (The Stationery Office).

***OGC* (2007d):**

OGC (2007), *Service Design.* ITIL. London: TSO (The Stationery Office).

***OGC* (2007e):**

OGC (2007), *Service Strategy.* ITIL. Norwich: TSO (The Stationery Office).

OGC (2007f):

OGC (2007), *Web Processing Service.* Version 1.0.0. Herausgegeben von OGC. Online verfügbar unter http://portal.opengeospatial.org/files/?artifact_id=24151, zuletzt aktualisiert am 11.03.2008, zuletzt geprüft am 09.06.2009.

OGC (2008):

OGC (2008), *Web Coverage Service (WCS).* Implementation Standard. Version 1.1.2. OGC. Online verfügbar unter http://portal.opengeospatial.org/files/?artifact_id=27297, zuletzt aktualisiert am 23.04.2008, zuletzt geprüft am 09.03.2009.

OGC (2009):

OGC (2009), *Web Coverage Processing Service (WCPS).* Language Interface Standard. Version 1.0.0. Herausgegeben von OGC. Online verfügbar unter http://portal.opengeospatial.org/files/?artifact_id=32319, zuletzt aktualisiert am 25.03.2009, zuletzt geprüft am 09.06.2009.

SatDSigG

Gesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten. SatDSigG, in der Fassung vom 23.11.2007.

Schmidt, H. (2005):

Schmidt, H. (2005), *Entwurf von Service Level Agreements auf der Basis von Dienstprozessen.* 2. Aufl. München: Utz.

Silberschmidt, R. (2001):

Silberschmidt, R. (2001), *Krieg im Internet.* Hacker wollen Lufthansa-Homepage attackieren. Online verfügbar unter http://www.onlinekosten.de/news/artikel/6004/0/Krieg-im-Internet-Hacker-wollen-Lufthansa-Homepage-attackieren-Update, zuletzt geprüft am 09.06.2009.

StGB:

Strafgesetzbuch. StGB, in der Fassung vom 13. November 1998.

TMG:

Telemediengesetz. TMG, in der Fassung vom 26.02.2007.

Tyurin, N. (2007):

Tyurin, N. (2007), *Aufbau und Zusammenhang der drei Service Level Management Vertragstypen SLA, OLA, UC.* Diplomarbeit. Fachhochschule Aalen Hochschule für Technik und Wirtschaft, Informatik - Wirtschaftsinformatik.

UrhG:

Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz). UrhG, in der Fassung vom 17. Dezember 2008.

W3C (2003):

W3C (2003), *QoS for Web Services.* Requirements and Possible Approaches. Herausgegeben von W3C. Online verfügbar unter http://www.w3c.or.kr/kr-office/TR/2003/ws-qos/, zuletzt geprüft am 09.05.2009.

W3C (2004):

W3C (2004), *Web Services Architecture.* Online verfügbar unter http://www.w3.org/TR/ws-arch/wsa.pdf, zuletzt geprüft am 08.04.2009.

Witt, B. C. (2006):

Witt, B. C. (2006), *IT-Sicherheit kompakt und verständlich.* Eine praxisorientierte Einführung. Wiesbaden: Vieweg.

Wöhr, H. (2004):

Wöhr, H. (2004), *Web-Technologien.* Konzepte, Programmiermodelle, Architekturen. Heidelberg: dpunkt-Verl.

Anlagenverzeichnis

System Requirements	
Server Manager	Microsoft Windows Server 2003, Windows XP, Windows Vista Enterprise, or Windows Server 2008 Hardware requirements *Pentium 4 or higher processor* *512 MB of RAM minimum, 1 GB or higher recommended* Microsoft .NET Framework 2.0
Server	Microsoft Windows Server 2003, Windows XP, Windows Vista Enterprise, or Windows Server 2008 Hardware requirements *Intel Pentium or Intel Xeon 1.0 GHz* *1 GB RAM*
Service Provider	Microsoft Windows Server 2003, Windows XP, Windows Vista Enterprise, or Windows Server 2008 Hardware requirements *Intel Pentium or Intel Xeon Processors* *1.0 GHz CPU minimum, 2.0 GHz or higher recommended* *Minimum of 1 GB RAM recommended*
Service Editor	ArcGIS Desktop 9.2 (ArcView minimum) installed with .NET support Hardware requirements as per ArcGIS Desktop 9.2 Microsoft .NET Framework 2.0
ArcGIS Image Server clients	Hardware requirements as per the application running the client ArcGIS Desktop clients require .NET 2.0 and ArcGIS .NET Support to be installed

Anlage 1 - Systemvoraussetzung[264]

[264] Quelle: eigene Darstellung, angelehnt an ESRI (2008a).

