Bundesamt
für Sicherheit in der
Informationstechnik

KRITIS-Sektorstudie

Informationstechnik und Telekommunikation (IKT)

Öffentliche Version – Revisionsstand 5. Februar 2015

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5098
E-Mail: upkritis@bsi.bund.de
Internet: https://www.bsi.bund.de

Danksagung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat 2014 vier Studien zur Analyse der „Kritischen Infrastrukturen“ (KRITIS) in Deutschland in Auftrag gegeben. Ziel der Studien ist es, einen umfassenden Überblick über die KRITIS-Sektoren und die darin erbrachten kritischen Dienstleistungen zu erhalten. Die Sektorstudien sollen weiterhin den sektorspezifischen Stand der Cyber-Sicherheit sowie Probleme und Trends zusammenfassen.

Die KPMG AG Wirtschaftsprüfungsgesellschaft hat durch das BSI Anfang 2014 den Auftrag erhalten, alle vier Sektorstudien in der Zeit von Januar bis Dezember 2014 zu erstellen.

Die Studien wurden durch das KPMG Security Consulting Team Berlin unter der Leitung von Herrn Wilhelm Dolle erstellt. Alle damit zusammenhängenden Tätigkeiten wurden studienübergreifend durch den KRITIS-Projektleiter, Herrn Torsten Redlich, koordiniert. Herr Paul Weissmann leitete fachlich die Studie im Sektor Informationstechnik und Telekommunikation (IKT).

Die Erstellung der KRITIS-Sektorstudien wäre ohne die enge Zusammenarbeit mit zahlreichen Vertretern von Betreibern und Verbänden in den KRITIS-Sektoren nicht möglich gewesen. Unser besonderer Dank gilt den Betreibern, die trotz des sensiblen Themas und der vollen Terminkalender Zeit und Motivation fanden, uns bei der Durchführung der Studie mit Experteninterviews aktiv zu unterstützen. Sie haben mit ihrem Fachwissen und Engagement wesentlich zum Gelingen der Studie beigetragen.

Wir sind ebenso den vielen Experten dankbar, die uns in Hintergrundgesprächen hilfreiche Diskussionsmöglichkeiten und wertvolle Impulse gegeben haben.

In gleicher Weise möchten wir uns bei den Mitarbeitern des BSI für die konstruktive und offene Zusammenarbeit bedanken, die eine kontinuierliche Studienbegleitung und letztlich den erfolgreichen Projektabschluss ermöglicht haben.

Berlin, im Dezember 2014

Wilhelm Dolle, Partner

Paul Weissmann, Manager

Vorwort

Dies ist die öffentliche Fassung der KRITIS-Sektorstudie Informationstechnik und Telekommunikation (IKT). Alle Inhalte der öffentlichen Fassung finden sich auch in einer nicht-öffentlichen Fassung. Gegenüber der nicht-öffentlichen Fassung der KRITIS-Sektorstudie Informationstechnik und Telekommunikation (IKT) wurden Teile herausgenommen:

- Informationen zu neuralgischen Punkten in kritischen Informationsinfrastrukturen, die geeignet sind, um besondere Ziele für Angriffe auf die Versorgungssicherheit auszuwählen, wurden herausgenommen.
- Die Diskussion der Versorgungsmerkmale ist Teil des Verfahrens zur Erstellung der Rechtsverordnung nach § 2 Abs. 10 Satz 2 und § 10 Abs. 1 BSIG (in der Fassung des Regierungsentwurfes für ein IT-Sicherheitsgesetz vom 17.12.2014).

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Einleitung

Kritische Infrastrukturen (KRITIS) sind „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ [BMI 2009]. Sie erbringen kritische Dienstleistungen, die für Deutschland einen bedeutenden Beitrag zur Sicherung des Gemeinwohls leisten. Das Dokument „UP KRITIS – Grundlagen und Ziele“ von 2013 definiert kritische Dienstleistungen wie folgt:

> „Kritische Dienstleistungen sind für die Bevölkerung wichtige, teils lebenswichtige Güter und Dienstleistungen. Bei einer Beeinträchtigung dieser kritischen Dienstleistungen würden erhebliche Versorgungsengpässe, Störungen der Öffentlichen Sicherheit oder vergleichbare dramatische Folgen eintreten“ [BSI 2014].

Die Auswahl an kritischen Dienstleistungen kann zum einem auf den staatlichen Auftrag zur Daseinsfürsorge zurückgeführt werden, zum anderen auf ihre Bedeutung als technische Basisinfrastrukturen für andere kritische Dienstleistungen. Die zuverlässige Erbringung der kritischen Dienstleistungen bildet die Grundlage vieler alltäglicher Prozesse und Abläufe für die Bevölkerung und in der Wirtschaft. Sie ist Voraussetzung für die ausreichende Versorgung der Bevölkerung mit Lebensmitteln, Wasser, Elektrizität, Gesundheitsleistungen und vielen anderen wichtigen oder lebensnotwendigen Ressourcen. Vor diesem Hintergrund ist der Schutz Kritischer Infrastrukturen eine gesamtgesellschaftliche Aufgabe, die im Zusammenspiel von Staat, Wirtschaft und Öffentlichkeit erfolgt.

Als Grundlage für die Kooperation von Staat und Wirtschaft beim Schutz Kritischer Infrastrukturen dient die Sektoren- und Brancheneinteilung. Sie bildet einen konzeptionellen Rahmen, der die Analyse und Behandlung einzelner technischer Basisinfrastrukturen und sozioökonomischer Dienstleistungs-infrastrukturen ermöglicht. Die Betreiber von KRITIS umfassen dabei sowohl staatliche als auch privatwirtschaftliche Organisationen.

Sektoren Kritischer Infrastrukturen	
Energie	Transport und Verkehr
Informationstechnik und Telekommunikation	Finanz- und Versicherungs-wesen
Gesundheit	Staat und Verwaltung
Wasser	Medien und Kultur
Ernährung	

Tabelle 1: Sektoreinteilung der Kritischen Infrastrukturen in Deutschland

Jeder KRITIS-Sektor ist in verschiedene Branchen aufgeteilt. Sowohl zwischen den Branchen innerhalb eines Sektors als auch zwischen den verschiedenen Sektoren existieren vielfältige Interdependenzen. Beispielsweise ist die Stromversorgung eine Grundvoraussetzung für die Erbringung praktisch aller anderen kritischen Dienstleistungen. Ein weiteres Beispiel sind die Leistungen des Sektors Transport und Verkehr, die Voraussetzung für die Logistik von Nahrungsmitteln, Materialien für die Gesundheitswirtschaft und weiteren Gütern sowie für die Beförderung von Personen sind. Der Sektor Informationstechnik und Telekommunikation nimmt hierbei vor dem Gedanken der starken Durchdringung von Informations- und Telekommunikationstechnologie in allen anderen Sektoren eine Sonderrolle ein. Eine effiziente Leistungserbringung in den Sektoren ist heute ohne die Inanspruchnahme der Informations- und Telekommunikationsdienstleistungen nicht mehr vorstellbar. Die weiter zunehmende Verbreitung und Durchdringung von Informations- und Kommunikationstechnologien in allen Sektoren birgt jedoch gleichzeitig bekannte und neue Risiken.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine der zentralen Stellen unter den zuständigen Behörden zum Schutz von Kritischen Infrastrukturen. Mit unterschiedlichen Aktivitäten wie der Organisation von Branchengesprächen, der Bereitstellung von Standards und Leitfäden zu wichtigen IT-Sicherheitsthemen und nationalen Projekten sowie der Koordination des UP KRITIS[1] verfolgt das BSI die Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) und der nationalen Cyber-Sicherheitsstrategie. In seinen Arbeiten ist das BSI auf genaue Kenntnisse zu den Funktionen kritischer Dienstleistungen und der damit verbundenen Bedeutung wichtiger Anlagen und Einrichtungen (KRITIS) angewiesen. Dabei ist es wichtig, die wirtschaftlichen, technologischen, politischen und regulatorischen Rahmenbedingungen und Besonderheiten der Sektoren und deren Branchen genau zu verstehen. Dies umfasst gleichermaßen die Kenntnis zukünftiger Entwicklungen.

Mehr als zehn Jahre nach der Erstellung der ersten KRITIS-Sektorstudien hat das BSI 2014 die Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG mit der Erarbeitung von vier Studien zu den folgenden Sektoren beauftragt:

- Energie (Projekt 100)
- Ernährung und Wasser (Projekt 101)
- Informationstechnik und Telekommunikation (Projekt 103)
- Transport und Verkehr (Projekt 104)

Die Erarbeitung der vier Sektorstudien erfolgte von Februar bis Dezember 2014. Ziel der Studien ist es, einen aktuellen Überblick über den Sektor, dessen Branchen sowie die im Sektor und den Branchen erbrachten kritischen Dienstleistungen zu gewinnen. Dies beinhaltet Analysen zur Kritikalität der sektortypischen Dienstleistungen sowie deren betriebsinternen Prozessen. Weiterhin soll der Grad der Abhängigkeiten betriebsinterner Prozesse von IKT ermittelt und die Frage beantwortet werden, welche Rolle Informationen, der Einsatz von IKT und die Nutzung von IKT-Prozessen für die Ausführung der betriebsinternen Prozesse spielt. Die Sektorstudien sollen sektor- und branchenspezifisch den Stand der IKT-Sicherheit zusammenfassen und aktuelle Probleme sowie zukünftige Trends in Bezug auf IKT-Sicherheit und -Zuverlässigkeit herausstellen.

Neben dem vorhandenen Expertenwissen sowie öffentlich verfügbaren Informationen und Unterlagen bildet die in allen vier Sektoren durchgeführte Betreiberbefragung eine wesentliche Informationsgrundlage der Sektorstudien. Hierfür wurden wichtige Betreiber, Verbände und ggf. weitere wichtige Akteure der jeweiligen Sektoren im Studienzeitraum in zahlreichen persönlichen und telefonischen Gesprächen zum Stand der Cyber-Sicherheit befragt. Die Angaben sind in anonymisierter Form in die Studien eingeflossen, sodass keine Rückschlüsse auf einzelne Befragte gezogen werden können.

Zur Vereinheitlichung unterliegen alle vier Studien der gleichen Struktur. Sie unterteilen sich in die folgenden Kapitel:

Kapitel 1 bietet einen **Überblick** über den in der jeweiligen Studie behandelten Sektor.

Kapitel 2 vertieft den Einblick in den Sektor, indem es die einzelnen **Branchen im Detail** vorstellt. In diesem Kapitel werden die Branchenstruktur, die Bedeutung der Branchen für Staat und Gesellschaft, der volkswirtschaftliche Kontext, die Marktteilnehmer, die Beziehungen innerhalb der Branche, die Rolle der öffentlichen Hand sowie die aktuellen Entwicklungen aufgegriffen und erläutert.

Kapitel 3 enthält eine detaillierte Auseinandersetzung mit den **kritischen Dienstleistungen.** Dies sind im vorliegenden Fall die Dienstleistungen „Sprach- und Datenübertragung“ (DL1) und „Datenspeicherung und -verarbeitung“ (DL2). Einer strukturellen Zerlegung der Dienstleistungen folgt die Analyse der kritischen betriebsinternen Prozesse und die Ermittlung der Risikoelemente.

1 Der UP KRITIS ist eine Kooperation zwischen (KRITIS-)Betreibern, Verbänden und staatlichen Stellen, u. a. dem BSI (siehe www.upkritis.de).

Kapitel 4 liefert eine Sammlung bedeutsamer **Sicherheitsvorfälle** im Sektor. Diese sind nach internationalen und nationalen Vorfällen differenziert sowie anhand wichtiger Eigenschaften zur Sensibilisierung und Aufklärung aufbereitet.

Kapitel 5 setzt sich sowohl mit den geltenden Normen und Standards als auch mit den gesetzlichen Anforderungen für IT-Sicherheit im betrachteten Sektor auseinander. Darüber hinaus wird auf den etablierten **Stand der Cyber-Sicherheit** sowie auf Herausforderungen und Trends in der IT-Sicherheit eingegangen, was insbesondere aus den Ereignissen der Betreiberbefragung ermittelt wurde.

Kapitel 6 führt die Ergebnisse aus den vorherigen Kapiteln als **Fazit** zusammen, schafft einen Überblick über die wesentlichen Erkenntnisse und stellt wichtige **Handlungsempfehlungen** zur Stärkung der IT-Sicherheit im betrachteten Sektor heraus.

1 Sektorüberblick

Der KRITIS-Sektor Informationstechnik und Telekommunikation (IKT) umfasst in der vorliegenden Studie die technische Basisinfrastruktur für die Nutzung von Sprach- und Datenkommunikation auf Basis von leitungsgebundenen und drahtlosen Netzen durch die deutsche Gesellschaft, Privatwirtschaft und öffentliche Hand sowie die Bereitstellung von Datenspeicherung und -verarbeitung.

Moderne Informations- und Kommunikationstechnologien haben seit Mitte der 1990er Jahre Einfluss auf viele Lebensbereiche und gehören mittlerweile zu den grundlegenden Funktionen unserer Gesellschaft. Der Austausch von Informationen ist in unserer modernen Gesellschaft zu einem wichtigen Wirtschaftsfaktor und Bestandteil des täglichen Lebens geworden. Fast die gesamte deutsche Bevölkerung (99 Prozent) ist im Besitz eines Telefons (Festnetz oder Mobil) und circa 80 Prozent der deutschen Haushalte verfügen über einen Internetanschluss [DESTATIS 2013d]. Im Bereich der Privatwirtschaft nutzen circa 88 Prozent der deutschen Unternehmen Computer und circa 87 Prozent der Unternehmen verfügen über einen Anschluss an das Internet [DESTATIS 2013a]. Der Verbreitungsgrad von Informations- und Kommunikationstechnik in privaten Haushalten und der Privatwirtschaft ist hoch.

Die Bedeutung von IKT für Deutschland wird auch in der IKT-Strategie der Bundesregierung „Deutschland Digital 2015“ verdeutlicht, in der die Informations- und Kommunikationstechnologien als entscheidende Rolle für den Hightech-Standort Deutschland und als Schlüssel für Produktivität in allen Branchen bezeichnet werden. Ein Kernelement der Strategie sind die digitalen Netze zum Austausch digitaler Informationen. Die Bundesregierung weist deutlich darauf hin, dass „künftige Netze und intelligente Netzplattformen als kritische Infrastruktur [...] sicher und zuverlässig gehalten werden“ [BMWi 2010].

Der KRITIS-Sektor IKT als Betreiber der technischen Basisinfrastruktur für Sprach- und Datenkommunikation und Einrichtungen zur Datenspeicherung und -verarbeitung spielt demnach eine wichtige Rolle für die deutsche Gesellschaft und ist durch seine Querschnittsfunktion in anderen Wirtschaftssektoren von elementarer Bedeutung.

1.1 Abgrenzung des IKT-Sektors

Der IKT-Sektor wird in dieser KRITIS-Studie als der für die grundlegende *IKT-Basisinfrastruktur* verantwortliche Wirtschaftssektor betrachtet. Die durch den Sektor bereitgestellte technische Infrastruktur ermöglicht IKT-Nutzern die Sprach- (Telefonie) und Datenkommunikation (Internet) sowie Datenspeicherung und -verarbeitung. Der Sektor stellt dazu Anschluss-, Vermittlungs-, Übertragungs-, Steuerungs- und Hostingdienstleistungen zur Verfügung.

Der KRITIS-Sektor IKT in dieser Studie wird im Folgenden anhand der Aufteilung der Volkswirtschaft in Wirtschaftszweige durch das Bundesamt für Statistik definiert (siehe Abbildung 1). Dies dient dem besseren Verständnis und der klaren Abgrenzung gegenüber anderen Teilen der Wirtschaft.

Der KRITIS-Sektor IKT umfasst im weiteren Verlauf dieser Studie die folgenden Wirtschaftszweige (WZ):

Telekommunikation: Übertragung von Sprache und Kommunikation über mobile, ortsgebundene und Satellitenkommunikation und Bereitstellung der jeweiligen Zugänge.

- WZ 61.1: Leitungsgebundene Telekommunikation
- WZ 61.2: Drahtlose Telekommunikation
- WZ 61.3: Satellitentelekommunikation
- WZ 61.9: Sonstige Telekommunikation (Internet)

Informationstechnik: Informationsdienstleistungen – Datenverarbeitung und -bereitstellung

- WZ 62.03: Betrieb von Datenverarbeitungseinrichtungen für Dritte

- WZ 63.11: Datenverarbeitung, Hosting und damit verbundene Tätigkeiten

Wirtschaftszweige wie IT-Beratung, Softwarevertrieb, Programmierung etc., die *nicht* zu den Betreibern der Infrastruktur zählen, gehören nicht zum IKT-Sektor.

Nicht zum KRITIS-Sektor IKT gehört weiterhin die „Internetwirtschaft“, die lediglich als Kunde die Infrastruktur des Sektors nutzt. Im „Monitoring Report Digitale Wirtschaft 2013“ des Bundesministeriums für Wirtschaft und Energie werden IKT und Internetwirtschaft klar voneinander abgegrenzt. Auch der Branchenverband BITKOM zählt in seiner IKT-Marktanalyse die Internetwirtschaft nicht zum IKT-Sektor [BITKOM 2014a; BITKOM 2009]. Zur Internetwirtschaft gehören u. a. Online-Applikationen, SaaS, IaaS, PaaS,[2] E-Commerce, Online-Werbung, Online-Plattformen und Content-Delivery-Netzwerke [eco 2009].

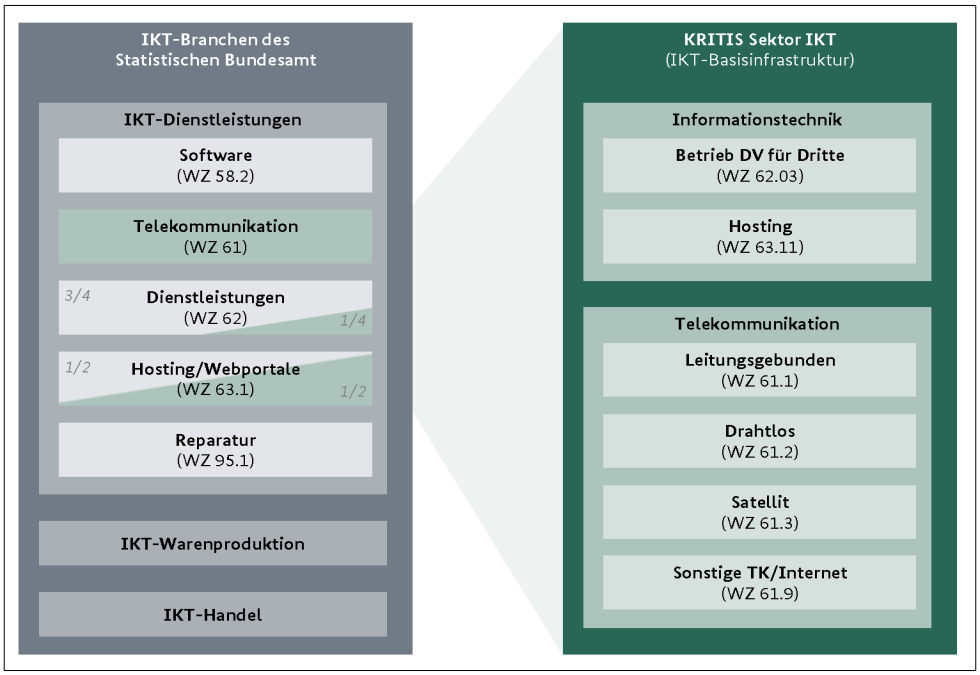

Abbildung 1: Definition des KRITIS-Sektors IKT

Quelle: eigene Darstellung

2 Software as a Service, Infrastructure as a Service sowie Platform as a Service bezeichnen reine Servicemodelle.

1.2 Wirtschaftliche Einordnung

Der KRITIS-Sektor IKT ist einer der größten und umsatzstärksten Bereiche der als „IKT-Branche“ zusammengefassten Wirtschaftszweige des Statistischen Bundesamts (siehe Tabelle 2). Die Definition des Statistischen Bundesamts dieser IKT-Branche ist, abweichend von der vorliegenden Studie, sehr weit gefasst und umfasst die drei Bereiche IKT-Dienstleistungen, IKT-Warenproduktion und IKT-Handel. Dabei enthält der Bereich IKT-Dienstleistungen den IKT-Sektor dieser Studie.

Bereich	*Umsatz 2010 (in Mrd. Euro)*	*Umsatz 2011 (in Mrd. Euro)*	*Tätige Personen 2010*	*Tätige Personen 2011*
IKT-Warenproduktion	38,52	36,78	137.327	117.920
IKT-Handel	81,77	85,09	119.239	137.139
IKT-Dienstleistungen	161,23	173,20	669.191	714.569
Gesamt „IKT-Branche“	**281,52**	**295,07**	**925.757**	**969.628**

Tabelle 2: Umsatz 2010 und 2011 der „IKT-Branche“ nach Definition destatis

Quelle: Aufteilung und Zahlen 2010: [DESTATIS 2013c]. Zahlen 2011 errechnet aus: [DESTATIS 2013b]

Der **KRITIS-Sektor IKT** ist Teil des Bereichs „IKT-Dienstleistungen“[3] und machte 2010 einen Umsatz von 86,88 und 2011 von 85,61 Mrd. Euro.

Bereich	*Umsatz 2010 (in Mrd. Euro)*	*Umsatz 2011 (in Mrd. Euro)*	*Tätige Personen 2010*	*Tätige Personen 2011*
WZ 61 (komplett)	72,66	70,03	131.029	118.758
WZ 62.03	10,42	9,78	44.362	44.361
WZ 63.11	3,80	5,80	25.991	34.234
KRITIS-Sektor IKT	**86,88**	**85,61**	**201.382**	**197.353**

Tabelle 3: Umsatz 2010 und 2011 des KRITIS-Sektors IKT

Quelle: Angaben für WZ aus [DESTATIS 2013c] und [DESTATIS 2013b]. Angaben für KRITIS-Sektor berechnet

Nach dem „Monitoring-Report Digitale Wirtschaft 2013“ des Bundesministeriums für Wirtschaft und Energie (BMWi) beträgt der Anteil der (dort auch weit gefassten) „IKT-Branche“ am gewerblichen Umsatz in Deutschland im Jahr 2013 4,2 Prozent [BMWi 2013]. Unabhängig von der genauen Definition gehört der KRITIS-Sektor IKT als Teilbereich der „Dienstleistungen“ zum stärksten Bereich in der deutschen Wirtschaft.[4]

Den IKT-Sektor zeichnen folgende Merkmale in der deutschen Gesellschaft aus:

- Große Abhängigkeit anderer KRITIS-Sektoren von den Dienstleistungen des IKT-Sektors.
- Hoher Verbreitungsgrad der IKT-Dienstleistungen in Gesellschaft, Wirtschaft und Wissenschaft.

3 Das Bundesamt zählt zu „IKT-Dienstleistungen“ nach DESTATIS 2013c die folgenden WZs: WZ 58.2, WZ 61, WZ 62, WZ 63.1, WZ 95.1.

4 Die Wertschöpfung der gesamten IKT-Branche übersteigt nach BMWi im Jahr 2013 die von „traditionellen Branchen“ wie Maschinenbau und Automobilwirtschaft.

1.3 Entwicklung des IKT-Sektors

Aufgrund der schnellen Entwicklung von Informations- und Kommunikationstechnologien befindet sich der IKT-Sektor in einem ständigen Umbruch. Betroffen sind Geschäftsmodelle und Wertschöpfungsketten von Unternehmen innerhalb und außerhalb des Sektors. Entwicklungen innerhalb des Sektors betreffen die technische Basisinfrastruktur direkt oder die Anforderungen an diese, da sich das Nutzerverhalten ändert.

Aus Sicht dieser Studie seien einige aktuelle, technische Entwicklungen genannt, die Einfluss auf die IKT-Basisinfrastruktur haben und die disruptive Entwicklung des Sektors darstellen:

- **Auslagerung von IT ins Internet**: In Internet-basierten Servicemodellen wie Cloud-Computing, IaaS, PaaS und SaaS lagern Unternehmen IT-Ressourcen (Speicherkapazität, Rechenleistung, Software) an externe Dienstleister aus und greifen über das Internet auf diese zu. Dabei werden diese Dienste (Services) auf der Infrastruktur von Rechenzentrumsbetreibern und IT-Hostern bereitgestellt. Dies erhöht die Abhängigkeit von einer funktionsfähigen und verlässlichen Netzanbindung der Unternehmen an das Internet. Die Beschleunigung der Entwicklung und Einführung von Cloud-Computing sind zwei der Ziele der IKT-Strategie der Bundesregierung „Deutschland Digital 2015“, womit die Abhängigkeit von Netzzugängen ebenfalls steigen wird [BMWi 2010].
- **Umstellung auf All-IP-Netze**: Traditionelle leitungsvermittelnde Telekommunikationsnetze werden durch paketvermittelnde Netzinfrastrukturen abgelöst. Dabei werden die historisch gewachsenen, teils sehr komplexen Netzarchitekturen und -technologien durch eine einheitliche, auf dem Internet Protokoll (IP) basierte Netzarchitektur ersetzt (All-IP). In diesem Zusammenhang wird auch von Netzen der nächsten Generation (Next Generation Networks) gesprochen. Dieser flächendeckende Ausbau einer neuen breitbandigen, IP-basierten Basisinfrastruktur resultiert in einer nahezu vollständigen Transformation der bisherigen Basisinfrastruktur. Aktuell befinden sich Netze deutscher Netzbetreiber bereits in der Transformation. Die Deutsche Telekom beispielsweise plant, bis Ende 2018 ihr gesamtes Netz in Deutschland auf die IP-Technologie (All-IP) umzustellen [Nemat 2013].
- **Long Term Evolution (LTE)**: Der wachsende Datenverkehr im Mobilfunk erfordert einen Ausbau der Leistungsfähigkeit mobiler Netze [BNetzA 2013a, S. 43ff]. Infolgedessen rüsten Netzbetreiber derzeit ihre Funkzugangsnetze mit Technik des Mobilfunkstandards Long Term Evolution (LTE) aus, die verglichen zur bisherigen Technik deutlich höhere Datenraten bei der Funkübertragung ermöglicht. Diese Generation der Netze wird auch als vierte Generation (4G) bezeichnet. Laut Angaben der Bundesnetzagentur erreichte die Abdeckung LTE-fähiger Netze Ende 2012 bereits circa 51 Prozent der deutschen Haushalte [BNetzA 2013a, S. 46]. Zusätzlich zum Anstieg des Datenverkehrs steigt das Sprachvolumen im Mobilfunk gegenüber dem Festnetz sehr stark an [BNetzA 2013a, S. 58].

Die Entwicklung des IKT-Sektors ist maßgeblich von der Größe und Struktur der Marktteilnehmer bestimmt. Ein oftmals hohes Investitionsvolumen führt dazu, dass entsprechende Investitionen in den Netzausbau und technische Innovationen meist nur durch die großen Unternehmen vorangetrieben werden. Europaweit gibt es eine Tendenz zu Märkten mit drei bis vier großen Unternehmen [EC 2013].

Neben technischen Entwicklungen im IKT-Sektor sind auch marktwirtschaftliche Rahmenbedingungen zu beobachten, die Einfluss auf die Entwicklung des Sektors haben:

- **Marktstellung der Deutschen Telekom**: Aufgrund der historischen Entwicklung des IKT- und speziell des Telekommunikationsmarktes besitzt die Deutsche Telekom (DTAG) im Bereich der sprachbasierten Telekommunikation einen Marktanteil von über 40 Prozent [VATM 2013]. Die Liberalisierung des Sektors durch das Telekommunikationsgesetz (TKG) im Jahr 1996 hat zwar Wettbewerbern den Zugang zum Markt ermöglicht, die leitungsgebundene Infrastruktur (z. B. Leitungen und Ortsverteiler-Stationen) ist jedoch noch immer größtenteils im Besitz der Deutschen Telekom. Wettbewerber der DTAG sind daher auf die Mitnutzung dieser Infrastruktur angewiesen. Dies betrifft insbesondere die Teilnehmeranschlussleitung (TAL), welche die Verkabelung zwischen dem Hausanschluss der Kunden und den Ortsverteiler-Stationen der DTAG bezeichnet.

- **Rolle der Kabelnetzbetreiber**: Neben der Anbindung von Kunden an Sprach- und Datennetze über die Infrastruktur der Deutschen Telekom haben sich in den vergangenen Jahren Betreiber der Kabelnetze etabliert, die neben der Übertragung von Fernsehsignalen auch Telefon- und Internetanschlüsse vermarkten. Die Nutzung der Breitbandkabelnetze für die Erbringung von Datendiensten kann eine wichtige Rolle bei der zukünftigen Entwicklung des Sektors spielen. Zwar werden noch immer 60 Prozent aller Telefonanschlüsse über die Anmietung der Teilnehmeranschlussleitung (TAL) realisiert, es wird jedoch ein weiterer Rückgang dieses Anteils erwartet [BNetzA 2013a].
- **Marktregulierung**: Der Einstieg in den Sektor und der Wettbewerb innerhalb des Sektors sind stark davon abhängig, dass übergeordnete Instanzen wie die Bundesnetzagentur den Zugang zur Netzinfrastruktur auch den Mitbewerbern der Deutschen Telekom ermöglichen. Diese Marktregulierung wiederum erfordert ein hohes Maß an Beteiligung durch den deutschen Staat, um Regularien kontinuierlich am technischen Fortschritt und infrastrukturellen Wandel auszurichten. So versucht der Staat auch Anreize für den Ausbau der IKT-Infrastruktur zu schaffen, zum Beispiel durch Förderung der Erschließung von ländlichen Gegenden [BNetzA 2010]. Dieser Ausbau bezieht sich dabei primär auf die oben beschriebenen Netze der nächsten Generation [BNetzA 2013c].

2 Branchen

Die Unterscheidung der vormaligen Branchen *Informationstechnik* (WZ 62.03 und WZ 63.11) und *Telekommunikation* (WZ 61.1, WZ 61.2 , WZ 61.3 und WZ 61.9) wird zunehmend unscharf. Die Basistechnologien und Infrastrukturen zur Übertragung von Sprache und Daten haben sich in den vergangenen Jahren immer mehr angeglichen. So werden Sprache und Daten zum größten Teil auf Basis der gleichen technischen Verfahren und über die gleichen Netze übertragen (Konvergenz) und durch eine Marktkonsolidierung erbringt eine Vielzahl der Markteilnehmer einen Großteil der Dienstleistungen des IKT-Sektors aus einer Hand (Konsolidierung) [OECD 2008].

Im weiteren Verlauf dieser Studie werden die früheren Branchen Informationstechnik (IT) und *Telekommunikation* (TK) aufgrund der **Konvergenz** und **Konsolidierung** in einer gemeinsamen Branche **Informationstechnik und Telekommunikation (IKT)** betrachtet (siehe Abbildung 2).