ArcGIS Image Server components or products	Microsoft .NET Framework 2.0	ArcGIS Desktop 9.3	ArcGIS Desktop 9.1 or 9.2	.NET support for ArcGIS	AutoCAD 2000, 2000i, 2002, 2004, 2005, 2006, and 2007	MicroStation 8.05	MapInfo 8.0 and 8.5	GeoMedia Professional 6
Server								
Service Provider		*(Requires ArcGIS Desktop or Engine)*						
Service Editor	x	x		x				
Developer Kit								
ArcGIS 9.1 or client*	x		x	x				
Image Server Viewer*	x							
AutoCAD client*					x			
MicroStation client*						x		
MapInfo client*							x	
GeoMedia client*								x

Anlage 2 – Komponenten und Produkte[265]

[265] Quelle: eigene Darstellung, angelehnt an ESRI (2008a)

```
<SLA name="TK100">

 <Obligations>
   <ServiceLevelObjective
        name="ServiceLevelObjective">
     <Expression>
     </Expression>
     <Obliged>
       Slaudo Karten (Provider)
     </Obliged>
     <Predicate
          xsi:type="True">
       <SLAParameter>
         Kapazität
       </SLAParameter>
       <Value>
         1000
       </Value>
       <ServiceLevelObjective>
         ServiceLevelObjective
       </ServiceLevelObjective>
     </Predicate>
   </ServiceLevelObjective>
</Obligations>
    <Parties>
     <ServiceProvider name="Slaudo Karten (Provider)">
   <Contact>
     <Person>
       Slaudo Marx
     </Person>
     <Addressvider>
     <ServiceConsumer name="Data GmbH (Consumer)">
   <Contact>
     <Person>
       Markus Müller
     </Person>
     <Address>
       Hauptstrasse 250, 01127 Dresden
     </Address>
   </Contact>
     </ServiceConsumer>
  </Parties>
  <Obligations>
  <ServiceLevelObjective
        name="ServiceLevelObjective">
     <Expression>
     </Expression>
  </ServiceLevelObjective>
  </Obligations>
<ServiceDefinition
     name="ServiceDefinition">
   <Metric
```

```
        name="Kapazität"
        type="double"
        unit="Transactions per hour">
      <Function
          xsi:type="wsla:Mean"
          resultType="double">
        <Metric>
          Kapazität
        </Metric>
      </Function>
      <Source>
        Slaudo Karten (Provider)
      </Source>
    </Metric>
    <SLAParameter
        name="Kapazität"
        type="double"
        unit="transactions / hour">
      <Metric>
        Kapazität
      </Metric>
      <Communication>
        <Source>
          Slaudo Karten (Provider)
        </Source>
        <Pull>
          Slaudo Karten (Provider)
        </Pull>
        <Push>
          Data GmbH (Consumer)
        </Push>
      </Communication>
    </SLAParameter>
  </ServiceDefinition>
</SLA>
```

Anlage 3 – Beispiel WSLA[266]

[266] Quelle: eigene Darstellung

Serviceeigenschaft	ETM	DTED
Anzahl der Raster	38	2040
Total Time taken for adding rasters	8.1 s	73.8 s
Time taken for computing pixel sizes	1.4 s	57.6 s
Time taken for generating service boundary	1.3 s	7.3 s
Time taken for extracting metadata	0.5 s	31.1 s
Time taken for computing output properties	0.6 s	1.3 s
Time taken for merging the derived images	0.3 s	0.6 s
Time taken for computing pixel sizes	3.8 s	65.3 s
Loading the image service definition	4.89 s	1.80 s
Compiling the Service	5.07 s	35.30 s
DerivedImageGenerator	1022.53 s	91.17 s
Zeit zur Erstellung des Service	1048.49 s	365.27 s
Zeit zur Erstellung des Service (gerundet)	~ 17 min	~ 6 min

Anlage 4 - Diensterstellung (Zeiten)[267]