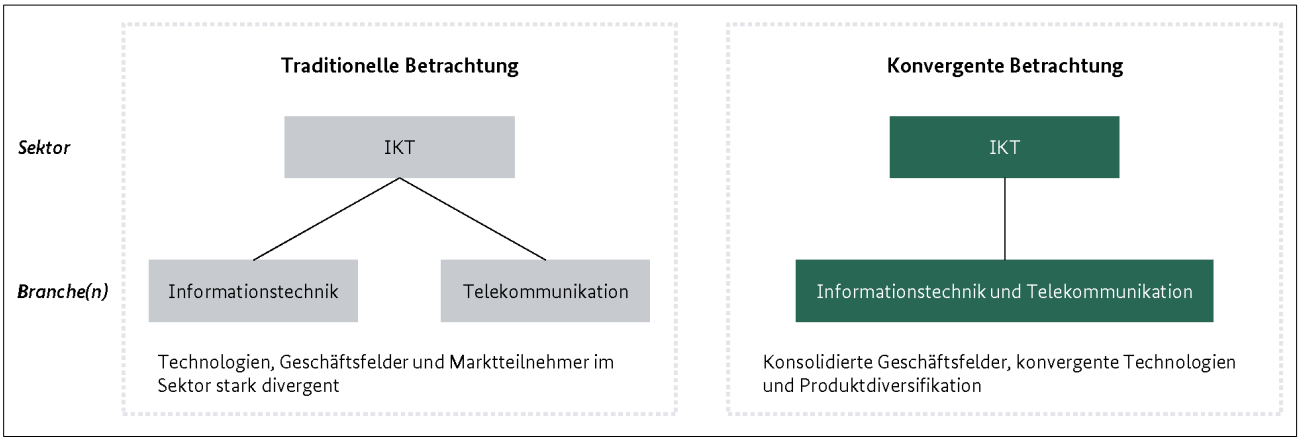

Abbildung 2: Konvergente Betrachtung der Branchen im IKT-Sektor

Quelle: eigene Darstellung

Für die technische **Konvergenz** innerhalb des KRITIS-Sektors IKT ist maßgeblich die Entwicklung der technischen Infrastrukturen im Übertragungsnetz verantwortlich. Anbieter auf dem deutschen Telekommunikationsmarkt stellen nach und nach heterogene Netzinfrastrukturen auf eine einheitliche, IP-basierte Infrastruktur (sogenannte NGN bzw. All-IP-Netze) um [Nemat 2013]. Innerhalb der betriebenen Netze werden Daten und Sprache gemeinsam einheitlich über das Internet Protokoll übertragen. Die bestehenden Netzinfrastrukturen (Festnetz-, Mobilfunk- und Kabelnetze) werden somit gleichermaßen zur Erbringung von Sprach- und Datendiensten eingesetzt. Eine Unterscheidung zwischen reinen Sprach- und Datennetzen ist dadurch im Regelfall nicht mehr gegeben.

Die Konvergenz ist ein anhaltender Prozess, der noch nicht vollständig in alle Bereiche durchgedrungen ist. Insbesondere im Bereich der Zugangsnetze, d. h. regionale Netze, die Endkunden mit den großen Sprach- und Datennetzen der Netzbetreiber verbinden (vgl. Abschnitt 2.1.2), ist die Konvergenz noch vergleichsweise gering. So unterscheiden sich z. B. traditionelle analoge Telefonnetze (PSTN) und Breitbandkabel-Zugangsnetze aus technischer Sicht weiterhin stark.

Dennoch werden bereits heute Dienste (Telefon und Datenübertragung) nahezu unabhängig von der Anschlusstechnologie bereitgestellt. So können Endkunden über das klassische Telefonnetz (PSTN) genauso telefonieren wie über Breitbandkabelnetze oder Datennetze (mittels VoIP). Spätestens beim Übergang von Zugangsnetzen zu nachgelagerten Sprach- und Datennetzen werden Sprache und Daten, aufgrund der hier sehr weit fortgeschrittenen Konvergenz, über gleichartige Netze übertragen. Die Vermittlung zwischen den Netzen erfolgt dabei durch den Einsatz von Gateways.

Ein weiterer Faktor, der die Struktur des IKT-Sektors maßgeblich beeinflusst, ist die **Konsolidierung** des Marktes seit der Marktöffnung im Jahr 1996. Aus dem Telekommunikationsbereich der Deutschen

Bundespost ist in mehreren Schritten durch die Privatisierung unter anderem die Deutsche Telekom AG (DTAG) entstanden. Die DTAG verlor durch die Liberalisierung des Telekommunikationsmarktes ihre Monopolstellung. Anfänglich war es für kleinere Unternehmen schwierig, sich am Markt zu positionieren, da die bestehende Infrastruktur vollständig im Besitz der Deutschen Telekom war. So fielen Kosten (für Vorleistungen) für die Mitbewerber an, sobald sie die Netze und Vermittlungsstellen der Telekom verwendeten, um eigene Verbindungen zu ermöglichen. Die Anzahl der Wettbewerber und deren relativer Anteil am Marktvolumen im Bereich Telekommunikation steigt seit der zunehmenden Regulierung des Marktes durch die Bundesnetzagentur kontinuierlich an (siehe Abbildung 3). Im Jahr 2012 besaß die Deutsche Telekom daher einen verringerten Marktanteil von 43,7 Prozent.

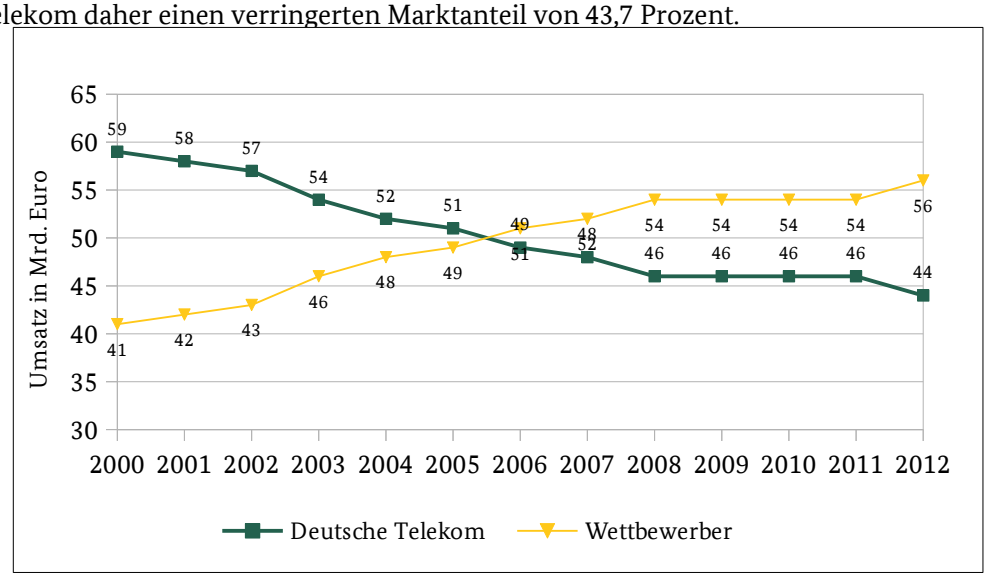

Abbildung 3: Umsatzanteil auf dem TK-Markt

Quelle: in Anlehnung an [statista 2014a]

In Deutschland gehören im Wesentlichen die Anbieter Deutsche Telekom, Vodafone (als Gesellschaft im Zusammenschluss mit Kabel Deutschland) und Telefónica (in geplanter Fusion mit E-Plus) zu den größten Marktteilnehmern (siehe Abschnitt 2.1.2.2) [MoKo 2013].

Im Zusammenhang mit den Anbietern und Betreibern der Basisinfrastruktur zum Austausch von Sprache und Daten sind auch die Infrastrukturen der beteiligten IT-Systeme und Netzkomponenten von Bedeutung und Teil dieser Branche. Dies umfasst insbesondere Rechenzentren, in denen das entsprechende IT-Equipment zur Datenverarbeitung für Dritte (z. B. Gesellschaft, öffentliche Hand, Wirtschaft), betrieben wird.

2.1 Informationstechnik und Telekommunikation

2.1.1 Branchenüberblick

2.1.1.1 Einführung in die Branche Informationstechnik und Telekommunikation

Die Branche Informationstechnik und Telekommunikation im KRITIS-Sektor IKT umfasst die Teile der Wirtschaft, die an der Leistungserbringung im Sektor beteiligt sind: der Bereitstellung der IKT-Basisinfrastruktur zum Austausch, Speicherung und Verarbeitung von Daten (Internet) und Übermittlung von Sprache (Telefonie). Die Leistungserbringung innerhalb der Branche ist in sechs Wirtschaftszweige untergliedert (siehe Tabelle 4).

Wirtschaftszweig	*Beschreibung*	*Beispielhafte Tätigkeiten*
Leitungsgebundene Telekommunikation (WZ 61.1)	Betrieb und Unterhalt von Einrichtungen zur Übertragung von Sprache, Daten, Text, Ton und Bild mittels leitungsgebundener Infrastruktur	• Bereitstellung von Zugängen zum Festnetz • Übermittlungsdienste • Betrieb von leitungsgebundenen Netzen
Drahtlose Telekommunikation (WZ 61.2)	Betrieb und Wartung von Einrichtungen zur Übertragung von Sprache, Daten, Text, Ton und Bild mittels drahtloser Infrastruktur	• Bereitstellung von Zugängen zum Mobilfunknetz • Betrieb von Mobilfunknetzen
Satellitentelekommunikation (WZ 61.3)	Betrieb und Wartung von Einrichtungen zur Übertragung von Sprache, Daten, Text, Ton und Bild mittels satellitengestützter Infrastruktur	• Bereitstellung von Zugängen zum Satellitennetz • Betrieb des Satellitennetzes
Sonstige Telekommunikation (WZ 61.9)	Umfasst unter anderem Internet Service Provider (ISP) und die Bereitstellung von Internet-Telefonie (VoIP) und sonstigen Diensten	• Bereitstellung von Zugängen zum Internet • Bereitstellung von Internetzugängen in öffentlichen Bereichen • Internettelefonie (VoIP)
Betrieb von Datenverarbeitungseinrichtungen für Dritte (WZ 62.03)	Betrieb und Verwaltung von Computersystemen für Kunden	• Betrieb Infrastruktur und Computer/ DV-Anlagen • Betrieb von Rechenzentren
Datenverarbeitung, Hosting und damit verbundene Tätigkeiten (WZ 63.11)	Betrieb von Infrastrukturen zum Hosting von Systemen und Diensten für Dritte	• Bereitstellung von Infrastruktur in Rechenzentren

Tabelle 4: Wirtschaftszweige innerhalb der KRITIS-Branche IKT

Quelle: nach [DESTATIS 2008]

Die Dienstleistungen der Branche werden nicht zwingend von einer einzigen Instanz erbracht, sondern sind das Ergebnis des Zusammenwirkens verschiedener Rollen.

Im weiteren Verlauf dieser Studie werden die Marktteilnehmer der Branche anhand ihrer Tätigkeiten verschiedenen Rollen zugeordnet (siehe Tabelle 5). Diese Rollen strukturieren die Tätigkeiten innerhalb der Branche und stellen idealtypische Betreiber dar, die einzelne Teile der Dienstleistungen erbringen. Daher können einzelne Marktteilnehmer auch mehrere Rollen haben, was die tatsächliche Position im Markt widerspiegelt.

Weiterhin wird das Rollenmodell auch dazu verwendet, um die Marktteilnehmer und ihre spezifischen Dienstleistungen genauer zu gruppieren (siehe Abschnitt 2.1.2.2) und die Beziehungen innerhalb der Branche darzustellen (siehe Abschnitt 2.1.2.3).

Rolle	*Rollenbeschreibung*	*Marktstruktur*
Service Provider	Bereitstellung von Zugängen zum Telefon- und Datennetz (über Kabel-, Fest- oder Mobilfunknetze)	Oligopol (dominiert von drei Anbietern)[5]
Netzbetreiber	Betrieb von nationalen, regionalen oder lokalen Netzen (Kabel-, Fest- oder Mobilfunknetz)	Oligopol (dominiert von der DTAG)
Knotenbetreiber	Betrieb von Telefonie- und Datenknoten	Großkonzerne, Vereine, KMU
Verwaltung	Pflege und Verwaltung von Datenbanken zur Vermittlung (Daten und Sprache)	Gemischt (teilweise monopolistische Struktur, aber auch KMU)
IT-Hoster	Betrieb von IT-Systemen und Hosting für Dritte zur Speicherung und Verarbeitung von Daten	Polypol
Rechenzentrums-betreiber	Betrieb von Rechenzentren und zugehöriger Infrastruktur	Polypol

Tabelle 5: Rollen der Marktteilnehmer innerhalb der IKT-Branche

2.1.1.2 Bedeutung für Staat und Gesellschaft

Die IKT-Branche hat für Staat und Gesellschaft eine große Bedeutung, da sie die Basisinfrastruktur zur Nutzung von Telefonie und Internet bereitstellt, die von weiten Teilen der Bevölkerung, der Wirtschaft und der öffentlichen Hand genutzt werden. Je nach Definition ist die IKT-Branche unter den fünf führenden gewerblichen Branchen Deutschlands, sowohl nach Umsatz als auch nach Anzahl der Beschäftigten [BMWi 2013].

Zu den Nutzern der Infrastruktur des Internets und der Telefonie zählt der Großteil der deutschen Wirtschaft:

- 87 Prozent der deutschen Unternehmen verfügen über einen Internetanschluss [DESTATIS 2013a]
- 39 Prozent der deutschen Unternehmen nutzen automatisierte Schnittstellen zum Datenaustausch [Bauer 2009]
- 74 Prozent der deutschen Unternehmen tätigen Bank- und Finanzgeschäfte im Internet [DESTATIS 2013a]
- 51 Prozent der deutschen Unternehmen nutzen Online-Dienste der öffentlichen Hand (E-Government) [DESTATIS 2013a]

Nach einer BITKOM-Studie sind 50 Prozent der deutschen Wirtschaft aufgrund ihres Geschäftsmodells zumindest teilweise vom Internet abhängig. Davon ist bei 18 Prozent der Unternehmen das Internet ein *starker* Einflussfaktor, bei zwei Prozent basiert das Geschäftsmodell *vollständig* auf dem Internet. Dabei ist tendenziell ein stärkerer Einfluss des Internets bei Dienstleistern und kleineren Unternehmen zu erkennen [BITKOM 2011b].

Insbesondere in den Teilen der Wirtschaft, die stark von der Informationsbeschaffung und dem Informationsaustausch abhängen (u. a. Handel, Dienstleistungen und Finanzwesen), ist die Nutzung des Internets zum schnellen und unkomplizierten Austausch von Informationen ein wichtiger Faktor und oftmals zentraler Bestandteil von Geschäftsprozessen. Auch in der Industrie spielen IKT-Technologien eine wichtige Rolle, etwa in der Vernetzung von Produktionssystemen und der Steuerung von Maschinen und

5 DTAG, Vodafone/Kabel Deutschland, Telefónica in geplanter Fusion mit E-Plus.

Anlagen. Der Austausch von Informationen zwischen einzelnen Produktionsstandorten erfolgt dabei oftmals auf Basis des Internets. Der fortwährende Ausbau der IKT-gestützten Vernetzung in der Industrie wird derzeit auch durch die Bundesregierung im Zukunftsprojekt „Industrie 4.0“, als Teil der Hightech-Strategie der Bundesregierung, gefördert [BMBF 2014]. Es ist davon auszugehen, dass durch die zunehmende Digitalisierung die Bedeutung der IKT-Basisinfrastruktur für die Industrie weiter zunimmt.

Auch in der öffentlichen Verwaltung wird moderne Kommunikations- und Informationstechnik eingesetzt und leistet einen wichtigen Beitrag zur Verwaltungsmodernisierung [CIOBund 2014]. Der elektronische Austausch von Informationen in Form von Sprache und Daten ist nicht nur innerhalb der Ministerien und Behörden wichtig, sondern auch im Kontakt mit den Bürgern. Mit dem im Jahr 2013 in Kraft getretenen „Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften“ (E-Government-Gesetz) verfolgt die Bundesregierung das Ziel, die elektronische Kommunikation mit der Verwaltung zu erleichtern und elektronische Verwaltungsdienste (auf Basis von IKT) anzubieten [Bundestag 2013].

Aus der E-Government-Strategie des Bundes ergeben sich viele Produkte und Dienste für die deutsche Gesellschaft und Wirtschaft. Der Umgang mit elektronischen Verwaltungsdiensten, etwa De-Mail, ElsterOnline oder der elektronischen Lohnsteuerkarte, erfordert für alle Beteiligten eine funktionsfähige und zuverlässige IKT-Basisinfrastruktur.

Ebenfalls von Bedeutung für weite Teile der Gesellschaft, Wirtschaft und den Staat sind Online-Dienste wie Suchmaschinen, E-Mail und Soziale Netzwerke. Die Grundlage für diese Dienste bilden Einrichtungen zur Datenverarbeitung, d. h. IT-Systeme. Diese IT-Systeme, mit deren Hilfe die Dienste zur Verfügung gestellt werden, sind in der Regel in Rechenzentren untergebracht, welche die zum reibungslosen Betrieb notwendige konstante Versorgung der Systeme mit Strom und Internetkonnektivität bereitstellen.

2.1.1.3 Wahrnehmung der Branche

Telefonie und Internet als ständige Begleiter sind gerade durch die Ausrichtung auf die schnelle Informationsbereitstellung, -übertragung und -verarbeitung stark im Fokus der Gesellschaft, des Staates und der Wirtschaft. Die Nutzer der Dienste zeigen dabei eine sehr geringe Toleranz gegenüber Ausfällen oder Geschwindigkeitsproblemen, etwa der Verzögerung beim Laden von Webseiten [Bhatti 2000].

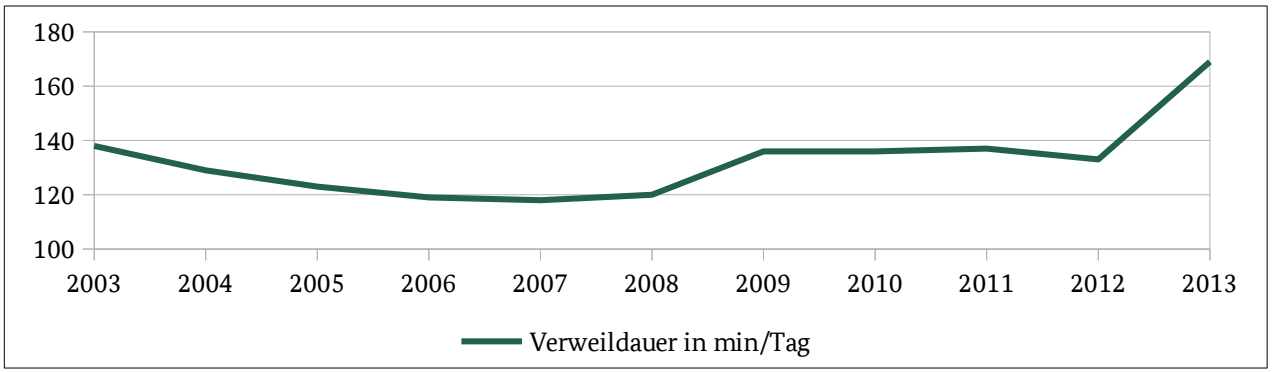

Abbildung 4: Durchschnittliche Verweildauer bei der Onlinenutzung

Quelle: in Anlehnung an [ARD/ZDF 2014]

Insgesamt ist die tägliche Nutzungsdauer des Internets in den letzten sieben Jahren einem positiven Trend gefolgt und betrug im Jahr 2013 durchschnittlich 165 Minuten (siehe Abbildung 4). Damit nutzt der durchschnittliche Nutzer das Internet mehr als zweieinhalb Stunden täglich.

Über 71 Prozent der Mobilfunknutzer bewerten die permanente private Erreichbarkeit als wichtig. In einer repräsentativen Studie der BITKOM gaben 88 Prozent der befragten Arbeitnehmer an, dass sie auch außerhalb der Arbeitszeiten zu erreichen sind, obwohl lediglich acht Prozent über ein mobiles Endgerät ihres Arbeitgebers verfügen. Damit wird verdeutlicht, dass auch die privaten Telefon- und Internetanschlüsse und Mobiltelefone für die berufliche Erreichbarkeit genutzt werden.

Das Internet wird von den Befragten vermehrt als Informationsquelle wahrgenommen, mit 55 Prozent zwar noch hinter Fernsehen und Radio; eine stark positive Entwicklung wird jedoch vorausgesehen [BITKOM 2011a]. Mit der vermehrten Verbreitung von IPTV ist zudem ein Aufgehen des klassischen Fernsehens in den Dienstleistungen der IKT-Branche zu erwarten. Die große Bedeutung des Internets wird zudem durch ein Urteil des Bundesgerichtshofes deutlich. Aus diesem Urteil geht hervor, dass der Zugang zum Internet als ein Grundbedürfnis der Gesellschaft anzusehen ist [BGH 2013]. Das Gericht kam zu folgender Begründung (Bundesgerichtshof, vom 24.01.2013):

> „(1) Die Nutzbarkeit des Internets ist ein Wirtschaftsgut, dessen ständige Verfügbarkeit seit längerer [...] Zeit auch im privaten Bereich für die eigenwirtschaftliche Lebenshaltung typischerweise von zentraler Bedeutung ist und bei dem sich eine Funktionsstörung als solche auf die materiale Grundlage der Lebenshaltung signifikant auswirkt."

Auch in der Wirtschaft wird die Nutzung des Internets als essentiell eingeschätzt. Ein einstündiger Ausfall des internen IT-Betriebs kostet Unternehmen durchschnittlich 41.000 Euro [CIO 2013]. In Verbindung mit der hohen IT-Vernetzung innerhalb der Organisationen haben fast alle Unternehmen in ihren Verträgen mit Internet Service Providern entsprechende Klauseln zur Leistungsgüte, sogenannte Service Level Agreements (SLAs), integriert. Selbst eine augenscheinlich hohe Verfügbarkeit von 98 Prozent kann bei einem 24-Stunden-Betrieb tägliche Ausfallzeiten bis zu etwa 29 Minuten bedeuten.

Dass die oft genutzten Internetdienste in Rechenzentren untergebracht sind, wird durch die Gesellschaft nicht sehr stark wahrgenommen. Die Gesellschaft erwartet eine hohe Dienstbereitschaft, ohne die komplexen Zusammenhänge dahinter zu betrachten. Auch Firmen nutzen teilweise Internetdienste in ihren Geschäftsprozessen (z. B. E-Mail-Dienste, aber auch Internetrecherche) [451Research 2014].

Zudem sind Unternehmen auf schnelle Entscheidungsfindungen angewiesen, die sie gerade durch Telefonie oder E-Mail-Dienste unterstützen können. Dabei muss zwischen der Kommunikation innerhalb von Firmennetzen und der Anbindung entfernter Standorte differenziert werden. Da auch outgesourcte Dienste zumeist über ein Netzwerk (z. B. das Internet) angebunden sind, besteht eine klare Abhängigkeit der Leistungserbringung. Durch die erhöhte Automatisierung in Industrie (z. B. Steuerung von Maschinen und Produktionsstraßen) und im Dienstleistungssektor sind zudem viele Unternehmen auch in der Wertschöpfung auf die Funktionsfähigkeit der IKT-Dienste angewiesen [BITKOM 2011b].

2.1.1.4 Volkswirtschaftlicher Kontext

Die Einordnung der Branche IKT in die deutsche Volkswirtschaft zeigt, dass trotz eines relativ geringen Anteils am BIP (3,8 Prozent[6]) die Kritikalität für die gesamtwirtschaftliche Wertschöpfung durch die großen intersektoralen Abhängigkeiten nicht zu vernachlässigen ist. Die Leistungserbringung anderer Branchen ist stark von der Querschnittsfunktion der IKT-Branche abhängig. In fast allen Wirtschaftsbereichen bestehen elektronische Schnittstellen zum Datenaustausch, zur Steuerung interner Systeme sowie Verbindungen zum Internet [DESTATIS 2013a].

In der **KRITIS-Branche IKT** (deckungsgleich mit KRITIS-Sektor IKT) waren im Jahr 2011 knapp 197.000 Personen in circa 6.800 Unternehmen tätig. Die Branche machte nach dieser Einteilung im Jahr 2011 knapp die Hälfte des Umsatzes und ein Viertel der tätigen Personen der Branche „IKT-Dienstleistungen" aus (siehe Tabelle 6).

Bereich	*Umsatz 2011 in Mrd. Euro*	*Tätige Personen 2011*
IKT-Warenproduktion	36,78	117.920
IKT-Handel	85,09	137.139
IKT-Dienstleistungen	173,20	714.569

6 Vgl. Abschnitt 1.2.

KRITIS-Branche IKT (siehe Tabelle 7)	(85,61)	(197.353)
Gesamt „IKT-Branche“ nach Definition destatis	**295,07**	**969.628**

Tabelle 6: Umsatz innerhalb der Branche IKT 2011

Quelle: [DESTATIS 2013b]. Angabe für KRITIS-Branche berechnet

In der KRITIS-Branche IKT machten **leitungsgebundene** (40,3 Prozent) und **drahtlose** (30,2 Prozent) **Telekommunikation** den größten Teil des Umsatzes aus, gefolgt von **Hosting/Betrieb von DV für Dritte** (18,2 Prozent kombiniert) und **Internetzugang** (10,8 Prozent) (siehe Tabelle 7).

Bereich	*Umsatz 2011 in Mrd. Euro (Anteil)*	*Tätige Personen 2011 (Anteil)*
WZ 61.1: Leitungsgebundene Telekommunikation	34,52 (40,3 %)	63.985 (32,4 %)
WZ 61.2: Drahtlose Telekommunikation	25,87 (30,2 %)	28.630 (14,5 %)
WZ 61.3: Satellitentelekommunikation	0,36 (0,4 %)	777 (0,4 %)
WZ 61.9: Sonstige Telekommunikation (Internet)	9,28 (10,8 %)	25.366 (12,9 %)
WZ 62.03: Betrieb von Datenverarbeitungseinrichtungen für Dritte	9,78 (11,5 %)	44.361 (22,5 %)
WZ 63.11: Datenverarbeitung, Hosting und damit verbundene Tätigkeiten	5,80 (6,8 %)	34.234 (17,3 %)
KRITIS-Branche IKT	**85,61 (100 %)**	**197.353 (100 %)**

Tabelle 7: Umsatz der Wirtschaftszweige der KRITIS-Branche IKT 2011

Quelle: [DESTATIS 2013b]. Angabe für KRITIS-Branche berechnet

Die Umsätze der KRITIS-Branche teilen sich wie folgt auf die beiden Dienstleistungen DL1 und DL2 (siehe Kapitel 3) auf:

Bereich	*Umsatz 2011 in Mrd. EUR (Anteil)*	*Tätige Personen 2011 (Anteil)*
DL1: Sprach- und Datenübertragung (WZ 61)	70,03 (81,7 %)	117.758 (60,2 %)
DL2: Datenspeicherung und -verarbeitung (WZ 62.03 und 63.11)	15,58 (18,3 %)	78.595 (39,8 %)
KRITIS-Branche IKT	**85,61 (100 %)**	**197.353 (100 %)**

Tabelle 8: Umsatz der kritischen Dienstleistungen der KRITIS-Branche IKT 2011

Quelle: [DESTATIS 2013b]. Angabe für KRITIS-Branche berechnet

Insgesamt entwickelt sich die Branche IKT, gemessen am Umsatz, in den letzten Jahren relativ stabil, folgt aber einem leichten Negativtrend (siehe Abbildung 5). Gleichzeitig sinkt der Preisindex[7] für Festnetztelefonie und Internet seit der Liberalisierung des Marktes stark [statista 2014b].

7 Kennzahl zum Vergleich der Preisentwicklung eines Gutes, hier normiert auf 2010.

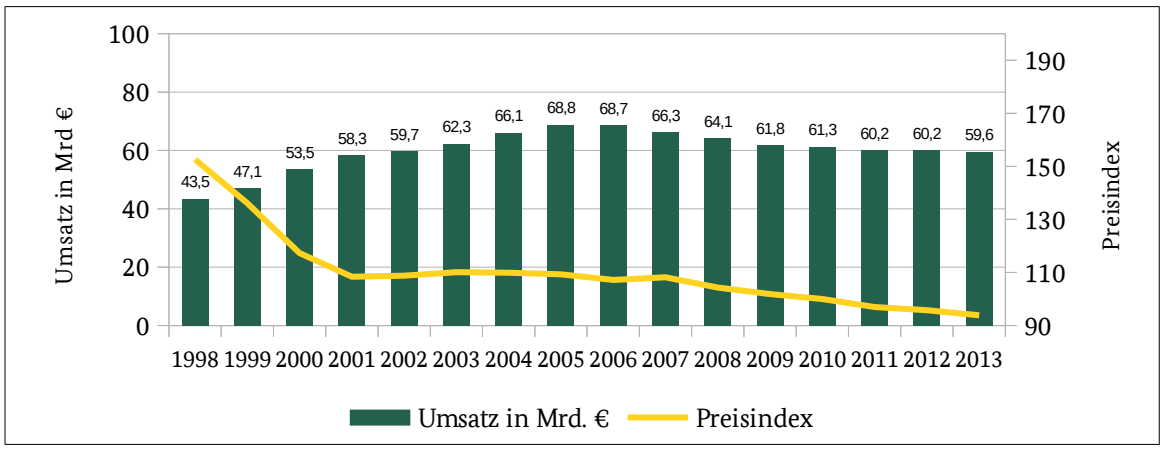

Abbildung 5: Umsatz- und Preisentwicklung IKT-Branche

Quelle: in Anlehnung an [statista 2014b]

2.1.2 Branchenstruktur

Im Folgenden wird die Struktur der KRITIS-Branche IKT beschrieben. Dabei werden Branche und Marktteilnehmer anhand von Rollen definiert, die Teile der Dienstleistungen erbringen (siehe Abbildung 6).