[267] Quelle: eigene Darstellung

X_{min} (WGS84)	y_{min} (WGS84)	x_{max} (WGS84)	y_{max} (WGS84)	rows	columns
11.50748546	53.68202997	13.47487287	56.65716319	182	182
7.598544735	53.07529145	8.968837112	53.47725177	813	813
4.769470434	48.54550697	6.095983953	49.4554503	706	706
7.190340794	47.93691042	10.30914471	52.47604849	328	328
11.62528342	50.72827467	13.59755465	52.78717695	225	225
5.610313674	52.05030176	9.955336732	55.3834508	1016	1016
14.33690967	54.37629658	15.72857641	58.397011	249	249
13.98657713	50.40097743	15.09528114	51.54394673	795	795
14.57553048	50.08475387	15.43668459	54.05882475	297	297
12.0189039	48.55374984	16.76218271	52.82794835	916	916
10.74674576	54.05308134	11.40606025	58.79563878	524	524
7.263796421	53.18398515	8.80408728	56.21141216	946	946
10.62699549	47.61817744	12.45933084	50.47637992	530	530
8.52341864	48.77316213	10.85043231	49.54006171	582	582
14.92975271	54.07356468	16.67753632	58.97363114	445	445
6.491788419	54.60462977	11.03759508	54.85855941	1021	1021
11.66913562	52.65865571	14.91119501	53.28859091	947	947
11.10388716	49.05616309	15.58797854	53.49406994	290	290
4.038053271	54.4532798	4.646366891	58.55196041	872	872
10.42047452	54.13738665	10.74848674	55.1984194	188	188
7.11993802	47.69431235	7.930323257	49.49190689	976	976
13.22181986	53.73153307	15.51284429	57.86041955	390	390
4.190665325	47.3220682	8.946062786	48.51639427	387	387
15.12721471	54.40571946	15.31923855	58.54011804	981	981
6.07244434	51.39661596	10.51611663	52.01010683	121	121
7.130020569	47.93278239	10.89111954	52.02830932	382	382
12.69134907	51.13307803	17.28741847	54.01504414	318	318
5.162568311	52.14629282	6.587431618	55.74133695	499	499
6.855701343	53.63082798	8.553948762	57.79655655	588	588
14.30117556	51.5941372	14.5348957	55.27164281	1005	1005
8.978001204	49.74425594	13.54323225	51.25181228	127	127
11.38106659	49.33375374	13.44945617	52.30662397	916	916
7.929114955	52.08407797	9.664731622	53.05188967	633	633
13.91943272	54.35052128	18.03103612	56.78825246	502	502
12.92243004	51.69142144	16.31818113	55.31936183	503	503
5.349253859	54.09238927	7.367299767	59.02245422	960	960
9.04273571	50.01372995	9.387685556	54.29506452	461	461
8.732892643	51.4814968	13.29489742	54.57665731	548	548
11.22951281	53.95859216	14.27870817	54.98451592	752	752
13.30348835	49.33076614	15.66069555	53.61051692	868	868
12.32931931	54.29590531	12.88917164	55.10636379	190	190
14.44319553	54.45161536	14.77651213	55.63871272	674	674
10.22577977	52.70526957	10.92966877	53.70336982	591	591
15.81855115	50.03570852	16.08062602	54.08736345	471	471
10.00311053	47.1339799	11.87539674	51.75453731	996	996
15.87286159	54.0799492	16.37133875	55.78238551	248	248
13.53621385	49.48549878	15.96447224	52.65476908	437	437

Anlage 5 - AOI 1[268]