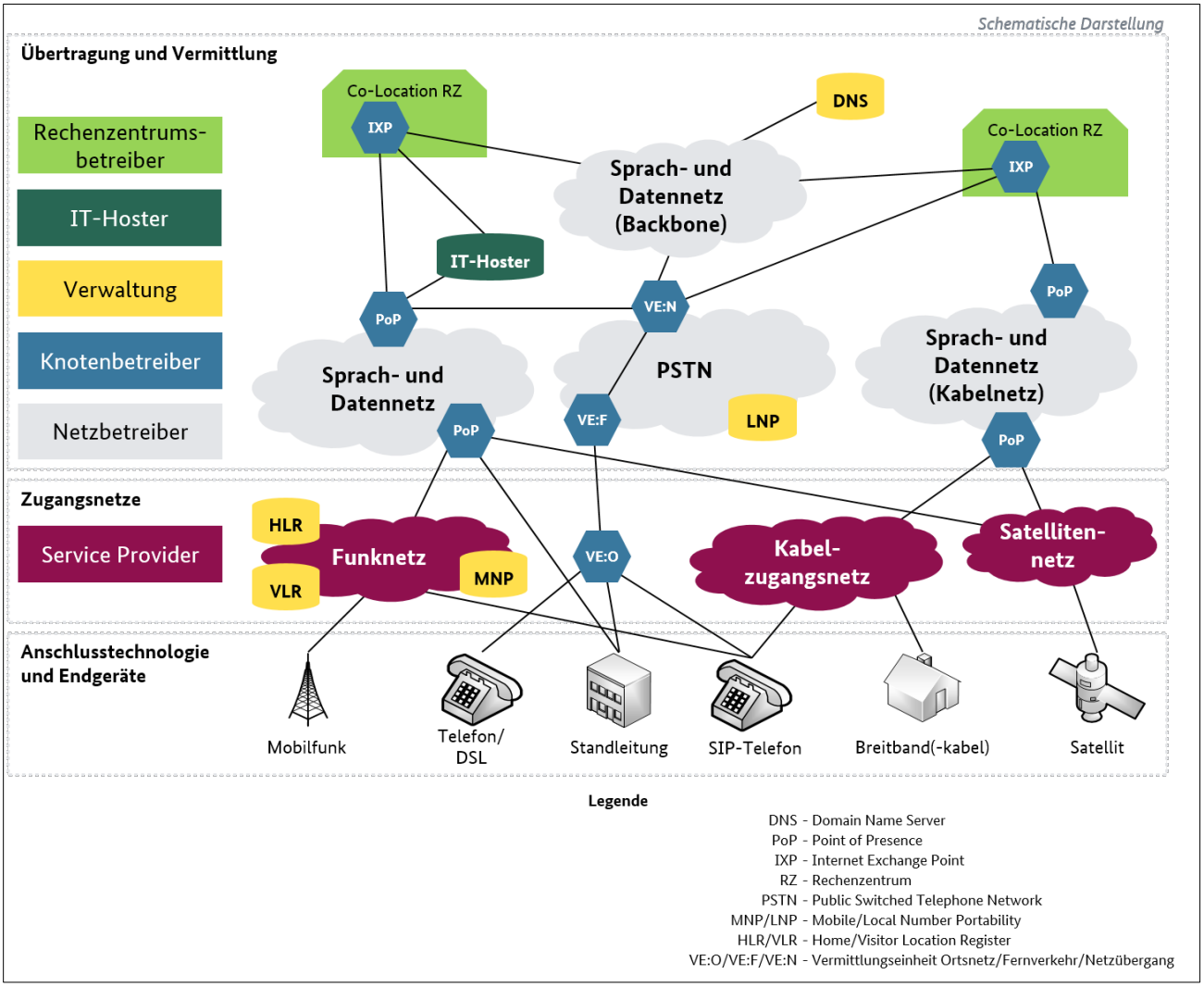

Abbildung 6: Vereinfachter struktureller Aufbau der IKT-Basisinfrastruktur und der KRITIS-Branche IKT

Quelle: eigene Darstellung

Abbildung 6 stellt den stark vereinfachten momentanen Aufbau der IKT-Basisinfrastruktur dar. Durch die Marktkonsolidierung ist eine genaue Abgrenzung einzelner idealtypischer Marktteilnehmer in dieser Übersicht schwer darzustellen. Für die idealtypischen Marktteilnehmer „Ganzheitlicher Betreiber“, „Mobilfunkprovider“ und „Kabelnetzbetreiber“ wird auf spezifische Darstellungen zum Aufbau im Anhang (vgl. Seiten 116-118) verwiesen.

Der Zugang zur IKT-Basisinfrastruktur wird den Endkunden der KRITIS-Branche IKT durch die Rolle der Service Provider bereitgestellt. Dabei bestehen unterschiedliche Zugangstechnologien und Endgeräte, die von den Endkunden genutzt werden können. Hinsichtlich der Konvergenz ist hier insbesondere zu beachten, dass Telefoniedienste über Datennetze und Datenübertragungsdienste über Telefonnetze erfolgen können.

Der Zugang zum analogen Festnetz (PSTN) erfolgt vom Hausanschluss über die TAL an die Vermittlungseinheit des Ortes (VE:O). Hier wird entweder ortsbezogen weitergeleitet oder an die Vermittlungseinheit zum Festnetz (VE:F) übergeben. Bleibt das Telefongespräch im Festnetz (PSTN), so wird es von einem weiteren VE:F aufgenommen und über den entsprechenden VE:O an das Ziel geleitet. Möglich ist auch, dass die Verbindung über eine Vermittlungseinheit mit Netzübergangsfunktion (VE:N) an andere Datennetze geleitet wird. Im Mobilfunk werden Teilnehmer über ein Funkzugangsnetz mit den Sprach- und Datennetzen verbunden. Standleitungen können entweder direkt an eines der vielen Datennetze in der Übertragungs- und Vermittlungsebene angebunden oder über Vermittlungseinheiten des PSTN in das Datennetz weitergeleitet werden. SIP-Telefone (Telefone, die VoIP-Technologie nutzen) können verschiedene Zugangstechnologien verwenden und sind das Sinnbild der technischen Konvergenz auch im Anschlussbereich. Sie können fast jede Zugangstechnologie nutzen, um Sprachdienste anzubieten. Über das Breitbandkabelzugangsnetz (umgangssprachlich auch Fernsehkabelnetz) kann eine Verbindung in die Übertragungs- und Vermittlungsebene erfolgen. Auch über Satelliten kann, je nach Satellitensystem, ein Zugang zu den Sprach- und Datennetzen der Übertragungs- und Vermittlungsebene erfolgen.

Die Übertragungs- und Vermittlungsebene beinhaltet eine Vielzahl unterschiedlicher Sprach- und Datennetze (in Abbildung 6 exemplarisch durch drei Netze dargestellt). Viele Netzbetreiber agieren auf regionaler und ortsbegrenzter Ebene, aber auch in der nationalen Verbreitung gibt es mehr als ein Sprach- und Datennetz. Gerade in dieser Übertragungs- und Vermittlungsebene ist die technische Konvergenz bereits heute sichtbar und wird in naher Zukunft komplett vollzogen sein. Alle dort befindlichen Netze sollen über das Internet Protocol (IP) kommunizieren, unabhängig davon, ob Sprache oder Daten übertragen werden.

Zugang zu den Netzen der Netzbetreiber erhalten Geschäftskunden über die sogenannten Points of Presence (PoP), in denen Netzbetreiber (vor allem in Ballungsräumen) technische Zugangspunkte zu ihren Netzen bereitstellen. Beim Übergang und der Vermittlung zwischen unterschiedlichen Betreibern ist ein Übergang zwischen den Netzen erforderlich. Dieser Übergang wird an Internet Exchange Points (IXPs) hergestellt. Dazu unterhalten die Netzbetreiber teilweise PoP in den Räumlichkeiten der IXPs, die Netzknoten in der Form von Schaltschränken, Servern oder kleineren Rechenzentren darstellen. Ein IXP ermöglicht die Zusammenführung von Netzen verschiedener Betreiber und ermöglicht somit den Netzübergang.

Die IXPs befinden sich meist in Rechenzentren, die Stellflächen für Externe zur Verfügung stellen (Housing oder Co-Location). Der Betrieb dieser Rechenzentren wird durch Rechenzentrumsbetreiber verantwortet, die meist unabhängig von den eigentlichen Netzbetreibern sind. IT-Hoster, die für Anbieter wichtiger Internetdienste ihre Rechenzentren, Server und Datenspeicher zur Verfügung stellen, sind meist direkt an große Netze oder IXPs angeschlossen. Grund hierfür ist die schnellere Datenanbindung und die Vermeidung von Transitgebühren.

Bei der Übertragung und Vermittlung von Sprache und Daten werden einige zentrale Netzinstanzen benötigt, die zur Auflösung und Ermittlung von Übertragungswegen notwendige Informationen bereitstellen. Im Bereich der Telefonie sind dies insbesondere die Datenbanken Telephone Number Portability (TNP) und Mobile Number Portability (MNP), die Informationen über die Zugehörigkeit von Teilnehmern zu Betreibern vorhalten. Im Mobilfunk werden zudem die Datenbanken Home Location Register (HLR) und Visitor Location Register (VLR) benötigt, die Informationen über die Mobilfunkteilnehmer vorhalten.

2.1.2.1 Strukturierung und Organisation der Branche

In Deutschland ist die Struktur der IKT-Branche noch immer maßgeblich durch die historische Monopolstellung der Deutschen Telekom AG beeinflusst. Durch die Liberalisierung der Märkte erfolgte jedoch ein Umbruch, der die Struktur anhaltend verändert.

Im Weiteren wird innerhalb der KRITIS-Branche zwischen den Rollen der Marktteilnehmer (siehe Tabelle 5) und zusätzlich den Verbänden und Regulierungsbehörden unterschieden:

- Service Provider
- Netzbetreiber
- Knotenbetreiber
- Verwaltung
- IT-Hoster
- Rechenzentrumsbetreiber
- Verbände und Regulierungsbehörden

In der Leistungserbringung gibt es zwischen den leistungserbringenden Rollen starke Wechselwirkungen. Ebenfalls gibt es Rollen, die innerhalb der Branche maßgeblichen Einfluss auf die Marktteilnehmer haben.

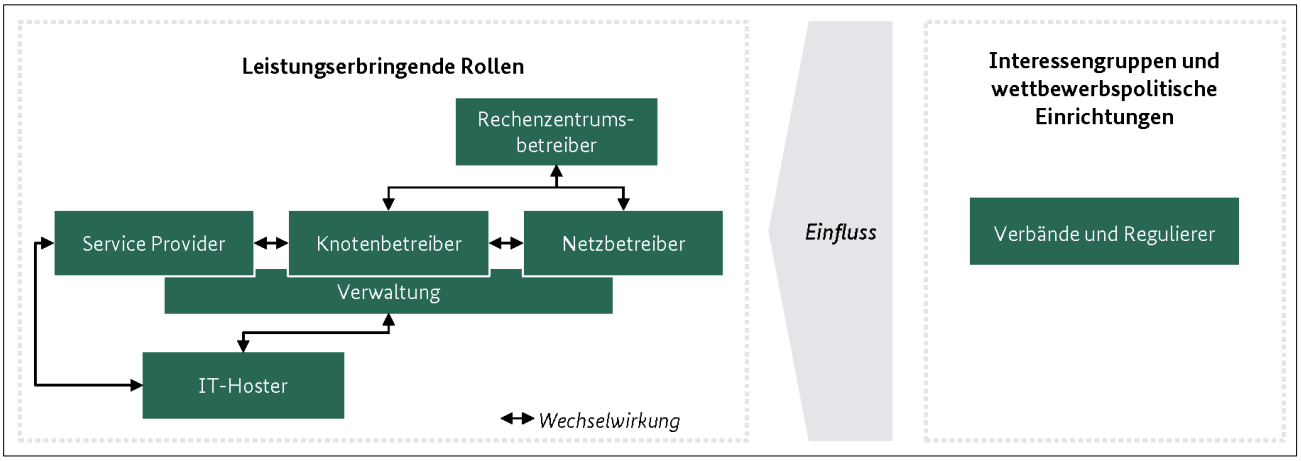

Abbildung 7: Rollen und Wechselwirkungen in der Branche IKT

Quelle: eigene Darstellung

Service Provider

Service Provider stellen Telefon- und Datenanschlüsse für Endkunden zur Anbindung an das Kabel-, Festnetz-, Satelliten- oder Mobilfunknetz bereit. Durch den direkten Kundenkontakt sind die Unternehmen dieser Rolle stark in der Öffentlichkeit präsent. Dabei kann eine Aufteilung der einzelnen Anschlussmöglichkeiten in Telefon- und Datenanschlüsse vorgenommen werden, die wiederum verschiedene technische Umsetzungsvarianten im Anschlussbereich besitzen (siehe Abbildung 8).

Telefonanschlüsse durch alternative Anbieter werden häufig durch Mitnutzung der bestehenden Teilnehmeranschlussleitung (TAL; meist im Besitz der Deutschen Telekom DTAG 2014b) realisiert. Dafür können Marktteilnehmer über die Entbündelung[8] der TAL diese anmieten und für die Bereitstellung eigener Anschlüsse nutzen. Zudem wird die Nutzung von Datenanschlüssen zur Erbringung von Telefoniedienstleistungen (VoIP) immer wichtiger. So setzen Service Provider wie beispielsweise die Deutsche Telekom vermehrt auf IP-basierte Technologien.[9]

8 Bereitstellung von Einzelleistungen, die vormals nur in Zusammenhang mit weiteren Leistungen (gebündelt) erhältlich waren.
9 Der Übergang zu „All-IP“ der Deutschen Telekom soll bis 2018 abgeschlossen sein.

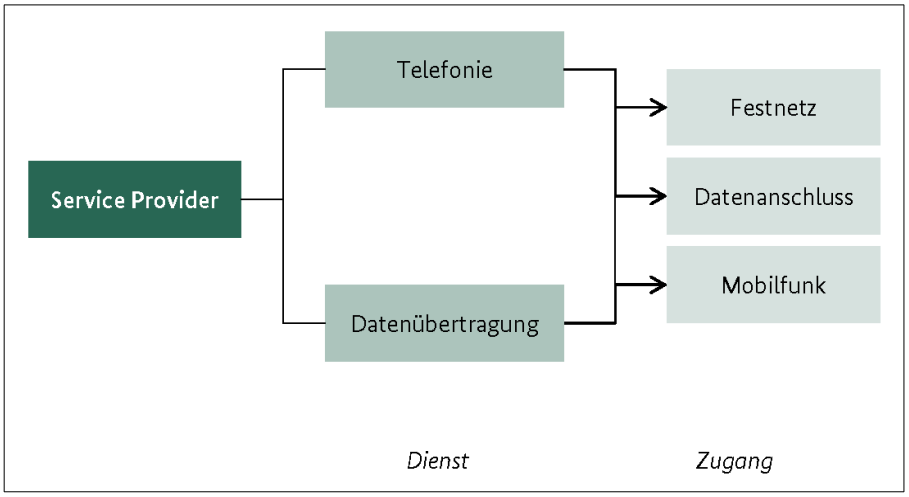

Abbildung 8: Anschlussdienste der Service Provider

Quelle: eigene Darstellung

Ein Großteil der Datenanschlüsse wird durch Festnetzanschlüsse (z. B. über DSL) realisiert (im Jahr 2012 circa 84 Prozent). Davon werden ungefähr 33 Prozent durch alternative Anschlussbetreiber umgesetzt, zumeist durch Anmietung der entbündelten TAL der Deutschen Telekom. Datenanschlüsse in Breitbandkabelnetzen machen circa 15 Prozent der leitungsgebundenen Datenanschlüsse bei positiver Tendenz aus. Anschlüsse an das Glasfasernetz (FTTH und FTTB[10]) sind mit einem Anteil von 1,1 Prozent nur gering vertreten [VATM 2013].

Mobilfunknetze nutzen drahtlose Zugangstechnologien (GSM, UMTS, LTE) und stellen über Funkmasten Telefon- und Datenanschlüsse bereit. Die Übertragung der (Sprach-)Daten erfolgt ab den Funkmasten in der Regel über leitungsgebundene Netze. Bei Verbindungen in unmittelbarer geographischer Nähe ist auch eine Verbindung zwischen einzelnen Funkzellen möglich (näher unter Rolle „Netzbetreiber“).

Daten- und Telefonanschlüsse über Satelliten machen nur einen geringen Teil des Gesamtmarktes aus (0,1 Prozent) und werden nicht gesondert betrachtet.[11]

Service Provider ohne eigene Netzinfrastruktur können unter Mitnutzung der Infrastruktur von Netzbetreibern auftreten, u. a. als sogenannte „Reseller“ und „Switched Reseller“.[12]

Netzbetreiber

Netzbetreiber innerhalb der Branche stellen Übertragungs- und Vermittlungsnetze bereit und sorgen für Wartung und Betrieb der Netze (Lastmanagement, Steuerung etc.). Die Gruppe der Netzbetreiber lässt sich in verschiedene Netzarten sowohl logisch als auch physisch und anhand der geographischen Verbreitung (siehe Abbildung 9) aufteilen.

10 Fiber-to-the-Home und Fiber-to-the-Building

11 Sollten im Verlauf dieser Studie neuralgische Punkte identifiziert werden, die in Zusammenhang mit der Satellitenkommunikation stehen, so wird dies an entsprechender Stelle besprochen.

12 Reseller sind Service Provider ohne eigene Netzinfrastruktur, die sowohl Transport- und Vermittlungsfunktionen von Netzbetreibern nutzen. Switched Reseller verfügen über eigene Vermittlungsinfrastrukturen.

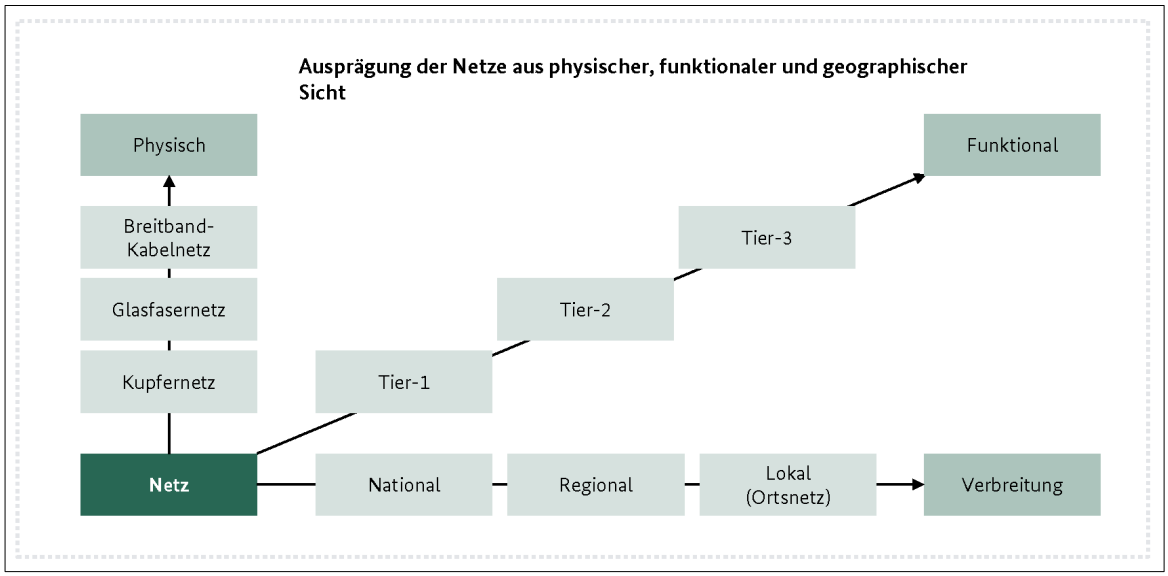

Abbildung 9: Verschiedene Netzarten der Netzbetreiber

Quelle: eigene Darstellung

Zwischen den funktionalen Netzarten und der geographischen Verteilung bestehen Abhängigkeiten. Funktional kann ein Datennetz in drei Klassen aufgeteilt werden, Tier 1 bis 3. Diese unterschiedliche Klassifizierung der Datennetze ist hauptsächlich von der Anzahl der Vernetzungen zu anderen Datennetzen beeinflusst. Für Deutschland sind die Tier-2-Netzwerke von größerer Bedeutung, die auf nationaler und regionaler Ebene Daten übertragen. Eine maßgebliche Unterscheidung der Klassen ist, dass Tier-1-Netze untereinander meist kostenneutral verbunden sind, wohingegen Betreiber von Tier-2-Netzen Transitgebühren an andere Netzbetreiber zahlen müssen. Praktisch kann man Tier-1-Netze jedoch als globale Netze und Tier-2-Netze als regionale/nationale Netze beschreiben. Das Tier-3-Netz bezeichnet das Zugangsnetz, also das Netz, an welches der Endkunde letztendlich direkt angebunden ist.

Um die Gesamtkosten der Anschlussbereitstellungen zu senken, haben einige Wettbewerber der DTAG eigene Netze aufgebaut (zumeist jedoch stark regional begrenzt). Diese kleineren Netze ermöglichten die Verbindung innerhalb eines Ortes ohne Nutzung des Netzes der Deutschen Telekom, waren aber noch immer von der Teilnehmeranschlussleitung zum Endverbraucher (TAL, „letzte Meile“) abhängig. Größere internationale Unternehmen haben damit begonnen, eigene nationale Netze auszubauen, um auch auf regionaler und nationaler Ebene unabhängiger von der Infrastruktur der Deutschen Telekom zu sein. Dennoch hat die Deutsche Telekom durch massive Investition in das Kernnetz[13] weiterhin eines der größten Netze Deutschlands (siehe Abschnitt 2.1.2.2). Andere Anbieter (Vodafone, Kabel Deutschland, Level 3 etc.) besitzen mittlerweile jedoch auch nationale Kernnetze in Deutschland. Auch auf der Ebene der lokal und regional begrenzten Ortsnetze (wie Metropolitan Area Networks, MANs) haben sich weitere Unternehmen etabliert (Telefónica, Kabel BW, NetCologne etc.).

Bei dem Verlegen von Leitungen arbeiten Netzbetreiber wegen der hohen Aufwände häufig eng mit Energieversorgern zusammen, die bei der Erweiterung ihrer Stromnetze meist neue Trassen ausheben müssen. Durch die hohen Kapitalaufwände haben sich auf dem Markt der Netzbetreiber nur eine handvoll Unternehmen etabliert. Viele der kleineren Unternehmen nutzen die größeren Netze der Mitbewerber, um ihre Dienste am Markt zu platzieren (sog. Switched Reseller, siehe Rolle „Service Provider“). Dabei kommt es zu verschiedenen Handelsbeziehungen zwischen den Unternehmen zum Austausch von Sprach- und Datenverkehr. Durch sogenannte Peering-, Interconnection- und Transitvereinbarungen werden diese Beziehungen vertraglich festgehalten (siehe Abschnitt 2.1.2.3).

13 Zentrales Netz mit nationaler Ausbreitung.

Knotenbetreiber

Knotenbetreiber übernehmen eine Schnittstellenfunktion zwischen den Service Providern und Netzbetreibern sowie zwischen den Netzbetreibern selbst. Vermittlungsstellen bestehen meist aus Infrastruktur und den Räumlichkeiten, in denen Netzwerke zusammengeführt werden können.

Im Bereich der klassischen Telefonie wurden nach der kompletten Umstellung von analogen Sprachsignalen in digitale Sprachpakete die folgenden vier Arten von Knotenbetreibern festgelegt, die untereinander vermascht sind: Vermittlungseinheit Ortsnetz (VE:O), Vermittlungseinheit Fernnetz (VE:F), Vermittlungseinheit mit Netzübergangsfunktion (VE:N) und Vermittlungseinheit Ausland (VE:A). Eine ähnliche Funktion wie die Vermittlungseinheiten übernimmt im Funknetz das Mobile Switching Center (MSC), das Mobilfunkverbindungen vermittelt.

In Datennetzen gibt es größere Knotenpunkte (PoP), in denen Datenverkehr verschiedener Anbieter ausgetauscht werden kann. Im engeren Sinne werden diese Netzwerkknoten nicht als Knotenbetreiber bezeichnet (sondern als IXP); sie werden in dieser Studie jedoch in diese Gruppe eingeschlossen, da sie eine ähnliche funktionale Aufgabe erfüllen.

Verwaltung

Eine wichtige Funktion bei der Übertragung von Informationen in digitalen Netzen ist die Zuordnung von Adressinformationen und die Weiterleitung von Informationen zu den jeweiligen Zielen. Neben dem Routing, das in den Netzen selbst stattfindet, spielt in diesem Zusammenhang die Verwaltung von IP-Adressbereichen, der Betrieb des Domain Name System (DNS), das den Gebrauch von textuellen Bezeichnern für IP-Adressen (Domainnamen) ermöglicht, und die Verwaltung von Domainnamen eine wichtige Rolle.

Im Bereich der Telefonie spielen in diesem Zusammenhang die Datenbanken zur Vorhaltung der Zugehörigkeit von Rufnummern zu Netzbetreibern, Local Number Portability (LNP) und Mobile Number Portability (MNP), eine wichtige Rolle. Diese Datenbanken beinhalten Informationen zur Zuordnung von Rufnummern, die im Rahmen der Übertragung notwendig sind, und werden teilweise gemeinschaftlich von mehreren Netzbetreibern betrieben.

Mobilfunk ist bei der Registrierung und Lokalisierung von Mobiltelefonen auf das Home Location Register (HLR) bzw. Visitor Location Register (VLR) angewiesen. In diesen Datenbanken werden die Anschlüsse und der aktuelle Standort registriert und die freigeschalteten Funktionen des jeweiligen Anschlusses hinterlegt.

Rechenzentrumsbetreiber

Betreiber von Rechenzentren bieten Einrichtungen und Infrastrukturen zur Datenverarbeitung für Dritte (z. B. Gesellschaft, öffentliche Hand, Wirtschaft) an. Dort befinden sich das technische Equipment und die IT-Systeme der Endkunden, z. B. von Netzbetreibern oder anderen Unternehmen. Rechenzentren zeichnen sich durch geschützte Räumlichkeiten mit einer zuverlässigen Stromversorgung, einer angemessenen Klimatisierung und Netzwerk- bzw. Internetkonnektivität aus.

Die Dienstleistung der Bereitstellung von Rechenzentrumsfläche zum Aufbau und Betrieb eigener IT-Systeme und technischen Equipments in einem Rechenzentrum wird als Housing oder Co-Location bezeichnet. In angemieteten Serverschränken oder Stellflächen können Kunden eigene Geräte betreiben. Die Wartung und Reparatur dieser Hardware liegt in der Verantwortung der Kunden. Betreiber von Rechenzentren stellen lediglich die grundlegende Infrastruktur (zugangsgeschützte Räumlichkeiten, Strom, Klima, Netzwerk) zur Verfügung.

IT-Hoster

IT-Hoster betreiben Einrichtungen und Infrastrukturen zur Datenverarbeitung für Dritte (z. B. Gesellschaft, öffentliche Hand, Wirtschaft), in denen sie eigene IT-Systeme an Kunden vermieten (sogenanntes Hosting). Welche Applikationen auf den Servern ausgeführt werden, obliegt den Kunden. Der IT-Hoster stellt lediglich die IT-Infrastruktur (Server und Datenspeicher) zur Verfügung und verantwortet deren Betrieb

und Wartung. IT-Hoster betreiben ihre Systeme im Regelfall innerhalb eines Rechenzentrums und kaufen daher Fläche in Rechenzentren ein (vgl. Rollenbeschreibung „Rechenzentrumsbetreiber“).

Auch die Betreiber von Internet-Diensten wie Suchmaschinen, E-Mail und Webhosting betreiben die IT-Infrastruktur ihrer Dienste im Regelfall in Rechenzentren und greifen dabei unter anderem auch auf die Dienstleistungen von Rechenzentrumsbetreibern oder IT-Hostern zurück. Mehrheitlich betreiben die IT-Hoster jedoch eigene Rechenzentren. Insbesondere bekannte Dienste amerikanischer Großkonzerne wie die Suchmaschine Google oder der E-Mail-Dienst Microsoft Hotmail laufen teilweise auf Systemen in Rechenzentren außerhalb Deutschlands.

Verbände und Regulierungsbehörden

Neben den Betreibern haben innerhalb der Branche sowohl Verbände als auch Regulierungsbehörden eine wichtige Rolle inne. Diese Rollen haben keinen unmittelbaren Einfluss auf die eigentliche Leistungserbringung oder Dienstbereitstellung, sondern treten als mittelbare Interessenvertreter sowie in steuernder Funktion auf.

Verbände können als gebündelte Vertreter mehrerer Unternehmen in der Branche politische oder regulatorische Forderungen mit größerem Nachdruck aussprechen. Durch den Einfluss des Staates in Form von Gesetzen und Regulierungsbehörden spielen diese Verbände eine wichtige Rolle bei der Entwicklung der IKT-Branche, da sie die wirtschaftlichen Interessen der Verbandsmitglieder nach außen hin vertreten.

Dem gegenüber bestehen Regulierungsbehörden wie die Bundesnetzagentur (BNetzA) und die deutsche und europäische Legislative, die besonders seit der Liberalisierung des Telekommunikationsmarkts im Jahr 1996 einen großen Einfluss auf die Gestaltung und Entwicklung des Marktes in Deutschland haben. Sie achten darauf, dass die dominante Marktposition der Nachfolger der Deutschen Bundespost, insbesondere durch den Besitz von Infrastruktur, nicht die Marktentwicklung beeinflusst. Neben marktwirtschaftlichen Aufgaben achten die Regulierungsbehörden auch auf die Umsetzung und Einhaltung von Anforderungen, welche die Entwicklung des IKT-Marktes fördern (z. B. Standards, technische Richtlinien, Verordnungen etc.) [BNetzA 2014c].

2.1.2.2 Marktteilnehmer

Eine Auswahl der wichtigsten Marktteilnehmer der Dienstleistung „Telekommunikation“ erfolgt nach aktuellen Statistiken zu Nutzerzahlen, Umsatz, regionaler Verbreitung und anderen signifikanten Merkmalen. Eine Unterscheidung zwischen den Rollen ist notwendig, um die wichtigsten Marktteilnehmer zu identifizieren. Dabei wird auch innerhalb der Dienstleistung unterschieden, welches Merkmal als Basis zur Identifikation herangezogen wird.

Die folgenden Tabellen listen die wichtigsten Marktteilnehmer pro Rolle (siehe Abschnitt 2.1.1.1) auf:

Rolle: Service Provider

Unternehmen	***Tätigkeiten***	***Nutzeranzahl [VATM 2013]***[14] *(Festnetz und Internet; Mobilfunk) in Mio.*	***Gesamtumsatz 2013*** *in Mrd. Euro*[15] *(Anteil*[16]*)*
Deutsche Telekom AG	Festnetz-, Mobilfunk-, Internetanschluss	49,9 (12,4; 37,5)	60,13 (72,1 %)
Vodafone, Kabel Deutschland	Festnetz-, Mobilfunk-, Internetanschluss	37,2 (5,0; 32,2)	11,46 (13,7 %)

14 Vergleiche hierzu auch die jeweilige Unternehmensdarstellung auf der Website.
15 Daten aus den Geschäftsberichten.
16 Anteil des Umsatzes des einzelnen Umsatzes am Gesamtumsatz der angeführten Unternehmen.