[268] Quelle: eigene Darstellung

x_{min} (WGS84)	y_{min} (WGS84)	x_{max} (WGS84)	y_{max} (WGS84)	rows	Columns
11.19215549	53.35481031	12.75866191	56.75625808	943	943
10.78438488	51.45492419	14.85841599	54.20886139	905	905
14.54472595	49.53001983	14.94891845	53.25785469	384	384
6.270103464	52.98670418	8.658241511	53.37902349	102	102
6.057845525	54.48255767	10.46583126	56.6380989	986	986
13.45595449	47.45344286	15.19252858	52.31942176	251	251
7.507799014	47.36982482	9.369936996	50.60343955	321	321
6.659992233	51.65791407	7.486654017	52.95344865	375	375
9.051204813	51.28891552	11.81434017	55.67220271	638	638
15.80509736	53.13601978	19.73488475	57.81806317	1002	1002
11.09800623	49.99938064	15.05599032	51.01178915	128	128
10.2955187	48.39171832	11.34181434	51.66124488	742	742
15.31256734	51.15117347	19.29759257	55.90179285	966	966
12.13046464	51.55967043	15.08265757	54.07519666	165	165
13.61394317	47.60288415	15.62433082	51.22942794	396	396
14.10071772	50.51312635	16.15185615	53.51268156	127	127
12.40292209	48.94135246	16.06651964	50.47781987	883	883
11.06528419	50.01329531	12.26548224	51.17704524	739	739
12.21269168	48.25568874	12.34033136	48.72432477	401	401
14.67363206	51.31801095	19.33399832	52.52108363	674	674
11.10472903	52.69918582	13.38558564	54.14723889	474	474
10.08213746	52.50655139	13.39579402	55.67653629	642	642
8.971309822	54.21863142	13.27758791	56.60876293	912	912
15.69897435	47.67044313	20.18732713	48.47239872	698	698
7.534773816	48.9234904	11.09465807	52.87650785	745	745
7.032033893	53.67057192	7.316529363	57.80629042	822	822
11.99777863	53.85061999	15.94778043	58.48933241	829	829
10.8073218	51.05516676	12.72209579	54.52679169	486	486
6.511218379	54.92929872	8.209576506	58.99827563	393	393
5.760349735	49.46855476	8.574680078	51.9335564	678	678
15.83672497	49.64706166	19.90068434	53.64455109	488	488
15.93166684	50.17727053	16.86042523	52.8442724	681	681
8.802714691	54.02852846	9.690982217	54.26088387	170	170
4.493916231	47.37704184	5.48177424	49.90452763	917	917
5.552589886	47.76957604	6.431178633	48.52692476	758	758
12.13490256	53.72869882	14.363067	57.82932831	101	101
13.52619257	51.97180584	15.31497173	56.01767231	356	356
5.543157927	51.05085937	5.893959268	51.72996889	127	127
14.72760341	52.83471235	15.9763836	55.71346729	902	902
13.12665448	54.91168902	17.12688731	59.67037765	153	153
11.63906074	49.24361917	13.5927377	54.17052561	582	582
4.665680611	50.13055331	6.117232891	53.85700043	934	934
4.022272564	47.32145848	7.759995417	48.45245095	336	336
13.60068106	49.48113652	16.71860606	53.01078992	603	603
10.94249271	53.19873968	14.92843184	54.18431453	157	157
6.548453675	53.40656042	9.391979832	58.2109025	727	727
4.044463492	51.27582921	7.866194825	53.63461346	395	395

Anlage 6 - AOI 2[269]

[269] Quelle: eigene Darstellung

ServiceProvider	connections	duration [s]	AOI	Service	requests	average request time [s]	max process time [s]	request per second
1	10	300	1	ETM	3657	0.19	2.38	12.19
2	10	300	1	ETM	3518	0.33	2.21	11.73
4	10	300	1	ETM	3617	0.57	2.30	12.06
1	40	300	1	ETM	3500	0.22	1.85	11.67
2	40	300	1	ETM	3580	0.36	3.32	11.93
4	40	300	1	ETM	3567	0.85	4.35	11.89
1	10	300	2	ETM	4378	0.16	1.27	14.59
2	10	300	2	ETM	4399	0.27	2.20	14.66
4	10	300	2	ETM	4387	0.47	2.06	14.62
1	40	300	2	ETM	4127	0.19	1.75	13.76
2	40	300	2	ETM	4176	0.32	2.43	13.92
4	40	300	2	ETM	4276	0.79	6.94	14.25
1	10	300	1	DTED	963	0.8	6.21	3.21
2	10	300	1	DTED	989	1.21	4.335	3.30
4	10	300	1	DTED	1019	2.31	7.523	3.40
1	40	300	1	DTED	995	0.61	1.73	3.32
2	40	300	1	DTED	962	1.225	4.76	3.21
4	40	300	1	DTED	1005	2.408	7.955	3.35
1	10	300	2	DTED	969	0.64	2.33	3.23
2	10	300	2	DTED	999	1.195	4.875	3.33
4	10	300	2	DTED	986	1.8	6.46	3.29
1	40	300	2	DTED	914	0.73	2.95	3.05
2	40	300	2	DTED	949	1.325	4.835	3.16
4	40	300	2	DTED	920	2.708	10.37	3.07

Anlage 7 - Ergebnis Lasttest (komplett)[270]

[270] Quelle: eigene Darstellung