Telefónica, E-Plus[17]	Festnetz-, Mobilfunk-, Internetanschluss	46,1 (2,3; 43,8)	8,44 (10,1 %)
1&1 (United Internet)	Festnetz-, Mobilfunk-, Internetanschluss, Switched Reseller	6,1 (4,75; 1,35)	2,39 (2,9 %)
Unitymedia (Kabel BW)	Festnetz-, Mobilfunk-, Internetanschluss	2,4 (2,01; 0,39)	1,02 (1,2 %)

Tabelle 9: Wichtige Marktteilnehmer der Rolle „Service Provider“

Rolle: Netzbetreiber

Unternehmen	***Tätigkeiten[18]***	***Netzgröße[19] in Deutschland***
Deutsche Telekom AG	Tier-1, Tier-2, Tier-3, Mobilfunknetz, TAL	312.000 km [BNetzA 2013a]
Vodafone, Kabel Deutschland	Tier-1 (National), Tier-2, Tier-3, Mobilfunknetz, Kabelnetz	58.000 km (Vodafone) [Vodafone 2014] 32.000 km (Kabel Deutschland) [KabelD 2014]
Telefónica, E-Plus	Tier-3, Mobilfunknetz	Keine Angabe
Level3	Tier-1, Tier-2	Keine Angabe
Versatel	Tier-2, Tier-3	52.000 km [Versatel 2014]

Tabelle 10: Wichtige Marktteilnehmer der Rolle „Netzbetreiber“

Rolle: Knotenbetreiber

Unternehmen	*Tätigkeiten*	*Standorte*	*Durchschnittlicher. Durchsatz (in Gbit/s)*
DE-CIX	Internetknoten	Frankfurt am Main, Hamburg	~ 1.900 [DECIX 2014]
ECIX (Peering GmbH)	Internetknoten	Frankfurt am Main, Hamburg, Amsterdam, Düsseldorf, Berlin	~ 40 [ECIX 2014]
BCIX	Internetknoten	Berlin	~ 17 [BCIX 2014]

Tabelle 11: Wichtige Marktteilnehmer der Rolle „Knotenbetreiber“

Rolle: Verwaltung

Unternehmen	***Tätigkeiten***	***Größe***
DENIC eG	Betrieb und Verwaltung der „.de“ Top-Level-Domain	circa 16 Mio. „.de“-Domains[20]

17 Die Übernahme von E-Plus durch Telefónica ist zum Zeitpunkt der Studienerstellung noch nicht vollständig abgeschlossen.
18 Die Einteilung erfolgt durch eine Analyse der jeweiligen Tätigkeiten der Netzbetreiber. Dabei sind die Produkte, Dienstleistungen und Informationen aus den Geschäftsberichten die Grundlage der Einteilung.
19 Die Netzgröße bezeichnet die Gesamtlänge der Netze des Betreibers, d. h. die Glasfaserstraßen-Kilometer. Einzelne Adern werden nicht addiert.
20 Vergleiche hierzu auch die jeweilige Unternehmensdarstellung auf der Website.

RIPE Network Coordination Centre	Vergabe und Verwaltung von IP-Adressbereichen	circa 654 Mio. IPv4-Adressen[21]

Tabelle 12: Wichtige Marktteilnehmer der Rolle „Verwaltung“

Rolle: Rechenzentrumsbetreiber

Unternehmen	***Tätigkeiten***	***RZ-Standorte*** *(Deutschland)*	***Ausgewählte Kennzahlen***
T-Systems	Globaler Rechenzentrumsbetreiber für Hosting (insbesondere für die DTAG), aber auch Co-Location	u. a. Magdeburg, Biere, Kiel, Frankfurt, Dresden, München, Göppingen, Bamberg, Krefeld	Circa 118.800 m² RZ-Fläche (global)
Interxion	Hauptsächlich Co-Location (insbesondere DE-CIX)	Düsseldorf, Frankfurt am Main, München	Circa 12.700 m² RZ-Fläche (Deutschland)
Level 3 Communications	Co-Location und Hosting (Managed Server)	Berlin, Düsseldorf, Frankfurt am Main, Hamburg, München	53 Rechenzentren weltweit
Equinix	Weltweiter Anbieter von Co-Location-Rechenzentren	Düsseldorf, Frankfurt am Main, München	Circa 45.800 m² RZ-Fläche (Deutschland)
Colt	Betreiber von 20 großen Co-Location-Rechenzentren in Europa	Berlin, Frankfurt am Main, Hamburg	circa 4.600 m² RZ-Fläche (Deutschland)

Tabelle 13: Wichtige Marktteilnehmer der Rolle „Rechenzentrumsbetreiber“

Rolle: IT-Hoster

Unternehmen	***Tätigkeiten***	***RZ-Standorte (Deutschland)***	***Ausgewählte Kennzahlen***
1 & 1	Großer deutscher Hosting-Anbieter (insbesondere Webhosting und E-Maildienste aber auch Managed Server)	Karlsruhe, Rheinmünster	19 Mio. verwaltete Domains circa 25.000 Server (Deutschland)
Strato	Europaweiter Hosting-Anbieter (insbesondere Webhosting, aber auch Managed Server)	Karlsruhe, Berlin	4 Mio. verwaltete Domains circa 55.000 Server (Deutschland) circa 4.000 m² RZ-Fläche (Deutschland)
Host Europe	Europäischer Hosting-Anbieter, der durch den Aufkauf von domainFactory eine wichtige Stellung im deutschen Markt erlangte	Köln, München, Frankfurt am Main	circa 25.000 Server (Deutschland)
IBM	Betreibt weltweit 40 Rechenzentren, davon mehrere in Deutschland (insbesondere Hosting von	Eschborn, Ehningen, Böblingen, Mainz, Frankfurt am Main	circa 15.500 m² RZ-Fläche (Deutschland)

21 Zuteilung von 39 „/8-Netzen“.

	Geschäftsanwendungen z. B. SAP)	(Schwalbach und Oberursel)	
T-Systems	Globaler Rechenzentrumsbetreiber für Hosting (insbesondere für die DTAG), aber auch Co-Location	u. a. Magdeburg, Biere, Kiel, Frankfurt, Dresden, München, Göppingen, Bamberg, Krefeld	circa 118.800 m² RZ-Fläche (Global)

Tabelle 14: Wichtige Marktteilnehmer der Rolle „IT-Hoster“

Rechenzentrumsbetreiber/IT-Hoster wichtiger Internetdienste

Große Teile der deutschen Bevölkerung nehmen täglich Internetdienste in Anspruch, die durch Unternehmen erbracht werden, welche eigene oder angemietete Rechenzentren beziehungsweise Server nutzen. In dieser Studie werden die Dienste E-Mail, Internetsuche und Webhosting als Betreiber von Rechenzentren untersucht und jene Anbieter aufgelistet, die in Deutschland am bekanntesten und weit verbreitet sind. Für die Untersuchung der Kritikalität hinsichtlich der Infrastruktur ist jedoch nicht der Dienstanbieter an sich relevant, sondern der jeweilige Betreiber des Rechenzentrums, in dem der Dienst untergebracht ist. Viele der aufgeführten Unternehmen besitzen mehrere Rechenzentren und sind weltweit tätig. Eine genaue Zuordnung des Dienstes zu einem Rechenzentrum ist daher mitunter nur schwer möglich. Ebenso betreiben einige Anbieter in Deutschland selbst keine Rechenzentren.

Unternehmen	***Tätigkeiten***	***Rechenzentrumsbetreiber***	***Ausgewählte Kennzahlen*** *(Deutschland)*
Google	Weltweit tätiges amerikanisches Unternehmen, insbesondere im Bereich Internetsuche in Deutschland marktdominant, aber auch E-Mail-Dienste (gmail) werden durch Google angeboten	Google betreibt eigene Rechenzentren an verschiedenen Standorten weltweit	91,2 % Marktanteil Suchmaschinen 6,5 % Marktanteil E-Mail
Microsoft	Weltweit tätiges amerikanisches Unternehmen, insbesondere im Bereich Internetsuche (bing) und E-Mail-Diensten (hotmail) in Deutschland relevant	Durch den Geschäftsbereich Global Foundation Services (GFS) betreibt Microsoft eigene Rechenzentren an verschiedenen Standorten weltweit	3,5 % Marktanteil Suchmaschinen 4,7 % Marktanteil E-Mail
Web.de und gmx.net (1 & 1 Mail & Media)	Dominanter Anbieter von E-Mail-Diensten im deutschen Markt	1 & 1 Internet AG (United Internet)	Über 50 % Marktanteil E-Mail
1 & 1 Internet AG	Hosting von Webseiten, insbesondere von Privatpersonen	1 & 1 Internet AG (United Internet)	19 Mio. verwaltete Domains

Tabelle 15: Wichtige Unternehmen und Rechenzentrumsbetreiber bekannter und weitverbreiteter Internetdienste

Rolle: Verbände und Regulierungsbehörden

Name	***Tätigkeiten***	***Mitglieder***	***Gemeinsamer Umsatz der Mitglieder*** *(in Mrd. Euro)*
BITKOM (Bundesverband Informationswirtschaft, Tele-	Branchenverband für deutschen IKT-Unternehmen	1.300	140,0 [BITKOM 2014b]

kommunikation und neue Medien e. V.)			
BREKO (Bundesverband Breitbandkommunikation e. V.)	Verband mit Ausrichtung auf IKT-Unternehmen mit eigener Netzinfrastruktur (außer der DTAG)	175	7,6 [BREKO 2012]
VATM (Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.)	Verband von neuen und etablierten Wettbewerbern der Deutschen Telekom	120	Keine Angabe

Tabelle 16: Wichtige Marktteilnehmer der Rolle „Verbände und Regulierungsbehörden" (hier Verbände)

Name	***Tätigkeiten***	***Exemplarische Regulierungen, Veröffentlichungen, Gesetze***
Bundesnetzagentur (BNetzA)	Wahrung der Wettbewerbschancengleichheit auf dem IKT-Markt, Prüfung der Einhaltung von Gesetzen, Mitwirkung bei Standardisierungsorganisationen, Überwachung der Einhaltung des Telekommunikationsgesetzes	Technische Richtlinie Notrufverbindungen, Leitfaden Verkehrsdatenspeicherung
Bundesregierung	Gesetzgebende Instanz für den deutschen IKT-Markt	Telekommunikationsgesetz, Telekommunikations-Überwachungsverordnung, IT-Sicherheitsgesetz, Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG)
Europäisches Parlament	Gesetzgebende Instanz für den europäischen IKT-Markt	Richtlinienpaket zur Novellierung des Regulierungsrahmens für Telekommunikationsnetze, R&TTE-Richtlinie

Tabelle 17: Wichtige Marktteilnehmer der Rolle „Verbände und Regulierungsbehörden" (hier Regulatoren)

Im Folgenden werden die wichtigsten Marktteilnehmer der Branche für diese Studie kurz beschrieben:

- **Deutsche Telekom AG:** Die Deutsche Telekom AG ging 1995 im Zuge der Privatisierung aus der ehemaligen Bundespost hervor und ist heutzutage mit einem Umsatz von 60,13 Mrd. Euro und weltweit knapp 220.000 Mitarbeitern eines der größten deutschen Unternehmen. Die DTAG ist ein Konzern mit den Gesellschaften Telekom Deutschland GmbH und T-Systems GmbH [DTAG 2013]. Nach wiederholter Umstrukturierung in den letzten Jahren bietet die Telekom Deutschland nun sämtliche Dienste für private und gewerbliche Endverbraucher in Deutschland direkt an. Dies umfasst Internet, IPTV, Telefonie und Mobilfunk. T-Systems ist auf die Betreuung von Großkunden, die Durchführung von IKT-Projekten sowie Forschung und Entwicklung spezialisiert. Als ehemaliger Monopolist für den TK-Markt besitzt die Deutsche Telekom eine große nationale und internationale Infrastruktur aus Festnetz, Glasfasernetz, Knotenbetreibern, TAL und Netzwerkmanagementzentren (NMC/NOC[22]). Die DTAG tritt in der Branche „IKT" in allen leistungserbringenden Rollen auf.[23] Im Bereich der Service Provider bietet sie Anschlüsse an Festnetz, Datennetz und Mobilfunknetz. Dabei werden sowohl eigene TAL als auch

22 Die Begriffe Network Management Center (NMC) und Network Operation Center (NOC) werden in dieser Studie synonym verwendet.

23 Vergleiche hierzu auch die jeweilige Unternehmensdarstellung auf der Website.

direkte Anschlüsse an Datennetze (z. B. FTTH) genutzt. Eine Initiative zur kompletten Umstellung aller Anschlüsse auf IP-Technologie soll in Deutschland bis 2018 durchgeführt werden [Nemat 2013]. In der Rolle der Knotenbetreiber ist die DTAG vor allem in der Telefonie stark vertreten, wo sie Vermittlungseinheiten für Orts- und Fernnetze betreibt. Die DTAG beteiligt sich nicht am öffentlichen Zusammenschluss verschiedener Datennetze (Public Peering; DTAG ist also nicht am DE-CIX vertreten), sondern lässt sich das Peering weitgehend von anderen Netzbetreibern bezahlen (Paid Peering) [DECIX 2013]. Aufgrund der Regulierung vermietet die DTAG ihre Infrastruktur auch an andere Marktteilnehmer und ermöglicht so die Mitnutzung, z. B. durch Entbündelung der TAL. Die Deutsche Telekom ist auf dem Markt weiterhin einer der größten Anbieter. Mit 43,7 Prozent Anteil am Festnetzmarkt ist die DTAG immer noch dominant. Im Mobilfunkmarkt hingegen wird die Telekom nach der (geplanten) Übernahme von E-Plus durch Telefónica nur noch der zweitgrößte Anbieter mit 37,5 Mio. Nutzern auf dem eigenen Mobilfunknetzwerk (D1) sein [VATM 2013]. Zukunftsorientierte Investitionen, z. B. in das Glasfasernetz oder die Umstellung auf „All-IP“, zeigen jedoch auch hier, dass der Umschwung im IKT-Umfeld in den nächsten Jahren für den Endkunden durch schnellere Anschlüsse spürbar sein wird [DTAG 2012].

- **Vodafone/Kabel Deutschland:** Vodafone, eine Gesellschaft der britischen Vodafone Group, hat durch die Übernahme von Kabel Deutschland im September 2013 sein Dienstleistungsportfolio um die Bereitstellung von Diensten über das Breitbandkabelnetz erweitert [Vodafone 2013a]. Da dieses Netz zu großen Teilen auch auf Glasfasertechnologie basiert, verfügt Vodafone damit über das zweitgrößte Glasfasernetzwerk Deutschlands und tritt folglich auch in der Rolle eines Netzbetreibers auf [Vodafone 2014]. Nach der allgemeinen Definition der Tier-Ebenen und der regionalen und nationalen Verbreitung der Netze macht dies Vodafone zu einem Tier-2- und Tier-3-Netzbetreiber. Vodafone bietet Telefonie, Internet, IPTV und Mobilfunk an. Zwar mit weniger als der Hälfte der Kunden im Internet- und Telefoniegeschäft gegenüber der Deutschen Telekom ist dennoch Vodafone der zweitgrößte alternative Anbieter in diesem Markt. Im Mobilfunk hat Vodafone mit 32,2 Mio. Endkunden knapp fünf Mio. Kunden weniger als die Telekom. Vodafone betreibt ein eigenes Mobilfunknetz (D2). Damit tritt Vodafone sowohl als Service Provider als auch als Netzbetreiber auf. Als Service Provider nutzt Vodafone hauptsächlich die entkoppelten TAL der Telekom, bringt jedoch auch teilweise durch Datenanschlüsse (z. B. FTTH) ihre Dienste direkt (d. h. ohne auf DTAG-Infrastruktur zurückzugreifen) an die Endkunden [Vodafone 2013b].
- **Telefónica/E-Plus:** Telefónica Deutschland ist eine Gesellschaft der spanischen Telefónica Gruppe und tritt in Deutschland mit der Mobilfunkmarke O_2 im Markt auf. Unter diesem Namen werden Festnetz-, Mobilfunk- und Datendienste angeboten. Telefónica plant die Übernahme von E-Plus, woraus der größte deutsche Mobilfunkanbieter mit 43,8 Mio. Kunden entstehen würde [MoKo 2013]. Beide Unternehmen besitzen eigene Mobilfunknetze im E-Netz, die jedoch nicht exklusiv von ihnen genutzt werden (DTAG und Vodafone besitzen dort auch einige wenige Frequenzen). In der Telefonie und dem Internetzugang ist Telefónica mit 2,8 Mio. Kunden drittgrößter Anbieter in Deutschland. Im Gegensatz zu den beiden großen Wettbewerbern bietet Telefónica/E-Plus nur Dienste in der Telefonie, Internet und Mobilfunk an; IPTV wurde hingegen eingestellt. Telefónica besitzt als Netzbetreiber lokal begrenzte Tier-3-Netze und städtische Metropolitan Area Netze (MANs)[24] auf Glasfasertechnologie.
- **United Internet (1&1):** Die United Internet GmbH spezialisiert sich auf die Bereitstellung von Anschlussdiensten im Endkundenmarkt. Dort besitzt das Unternehmen mit einem Anteil von 11,9 Prozent an allen Breitbandanschlüssen eine relativ starke Marktposition gegenüber den anderen Marktteilnehmern. Da United Internet keine eigene Netzinfrastruktur betreibt, müssen jedoch Transitvereinbarungen mit anderen Unternehmen geschlossen werden. Unter anderem nutzt United Internet hierfür das Netz von Plusnet [UnitedInt 2013]. Auch im Bereich des Hostings ist 1&1 ein wichtiger Markteilnehmer. Mit über drei Mio. Kunden zählt das Unternehmen zu den größten IT-Hostern Europas. Die Rechenzentren stehen in München, Karlsruhe und Frankfurt am Main. Zudem vereint das Unternehmen mit den beiden E-Maildiensten gmx und web.de mehr als 50 Prozent der hauptsächlich genutzten E-Mail-Adressen.

24 Lokale Netze in Großstädten.

- **Unitymedia Kabel BW:** Die Unitymedia Kabel BW ist ein regionaler Kabelnetzbetreiber und Service Provider. Sie ist eine Tochtergesellschaft des amerikanischen Unternehmens Liberty Global. Das Unternehmen versorgt hauptsächlich Kunden in Nordrhein-Westfalen sowie Hessen und bietet Daten-, Telefonie- und Fernsehdienste auf Basis eines rückkopplungsfähigen (bi-direktionalen) Breitbandanschlusses im eigenen Netz an. Teilweise setzt das Unternehmen Glasfasertechnologie zum Anschluss der Verteiler an das Übertragungsnetz (FTTN[25]) ein [Unitymedia 2014]. Auch Mobilfunkdienste werden durch Unitymedia angeboten, diese werden jedoch ausschließlich über das Netz von Telefónica (bzw. O2) angeboten.
- **Level 3 Communications:** Als global agierendes Unternehmen besitzt Level 3 Communications ein 120.000 km langes Weitverkehrsnetz (Tier-1-Netz). In Deutschland ist das Unternehmen hauptsächlich am Standort des Internetknoten DE-CIX in Frankfurt am Main aktiv. Dort ist das globale Level-3-Netzwerk mit anderen Netzen durch Peering verbunden. Level 3 ist Betreiber der Rechenzentren, in denen die eigentliche Hardware zum Peering bereitsteht. Level 3 tritt auch als Rechenzentrumsbetreiber auf. Hier spezialisiert Level 3 sich hauptsächlich auf Co-Location-Dienste, bietet allerdings auch Hosting in seinen Rechenzentren an. Dadurch, dass Level 3 auch Glasfaserverbindungen zwischen den meisten größeren deutschen Städten besitzt, tritt das Unternehmen in Deutschland auch als nationaler Netzbetreiber auf [Level3 2014]. Weltweit besitzt das Unternehmen 53 Rechenzentren, die meisten mit direktem Anschluss an das weltweite Weitverkehrsnetz.
- **Versatel:** Die Versatel GmbH ist ein Anbieter von IKT-Diensten für Privat- und Geschäftskunden mit einem rund 50.000 km langem Glasfasernetz, primär auf lokaler (örtlicher) und regionaler Ebene. Versatel betreibt unter anderem Metro-Netze (MAN) in den größeren deutschen Städten. Versatel gehört zu den wenigen Unternehmen, die einen direkten Anschluss von Kunden an ihr Netz ermöglichen und somit keine Vorleistung der DTAG in Anspruch nehmen müssen. Um Mobilfunkleistungen anzubieten, nutzt Versatel das Netz von E-Plus.
- **DE-CIX:** Die DE-CIX Management GmbH betreibt mit dem DE-CIX, nach Durchsatz (~1.900 Gbit/s) gemessen, einen der größten Internetknoten der Welt [DECIX 2014]. Dafür verwaltet und koordiniert sie das Peering verschiedener Netze an mehreren Standorten in Frankfurt am Main (darunter jedoch nicht das Netz der Deutschen Telekom AG). Die Vermittlung zwischen verschiedenen Datennetzen (Peering) in Deutschland findet zu einem Großteil bei DE-CIX statt. Dabei wird sowohl nationaler als auch globaler Verkehr über die Infrastruktur des DE-CIX ausgetauscht. Der Betrieb der Rechenzentren sowie die Wartung wird durch Dienstleistungserbringer wie Level 3 Communications oder Interxion durchgeführt.
- **Peering GmbH:** Die Peering GmbH betreibt mit dem EXIC den zweitgrößten Internetknoten Deutschlands (~40 Gbit/s) [ECIX 2014]. Dieser Knoten ist über mehrere Standorte verteilt (Frankfurt am Main, Hamburg, Düsseldorf, Berlin und Amsterdam), die untereinander durch Glasfaserleitungen verbunden sind.
- **T-Systems:** Die T-Systems GmbH, als Tochtergesellschaft der DTAG, betreibt die Rechenzentren für sämtliche Dienstleistungen der Deutschen Telekom. Mit mehr als 90 Rechenzentren in allen größeren deutschen Städten und weltweit besitzt T-System einen hohen geographischen Deckungsgrad. Auch andere Unternehmen nutzen die Dienstleistungen der Rechenzentren von T-Systems; einerseits, um ihre eigene IT zu entlasten (zum Beispiel für bessere Skalierbarkeit), andererseits, um kritische Informationen und Prozesse in Hochsicherheitsrechenzentren vor Verlust und Ausfall zu schützen. Im Umfeld der IKT-Basisinfrastruktur sind die von T-Systems betriebenen Rechenzentren insbesondere wichtig für die PoP der DTAG, an denen andere Netzbetreiber ihre Netze mit dem Netz der DTAG zusammenschließen.
- **Interxion:** Die Interxion AG ist ein wichtiger Betreiber von Co-Location-Rechenzentren, also Rechenzentren, in denen andere Unternehmen ihre eigene Hardware unterbringen können. Der Betreiber ist dann ausschließlich für die Versorgung mit Bandbreite, Strom (inkl. Notstrom), Kühlung, Überwachung und weiteren gebäudebezogenen Diensten verantwortlich. Interxion ist zudem „carrier-neutral“ und damit für alle Service Provider und Netzbetreiber nutzbar. Hierdurch sind die

25 Fiber-to-the-Node.

Rechenzentren besonders für Interconnection (also den Zusammenschluss verschiedener Netze) interessant. Der größte Internetknoten Deutschlands (DE-CIX) ist in den Rechenzentren von Interxion in Frankfurt am Main untergebracht.

- **Equinix:** Equinix Inc. ist ein weltweiter Betreiber von „carrier-neutralen" Rechenzentren. Das Unternehmen bezeichnet sich selbst als den größten Co-Location-Anbieter der Welt.[26] Neben der globalen Ausrichtung bestehen auch fünf große Rechenzentren in Frankfurt (mit direkter Anbindung an den DE-CIX), drei in München und zwei in Düsseldorf. Damit ist Equinix an wichtigen Punkten der Interconnection innerhalb Deutschlands präsent.
- **Strato:** Die Strato AG ist ein großer deutscher Hosting-Anbieter. Zwar liegt das Hauptgeschäftsfeld im Bereich des Webhostings, dennoch bietet das Unternehmen auch Managed Server für Geschäftskunden an. Diese Server sind in Rechenzentren in Berlin und Karlsruhe untergebracht. Strato ist eine Tochtergesellschaft der Deutschen Telekom AG.
- **Host Europe (domainfactory):** Die Host Europe Group Ltd. gehört mit mehr als einer Million Kunden und über fünf Mio. verwalteten Domains zu einem der größten europäischen Hosting-Anbieter. Durch den Aufkauf der beiden deutschen Unternehmen Telefónica Online Services (einer Tochter von Telefónica Germany) und domainfactory GmbH erweiterte das Unternehmen seine Präsenz auf dem deutschen Markt. Das Unternehmen betreibt mehrere Rechenzentren in Europa, unter anderem zwei Rechenzentren in Deutschland (München und Köln).
- **IBM:** IBM Corporation ist eine US-amerikanische Firma mit globaler Präsenz. Neben Dienstleistungen im Bereich der Beratung und der IT bietet das Unternehmen in weltweit verteilten Rechenzentren Hosting an. Diese Rechenzentren hosten meist Applikationen und speichern Daten größerer Unternehmen.
- **Colt:** Die Colt Group S.A. ist ein in Europa agierendes Unternehmen, das Kommunikations-dienstleistungen für mittelständische und große Unternehmen anbietet. Neben einer Vielzahl von Rechenzentren in ganz Europa mit einer Nutzfläche von mehr als 30.000 m² werden auch drei große Co-Location-Rechenzentren in Deutschland betrieben. Zudem unterhält Colt ein (europäisches) Datennetzwerk mit eigenen Infrastrukturkomponenten.

2.1.2.3 Beziehungen innerhalb der Branche

Beziehungen bestehen zwischen den Marktteilnehmern der Branche sowohl auf horizontaler (Input-Output-Beziehung) als auch auf vertikaler Ebene (Handelsbeziehung). Die wichtigsten brancheninternen Beziehungen sind dabei Interconnection (Terminierung, Transit, Originierung), Peering, TAL-Anmietung, Bitstromzugang, Netzanmietung (Wholesale Internet Access), Co-Location, Hosting und Internetdienste.

Interconnection bezeichnet die Zusammenschaltung von mehreren, untereinander unabhängigen Netzen. Hier ist in Deutschland insbesondere die Deutsche Telekom tätig, welche die Zusammenführung (d. h. die Herstellung einer Verbindung zwischen Netzen) von Netzen anderer Netzbetreiber oder Service Provider übernimmt. Bei der *Terminierung* werden den Mitbewerbern Zugänge in das eigene Netz von einem Mitbewerberanschluss aus ermöglicht. *Transit* ist die Weiterleitung über das eigene (regionale/nationale) Kernnetz auf dem gesamten Weg, d. h. vom Anschlussnetz bis zum Zielnetz. *Originierung* bezeichnet die Herstellung einer Verbindung aus dem eigenen Netz in ein Netz eines Mitbewerbers. Gerade durch das große nationale Netz der DTAG müssen andere Service Provider oftmals bei der Deutschen Telekom Leistungen einkaufen, deren Entgelte stark durch die Bundesnetzagentur reglementiert sind. Durch die Bereitstellung dieser Dienste wird kleineren Service Providern ohne eigene Infrastruktur die Möglichkeit gegeben, Anschlussdienste am Markt zu anzubieten.

Peering ist der Austausch von Datenverkehr zwischen separaten Datennetzen. Netzbetreiber sind bestrebt, durch Peering-Vereinbarungen Verkehr von ihren eigenen Netzen möglichst strategisch mit anderen Betreibern auszutauschen. Dies bedeutet, dass die Netzbetreiber bestrebt sind, mit möglichst vielen Netzen

26 Vergleiche hierzu auch die jeweilige Unternehmensdarstellung auf der Website.

der Mitbewerbern direkt zu „peeren“, um Transitkosten durch andere Netze zu vermeiden oder aber um selbst Transitdienste anbieten zu können. Tier-1-Netzbetreiber haben untereinander kostenneutrale Vereinbarungen. Auf den Ebenen darunter fallen jedoch teilweise Peeringkosten (Paid Peering) an. Werden an einem Ort mehrere Netze zusammengeführt und wird an diesem Ort die Peering-Infrastruktur gemeinsam oder durch einen Dritten betrieben, so spricht man von Public Peering. Im Gegensatz dazu kann ein großer Netzbetreiber auch Private Peering durchführen, also nur Peering zwischen seinem und einem anderen Mitbewerbernetzwerk.

Die Möglichkeit der **Anmietung der Teilnehmeranschlussleitungen** ist ein Ergebnis der Liberalisierung des TK-Marktes. Diese meist im Besitz der Deutschen Telekom liegende „letzte Meile“ ist für Service Provider bei der Bereitstellung ihrer Dienstleistungen von großer Bedeutung. Die TAL ist das letzte Verbindungsstück zwischen den Kabelverzweigern (KVz) und den physischen Anschlüssen beim Endverbraucher. Durch die Entbündelung können Service Provider diese Verbindung nutzen, um ihre Produkte direkt den Kunden zu bringen. Dabei ist die Anmietung der TAL mit Kosten verbunden, die an den Besitzer entrichtet werden. Die direkte Anbindung von Kundenanschlüssen an das eigene Netz, z. B. über FTTH oder Breitbandkabel, ist von großer Bedeutung für die Entwicklung auf dem IKT-Markt.

Der **Bitstromzugang** ist, ähnlich der TAL-Anmietung, für IKT-Unternehmen ohne eigene Infrastruktur auf der „letzten Meile“ eine Möglichkeit, Datenverbindungen bereitzustellen. In Deutschland bedeutet dies, dass Betreiber durch bestehende Infrastrukturen (eigene oder gemietete, entbündelte TAL) Datenverbindungen zum Endkunden herstellen und diese an die Wettbewerber vermieten. Diese Verbindungen ermöglichen es Service Providern, Endkunden DSL-Anschlüsse anzubieten, ohne eine eigene physische Infrastruktur betreiben zu müssen.

Die komplette **Netzanmietung** durch einen Marktteilnehmer (Wholesale Internet Access) ermöglicht das Anbieten von Leistungen ohne jegliche eigene Infrastruktur. Verbindungen werden über die angemieteten Anschlüsse via Terminierung, Transit und Originierung hergestellt. Der Anbieter mietet sämtliche Infrastruktur von etablierten Netzbetreibern an.

Eine wichtige Entwicklung innerhalb der Branche sind neuartige Beziehungen zwischen Netzbetreibern und Service Providern. Durch Open Access-Netzwerke soll das Errichten und der Betrieb von Netzwerken von der Nutzung getrennt werden [ONForum 2014]. Praktisch bedeutet dies, dass Service Provider Netzwerke je nach Bedarf anmieten können. Durch die erhöhte Skalierbarkeit können sich diese besser an die tatsächliche Auslastung anpassen. Auf der anderen Seite soll für die Netzbetreiber durch die Vermietung an mehrere Partner der Betrieb der Netze lukrativer und die hohen Investitionskosten schneller amortisiert werden [VDE 2009].

Die Rechenzentrumsbetreiber erbringen für die anderen Organisationen der IKT-Branche Dienstleistungen durch die Bereitstellung von Hardware-Ressourcen und Rechenzentren. Dafür betreiben sie Rechenzentren, z. B. in Gebieten mit hoher Dichte an Netzknoten; in Deutschland gehören hierzu unter anderem Frankfurt am Main (insbesondere mit dem DE-CIX) und der Großraum München (insbesondere für das Peering der DTAG). Bei dem Dienst der **Co-Location** werden durch den Rechenzentrumsbetreiber lediglich die Räume der Rechenzentren zur Verfügung gestellt. Der Rechenzentrumsbetreiber ist zudem für den physischen Zugangsschutz, die Kühlung, die Stromversorgung und die Internetanbindung verantwortlich. Die Organisation stellt lediglich den Server. Diese Anmietung von Platz in den Serverschränken des Rechenzentrumsbetreibers ist insbesondere im Bereich des Public Peerings gängig, da hier oftmals unterschiedliche Netzinfrastrukturen von verschiedenen Netzbetreibern zusammengeführt werden. IXPs sind daher oftmals in Co-Location-Rechenzentren untergebracht.

Unternehmen, die nur ihre Applikationen, Datenbanken oder sonstige Software ohne eigene Hardware in einem Rechenzentrum betreiben lassen, nutzen hingegen den Dienst **Hosting.** Hier bieten IT-Hoster dedizierte Server und Serverschränke (Racks) für die Kunden, die auf dieser Infrastruktur eigene Dienste und Software installieren können. Dieser Dienst wird zum Betrieb der IKT-Basisinfrastruktur durch Organisationen genutzt, um Datenbanken oder auch Steuerungssoftware dezentral verfügbar zu machen. Auch für eine redundante Datenhaltung, z. B. für die Datenbanken zur Rufnummernmitnahme, eignet sich dieser Dienst.

Die Bereitstellung von wichtigen **Internetdiensten** steht nur in indirekter Abhängigkeit von den anderen Teilnehmern des Marktes, da deren Betreiber in die Branche Internetwirtschaft einzuordnen sind. Die Dienste werden in Rechenzentren betrieben und über die Netzinfrastruktur der Netz- und Knotenbetreiber durch die Anschlussdienste der Service Provider für den Endkunden bereitgestellt. Ohne die Übertragung der Daten zwischen den Dienstanbietern und den Endkunden wäre die Diensterbringung nicht möglich. Gleiches gilt für die Funktionsfähigkeit der jeweiligen Rechenzentren (bei Co-Location) oder Server (bei Hosting).

2.1.2.4 Rolle der öffentlichen Hand

Nach der Privatisierung der Deutschen Telekom hat Deutschland mit dem Telekommunikationsgesetz (TKG) aus dem Jahr 1996 den Telekommunikationsmarkt liberalisiert. Mit dem erklärten Ziel, die Monopolstellung der Deutschen Telekom durch die Öffnung für weitere Wettbewerber zu beenden, wurde die Bundesnetzagentur beauftragt, für die Einhaltung der regulatorischen Vorgaben und Gesetze zu sorgen. Das Zusammenspiel zwischen Liberalisierung und Regulierung ist maßgeblich für die Entwicklung in der Branche. Die (gesetzlich festgelegte) Bereitstellung von Infrastrukturen der Deutschen Telekom an Wettbewerber wird stark reguliert. Dabei soll sichergestellt werden, dass Wettbewerber keine unverhältnismäßigen Preise gegenüber den tatsächlichen Kosten zum Betrieb der Infrastruktur bezahlen müssen (zum Beispiel für die Nutzung der TAL) [BNetzA 2014c].

Zusätzlich zur Wahrung der Chancengleichheit auf dem IKT-Markt ist die Bundesnetzagentur gleichermaßen in anderen Bereichen aktiv. So arbeitet sie intensiv mit verschiedenen Standardisierungsorganisationen (u. a. ITU-T, ISO, ETSI) zusammen und gibt Technische Richtlinien (TR) heraus. Im Mobilfunk ist sie zudem für die Regulierung und Aufteilung von Übertragungsfrequenzen zuständig.

Neben regulatorischen Anforderungen an Markt und Infrastruktur schreibt das Telekommunikationsgesetz (TKG) Dienstanbietern auch technische Schutzmaßnahmen und Meldepflichten für Sicherheitsvorfälle vor (zu Details vgl. Abschnitt 5.2).

Weiterhin übt die Europäische Union Einfluss auf die Branche in Deutschland aus. Im Jahre 2009 wurde mit dem Richtlinienpaket zur Novellierung des Regulierungsrahmens für Telekommunikationsnetze ein Rahmenwerk geschaffen. Dieses gesetzliche Rahmenwerk soll mehr Wettbewerb im IKT-Markt schaffen, für mehr Investitionen und schnellere Kommunikationsnetze (vor allem NGNs) sorgen. Relevant für den deutschen Markt sind vor allem Subventionen für den Ausbau von Netzen und die Möglichkeit der Risikoteilung etablierter Netzbetreiber. Durch eine Risikoteilung können die Kosten für Investitionen in den Netzausbau an die späteren Netznutzer weitergegeben werden [EU 2009].

Für die Entwicklung der IKT-Branche ist auch das geplante IT-Sicherheitsgesetz relevant. Die Bundesregierung will mit diesem Gesetz insbesondere Kritische Infrastrukturen schützen. Wichtige Elemente des Gesetzes sind die Meldepflicht von Sicherheitsvorfällen in Unternehmen und die Umsetzung von Mindeststandards für die IT-Sicherheit bei Netzbetreibern [BITKOM 2013].

Mit dem Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen (PTSG) werden Betreiber von (u. a.) Telekommunikationsdiensten verpflichtet, bei „erheblichen Störungen“ eine Mindestversorgung für bestimmte Empfänger sicherzustellen (§ 1 PTSG).

Der Bund ist als großer Anteilseigner am dominanten Marktteilnehmer, der DTAG, beteiligt [BMF 2013].[27]

27 Davon 14,5 % im Direktbesitz und 17,4 % indirekt über die Kreditanstalt für Wiederaufbau (KfW).

3 Kritische Dienstleistungen

Im Kapitel „Kritische Dienstleistungen“ werden diejenigen Dienstleistungen des Sektors Informations- und Kommunikationstechnologie identifiziert und beschrieben, die für eine Industrienation wie Deutschland eine bedeutende Rolle zur Sicherung des Gemeinwohls leisten. Kritische Dienstleistungen sind Dienstleistungen, deren Ausfall oder Beeinträchtigung zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen kann [BMI 2009].

Diese Auswahl an kritischen Dienstleistungen kann zum einen auf den staatlichen Auftrag zur Daseinsfürsorge zurückgeführt werden, zum anderen auch auf ihre Bedeutung als technische Basisinfrastrukturen für andere kritische Dienstleistungen innerhalb und außerhalb des Sektors Informations- und Kommunikationstechnologie. Diese Abhängigkeiten zeichnen sich durch eine Vielzahl von Verbindungen und Wechselwirkungen aus, sodass man von einer komplexen Interdependenz zwischen den Sektoren und den damit verbundenen kritischen Dienstleistungen ausgehen muss [BMI 2011].

Im Rahmen dieser Studie werden im Sektor Informations- und Kommunikationstechnologie zwei kritische Dienstleistungen untersucht:

– die **Sprach- und Datenübertragung** (DL1);

– die **Datenspeicherung und -verarbeitung** (DL2).

Die Begründung der Auswahl wird in dem jeweiligen Kapitel der kritischen Dienstleistung aufgeführt und durch beispielhafte Szenarien der dramatischen Folgen eines Ausfalls verdeutlicht. Diese Szenarien orientieren sich an realen Vorfällen oder basieren auf skizzierten Ursachen und Folgen, die nach Expertenmeinungen als realistisch angesehenen werden.

Im jeweiligen Abschnitt der **Dienstleistung (DL)** wird diese als ein Gesamtprozess betrachtet und in ihrer Funktion beschrieben. Hierzu wird die kritische Dienstleistung in **Prozessschritte (PS)** untergliedert. Diese ermöglichen eine übersichtliche Betrachtung der zur Erbringung der Dienstleistung nötigen Schritte oder Komponenten (siehe Abbildung 10). Jedem Prozessschritt sind **betriebsinterne Prozesse (BP)** zugeordnet, welche die detaillierteste Betrachtungsebene im Rahmen dieser grundlegenden Sektorstudie darstellen. Diese Prozesse bilden einen allgemeinen und von der Realität teils abstrahierten Blick auf den Gesamtprozess. Es werden jedoch keine Betreiber-spezifischen Eigenheiten betrachtet.

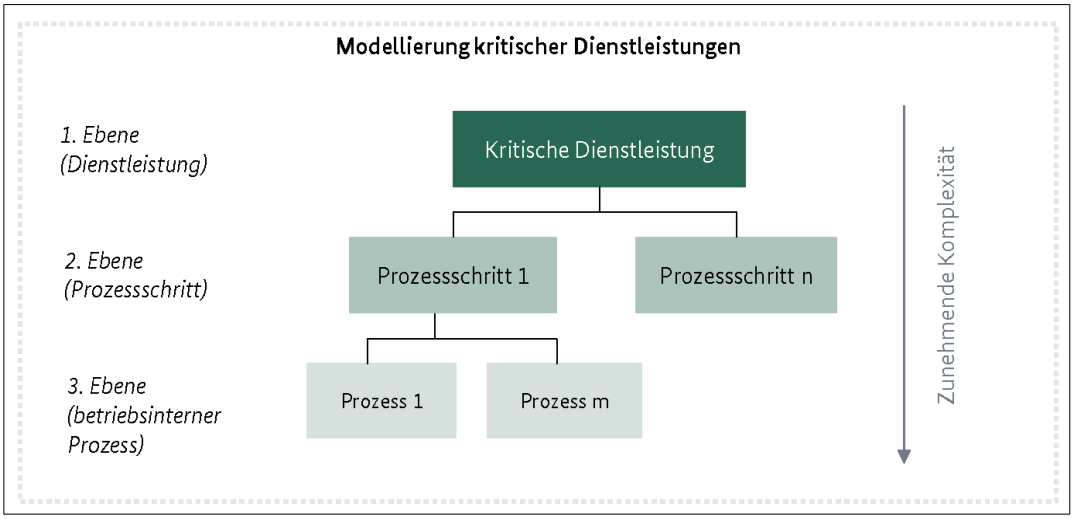

Abbildung 10: Modellierung kritischer Dienstleistungen

Quelle: eigene Darstellung

In die Studie werden nur jene betriebsinternen Prozesse aufgenommen, deren Ausfall oder Störung zu einem Ausfall oder einer Beeinträchtigung der gesamten Dienstleistung führen können. In diesem Sinne sind sie die **kritischen betriebsinternen Prozesse** der Dienstleistung. Auf diese Prozesse wird inhaltlich näher eingegangen, um den Bezug zu betroffenen Anlagen und Betriebsstätten (feste Geschäftseinrichtungen, die der Tätigkeit des Unternehmens dienen) sowie Abhängigkeiten und Zusammenhänge von und zu anderen kritischen betriebsinternen Prozessen herauszustellen.

Zur Überleitung in die Analyse der Abhängigkeiten der kritischen Dienstleistungen von Informations- und Kommunikationstechnologie (IKT) und zur Bestimmung des aktuellen Stands der Cybersicherheit werden in der Beschreibung der betriebsinternen Prozesse **Risikoelemente** vom Typ „Systeme der Informationstechnik (IT) und Kommunikationstechnik (KT)“ identifiziert.

Zu beachten ist, dass aufgrund der Komplexität und Heterogenität der Prozesse Details ausgeblendet werden müssen und Zusammenhänge nicht immer vollständig aufgelöst werden können. Die Ausführungen in dieser Studie haben vorrangig zum Ziel, die weitergehenden Fragestellungen zur Cybersicherheit verorten zu können und mit dem grundlegenden Verständnis der Dienstleistungen gezielt auf künftige Herausforderungen und Fragestellungen eingehen zu können.

Im Folgenden werden die kritischen Dienstleistungen in jeweils eigenen Abschnitten betrachtet.

3.1 Sprach- und Datenübertragung (DL1)

Die kritische Dienstleistung „Sprach- und Datenübertragung“ stellt die technische Basisinfrastruktur zur Übertragung von Sprache und Daten bereit. Die Dienstleistung wird durch die Marktteilnehmer des KRITIS-Sektors IKT angeboten und durch die deutsche Gesellschaft, Privatwirtschaft und öffentliche Hand zum Austausch von Sprache (Telefonie) und Daten (Internet) genutzt.

Die Bereitstellung der Infrastruktur für den Austausch von Sprache und Daten besteht aus technisch und logisch komplexen Vorgängen, die diese Studie zur Analyse kritischer Zusammenhänge und Abhängigkeiten in logische Teilbereiche, sogenannte Prozessschritte, unterteilt (siehe Abbildung 11). Jeder Prozessschritt leistet einen wesentlichen Beitrag zur Erbringung der Dienstleistung und beeinträchtigt bei Störung oder Ausfall die gesamte Dienstleistung. Dabei ist im Kontext der Leistungserbringung von idealtypischen Unternehmen zu beachten, dass nur einige der betriebsinternen Prozesse selbstständig durchgeführt werden. Im Anhang finden sich jeweils Darstellungen der idealtypischen Unternehmen „Ganzheitliche Betreiber“, „Mobilfunkbetreiber“ und „Kabelnetzbetreiber“ sowie deren Abhängigkeiten von anderen betriebsinternen Prozessen.

Für die Dienstleistung „Sprach- und Datenübertragung“ werden im weiteren Verlauf der Studie die folgenden Prozessschritte betrachtet:

- **Zugang (PS1):** Anschlussmöglichkeiten für den Zugang zu Kommunikationsnetzen zum Austausch von Sprache und Daten. Der Zugang stellt den Endkunden über Zugangsnetze eine Schnittstelle zur Nutzung der Kommunikationsinfrastruktur (Kernnetz) mit den eigenen Endgeräten bereit.
- **Übertragung (PS2):** Betrieb der Netzinfrastrukturen (Backbone) zur Übertragung von Sprache und Daten zwischen Kommunikationsteilnehmern oder Netzbetreibern.
- **Vermittlung (PS3):** Betrieb von Einrichtungen zum Austausch zwischen Netzen unterschiedlicher Betreiber (Vermittlungsfunktion).
- **Steuerung (PS4):** Unterstützende Leistungen, die für die Bereitstellung der Dienstleistung von wesentlicher Bedeutung sind.

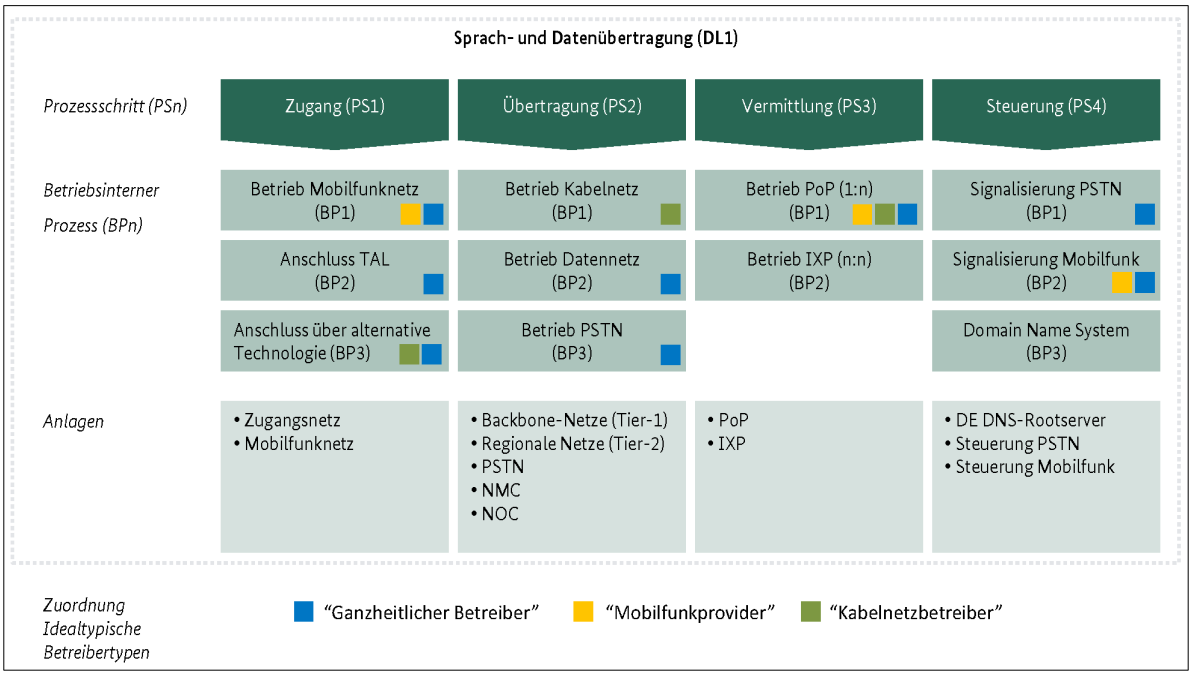

Abbildung 11: Schematische Darstellung der kritischen Dienstleistung „Sprach- und Datenübertragung"

Quelle: eigene Darstellung

Ausfall der Sprach- und Datenübertragung

Ein Ausfall der Sprach- und Datenübertragung kann vielfältige Ursachen haben, die aufgrund der Komplexität und des Aufbaus der Netze, über welche Sprache und Daten übertragen werden, unterschiedliche Folgen haben können.

Mögliche Ursachen können zum Beispiel sein:

- **Technisches Versagen**: Ausfälle der Sprach- und Datenübertragung verursacht durch Ausfall oder technisches Fehlverhalten von Infrastrukturkomponenten
- **Menschliches Versagen**: Ausfälle der Sprach- und Datenübertragung verursacht durch menschliches Fehlverhalten, etwa bei großflächigen Konfigurationsänderungen in Infrastrukturkomponenten
- **Kriminelle oder terroristische Handlungen**: Ausfälle der Sprach- und Datenübertragung verursacht durch absichtliche Manipulationen oder Cyber-Angriffe auf Infrastrukturkomponenten

Unter dem Begriff „Ausfall" werden im Folgenden ein vollständiger Ausfall der Dienstleistung, eine gravierende Störung der Dienstleistung mit konkreten Folgen oder die Zerstörung von Infrastrukturen (meist verbunden mit Ausfällen) verstanden.

Exemplarisch seien an dieser Stelle einige Ausfall-Szenarien aufgeführt:

- Werden fehlerhafte Konfigurationsänderungen oder Softwareupdates gleichzeitig an einer Vielzahl wichtiger Netzelemente (z. B. Router) vorgenommen, können großflächige Fehlfunktionen bei der Übertragung, Vermittlung und Steuerung zu einem Komplettausfall der Netze führen. Als Beispiel hierfür sei auf den bundesweiten Netzausfall des T-Mobile-Mobilfunknetzes im Jahre 2009 verwiesen. Als Fehlerquelle nannte der Netzbetreiber Software-Fehler in einer zentralen Datenbank. Der Betreiber konnte den Fehler zeitnah identifizieren und die Funktionsfähigkeit des Netzes innerhalb weniger Stunden wiederherstellen [Spiegel 2009].
- Ein Stromausfall bei Netzelementen kann zum Ausfall der Verfügbarkeit der Sprach- und Datenübertragung einzelner Netzsegmente führen. Ein Stromausfall in Ortsvermittlungsstellen führt beispielsweise zur Nichterreichbarkeit einzelner regionaler Bereiche. Kunden können in Folge dessen

keine Sprache und Daten über das Festnetz austauschen. Notstromaggregate können kurzfristige Stromprobleme kompensieren, stehen aber oftmals nur zeitlich begrenzt zur Verfügung. Sind zentralere Knotenpunkte, beispielsweise große IXPs (DE-CIX etc.) betroffen, kann dies großflächige Auswirkungen in den Netzen haben. Solche wichtigen, zentralen Infrastrukturen verfügen jedoch in der Regel über Notstromaggregate, die Probleme in der Stromversorgung über mehrere Tage überbrücken können (z. B. durch den Einsatz von Dieselaggregaten).

- Menschliche Fehler können zum Ausfall der Dienstleistung führen, etwa bei der fehlerhaften Konfiguration wichtiger Netzelemente. Im Jahr 2008 kam es bundesweit zu Störungen und teilweisen Netzausfällen des Vodafone-Mobilfunknetzes. Als Ursache hierfür nannte das Unternehmen fehlerhafte Eingaben in einem System, die durch einen Mitarbeiter im Rahmen einer Routinewartung vorgenommen wurde [Spiegel 2008].
- Kapazitäts- bzw. Lastprobleme in Netzelementen können ebenfalls zu massiven Problemen führen. Aufgrund redundanter Netzarchitekturen führen Lastprobleme einzelner Komponenten jedoch in der Regel nicht zu einem vollständigen Ausfall. Betroffen sind in solchen Fällen oftmals Teilnetze, z. B. regionale Zugangsnetze.

Folgen eines Ausfalls der Sprach- und Datenübertragung

Die Folgen eines Ausfalls der Sprach- und Datenübertragung unterscheiden sich in den einzelnen Teilen der Gesellschaft:

- Die **Bevölkerung** ist durch einen großflächigen Ausfall der Dienstleistung unmittelbar betroffen und in der privaten und beruflichen Kommunikation stark eingeschränkt. Entfällt hierdurch die Möglichkeit, Notrufe abzusetzen, entsteht eine direkte Gefährdung von Menschenleben.
- Für die **Wirtschaft** ist bei Ausfall der Sprach- und Datenübertragung von großen finanziellen Auswirkungen auszugehen. Bei einem Großteil der deutschen Wirtschaft bestehen hohe IKT-Abhängigkeiten in Prozessen und Wertschöpfung. Ein Ausfall der in dieser Studie betrachteten IKT-Basisinfrastruktur kann bereits nach wenigen Stunden zu einem Stillstand in größeren Produktionsunternehmen führen, da zentrale Computersysteme in der Produktion und Logistik nicht miteinander kommunizieren können.
- Auch der **Staat** ist von einem Ausfall der Sprach- und Datenübertragung unmittelbar betroffen. Die Wahrung der Staatsfunktion zum Schutz der Bevölkerung wäre beispielsweise in der Erreichbarkeit von Notrufzentralen oder Einsatzkräften durch die Bevölkerung massiv eingeschränkt. Einsatzkräfte untereinander können zur Kommunikation u. U. auf alternative Infrastrukturen, z. B. den digitalen BOS-Funk[28] (die vollständige Umsetzung der Digitalisierung ist für Ende 2014 erwartet), ausweichen. Die Schnittstelle zur Bevölkerung und weitere Kommunikationskanäle sind dennoch massiv eingeschränkt.

3.1.1 Prozessschritt „Zugang“ (PS1)

Der Prozessschritt „Zugang“ (PS1) stellt Anschlussmöglichkeiten zum Zugang zu Kommunikationsnetzen für den Austausch von Sprache und Daten bereit. Als Dienstleister sind in diesem Prozessschritt vor allem Marktteilnehmer der Rolle „Service Provider“ involviert.

Der Zugang zu den Netzen kann dabei über verschiedene Zugangstechnologien realisiert werden. Dies hängt maßgeblich vom Endgerät (Mobiltelefon, analoges Telefon, ISDN-Telefon, VoIP-Telefon, Computer, Maschine, Embedded System etc.) sowie dem Anschlusstyp (Mobilfunk, Festnetz, Breitbandkabel etc.) ab.

Die unterschiedlichen Anschlusstypen werden nachfolgend getrennt als sogenannte betriebsinterne Prozesse betrachtet, um insbesondere die jeweiligen prozessualen und technischen Gegebenheiten bei der Bereitstellung des Zugangs zu berücksichtigen (siehe Abbildung 12).

28 Funknetz für Behörden und Organisationen mit Sicherheitsaufgaben.

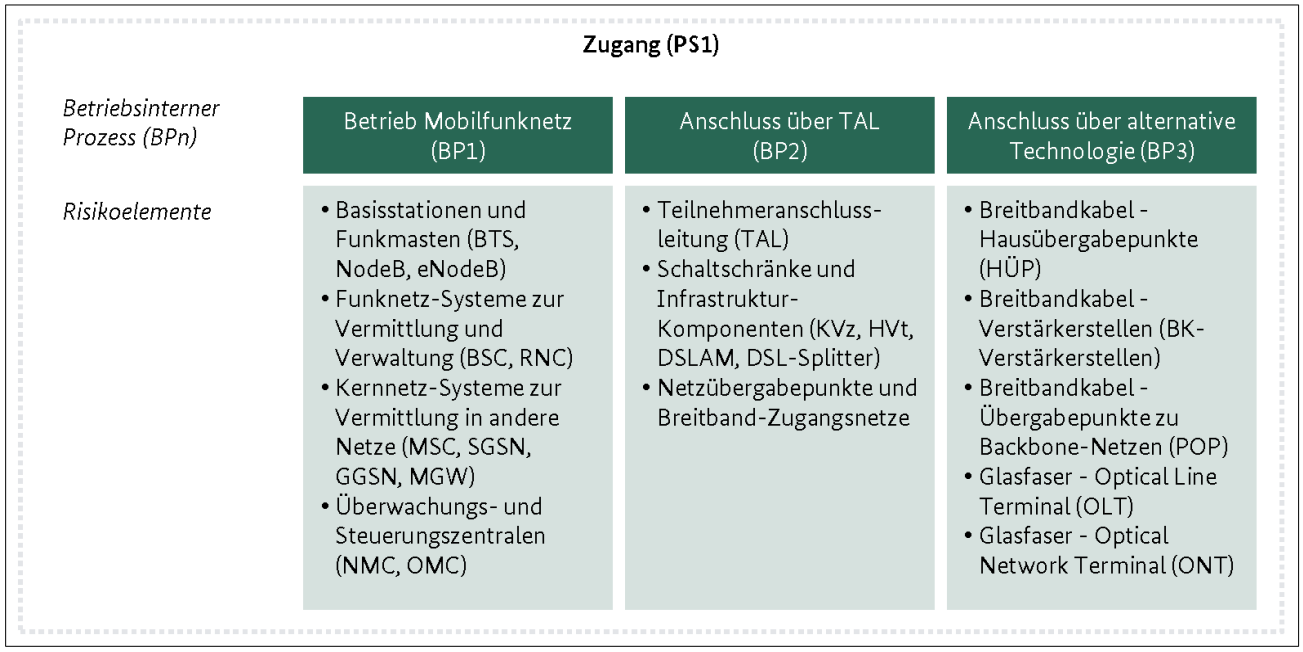

Abbildung 12: Prozessschritt „Zugang“ der Dienstleistung „Sprach- und Datenübertragung“

Quelle: eigene Darstellung

Für den Prozessschritt „Zugang“ werden im weiteren Verlauf der Studie die folgenden betriebsinternen Prozesse betrachtet:

- **Betrieb Mobilfunknetz (BP1):** Netz-Anschluss über eine Funkverbindung für mobilfunkfähige Endgeräte (Mobiltelefone, Smartphones, Datenkarten, Embedded Systems etc.).
- **Anschluss über TAL (BP2):** Leitungsgebundener Anschluss unter Verwendung der Teilnehmeranschlussleitung (TAL).
- **Anschluss über alternative Technologien (BP3):** Dedizierter, leitungsgebundener Anschluss, der nicht auf Basis der Teilnehmeranschlussleitung erfolgt (z. B. Kabelnetz oder Glasfaser).

3.1.1.1 Betriebsinterner Prozess „Betrieb Mobilfunknetz“

DL	PS	BP	Betrieb Mobilfunknetz	
1	**1**	**1**		
Zusammenfassung			Der betriebsinterne Prozess „Betrieb Mobilfunknetz“ stellt den Betrieb der technischen Infrastruktur dar, auf Basis derer die Übertragung von Sprache und Daten des Mobilfunks stattfindet. Dies umfasst auch Wartung, Steuerung und Aufbau neuer Mobilfunkanlagen.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• Basisstationen und Funkmasten (BTS, Node B, eNode B) • Funknetz-Systeme zur Vermittlung und Verwaltung (BSC, RNC) • Kernnetz-Systeme zur Vermittlung in andere Netze (MSC, SGSN, GGSN, MGW) • Überwachungs- und Steuerungszentralen (NMC/NOC, OMC)	

Tabelle 18: Betriebsinterner Prozess „Betrieb Mobilfunknetz“ (DL1 PS1 BP1)

Prozessbeschreibung

Je nach Mobilfunkstandard (GSM, UMTS, LTE) unterscheidet sich der technische Aufbau der Netze; auch ist die Terminologie der einzelnen Netz-Komponenten verschieden. Der grundlegende Aufbau ist jedoch identisch und wird nachfolgend vereinfacht beschrieben.

Mobilfunknetze bestehen aus einem Kern- und mehreren Zugangsnetzen. Die Zugangsnetze sind in der Regel Funknetze und werden daher auch als Funkzugangsnetze (GERAN, UTRAN, E-UTRAN) bezeichnet. Im Funkzugangsnetz bilden geografisch verteilte Basisstationen und daran angeschlossene Antennen (BTS, Node B, eNode B) die Schnittstelle zwischen den Endgeräten der Mobilfunkteilnehmer und dem Netz (Funkzelle). Den Basisstationen nachgelagerte Systeme (BSC, RNC) übernehmen die Übertragung der Daten vom und zum Kernnetz sowie diverse Verwaltungsaufgaben der Funknetzressourcen (Zellwechsel, Sprachkodierung etc.).

Die Störung oder der Ausfall einzelner Funkzellen (Basisstationen) hat Auswirkungen auf eine begrenzte Anzahl an Mobilfunkteilnehmern, die über die betroffenen Funkzellen mit dem Netz verbunden sind. Da sich Funkzellen oftmals überlappen, kann ein Ausfall einzelner Zellen ggf. durch benachbarte Funkzellen kompensiert werden. Im Kernnetz befinden sich zentrale Vermittlungssysteme. Hauptbestandteil des Kernnetzes sind dabei zentrale Gateways (MSC, SGSN, GGSN, MGW) zur Vermittlung der Daten in andere Netze (z. B. Telefonnetz oder Internet).

Die Störung oder der Ausfall der zentralen Gateways kann, je nach Aufbau und Redundanz des Netzes, Auswirkungen auf die Funktionsweise des gesamten Netzes haben.

Weiterhin verfügen Mobilfunknetze über komplexe Überwachungs- und Steuerungszentralen (NMC/NOC, OMC), die für Betrieb und Wartung der Netze essentiell sind. In diesen Steuerungszentralen übt das Betriebspersonal der Netzbetreiber u. a. die Fernkonfiguration von Netzwerkkomponenten, die Überwachung der Lastverteilung sowie andere Fernwartungsaktivitäten aus.

Die Störung oder der Ausfall der Überwachungs- und Steuerungszentralen kann je nach Aufbau und regionaler Organisation der Einsatzzentralen Auswirkungen auf Teile oder das Gesamtnetz haben.

3.1.1.2 Betriebsinterner Prozess „Anschluss über TAL“

DL	PS	BP	Anschluss über TAL
1	**1**	**2**	
Zusammenfassung			Der betriebsinterne Prozess „Anschlussbereitstellung über TAL“ stellt die Bereitstellung eines Anschlusses zur Sprach- und Datenübertragung (Telefon- und Internetanschlüsse) über die Teilnehmeranschlussleitung (TAL) dar.
Abhängigkeit Logistik			unwesentlich / wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden. Die Lieferung von Geräten für die Nutzung des bereitgestellten Anschlusses erfolgt zumeist auf postalischem Weg und stellt somit auch eine indirekte Abhängigkeit dar.
Risikoelemente (IKT)			• Teilnehmeranschlussleitung (TAL) • Schaltschränke und Infrastruktur-Komponenten (KVz, HVt, DSLAM, DSL-Splitter) • Netzübergabepunkte und Breitband-Zugangsnetze

Tabelle 19: Betriebsinterner Prozess „Anschluss über TAL“ (DL1 PS1 BP2)

Prozessbeschreibung

Die Teilnehmeranschlussleitung (auch Amtsleitung oder „Letzte Meile“ genannt) ist eine Kabelverbindung zwischen dem Teilnehmeranschluss im Haus und den Kabelverzweigern (KV). KV sind Schaltschränke am Straßenrand, an denen die TAL verschiedener Häuser und Endkunden zusammenlaufen und mit den Hauptverteilern (HVt) in den Ortsvermittlungsstellen verbunden werden. Die TAL stellt aus Endkundensicht somit die physische Verbindung zum Festnetz dar. Die TAL sind in Deutschland großflächig durch die Deutsche Telekom verlegt worden und daher hauptsächlich in deren Besitz.

Mit Verbreitung des Breitband-Internetzugangs durch die DSL-Technologie (Digital Subscriber Line) sind viele Endkunden über die TAL nicht mehr ausschließlich zur Telefonie angebunden, sondern auch für den schnellen Internetzugang. Dabei werden über Kabelverbindungen der TAL Sprach- und Breitbanddaten auf unterschiedlichen Frequenzbändern getrennt übertragen. Dies erfordert an beiden Enden der TAL (also bei Kunden und Netzbetreibern) entsprechende Frequenzweichen, sogenannte DSL-Splitter. Hinzu kommen auf Seiten der Netzbetreiber sogenannte DSLAM (Digital Subscriber Line Access Multiplexer), welche die DSL-Teilnehmerleitungen konzentrieren und mit Breitband-Zugangsnetzen verbinden.

Die Störung oder der Ausfall einer TAL hat nur Auswirkungen auf einzelne Kunden. Die Störung oder der Ausfall der örtlich verteilten Schaltschränke und Netz-Komponenten (KVz, HVt, DSLAM, Ortsvermittlungsstelle) hat Auswirkungen auf eine regional begrenzte Nutzergruppe.

Telefon- und Internetanschlüsse werden durch die Service Provider vermarktet. Ein Service Provider kann auch gleichzeitig Netzbetreiber sein, wie im Fall der Deutschen Telekom. Service Provider ohne eigenes Netz, sogenannte (Switched) Reseller, können Netz-Zugänge über die TAL der Deutschen Telekom realisieren. Wird der Anschluss über die TAL nicht allein durch die Deutsche Telekom als Service Provider und Netzbetreiber erbracht, wird zwischen verschiedenen Szenarien unterschieden:

- Beim Line-Sharing werden die herkömmlichen Festnetz-Dienste (analoges Telefon, ISDN) und der DSL-basierte Internetanschluss von unterschiedlichen Anbietern bereitgestellt.

- Bei der TAL-Entbündelung wird die TAL von einem alternativen Service Provider zur Bereitstellung herkömmlicher Festnetz-Dienste und/oder DSL-Internetanschluss genutzt.
- Bei einem Bitstromzugang wird die TAL von einem alternativen Service Provider ausschließlich zur Bereitstellung eines DSL-Anschlusses genutzt, d. h. es erfolgt kein Zugang zu herkömmlichen Festnetz-Diensten.

Die Möglichkeit der Bereitstellung von Zugängen durch Nicht-Netzbetreiber hat zur Folge, dass Service Provider teilweise eigene technische Infrastrukturkomponenten betreiben und diese mit den Komponenten der Netzbetreiber verbinden müssen (z. B. an einem DSLAM oder einem PoP).

Die Störung oder der Ausfall dieser Infrastrukturkomponenten von Service Providern ohne eigenes Netz hat Auswirkungen auf eine begrenzte Nutzergruppe, die Endkunden die über einen Anschluss des jeweiligen Service Providers verfügen und deren Anbindung über die betroffenen Komponenten erfolgt.

Die Endgeräte auf Endkunden-Seite (z. B. Splitter, DSL-Modem, Telefon etc.) werden in der Studie nicht weiter betrachtet, da diese allein die Nutzung des bereitgestellten Anschlusses ermöglichen.

3.1.1.3 Betriebsinterner Prozess „Anschluss über alternative Technologien“

DL	PS	BP	Anschluss über alternative Technologien
1	**1**	**3**	
Zusammenfassung			Der betriebsinterne Prozess „Anschluss über alternative Technologien“ stellt die Bereitstellung eines Anschlusses zur Sprach- und Datenübertragung (Telefon- und Internetanschlüsse) über alternative Technologien dar. Als alternative Technologien werden nachfolgend Anschlüsse des Breitbandkabelnetzes, Glasfaseranschlüsse und Satellitenanschlüsse betrachtet. Zusätzlich ist der Zugang zur Telefonie über SIP-Endpunkte in diesem betriebsinternen Prozess untergebracht, obwohl er selbst keine eigene Zugangstechnologie darstellt, sondern andere Technologien zur Übermittlung der Daten nutzt.
Abhängigkeit Logistik			unwesentlich / wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.
Risikoelemente (IKT)			• Breitbandkabel: Hausübergabepunkte (HÜP) • Breitbandkabel: Verstärkerstellen (BK-Verstärkerstellen) • Breitbandkabel: Übergabepunkte zu Backbone-Netzen (PoP) • Glasfaser: Optical Line Terminal (OLT) • Glasfaser: Optical Network Terminal (ONT) • Satellit: Satelliten • Satellit: Bodenstation • SIP: Registrierungsserver • SIP: SIP-Server • SIP: Gateways

Tabelle 20: Betriebsinterner Prozess „Anschluss über alternative Technologien“ (DL1 PS1 BP3)

Prozessbeschreibung

Breitbandkabelnetze wurden ursprünglich für die Übertragung des Kabelfernsehens genutzt, stellen heute jedoch auch einen Anschluss an Datennetze wie z. B. das Internet bereit. Breitbandkabelnetze sind ähnlich hierarchisch aufgebaut wie Telefon- und Datennetze. In Bezug auf die Zugangsnetze sind die wichtigen Komponenten die Hausübergabepunkte (HÜP), Breitbandkabel-Verstärkerstellen (BK-Verstärkerstellen) und Übergabepunkte (Points of Presence, PoP) zu Backbone-Netzen.

Glasfaser-Anschlüsse stellen eine breitbandige Alternative zu herkömmlichen Anbindungen über die TAL dar. Abhängig vom Ort des Glasfasernetzabschlusses werden je nach Netzausbaustufe verschiedene Ausbaustufen (FTTx) unterschieden: Für den Zugang sind vor allem Fiber-to-the-Building (FTTB) und Fiber-to-the-Home (FTTH) relevant, bei denen eine Glasfaserleitung vom Gebäude bzw. der Wohnung der Endkunden zu den örtlichen Knotenpunkten verlegt wird. Je nach Ausbaustufe der örtlichen Infrastruktur werden Glasfaser-Kunden an die Kabelverzweiger (KVz), Hauptverteiler (HVt) oder direkt an die Ortsvermittlungsstellen angeschlossen. Für die Glasfasertechnologie sind Vermittlungsstellen mit Optical Line Terminal (OLT) ausgestattet, die den Übergang vom Zugangsnetz zum Backbone-Netz herstellen. Auf

Endkundenseite werden Optical Network Termination (ONT) eingesetzt, die das optische Signal terminieren und den Endkunden herkömmliche Schnittstellen (z. B. RJ45) zur Verfügung stellen.

Eine Betrachtung von Zugängen zur Sprach- und Datenübertragung über Satelliten ist durch die geringe Verbreitung in Deutschland als Kritische Infrastruktur vernachlässigbar (siehe Abschnitt 2.1.2.1 „Service Provider“). Vor dem Hintergrund der Nutzung von Satelliten zur Bereitstellung von Verbindungen in nicht erschlossenen Gegenden oder im Krisenfall wird diese Zugangsart in dieser Studie dennoch kurz erläutert.

Der Endkunde erhält Zugriff auf das Satellitennetz über ein Satellitentelefon. Befindet sich im Empfangsbereich des Satellitentelefons ein Satellit, so können Daten direkt zwischen den beiden Komponenten ausgetauscht werden. Der Satellit sendet die Daten über die nächstgelegenen anderen Satelliten weiter, bis der Satellit erreicht wird, bei dem das angerufene Satellitentelefon registriert ist. Erfolgt ein Anruf vom Satellitentelefon in das Fest- oder Mobilfunknetz, so werden die Daten bis zu einem Satelliten weitergeleitet, der sich über einer Bodenstation befindet. Von dort erfolgt die Einspeisung in die Datennetze.

Hinweis:

Zwar können die Satellitentelefone direkt über die Satelliten ohne Beteiligung einer Bodenstation kommunizieren. Jedoch hat die Bodeninfrastruktur Aufgaben bzgl. Monitoring sowie Command and Control. Das bedeutet, dass das Signalling (Steuerung des Auf- und Abbaus der Verbindungen) von der Vermittlungsinfrastruktur am Boden vorgenommen wird. Das "Suchen" des gerufenen Teilnehmers im System während des Verbindungsaufbaus kann i. d. R. nicht durch die Satelliten selbst geleistet werden.

Darüber hinaus ist die Aussage, dass der Satellit die Daten über die nächstgelegenen Satelliten bis zu dem Satellit, bei dem das angerufene Satellitentelefon registriert ist, weiterleitet, auf die Satelliten eines Betreibers bezogen.

3.1.2 Prozessschritt „Übertragung“ (PS2)

Der Prozessschritt „Übertragung“ (PS2) stellt die Infrastruktur zur Übertragung von Sprache und Daten zwischen einzelnen Teilnehmeranschlüssen über Weitverkehrsnetze bereit. Als Dienstleister sind in diesem Prozessschritt Marktteilnehmer der Rolle „Netzbetreiber“ involviert.

Die Übertragung von Sprache und Daten erfolgt in Abhängigkeit des jeweiligen Zugangsnetzes (vgl. Prozessschritt „Zugang“) über verschiedenartige Netze.

Die unterschiedlichen Netze werden nachfolgend getrennt als sogenannte betriebsinterne Prozesse betrachtet, um insbesondere die jeweiligen prozessualen und technischen Gegebenheiten bei der Übertragung von Sprache und Daten zu berücksichtigen (siehe Abbildung 13).

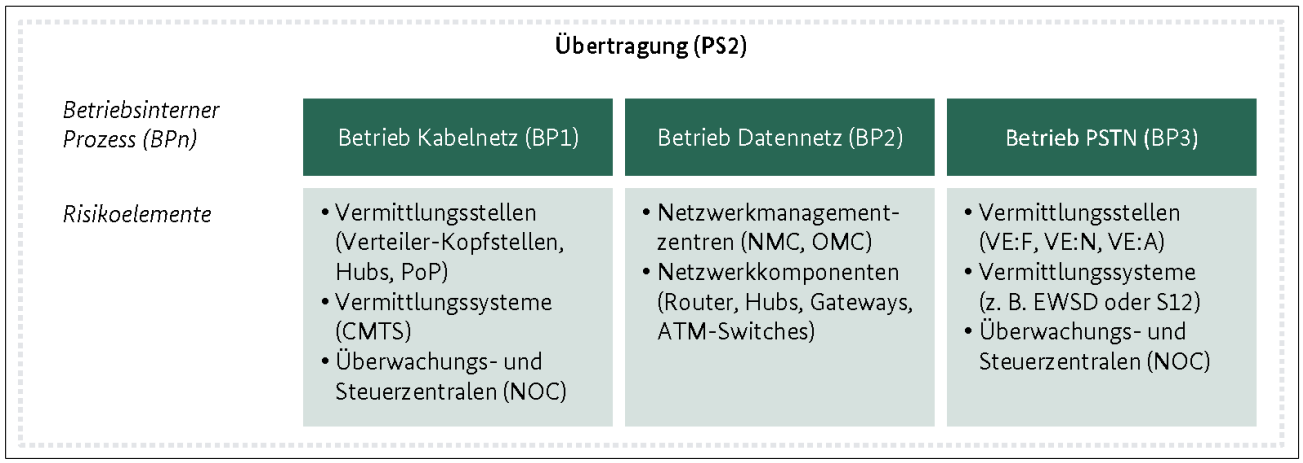

Abbildung 13: Prozessschritt „Übertragung“ der Dienstleistung „Sprach- und Datenübertragung“

Quelle: eigene Darstellung

Für den Prozessschritt „Übertragung“ (PS2) werden im weiteren Verlauf der Studie die folgenden betriebsinternen Prozesse betrachtet:

- **Betrieb Kabelnetz (BP1):** Betrieb der Kernnetze der Breitbandkabelnetz-Technologie.
- **Betrieb Datennetz (BP2):** Betrieb der Kernnetze, die unabhängig von der Zugangstechnologie (DSL, Glasfaser, Mobilfunk etc.) Daten übertragen.
- **Betrieb PSTN (BP3):** Betrieb der Festnetz-Kernnetze (PSTN), an die Kunden der Zugangstechnologie „Analoge Telefonie und ISDN“ angeschlossen sind.

An dieser Stelle sei angemerkt, dass zwischen den einzelnen Netzen Verbindungen existieren. Diese Zusammenschaltung von Netzen wird im Prozessschritt „Vermittlung“ betrachtet. Die Steuerung der Netze, z. B. die Konfiguration von Systemen und Netzkomponenten sowie der Austausch von Steuerungsinformationen, werden im Prozessschritt „Steuerung“ betrachtet.

Vor dem Hintergrund der technischen Konvergenz (siehe Abschnitt 2.1.2) ist der Betrieb des Datennetzes auch für das Kabelnetz und das PSTN von Bedeutung, da diese Sprache und Daten teilweise auch über Datennetze austauschen (siehe Abbildung 6).

3.1.2.1 Betriebsinterner Prozess „Betrieb Kabelnetz“

DL	PS	BP	Betrieb Kabelnetz	
1	**2**	**1**		
Zusammenfassung			Der betriebsinterne Prozess „Betrieb Kabelnetz“ stellt den Betrieb des Breitbandkabelnetzes dar. Im Gegensatz zum Prozessschritt „Zugang“ zählen hierzu nicht die Zugangsnetze, sondern ausschließlich die Kernnetze (Backbone). Eine wichtige Abgrenzung des Kabel-Kernnetzes vom Datennetz entsteht durch die Nutzung eines eigenen Übertragungsstandards (Data Over Cable Service Interface Specification – DOCSIS) sowie eigener Anlagen (z. B. Kopfstellen und Vermittlungssysteme). Zudem unterscheiden sich durch die historische Entwicklung die Betreiber beider Übertragungsnetze voneinander.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• Vermittlungsstellen (Verteiler-Kopfstellen, Hubs, PoP) • Vermittlungssysteme (CMTS) • Überwachungs- und Steuerungszentralen (NMC/NOC)	

Tabelle 21: Betriebsinterner Prozess „Betrieb Kabelnetz“ (DL1 PS2 BP1)

Prozessbeschreibung

Breitbandkabelnetze sind in der Regel hierarchisch aufgebaut. Den Backbone des Netzes bildet dabei das verbindende Kernnetz, das einzelne, oft regional aufgebaute Teilnetze zusammenführt und Verbindungen zwischen den einzelnen Netzsegmenten und Teilnehmern ermöglicht. Es verbindet somit Verteiler-Kopfstellen [Keller 2005], in denen sich zudem das Vermittlungssystem (CMTS), das für die korrekte Weiterleitung von Anfragen im Kabelnetz verantwortlich ist, befindet.

Zum Schutz vor Ausfällen sind die Komponenten des Kernnetzes in der Regel redundant ausgelegt. Die Störung oder der Ausfall des Kernnetzes hat Auswirkungen auf das gesamte Breitbandkabelnetz.

An die Verteiler-Kopfstellen angeschlossen sind mehrere Netzknoten. Diese Netzknoten (teilweise auch Hubs oder übergeordnete Breitbandkabelverstärker genannt) bilden Übergangspunkte zu anderen Netzsegmenten des Kabelnetzes, also den regionalen Zugangsnetzen.

Die Störung oder der Ausfall einzelner Netzknoten wird unter Berücksichtigung von Redundanzen im Regelfall nur Auswirkungen auf einen Teil des Netzes haben (z. B. auf ein regionales Zugangsnetz), jedoch nicht zum Ausfall des Gesamtnetzes führen.

Weiterhin verfügen Breitbandkabelnetze über komplexe Überwachungs- und Steuerungszentralen (NMC/NOC), die für Betrieb und Wartung der Netze essentiell sind. In diesen Steuerungszentralen übt das Betriebspersonal der Netzbetreiber u. a. die Fernkonfiguration von Netzwerkkomponenten, die Überwachung der Lastverteilung und andere Fernwartungsaktivitäten aus.

Die Störung oder der Ausfall der Überwachungs- und Steuerungszentralen kann je nach Aufbau und regionaler Organisation der Einsatzzentralen Auswirkungen auf Teile oder das Gesamtnetz haben.

3.1.2.2 Betriebsinterner Prozess „Betrieb Datennetz“

DL	PS	BP	Betrieb Datennetz	
1	**2**	**2**		
Zusammenfassung			Der betriebsinterne Prozess „Betrieb Datennetz“ stellt den Betrieb von Weitverkehrsnetzen zur Übertragung von Daten aus verschiedenen (Zugangs-)Netzen dar.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• Netzwerkmanagementzentren (NMC/NOC, OMC) • Backbone-Komponenten (Router, Switches) • Verstärkerstationen	

Tabelle 22: Betriebsinterner Prozess „Betrieb Datennetz“ (DL1 PS2 BP2)

Prozessbeschreibung

Diese auch als Kernnetz, Backbone, oder Transportnetz bezeichneten Netze ermöglichen die Datenübertragung über große geographische Entfernungen. Hierfür werden die Daten an dedizierten Übergabepunkten (z. B. aus dem Mobilfunknetz, dem Breitbandkabelnetz oder dem PSTN) in das Datennetz eingespeist und dort über Glasfaserleitungen bis hin zur erneuten Einspeisung in das Zugangsnetz weitergeleitet.

Für Backbone-Netze werden zurzeit meist Technologien wie MPLS, DWDM, SDH, Carrier-grade Ethernet auf geteilten oder privaten Glasfaserverbindungen genutzt. Der größte Teil der heutzutage übertragenen Daten besteht aus der IP-Protokollfamilie.

Datennetze sind in der Regel hierarchisch aufgebaut. Nationale bzw. globale Netze bilden dabei die oberste Netzebene. Darunterliegende Netze sind oftmals regionale Netze, die über einen Backbone an andere größere Netze angeschlossen sind. Das Kernnetz zeichnet sich insbesondere durch hohe Datenübertragungsraten von 10 Gbit/s bis 40 Gbit/s aus. Netzbetreiber des Kernnetzes verfügen meist über Verbindungen zu wichtigen großen Knotenpunkten (in Deutschland z. B. Frankfurt, Hamburg, München, Berlin).

Die Leitungen des Datennetzes werden in Form von Glasfasertrassen verlegt. In einer Glasfasertrasse werden dicke Glasfaserstränge zusammengefasst und i. d. R. unterirdisch in Leerrohren verlegt. Die Verlegung solcher Trassen ist mit regulatorischen und rechtlichen Aspekten verbunden. Für die Verlegung solcher Trassen über öffentliche Wege ist eine Nutzungsberechtigung erforderlich (vgl. TKG Abschnitt 3 Wegerechte). Vor allem Energieversorger verfügen für ihre Strom- und Gasleitungen bereits über solche Wegerechte. Für sie ist der Ausbau der vorhandenen Strom- und Gastrassen mit Glasfasertrassen vergleichsweise günstig und mit relativ wenig bürokratischem Aufwand verbunden.

So haben sich beispielsweise 15 deutsche Ferngas- und Regionalgasgesellschaften zur GasLINE mbH & Co. KG zusammengeschlossen und bieten über diese gemeinsame Organisation deutschlandweit eine großflächige Glasfaser-Infrastruktur. Netzbetreiber können dort z. B. Leerrohre zur Verlegung eigener Glasfasern oder vorhandene, unbeschaltete Glasfaserleitungen (sogenannte Dark-fibre) einkaufen. Diese Leitungen werden dann durch die Netzbetreiber zusammengeschaltet und bilden die Übertragungsstrecke des Datennetzes. [GasLine 2014]

Aufgrund des Signalverlusts während der Übertragung auf Glasfasern müssen die Signale auf den Fasern im Abstand einiger hundert Kilometern verstärkt werden. Aus diesem Grund stehen an Glasfasertrassen sogenannte Repeaterstationen (Verstärkerstationen). Dort werden die Glasfasern aus den Trassen geholt und die Signale verstärkt. Um möglichst viele Signale über einzelne Glasfasern zu übertragen, werden moderne Multiplexverfahren eingesetzt (stark verbreitet sind DWDM und SDH), welche auf einer Glasfaser mehrere optische Kanäle parallel zur unabhängigen Datenübertragung zur Verfügung stellen. Bei Ein- und Ausspeisung von Signalen werden aus diesem Grund zusätzliche (De-)Multiplexer eingesetzt.

Die Störung oder der Ausfall einzelner Glasfaserstrecken hat Auswirkungen auf einzelne Teilnetze. Oftmals sind Verbindungen redundant ausgelegt, sodass beim Ausfall einzelner Strecken alternative Verbindungen genutzt werden können.

Um die Funktionalität des Kernnetzes zu gewährleisten, werden Netzwerkmanagementzentren (NMC) betrieben, die für die Überwachung der einzelnen Datennetze und die Steuerung der technischen Komponenten verantwortlich sind.

Die Störung oder der Ausfall von Netzwerkmanagementzentren hat, je nach Redundanz und Zuständigkeitsbereich der betroffenen NMC, Auswirkungen auf gesamte Datennetze, da Steuerungstätigkeiten wie z. B. die Lastverteilung oder die Festlegung von Ersatzrouten nicht mehr durchgeführt werden können.

Neben Kabelverbindungen bzw. Glasfaserleitungen werden im Backbone-Bereich teilweise auch Satellitenverbindungen eingesetzt, jedoch meist nur zur Lastverteilung oder als Fallback-Lösung.

Der Betrieb des Datennetzes umfasst zudem die interne Steuerung, also die Festlegung von Transportrouten und anderen Steuerungsparametern. Zur Übertragung von Daten wird in Datennetzen das Internet Protokoll (IP) eingesetzt. Die im Backbone eingesetzten Router zur Weiterleitung und Vermittlung von Daten übernehmen die Signalisierung im Datennetz. Ein dediziertes Signalisierungsnetz wie z. B. im Mobilfunk ist nicht erforderlich. Der wichtigste Teil der Signalisierung ist der Austausch von Routing- und Erreichbarkeitsinformationen zwischen den IP-basierten Backbone-Netzen unterschiedlicher Betreiber. Die logischen Backbone-Netze werden Autonome Systeme (AS) genannt, sie enthalten alle öffentlichen Internet-Adressen (IP) des Betreibers. Betreiber tauschen untereinander Routing-Informationen mit Routing-Protokollen aus, im Internet vor allem per BGP. IP-Verkehr im Internet wird zwischen den AS verschiedener Betreiber per IP ausgetauscht, auch Peering genannt.

3.1.2.3 Betriebsinterner Prozess „Betrieb PSTN“

DL	PS	BP	Betrieb PSTN	
1	**2**	**3**		
Zusammenfassung			Der betriebsinterne Prozess „Betrieb PSTN“ stellt den Betrieb der Infrastruktur zur Übertragung von Sprache im Kernnetz der Festnetztelefonie dar. Dies umfasst auch die Bereitstellung von Schnittstellen zu anderen Netzen, insbesondere dem Datennetz.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• Vermittlungsstellen (VE:F, VE:N, VE:A) • Vermittlungssysteme (z. B. EWSD oder S12) • Überwachungs- und Steuerungszentralen (NMC/NOC)	

Tabelle 23: Betriebsinterner Prozess „Betrieb PSTN“ (DL1 PS2 BP3)

Prozessbeschreibung

Das Public Switched Telephone Network (PSTN) bezeichnet die Gesamtheit der leitungsgebundenen Festnetze der analogen Telefonie. In Deutschland umfasst das PSTN damit hauptsächlich das Telefonnetz der DTAG. Andere Betreiber von Telefonnetzen (z. B. NetCologne) agieren zumeist nur im regionalen Bereich und nutzen für Verbindungen zu weit entfernten Standorten ebenfalls das Telefonnetz der Deutschen Telekom. Das PSTN wird heutzutage von klassischer analoger Festnetztelefonie, aber auch von Datenverbindungen im Zugangsnetz (z. B. DSL), genutzt.

Der Anschluss regionaler Zugangsnetze an das Kernnetz des PSTN erfolgt an regional verteilten Vermittlungsstellen (Fernvermittlungsstelle, VE:F), an welche die ortsbezogenen Hauptverteiler (Ortsvermittlungsstelle) angeschlossen sind. Die Fernvermittlungsstellen sind untereinander redundant verbunden (vermascht). Bleibt das Telefongespräch innerhalb des PSTN (z. B. Festnetz-zu-Festnetz-Telefonie), wird es zwischen den Fernvermittlungsstellen weitergeleitet und über den entsprechenden Ortsvermittlungsstellen an das Ziel übertragen.

Die Störung oder der Ausfall von Fernvermittlungsstellen hat Auswirkungen auf Endkunden, die mit den angeschlossenen Ortsvermittlungsstellen verbunden sind. Da DSL-Verbindungen (über die TAL) bereits ab der Ortsvermittlungsstelle durch ein Gateway in das Datennetz eingeleitet werden, ist bei Ausfall jedoch nur die Sprachübertragung betroffen. Daten sind weiterhin über das Datennetz übertragbar, wohingegen Sprachanrufe im PSTN nicht mehr übertragen werden können.

Eine wichtige Funktion übernimmt die Vermittlungsstelle für den Übergang zwischen verschiedenen PSTN-Netzen (Netzvermittlungsstelle, VE:N). Hier wird bei Bedarf der Übergang in andere Festnetze bereitgestellt; u. a. für Verbindungen über Landesgrenzen hinweg werden sogenannte Auslandsvermittlungseinheiten (VE:A) eingesetzt.

Die Störung oder der Ausfall der Netzvermittlungsstellen hat Auswirkung auf die Verbindungen zwischen Netzen unterschiedlicher PSTN-Betreiber.

Innerhalb der einzelnen Vermittlungsstellen werden Systeme zur Vermittlung der Sprachverbindungen eingesetzt (z. B. EWSD oder S12). Diese Systeme sind für das korrekte Vermitteln der Sprachdaten verantwortlich.

Die Störung oder der Ausfall der Vermittlungssysteme ist dem Ausfall der Vermittlungsstelle gleichgestellt. Verbindungen über die Vermittlungsstelle sind dann nicht mehr möglich.

Weiterhin verfügt das PSTN über komplexe Überwachungs- und Steuerungszentralen (NOC), die für Betrieb und Wartung der Netze essentiell sind. In diesen Steuerungszentralen ist das Betriebspersonal der Netzbetreiber u. a. Für die Fernkonfiguration von Netzwerkkomponenten, Überwachung der Lastverteilung und andere Fernwartungsaktivitäten verantwortlich.

3.1.3 Prozessschritt „Vermittlung“ (PS3)

Der Prozessschritt „Vermittlung“ (PS3) stellt die Infrastruktur zur Vermittlung von Sprache und Daten in Netzen dar. Als Dienstleister sind in diesem Prozessschritt vor allem Marktteilnehmer der Rolle „Knotenbetreiber“ involviert (dies kann auch Netzbetreiber umfassen).

Damit der Austausch zwischen Netzen unterschiedlicher Netzbetreiber, unterschiedlicher Technologien oder selbst zwischen gleichartigen Teilnetzen möglich ist, werden Knotenpunkte benötigt. Diese Knotenpunkte, auch als Points of Presence (PoP) bezeichnet, stellen Zugänge zu Netzen her und werden u. a. zum Zusammenschluss von Netzen eingesetzt. Erst der Zusammenschluss von Netzen ermöglicht die Erreichbarkeit von Kommunikationsteilnehmern unterschiedlicher Netze, Anbieter etc.

Nachfolgend werden die hierzu notwendigen Infrastrukturen als betriebsinterne Prozesse betrachtet (siehe Abbildung 14).

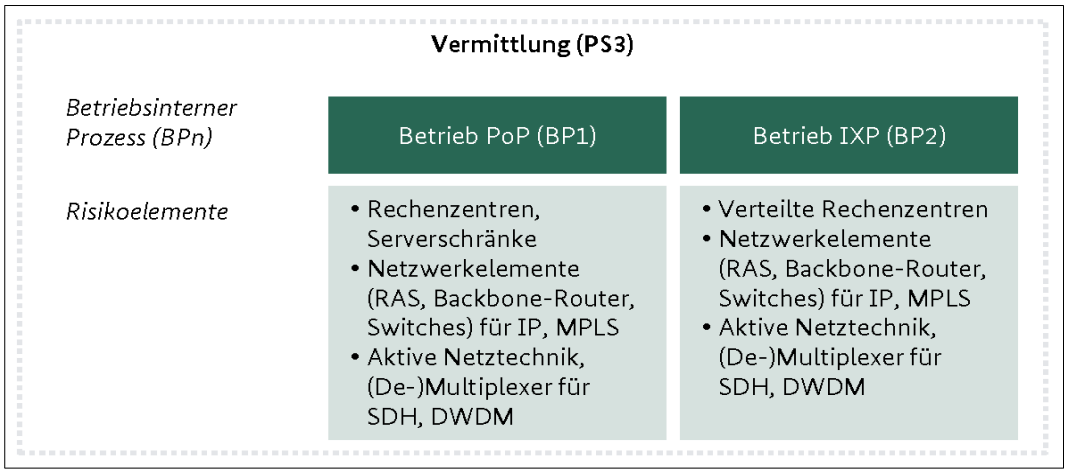

Abbildung 14: Prozessschritt „Vermittlung“ der Dienstleistung „Sprach- und Datenübertragung“

Quelle: eigene Darstellung

Für den Prozessschritt „Vermittlung“ (PS3) werden im weiteren Verlauf der Studie die folgenden betriebsinternen Prozesse betrachtet:

- **Betrieb PoP (BP1):** Betrieb von PoP-Infrastrukturen, die Zugang zu Netzen ermöglichen.
- **Betrieb IXP (BP2):** Betrieb von physischen Infrastrukturen, sogenannten Internet Exchange Points (IXPs), an denen Netzbetreiber ihre Netze untereinander zusammenschalten und somit eine netzübergreifende Kommunikation ermöglichen.

3.1.3.1 Betriebsinterner Prozess „Betrieb PoP (1:n)“

DL	PS	BP	Betrieb PoP (1:n)	
1	**3**	**1**		
Zusammenfassung			Der betriebsinterne Prozess „Betrieb PoP“ stellt den Betrieb von Infrastruktur zum Austausch von Daten zwischen Zugangsnetz/Infrastruktur und i. d. R. einem Backbone dar. Dies umfasst z. B.: Daten-, Kabel-, Mobilfunk- und leitungs-gebundenen Netzen (PoP).	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• Rechenzentren, Serverschränke • Netzwerkelemente (RAS, Backbone-Router, Switches) für IP, MPLS usw. • Aktive Netztechnik, (De-)Multiplexer für SDH, DWDM	

Tabelle 24: Betriebsinterner Prozess „Betrieb PoP (1:n)“ (DL1 PS3 BP1)

Prozessbeschreibung

Netzzugangspunkte, sogenannte Points of Presence (PoP), bieten Zugang zu Netzen. Diese Netzzugänge werden u. a. für das Zusammenschalten von Netzen bzw. für die Anbindung anderer Netze an ein Netz eingesetzt. Das kann auch die Anbindung von Endkunden an ein Netz einschließen.

PoP werden u. a. dazu verwendet, um Zugangsnetze an Kernnetze (Backbone-Netze) anzuschließen. PoP sind daher in Räumlichkeiten mit direktem Zugang zu Netzen untergebracht. Diese Räumlichkeiten können von Rechenzentren (bei größeren Netzen) bis hin zu kleinen Schaltschränken (Anbindung von Zugangsnetzen) reichen. Teilweise sind PoP auch in Repeaterstationen aufzufinden. Repeaterstationen kommen meist in Containern unter, die nahegelegen zu Glasfasertrassen zum Zweck der Signalverstärkung aufgestellt werden. Eine solche Signalverstärkung ist, in Abhängigkeit der eingesetzten Fasern und Modulationsverfahren (z. B. DWDM), im Abstand von mehreren hundert Kilometer notwendig.

Innerhalb der PoP werden verschiedene herkömmliche Netzwerkelemente (RAS, Backbone-Router, Switches) genutzt. Hinzu kommen technische Komponenten zur Wandlung elektrischer und optischer Signale (OE-Konverter) und zum Demultiplexen von Verbindungen (z. B. nach DWDM Technologie), um Anschlüsse zu einzelnen Leitungen herzustellen.

Die Störung oder der Ausfall von PoP kann zu großflächigen Störungen führen, insbesondere wenn die betroffenen PoP große Transitnetzwerke anbinden.

3.1.3.2 Betriebsinterner Prozess „Betrieb IXP (n:n)“

DL	PS	BP	Betrieb IXP (n:n)	
1	**3**	**2**		
Zusammenfassung			Der betriebsinterne Prozess „Betrieb IXP“ stellt den Betrieb von Infrastrukturen zum Zusammenschluss von mehreren Netzen unterschiedlicher Netzbetreiber an einem zentralen und gemeinsam genutzten Ort dar.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• (Verteilte) Rechenzentren • Netzwerkelemente (RAS, Backbone-Router, Switches) für IP, MPLS usw. • Aktive Netztechnik, (De-)Multiplexer für SDH, DWDM	

Tabelle 25: Betriebsinterner Prozess „Betrieb IXP (n:n)“ (DL1 PS3 BP2)

Prozessbeschreibung

Sogenannte Internet Exchange Points (IXPs) stellen Netzbetreibern Räumlichkeiten und Infrastrukturen zur Verbindung ihrer Netze zur Verfügung. Solche Internet-Knoten fungieren dabei als Schnittstelle zwischen verschiedenen Netzen. Kommerzielle Internet-Knoten werden auch *Commercial Internet Exchange* (CIX) genannt. IXPs sind in der Regel große Rechenzentren, in denen die Netzbetreiber PoP betreiben und diese nach Bedarf zusammenschalten. In den Rechenzentren erfolgt die Vermittlung durch typische Netzwerkelemente (RAS, Backbone-Router, Switches).

Der Unterschied zwischen IXPs und PoP besteht hauptsächlich in der Art des Zusammenschlusses. Ein IXP verbindet mehrere Datennetze untereinander (Vermaschung, n:n-Beziehung), wohingegen ein PoP den Zugangspunkt für die Verbindung genau eines Netzes zu verschiedenen anderen Netzen darstellt (1:n-Beziehung). Auch im Aufbau unterscheiden sich beide Knotenpunkte, da IXPs fast immer in großen (Co-Location-)Rechenzentren untergebracht sind, PoP hingegen auch nur aus einem Serverschrank bestehen können.

IXPs werden oftmals an mehreren Standorten redundant betrieben, um bei einem Ausfall möglichst geringe Auswirkungen auf die Netzverfügbarkeit auszuüben. Diese Redundanz wird untereinander teilweise durch die Nutzung von dedizierten Glasfaserleitungen realisiert, die im Notfall Datenverkehr schnell an einen zusätzlichen Standort weiterleiten können. IXPs sind damit nicht nur als einzelne Einrichtung zu sehen, sondern vielmehr als verteiltes Vermittlungsnetz zu betrachten.

Die Störung oder der Ausfall eines IXPs hat Auswirkungen auf eine große Anzahl von Kommunikationsbeziehungen, da Netzübergänge nicht mehr zur Verfügung stehen. Durch die zunehmende Zentralisierung in einigen großen IXPs (z. B. DE-CIX oder AMS-IX) hat ein Ausfall in diesen Bereichen großflächige Auswirkungen [Ryan 2012].

3.1.4 Prozessschritt „Steuerung“ (PS4)

Der Prozessschritt „Steuerung“ (PS4) stellt die Infrastruktur zur Steuerung von Kommunikationsverbindungen dar. Dies umfasst insbesondere Komponenten und Prozesse zur Signalisierung, die in den Netzen elementarer Bestandteil zum Austausch und Transfer von Sprache und Daten sind. Als Dienstleister sind in diesem Prozessschritt vor allem Marktteilnehmer der Rolle „Verwaltung“ involviert.

Nachfolgend werden die hierzu notwendigen Komponenten als betriebsinterne Prozesse betrachtet (siehe Abbildung 15).

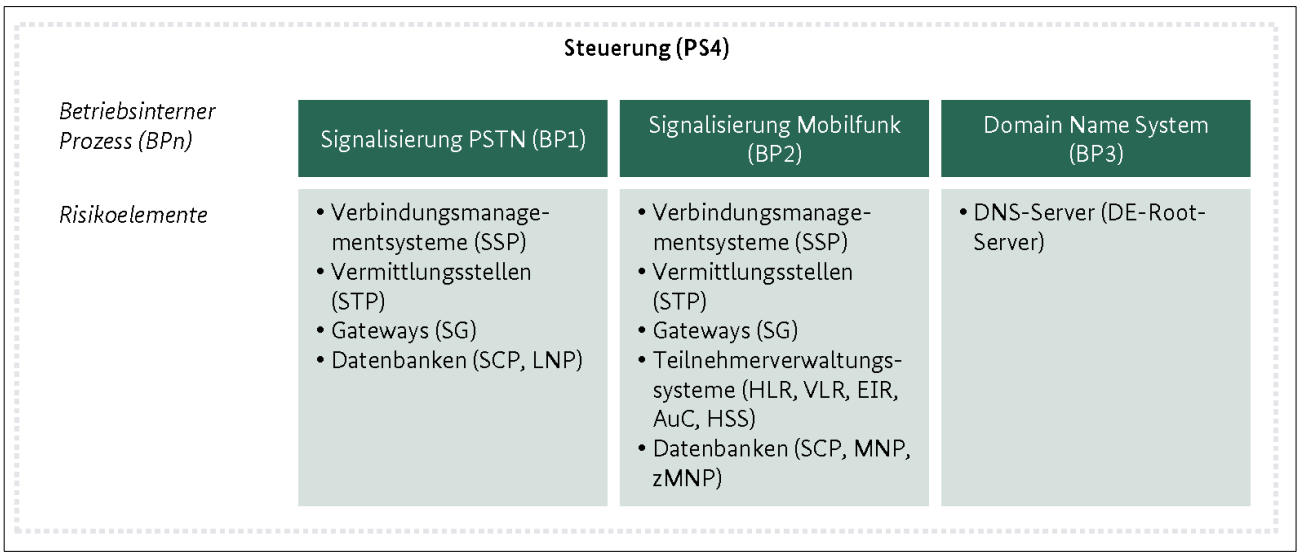

Abbildung 15: Prozessschritt „Steuerung“ der Dienstleistung „Sprach- und Datenübertragung“

Quelle: eigene Darstellung

Für den Prozessschritt „Steuerung“ (PS4) werden im weiteren Verlauf der Studie die folgenden betriebsinternen Prozesse betrachtet:

- **Signalisierung PSTN (BP1):** Betrieb von Signalisierungskomponenten und zentralen Datenbanken, welche für die Funktionsfähigkeit des PSTN von elementarer Bedeutung sind.
- **Signalisierung Mobilfunk (BP2):** Betrieb von Signalisierungskomponenten und zentralen Datenbanken, welche für den Betrieb von Mobilfunknetzen von elementarer Bedeutung sind.
- **Domain Name System (BP3):** Betrieb von DNS-Servern zur Auflösung von Hostnamen und IP-Adressen.

Die Steuerung im Datennetz wird in diesem Prozessschritt nicht gesondert aufgeführt, da diese technologisch bedingt nicht in getrennten Systemen implementiert ist (siehe Prozessschritt „Betrieb Datennetz“).

3.1.4.1 Betriebsinterner Prozess „Signalisierung PSTN“

DL	PS	BP	Signalisierung PSTN	
1	**4**	**1**		
Zusammenfassung			Der betriebsinterne Prozess „Signalisierung PSTN“ stellt die korrekte Signalisierung (d. h. Verbindungsherstellung, -weiterleitung, -beendigung) von Telefongesprächen im PSTN sicher.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• Verbindungsmanagementsysteme (SSP) • Vermittlungsstellen (STP) • Gateways (SG) • Datenbanken (SCP, LNP)	

Tabelle 26: Betriebsinterner Prozess „Signalisierung PSTN“ (DL1 PS4 BP1)

Prozessbeschreibung

Im deutschen PSTN ist hierfür ein dediziertes Signalisierungsnetz in Betrieb, das auf Basis des Signalisierungssystems 7 (SS7) arbeitet. SS7 umfasst eine Vielzahl von Komponenten und Protokollen. Diese Komponenten werden als Signalisierungspunkte (engl. Signaling Points, SPs) bezeichnet und übernehmen Teilfunktionen im Signalisierungsnetz. Ein Beispiel hierfür ist der Service Switching Point (SSP), eine Komponente, die für Aufbau, Verwaltung und Terminierung von Gesprächen zuständig ist. Eine Funktion der Signalisierungspunkte ist die Terminierung und Originierung im Zugangsnetz (SSP), die für den korrekten Verbindungsaufbau und die Weiterleitung innerhalb des PSTNs verantwortlich sind.

Die Störung oder der Ausfall der Terminierung und Originierung hat Auswirkungen auf Kunden, deren Telefongespräche über den betroffenen SP gesteuert werden.

Vermittlungsstellen im Signalisierungsnetz (Signalling Transfer Point, STP) ermöglichen den Austausch von Daten im Kernnetz des SS7 sowie die Weiterleitung von Signalisierungsdaten in andere Netze.

Die Störung oder der Ausfall der Vermittlungsstellen im Signalisierungsnetz hat lediglich Auswirkungen auf einige Kunden. Anschlüsse im Zuständigkeitsbereich der Vermittlungsstelle sind nicht mehr erreichbar.

Im Signalisierungsnetz eingebundene Datenbanken (SCPs) ermitteln die optimale Transportroute für das Telefongespräch und kommunizieren diese an die Vermittlungsstellen. Eine wichtige Datenbank im Signalisierungsnetz ist die Rufnummermitnahmedatenbank (LNP), durch die Telefonnummern nicht mehr örtlich gebunden sind.

Die Störung oder der Ausfall der Datenbanken hat Auswirkungen auf sämtliche Kunden des PSTNs. Dies könnte zum Beispiel durch falsche Vermittlung oder durch nicht-optimale Verbindungswege hervorgerufen werden.

Netzübergange vom PSTN in das Datennetz, z. B. beim Anrufen von VoIP-Anschlüssen (von einem Analoganschluss aus), werden über Gateways signalisiert (SGs). Hier erfolgt eine Wandlung der SS7-

Steuerungsbefehle in ein für das Internet Protokoll (IP)[29] kompatibles Format, um eine Weitervermittlung innerhalb des Datennetzes zu ermöglichen.[30]

29 Unter Einsatz des Stream Control Transmission Protocols (SCTP).

30 Im weiteren Verlauf einer Verbindung werden die SS7-Steuerungsbefehle in das SIP-Protokoll überführt und bei Austritt aus dem Datennetz wieder auf SS7-Basis zurückkonvertiert.

3.1.4.2 Betriebsinterner Prozess „Signalisierung Mobilfunk“

DL	PS	BP	Signalisierung Mobilfunk	
1	**4**	**2**		
Zusammenfassung			Der betriebsinterne Prozess „Signalisierung Mobilfunk“ stellt die korrekte Signalisierung (u. a. zur Verbindungsherstellung, -weiterleitung, -beendigung) von Telefongesprächen im Mobilfunknetz sicher.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• Verbindungsmanagementsysteme (SSP) • Vermittlungsstellen (STP) • Gateways (SG) • Teilnehmerverwaltungssysteme (HLR, VLR, EIR, AuC, HSS) • Datenbanken (SCP, MNP, zMNP)	

Tabelle 27: Betriebsinterner Prozess „Signalisierung Mobilfunk“ (DL1 PS4 BP2)

Prozessbeschreibung

In den Mobilfunknetzen ist hierfür ein dediziertes Signalisierungsnetz in Betrieb, das auf Basis des Signalisierungssystems 7 (SS7) und der darin enthaltenen Signalisierungspunkte arbeitet. SS7 umfasst eine Vielzahl von Komponenten und Protokollen.

Die Störung oder der Ausfall einzelner Signalisierungspunkte hat, je nach Redundanz des Systems, Auswirkungen auf eine Vielzahl an Telefongesprächen, die über die jeweiligen Signalisierungspunkte gesteuert werden.

Vermittlungsknoten im Signalisierungsnetz (STPs) ermöglichen den Austausch von Signalisierungsdaten zwischen einzelnen Netzelementen.

Die Störung oder der Ausfall von Vermittlungsknoten im Signalisierungsnetz hat, je nach Redundanz des Systems, Auswirkungen auf eine Vielzahl an Kunden.

Zur Bereitstellung von Mehrwertfunktionen wie z. B. der Übertragung der eigenen Rufnummer zum Angerufenen oder dem Halten von Mehrteilnehmergesprächen werden sogenannte Service Control Points (SCP) eingesetzt. Die SCP agieren direkt mit den Systemen zur Teilnehmerverwaltung (HLR, VLR, EIR, AuC, HSS). Die Teilnehmerverwaltung wird u. a. für die Registrierung und Lokalisierung von Mobilfunkteilnehmern im Netz benötigt.

Weiterhin werden auch im Mobilfunknetz seit Einführung der Rufnummernmitnahme beim Wechsel des Anbieters Komponenten benötigt, die die Zuweisung von Rufnummern zu Anbietern vorhalten. Eine wichtige Komponente ist die Mobile Number Portability Datenbank (MNP). In Deutschland wird eine zentralisierte MNP-Datenbank genutzt, um die Portierung von Rufnummern zwischen Mobilfunkanbietern zu realisieren.

Die Störung oder der Ausfall der MNP-Datenbanken und Systeme der Teilnehmerverwaltung kann Auswirkungen auf einen Großteil der Mobilfunk-Teilnehmer des jeweiligen Mobilfunknetzbetreibers haben. Das Ausmaß des Ausfalles hängt stark von der jeweiligen Komponente ab; so würden bei einem Ausfall der MNP nur solche Teilnehmer beeinträchtigt werden, die ihre Nummer portiert haben. Fällt hingegen ein System der Teilnehmerverwaltung aus, sind alle Teilnehmer davon betroffen.

Netzübergange vom Mobilfunknetz in das Datennetz, z. B. bei Anrufen an VoIP-Anschlüsse, werden über Gateways signalisiert (SGs). Hier erfolgt eine Wandlung der SS7-Steuerungsbefehle auf IP, um eine Weitervermittlung innerhalb des Datennetzes zu ermöglichen [BNetzA 2014a].

3.1.4.3 Betriebsinterner Prozess „Domain Name System“

DL	PS	BP	Domain Name System	
1	**4**	**3**		
Zusammenfassung			Betrieb von DNS-Servern zur Auflösung von Hostnamen und IP-Adressen durch DNS-Rootserver.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• DNS-Server (DE-Rootserver)	

Tabelle 28: Betriebsinterner Prozess Domain Name System (DL1 PS4 BP3)

Prozessbeschreibung

Das Domain Name System (DNS) ist hierarchisch aufgebaut. In Deutschland werden die Verbindungsdaten der Top-Level-Domain „.de“ in den hierarchisch höchsten DNS-Knoten, den DE-Rootservern, verwaltet. Diese Rootserver agieren als zentrale Datenbank und haben autoritativen Charakter für hierarchisch niedrigere DNS-Server (Referenzpunkt für andere DNS-Server). Nicht-autoritative DNS-Server speichern die Daten der Rootserver anderer DNS-Server und spiegeln die Einträge, aktualisieren die Daten jedoch in zeitlichen Abständen durch Abfrage der Rootserver. Wie oft und wann eine solche Aktualisierung stattfindet, hängt vom jeweiligen DNS-Server und seiner Sicherheits-Policy ab. Standardmäßig wird ein Eintrag nach spätestens 24 Stunden erneuert, teilweise bestehen jedoch auch Zeiten von lediglich einigen hundert Sekunden.[31]

Die Störung oder der Ausfall des DE-Rootservers kann Auswirkungen auf die Erreichbarkeit von Domains unter der Top-Level-Domain „.de“ haben.

31 Die Zeit bis zur Aktualisierung wird als time-to-live (TTL) bezeichnet und bei jeder Abfrage vom Rootserver übertragen. Sie wird in Sekunden angegeben und als 32-Bit-Wert zu jedem DNS-Eintrag im Cache gespeichert.

3.2 Datenspeicherung und -verarbeitung (DL2)

Die kritische Dienstleistung „Datenspeicherung und -verarbeitung“ stellt die technische Basisinfrastruktur zur Speicherung und Verarbeitung von Daten für Dritte bereit. Die Dienstleistung wird durch die Marktteilnehmer in den Rollen „IT-Hoster“ und „Rechenzentrumsbetreiber“ des KRITIS-Sektors IKT angeboten und durch die deutsche Gesellschaft, Privatwirtschaft und öffentliche Hand für vielfältige Dienste genutzt. Eine wichtige Dienstleistung ist die Bereitstellung von Infrastrukturen für Dienste wie das Hosting von Anwendungen und Webseiten, Internetsuche und E-Mail-Dienste.

Die Bereitstellung der Infrastruktur für die Datenspeicherung und -verarbeitung besteht aus technisch und logisch komplexen Vorgängen, die diese Studie zur Analyse kritischer Zusammenhänge und Abhängigkeiten in logische Teilbereiche, sogenannte Prozessschritte, unterteilt (siehe Abbildung 16). Jeder Prozessschritt leistet einen wesentlichen Beitrag zur Erbringung der Dienstleistung und beeinträchtigt bei Störung oder Ausfall die gesamte Dienstleistung.

Zudem nutzen Betreiber von Internetdiensten teilweise die Infrastruktur von IT-Hostern zur Bereitstellung von wichtigen und beliebten Internetdiensten wie z. B. E-Mail, Internetsuche und Web-Hosting. Diese Bereitstellung ist maßgeblich von den betriebsinternen Prozessen beider kritischen Dienstleistungen abhängig.

Für die Dienstleistung „Datenspeicherung und -verarbeitung“ werden im weiteren Verlauf der Studie die folgenden Prozessschritte betrachtet:

- **Betrieb Rechenzentrum (Housing) (PS1):** Betreiber von Rechenzentren betreiben Einrichtungen und Infrastrukturen zur Datenverarbeitung für Dritte, in denen technisches Equipment und IT-Systeme, z. B. von Netzbetreibern oder anderen Unternehmen, betrieben werden.
- **Betrieb IT-Hosting (PS2):** IT-Hoster betreiben Einrichtungen und Infrastrukturen zur Datenverarbeitung für Dritte in Form von Server-Systemen, die an Kunden vermietet werden, welche ihre Anwendungen auf den Servern ausführen (sogenanntes Hosting).

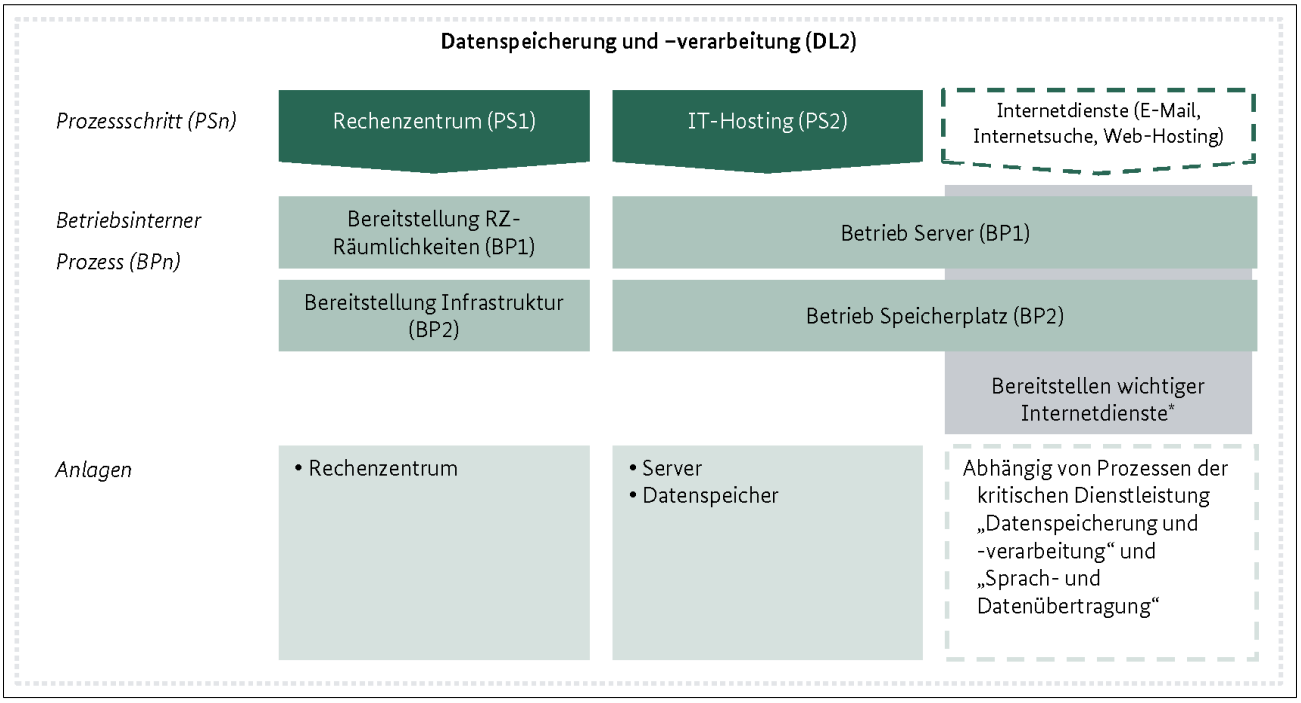

Abbildung 16: Schematische Darstellung der kritischen Dienstleistung „Datenspeicherung und -verarbeitung“

Quelle: eigene Darstellung

Ausfall der Datenspeicherung und -verarbeitung

Ein Ausfall der Datenspeicherung und -verarbeitung kann vielfältige Ursachen haben, die aufgrund der Komplexität und der Wechselwirkungen der verbundenen Rechenzentren wiederum unterschiedliche Folgen nach sich ziehen können.

Mögliche Ursachen können zum Beispiel sein:

- **Technisches Versagen**: Ausfälle der Datenspeicherung und -verarbeitung verursacht durch Ausfall oder technisches Fehlverhalten von Infrastrukturkomponenten
- **Menschliches Versagen**: Ausfälle der Datenspeicherung und -verarbeitung verursacht durch menschliches Fehlverhalten, etwa bei großflächigen Konfigurationsänderungen in Infrastrukturkomponenten
- **Kriminelle oder terroristische Handlungen**: Ausfälle der Datenspeicherung und -verarbeitung verursacht durch absichtliche Manipulationen oder Cyber-Angriffe auf Infrastrukturkomponenten

Unter dem Begriff „Ausfall" werden im Folgenden ein vollständiger Ausfall der Dienstleistung, eine gravierende Störung der Dienstleistung mit konkreten Folgen oder die Zerstörung von Infrastrukturen (meist verbunden mit Ausfällen) verstanden.

Exemplarisch seien an dieser Stelle einige Ausfall-Szenarien aufgeführt:

- Durch fehlerhafte Konfiguration wichtiger Infrastrukturkomponenten innerhalb der Rechenzentren kann ein Komplettausfall der Dienstleistung auftreten. Dabei erfolgt ein Komplettausfall meist dann, wenn zentrale Elemente der Rechenzentrumsinfrastruktur von Fehlern betroffen sind. So zum Beispiel beim Ausfall im Rechenzentrum von 1 & 1 am 26. November 2012; dort hatten Fehlfunktionen im internen Routing-System zu stundenlangen Ausfällen geführt [1&1 2012].
- Ein Stromausfall kann zu erheblichen Störungen in der Bereitstellung der Dienstleistung führen. Zwar sind viele der Rechenzentren großer Betreiber mit Notfallkomponenten ausgestattet (z. B. Notstromaggregate), diese liefern Ersatzstrom im Bedarfsfall jedoch oftmals nur für eine bestimmte Zeit und sind bei schlechter Wartung u. U. nicht voll funktionsfähig. So kam es 2012 beim französischen Rechenzentrumsbetreiber Intergenia zu einem Stromausfall, in dessen Folge zwar das Notstromaggregat startete, die Kühlsysteme jedoch nicht auf den Notstrom geschaltet wurden. Aufgrund der ansteigenden Temperatur wurden die IT-Systeme im Rechenzentrum automatisch heruntergefahren und waren nicht mehr erreichbar.
- Gehostete Anwendungen in Rechenzentren sind zudem häufig Ziel für Angriffe von Externen. Insbesondere DDoS-Angriffe gehören zu einer weitverbreiteten Angriffsart. So zum Beispiel auch beim Betreiber 1 & 1 am 27. Januar 2011, bei dem teilweise die eigenen Portale des Unternehmens nicht mehr erreichbar waren. Aber auch gezielte Hacking-Angriffe gegen Rechenzentren werden öfter registriert. So zum Beispiel der Angriff eines 18-jährigen Schülers auf das Landesrechenzentrum von Sachsen-Anhalt im September 2013 [HA 2013].
- Bei der Zerstörung von Infrastruktur oder ganzen Rechenzentren kann es zu einem langfristigen Ausfall der Dienstleistung kommen. Insbesondere Rechenzentren, in denen Server betrieben werden, die nicht zusätzlich an einem anderen Standort redundant betrieben werden, sind bei einer Zerstörung einem kompletten Datenverlust ausgesetzt. Im Rechenzentrum des US-amerikanischen Nachrichtendienstes NSA war vor Inbetriebnahme durch Blitzeinschläge wichtige Technik zerstört worden. Dadurch verzögerte sich die Inbetriebnahme des Rechenzentrums um mehr als ein Jahr [Welt 2013].

Folgen eines Ausfalls der Datenspeicherung und -verarbeitung

Die Folgen eines Ausfalls der Datenspeicherung und -verarbeitung unterscheiden sich in den einzelnen Teilen der Gesellschaft:

- Die **Bevölkerung** ist durch einen großflächigen Ausfall der Dienstleistung unmittelbar betroffen. Gerade durch die tägliche Nutzung wichtiger Internet-Dienste wäre ein Ausfall bemerkbar. Da gängige Internet-

Dienste in der Regel redundant konzipiert und mit redundantem Equipment an verschiedenen Standorten betrieben werden, hat ein Ausfall einzelner Rechenzentren/Server jedoch keine schwerwiegenden Folgen.

- Für die **Wirtschaft** ist bei einem Ausfall der Datenspeicherung und -verarbeitung von finanziellen Auswirkungen auszugehen. Unternehmen nutzen Dienste von IT-Hostern und Rechenzentrumsbetreibern, um ihre eigene IT betreiben zu lassen. Durch das komplexe Zusammenspiel zwischen Geschäftsprozessen und der IT (insbesondere den Anwendungen) könnten viele Leistungen nicht erbracht werden.
- Auch der **Staat** ist von einem Ausfall der Datenspeicherung und -verarbeitung betroffen. Die öffentliche Verwaltung nutzt jedoch größtenteils landes- bzw. bundeseigene Rechenzentren und IT-Dienstleister um verschiedene Anwendungen der öffentlichen Verwaltung zu betreiben. Bei einem Ausfall können Bürger diese Dienste nicht mehr nutzen und wichtige Tätigkeiten der Verwaltung können durch die öffentliche Hand nicht mehr wahrgenommen werden.

3.2.1 Prozessschritt „Rechenzentrum (Housing)“ (PS1)

Der Prozessschritt „Rechenzentrum (Housing)“ beschreibt den Betrieb von Einrichtungen und Infrastrukturen in denen technisches Equipment und IT-Systeme zur Datenverarbeitung für Dritte (z. B. Gesellschaft, öffentliche Hand, Wirtschaft), z. B. von Netzbetreibern oder anderen Unternehmen, betrieben werden. Als Dienstleister sind in diesem Prozessschritt vor allem Marktteilnehmer der Rolle „Rechenzentrumsbetreiber“ involviert, aber auch „Netzbetreiber“ und „Vermittlungsstellen“ bieten solche Dienste an.

Genutzt wird diese Dienstleistung durch unterschiedliche Endkunden. Im Fall von Co-Location insbesondere durch die Netzbetreiber und Knotenbetreiber. Daher sind IXP meist in Rechenzentren untergebracht. Die Unterbringung von Servern und Datenspeichern bei einem Rechenzentrumsbetreiber wird jedoch auch von Organisationen anderer Wirtschaftsbereiche genutzt.

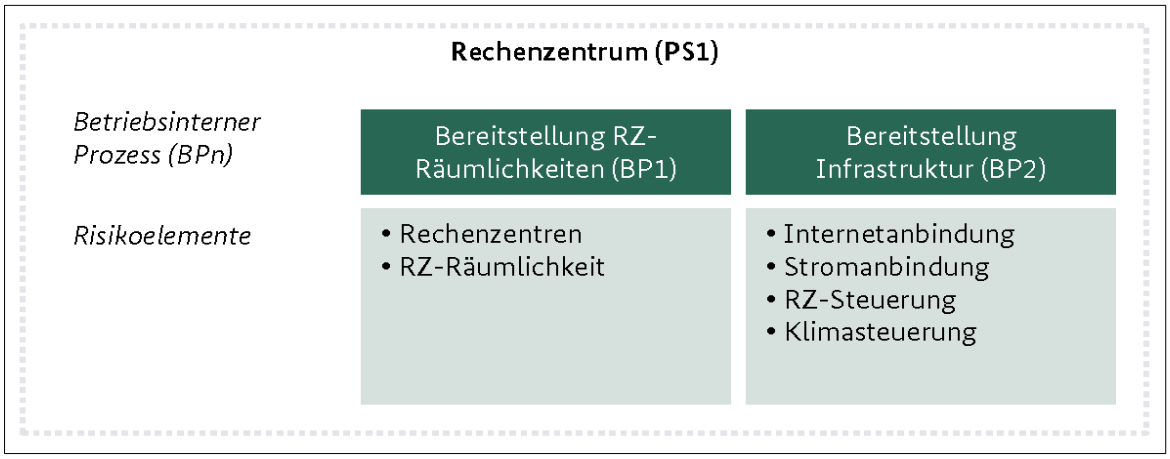

Abbildung 17: Prozessschritt „Rechenzentrum“ der Dienstleistung „Datenspeicherung und -verarbeitung“

Quelle: eigene Darstellung

Für den Prozessschritt „Rechenzentrumsbetrieb (Housing)“ (PS1) werden im weiteren Verlauf der Studie die folgenden betriebsinternen Prozesse betrachtet:

- **Bereitstellung RZ-Räumlichkeiten (BP1):** Stellt die Bereitstellung von Räumlichkeiten zur Unterbringung von Servern und Datenspeichern von Externen sicher.
- **Bereitstellung Infrastruktur (BP2):** Stellt sicher, dass die Räumlichkeiten mit entsprechender Infrastruktur (Strom, Kühlung, Internetanbindung, Netzwerk) versorgt sind.

3.2.1.1 Betriebsinterner Prozess „Bereitstellung RZ-Räumlichkeiten“

DL	PS	BP	Bereitstellung RZ-Räumlichkeiten	
2	**1**	**1**		
Zusammenfassung			Der betriebsinterne Prozess „Bereitstellung RZ-Räumlichkeiten“ stellt die Bereitstellung von Räumlichkeiten zur Unterbringung von Servern und Datenspeichern von Dritten sicher.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• Rechenzentrum • RZ-Räumlichkeit	

Tabelle 29: Betriebsinterner Prozess „Bereitstellung RZ-Räumlichkeiten“ (DL2 PS1 BP1)

Prozessbeschreibung

Die Bereitstellung umfasst die Planung und Konzeption, die Umsetzung, den Betrieb und die Notfallvorsorge von Rechenzentren.

Innerhalb von Rechenzentren erhalten Kunden Stellfläche zum Aufbau und Betrieb ihres IT-Equipments. Oft vermieten Rechenzentrumsbetreiber auch einzelne Serverschränken (Racks) an Kunden. Einzelne Räume, Kundenstellflächen und Serverschränke innerhalb eines Rechenzentrums sind in der Regel jeweils durch Zutrittskontrollen (z. B. Schloss, elektronische Zutrittskartenleser) vor unbefugtem Zugang gesichert.

Auch Maßnahmen zur Notfallvorsorge gehören zur Planung und Betrieb von Rechenzentren. Dazu gehören etwa die Einrichtung von Brandabschnitten, physische Sicherheitskontrollen und Überwachung.

Ein Ausfall oder eine Störung der Bereitstellung von RZ-Räumlichkeiten hat zur Folge, dass keine Hardware im Rechenzentrum untergebracht und betrieben werden kann und folglich auch der Prozessschritt nicht abgeschlossen werden kann.

3.2.1.2 Betriebsinterner Prozess „Bereitstellung Infrastruktur“

DL	PS	BP	Bereitstellung Infrastruktur	
2	**1**	**2**		
Zusammenfassung			Der betriebsinterne Prozess „Bereitstellung Infrastruktur“ stellt sicher, dass die Räumlichkeiten der Rechenzentren mit entsprechender Infrastruktur (Strom, Kühlung, Internetanbindung, Netzwerk) versorgt sind.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• Internetanbindung • Stromanbindung • RZ-Steuerung • Klimasteuerung	

Tabelle 30: Betriebsinterner Prozess „Bereitstellung Infrastruktur“ (DL2 PS1 BP2)

Prozessbeschreibung

Innerhalb von Rechenzentren werden grundlegende Infrastrukturdienstleistungen bereitgestellt, die zum Betrieb der untergebrachten Server und Datenspeicher notwendig sind. Hierzu zählen insbesondere Strom und Kühlung sowie die Möglichkeit zur Vernetzung der Systeme und der Anbindung an das Internet.

Die Stromversorgung als maßgebliches Element der Erbringung des Prozesses ist hohen Anforderungen ausgesetzt. Je nach Klassifizierung und Service Level bestehen in den Rechenzentren hier unterschiedliche Lösungen. Als grundlegendes Element kann eine Notstromversorgung bei einem Rechenzentrum vorausgesetzt werden, die bei Problemen mit der externen Stromversorgung für eine konstant verfügbare Stromversorgung sorgt. Deshalb verfügen Rechenzentren im Normalfall über batteriebasierte Stromreserven und/oder Notstromaggregate (z. B. Dieselgeneratoren).

Aufgrund der Abwärme elektronischer Geräte ist das IT-Equipment (Server, Datenspeicher) in Rechenzentren auf eine konstante Kühlung angewiesen. Der Betrieb der dafür notwendigen technischen Systeme obliegt im Regelfall dem Rechenzentrumsbetreiber.

Ein Ausfall oder eine Störung der Bereitstellung von Infrastruktur hat zur Folge, dass die untergebrachten Server und Datenspeicher ihre Dienste nicht mehr erbringen können, da sie z. B. Aufgrund fehlender Stromversorgung oder Kühlung nicht betriebsfähig sind oder vom Internet aus nicht erreichbar sind.

3.2.2 Prozessschritt „IT-Hosting“ (PS2)

Der Prozessschritt „IT-Hosting“ beschreibt den Betrieb von Einrichtungen und Infrastrukturen zur Datenverarbeitung für Dritte (z. B. Gesellschaft, öffentliche Hand, Wirtschaft), wobei IT-Hoster eigene IT-Systeme an Kunden vermieten (sogenanntes Hosting). Als Dienstleister sind in diesem Prozessschritt vor allem Marktteilnehmer der Rolle „IT-Hoster“ involviert.

IT-Hoster stellen ihre Dienstleistungen Dritten zur Verfügung, um Anwendungen, Datenarchive oder ganze Plattformen extern betreiben zu lassen. Auch für private Endkunden stellen die IT-Hoster Dienste zur Verfügung, die sie z. B. über Internetportale anbieten. Auch wichtige Internetdienste (Firmen-E-Mail und Hosting von Webseiten) werden durch IT-Hoster betrieben.

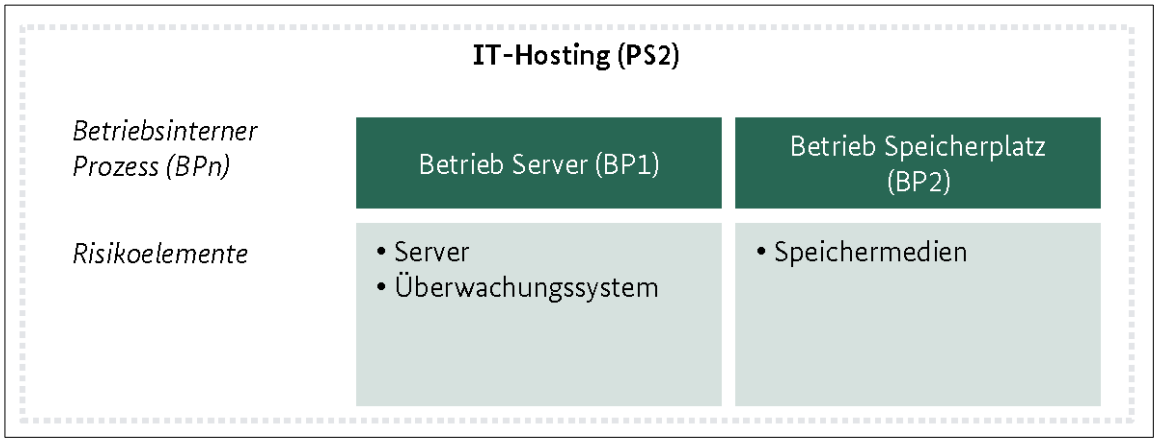

Abbildung 18: Prozessschritt „IT-Hosting“ der Dienstleistung „Datenspeicherung und -verarbeitung“

Quelle: eigene Darstellung

Für den Prozessschritt „IT-Hosting“ (PS2) werden im weiteren Verlauf der Studie die folgenden betriebsinternen Prozesse betrachtet:

- **Betrieb Server (BP1):** Stellt die Planung, den Betrieb und die Überwachung (Monitoring) der Servern von IT-Hostern sicher.
- **Betrieb Speicherplatz (BP2):** Stellt die Planung, den Betrieb und die Überwachung (Monitoring) der Datenspeicher von IT-Hostern sicher.

3.2.2.1 Betriebsinterner Prozess „Betrieb Server“

DL	PS	BP	Betrieb Server	
2	**2**	**1**		
Zusammenfassung			Der betriebsinterne Prozess „Betrieb Server“ stellt Planung, Betrieb und Überwachung (Monitoring) von Diensten und Servern dar.	
Abhängigkeit Logistik			unwesentlich	wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.	
Risikoelemente (IKT)			• Server • Überwachungssysteme	

Tabelle 31: Betriebsinterner Prozess „Betrieb Server“ (DL2 PS2 BP1)

Prozessbeschreibung

IT-Hoster betreiben Systeme, um diese Dritten zum Betrieb ihrer Anwendungen und Dienste zur Verfügung zu stellen. Die Wertschöpfung im IT-Hosting kann dabei unterschiedlich ausgeprägt sein. Hoster können z. B. nur die Hardware betrieben, falls Kunden das Betriebssystem und die Anwendungsprogramme selbst verantworten möchten. Ebenso gibt es Anwendungsfälle, in denen Hoster Hardware, Betriebssystem und Anwendungsprogramme (z. B. einen Webserver) betreiben und Kunden nur Teile dessen zur Verfügung stellen (z. B. um eine Webseite zu betreiben).

Neben dem Betrieb der eigentlichen Systeme gehören auch die Mandantentrennung, der Betrieb der Netzwerk-/Internetanbindung und die Überwachung (Monitoring) der Systeme zum Aufgabengebiet von IT-Hostern.

Ein Ausfall oder eine Störung des Betriebs von Servern kann zur kompletten Nicht-Erreichbarkeit der darauf laufenden Dienste führen.

3.2.2.2 Betriebsinterner Prozess „Betrieb Speicherplatz“

DL	PS	BP	Betrieb Speicherplatz
2	**2**	**2**	
Zusammenfassung			Der betriebsinterne Prozess „Betrieb Speicherplatz“ stellt die Planung, den Betrieb und die Überwachung (Monitoring) von Speicherplatz dar.
Abhängigkeit Logistik			unwesentlich / wesentlich (KRITIS-relevant)
			Es bestehen nur indirekte Abhängigkeiten vom Sektor Logistik. Bei der Wartung von Systemen nutzen die Betreiber vorrätige Ersatzteile. Sollte ein Ersatzteil nicht vorhanden sein, so muss dieses bestellt und geliefert werden.
Risikoelemente (IKT)			• Speichermedien

Tabelle 32: Betriebsinterner Prozess „Betrieb Speicherplatz“ (DL2 PS2 BP2)

Prozessbeschreibung

Die Bereitstellung von Datenspeichern erfolgt insbesondere für Endkunden, die große Datenmengen speichern. So bieten IT-Hoster z. B. Archivierungsdienstleistungen an oder hosten Datenbestände von Datenbanken ihrer Kunden.

Die von IT-Hostern betriebenen Datenspeicher verfügen im Normalfall über eine Netzwerkschnittstelle und sind durch Schutzmechanismen vor Integritätsschäden und Datenverlust geschützt.

Ein Ausfall oder eine Störung des Betriebs von Speicherplatz kann zur zeitweisen Nicht-Verfügbarkeit oder dem Verlust der auf den Speichermedien gesicherten Daten führen.

4 Vorfallsammlung

Der Sektor Informationstechnik und Telekommunikation erfährt eine steigende Zahl von Sicherheitsvorfällen im Bereich IT. In diesem Kapitel werden in der Vergangenheit aufgetretene Vorfälle aufgeführt, die durch IT-Versagen oder IT-Angriffe hervorgerufen wurden. Dabei handelt es sich sowohl um Vorfälle nationaler als auch internationaler Bedeutung. Die aufgeführten Sicherheitsvorfälle stellen eine Auswahl von bekannten Fällen dar, die zur Verdeutlichung der Auswirkungen auf kritische Dienstleistungen dienen sollen und sich zur Sensibilisierung eignen.

Um der Tatsache Rechnung zu tragen, dass eine trennscharfe Kategorisierung der Eigenschaften der gesammelten Vorfälle nicht immer möglich ist, werden die Vorfälle jeweils konsolidiert in einer Tabelle dargelegt. Jeder Vorfall wird mit einem individuellen Titel bezeichnet und mit einer Identifikationsnummer (ID) versehen. Anhand dieser ist eine Zuordnung der einzelnen Attribute zu einem bestimmten Vorfall möglich.

Zu den gesammelten Vorfällen liegt, sofern dies konkret möglich ist, eine Zuordnung zu der jeweiligen vom Vorfall betroffenen Kritische Dienstleistung (DL) aus dem Sektor, dem jeweiligen Prozessschritt der kritischen Dienstleistung (PS) und dem jeweiligen betriebsinternen Prozess der kritischen Dienstleistung (BP) vor.

Die Auswirkungen auf die betroffene kritische Dienstleistung besitzen je nach Sicherheitsvorfall einen individuellen Schweregrad. Zur Einschätzung der Schwere eines Sicherheitsvorfalls werden die ermittelten Sicherheitsvorfälle mithilfe der drei Klassen „hohe Auswirkungen“, „mittlere Auswirkungen“ und „geringe Auswirkungen“ bewertet. Die Definition der Klassen ist dabei wie folgt:

- **Hohe Auswirkungen**
  Ein Vorfall, bei dem offiziellen Angaben zufolge ein großer Schaden oder Ausfall der Dienstleistungen eingetreten ist.
- **Mittlere Auswirkungen**
  Ein Vorfall, bei dem offiziellen Angaben zufolge kein schwerwiegender Schaden eingetreten ist, der jedoch zu einem Schaden mit hohen Auswirkungen hätte führen können.
- **Geringe Auswirkungen**
  Ein Vorfall, bei dem offiziellen Angaben zufolge kein oder geringer Schaden eingetreten ist.

Bei den gesammelten Vorfällen sind in vielen Fällen konkrete Anlagen bzw. IKT-Risikoelemente im Zusammenhang mit dem betriebsinternen Prozess der kritischen Dienstleistung betroffen. Diese werden benannt, sofern eine solche Zuordnung möglich ist.

Wenn die Reaktion (technisch oder nicht-technisch) der betroffenen Betreiber bekannt ist, wird diese ebenfalls aufgeführt. Einige Vorfälle führten zu Reaktionen (technisch oder nicht-technisch) innerhalb des betroffenen Sektors bzw. der Branche. Diese werden, soweit identifiziert, dargestellt. Zum Teil können zudem Reaktionen von beteiligten Behörden aufgeführt werden. Diese beziehen sich auf organisatorische oder regulatorische Maßnahmen, unter anderem in Form von Veröffentlichungen von Handlungsempfehlungen oder gar Gesetzen und Verordnungen.

Nachfolgend ist die Struktur der Vorfallbeschreibungen zusammenfassend erläutert. Daraus geht die konkrete Zuordnung der vorgenannten Eigenschaften der Vorfälle zu den Feldern in den Tabellen hervor.

Die Beschreibung der Vorfälle erfolgt anhand öffentlich zugänglicher Daten und Informationen. Unterschiede hinsichtlich des Detailgrades sind darauf zurückzuführen. Das Vorfalldatum („Aktualität“) variiert ebenfalls je nach Datenverfügbarkeit.

Zellentitel	Inhalt
ID	Identifikationsnummer des Vorfalls
Titel des Vorfalls	Titel des Vorfalls
DL	Gegebenenfalls Nummer der betroffenen kritischen Dienstleistung aus dem Sektor
PS	Gegebenenfalls Nummer des betroffenen Prozessschritts der betroffenen kritischen Dienstleistung
BP	Gegebenenfalls Nummer des betroffenen betriebsinternen Prozesses der betroffenen kritischen Dienstleistung
Aktualität	Datierung der Quelle des Vorfalls
Herkunft	Nationaler oder internationaler Ursprung des Vorfalls
Grad der Auswirkung auf die kritische DL	Kategorisierung der Auswirkung des Vorfalls auf die Verfügbarkeit der kritischen Dienstleistung des Betreibers anhand der Kategorien „hohe Auswirkung“, „mittlere Auswirkung“ und „niedrige Auswirkung“
Anlagen	Gegebenenfalls Abbildung der betroffenen Anlagen der Prozessschritte der kritischen Dienstleistung
Risikoelemente	Gegebenenfalls Darlegung der betroffenen Risikoelemente des betroffenen betriebsinternen Prozess der Prozessschritte
Vorfallkurzbeschreibung	Kurze Darstellung des Hergangs und Kontextes des beschriebenen Vorfalls
Einfluss auf Versorgungsdienstleistung	Darstellung des Einflusses des Vorfalls auf die betroffene kritische Dienstleistung
Reaktion Betreiber	Darstellung der Reaktionen des Betreibers auf den konkreten Sachverhalt des Vorfalls
Reaktion beteiligte Behörde	Darstellung der Reaktionen von Behörden bzw. Institutionen aufgrund des konkreten Sachverhalts des Vorfalls
Auswirkungen Sektor/Branche	Darstellung der Auswirkungen auf den Sektor bzw. die Branche des Betreibers aufgrund des konkreten Sachverhalts des Vorfalls
Quellen	Angabe der Quelle(n) des Vorfalls und Datum des Quellenabrufs

Tabelle 33: Überblick der Eigenschaften der gesammelten Vorfälle

4.1 Nationale Vorfälle

Die BNetzA definiert im Rahmen der Meldepflichten von Betreibern im Umsetzungskonzept zu § 109 Absatz 5 TKG Sicherheitsvorfälle mit „eindeutig beträchtlichen Auswirkungen“, wenn mindestens der Schwellwert von „drei Millionen [...] betroffenen Nutzerstunden“ überschritten wird. Weitere Kriterien für Sicherheitsverletzungen und Vorfälle, die zu Meldepflichten führen können oder sollen, sind nach dem Umsetzungskonzept [BNetzA 2013b] die Folgenden:

- Betroffene Nutzerstunden (Produkt aus betroffenen Anschlüssen/Teilnehmern und Ausfalldauer in Stunden);
- Auswirkung auf Zusammenschaltung (Interconnection);
- Beeinflussung von TK-Netzen, TK-Diensten oder technischer Ausrüstung in anderen Ländern;
- Geografische Ausbreitung/Region;
- Auswirkung auf den Notruf;
- Auswirkung auf sensible Versorgungs- und/oder Dienstsegmente.

Nachfolgend werden in Deutschland aufgetretene Sicherheitsvorfälle aufgeführt.

ID	1	Störung des Festnetzes von 16.000 Kunden und Unternehmen nach Stromausfall	
DL	1	**Aktualität**	23.05.2013
PS	3	**Herkunft**	national
BP	1, 2	**Grad der Auswirkung auf die kritische DL**	Hohe Auswirkung
Betroffene Anlagen			Ortsvermittlungsstelle
Betroffene Risikoelemente			• Vermittlungsstellen (VE:F, VE:N, VE:A) • Vermittlungssysteme (z. B. EWSD oder S12) • Netzwerkelemente (RAS, Backbone-Router, Switches)
Vorfallkurzbeschreibung			
Durch einen Stromausfall in einer Vermittlungsstelle in Leipzig waren ca. 16.000 Haushalte und Unternehmen circa fünf Stunden nicht über Festnetz erreichbar. Es waren ebenso mehrere Krankenhäuser und Kliniken betroffen. Eine direkte Notstromversorgung nach Auftreten des Stromausfalls konnte nicht geleistet werden.			
Einfluss auf Versorgungsdienstleistung			
Die Versorgungsdienstleistung war direkt betroffen, Telefonate vom Festnetz waren nicht mehr möglich. Die Festnetzverbindungen fielen aus und Krankenhäuser mussten über Notrufnummern erreicht werden.			
Reaktion Betreiber			
Die Stromversorgung konnte nach zwei Stunden wiederhergestellt werden. Um jedoch einer Überlastung vorzubeugen, wurden die einzelnen Komponenten in der Vermittlungsstelle nacheinander hochgefahren, sodass erst drei Stunden später alle Kunden wieder Zugang zum Festnetz hatten.			
Reaktion beteiligte Behörde			
Es sind keine Reaktionen von Behörden bekannt.			
Auswirkungen Sektor/Branche			
Es sind keine Auswirkungen bekannt.			
Quellen	[teltarif 2013b]		

ID	2	Ausfall von Internet- und Telefoniediensten durch Brand in einer Kabelführung	
DL	1	**Aktualität**	23.05.2011
PS	2	**Herkunft**	national
BP	1, 2, 3	**Grad der Auswirkung auf die kritische DL**	Hohe Auswirkung
Betroffene Anlagen			-
Betroffene Risikoelemente			• Netzwerkelemente (RAS, Backbone-Router, Switches)

Vorfallkurzbeschreibung

In Berlin kam es in einer Kabelführung zu einem Brand, wodurch ein Großteil der Leitungen zerstört wurde. Der Vorfall ereignete sich in einer Kabelbrücke am Berliner Ostkreuz, in der sich auch Glasfaserleitungen von Vodafone befanden. Mehrere tausend Kunden konnten durch den Ausfall keine Internet- und Telefoniedienste in Anspruch nehmen. Der Grund für den Brand konnte nicht abschließend geklärt werden, Vandalismus wurde von der Polizei jedoch nicht ausgeschlossen.

Einfluss auf Versorgungsdienstleistung

DSL, Festnetz und Mobilfunk waren teilweise stark gestört. Durch den Ausfall von DSL-, Festnetz- und Mobilfunkverbindungen waren mehrere tausend Endkunden sowie viele andere Kunden der Dienstleistungen betroffen.

Reaktion Betreiber

Der Betreiber leitete den Datenverkehr über andere Netzrouten und begann mit der Reparatur der zerstörten Leitungen.

Reaktion beteiligte Behörde

Die Polizei hat Ermittlungen wegen Brandstiftung eingeleitet.

Auswirkungen Sektor/Branche

Durch die Abhängigkeiten anderer Dienstleister zu dieser Kabelverbindung fielen weitere Dienste aus. So wurden über die ausgefallenen Leitungen unter anderem auch BSC an den Backbone angebunden. Auch die Bahn nutzte die Leitungen zur Bereitstellung von Online-Diensten, die demnach ebenso ausfielen.

Quellen	[BZ 2011]

ID	3	Ausfall eines Datennetzes durch fehlerhafte Routerkonfiguration	
DL	1	**Aktualität**	13.06.2013
PS	3	**Herkunft**	national
BP	1	**Grad der Auswirkung auf die kritische DL**	Hohe Auswirkung
Betroffene Anlagen			-
Betroffene Risikoelemente			• Rechenzentren, Serverschränke • Netzwerkelemente (RAS, Backbone-Router, Switches)
Vorfallkurzbeschreibung			
Bei dem Anbieter 1&1 kam es durch eine fehlerhafte Konfiguration eines Backbone-Routers zu einem bundesweiten Ausfall von Internet- und Telefonverbindungen bei einem Teil der Kunden. Der Ausfall dauerte mehrere Stunden und betraf unter anderem die Regionen Berlin, München und Mannheim.			
Einfluss auf Versorgungsdienstleistung			
Durch den Ausfall waren Kunden im gesamten Bundesgebiet betroffen. Der Zugang zum Internet und Telefonie waren unterbrochen.			
Reaktion Betreiber			
Der Fehler wurde durch den Betreiber in Zusammenarbeit mit dem Technologiepartner Vodafone behoben.			
Reaktion beteiligte Behörde			
Es sind keine Reaktionen von Behörden bekannt.			
Auswirkungen Sektor/Branche			
Es sind keine Auswirkungen bekannt.			
Quellen	[teltarif 2013a]		

ID	4	Teilausfall des Name Services für „.de“-Domains	
DL	1	**Aktualität**	14.05.2010
PS	4	**Herkunft**	national
BP	3	**Grad der Auswirkung auf die kritische DL**	Hohe Auswirkung
Betroffene Anlagen			Rechenzentren
Betroffene Risikoelemente			• DNS-Server (DE-Rootserver)
Vorfallkurzbeschreibung			
Beim Betreiber der „.de“-Top-Level-Domain (DENIC e. G.) kam es beim regulären Update der Name-Service-Daten zu einem Übertragungsfehler. 12 der 16 Anlagen waren von diesem Fehler betroffen und lieferten bei Anfragen aus dem Internet falsche Antworten. Durch das Zwischenspeichern der DNS-Einträge in DNS-Servern von Internet Service Providern kam es auch nach der Lösung des Problems durch DENIC weiterhin zu Störungen bei Endkunden.			
Einfluss auf Versorgungsdienstleistung			
Durch den Ausfall waren Kunden im gesamten Bundesgebiet und auf dem gesamten Globus betroffen. Durch Verweise von Diensten aus anderen Top-Level-Domains (z. B. E-Mail-Dienste) auf „.de“-Domains kam es teilweise sogar zu Ausfällen aus anderen Top-Level-Domains.			
Reaktion Betreiber			
DENIC e. G. startete circa 40 Minuten nach Bekanntwerden des Fehlers mit entsprechenden Gegenmaßnahmen, sodass der Fehler nach circa zwei Stunden an allen betroffenen Standorten behoben war. Durch das Zwischenspeichern der fehlerhaften Einträge auf den DNS-Servern von ISP kam es bis zu zwei Stunden nach Behebung durch die DENIC bei Kunden noch zu Störungen.			
Reaktion beteiligte Behörde			
Es sind keine Reaktionen von Behörden bekannt.			
Auswirkungen Sektor/Branche			
Andere Betreiber von DNS-Infrastruktur (z. B. ISP) verzeichneten ein erhöhtes Datenvolumen Gleichzeitig konnte an wichtigen Knotenpunkten (z. B. DE-CIX) ein Rückgang des Datenverkehrs um bis zu 30 Prozent registriert werden.			
Quellen	[DENIC 2010]		

ID	5	Einschränkungen der VoIP-Dienste eines Betreibers über mehrere Tage	
DL	1	**Aktualität**	02.09.2014
PS	2	**Herkunft**	national
BP	2	**Grad der Auswirkung auf die kritische DL**	Mittlere Auswirkung
Betroffene Anlagen			-
Betroffene Risikoelemente			• Rechenzentren, Serverschränke • Netzwerkelemente (RAS, Backbone-Router, Switches)

Vorfallkurzbeschreibung

Die IP-Telefonie-Dienste der Deutschen Telekom AG waren Ende August bis Anfang September teilweise erheblich gestört. Kunden konnten in bestimmten Bundesgebieten keine Anrufe empfangen oder selbst tätigen. Das Ausmaß der Einschränkung lässt sich lediglich abschätzen. Anhand von Beitragen in sozialen Medien und Webseiten und der Reaktion der DTAG kann jedoch davon ausgegangen werden, dass eine große Anzahl von Nutzern betroffen waren. Verantwortlich für die Störungen waren Netzwerkkomponenten und darauf laufende Software. Router der Endkunden konnten sich daraufhin nicht mehr bei den zentralen Servern der DTAG registrieren und hatten somit keinen Zugriff auf die Dienste. Die DTAG versichert in einer Pressemitteilung, dass die Störung explizit nicht durch eine Überlastung hervorgerufen wurde.

Einfluss auf Versorgungsdienstleistung

Durch den Ausfall konnten Kunden der VoIP-Dienste der DTAG keine Telefonate mehr führen. Sie konnten weder angerufen werden noch anrufen. Für die betroffenen Kunden fiel somit die gesamte Dienstleistung aus.

Reaktion Betreiber

Die DTAG arbeitet zusammen mit ihrem Zulieferer der entsprechenden Netzwerkkomponenten an einer dauerhaften Lösung. Hierzu wurde eine „Task Force“ gebildet, um möglichst schnell einen reibungsfreien Ablauf wiederherzustellen.

Reaktion beteiligte Behörde

Es sind keine Reaktionen von Behörden bekannt.

Auswirkungen Sektor/Branche

Durch den geplanten Wechsel von der analogen Telefonie zu einem All-IP-Netz der DTAG ist dieser Vorfall von großer Bedeutung. Die Pressemitteilung der DTAG weist demnach auch darauf hin, dass der Vorfall nicht in Zusammenhang mit Kapazitätsengpässen steht.

Quellen	[DTAG 2014a]

4.2 Internationale Vorfälle

Nachfolgend werden Sicherheitsvorfälle aufgeführt, die außerhalb Deutschland aufgetreten sind.

ID	6	Angriff auf Glasfaserleitungen und Transformatoren	
DL	1	**Aktualität**	16.04.2013
PS	2	**Herkunft**	international
BP	1, 2, 3	**Grad der Auswirkung auf die kritische DL**	Hohe Auswirkung
Betroffene Anlagen			-
Betroffene Risikoelemente			• Rechenzentren, Serverschränke • Netzwerkelemente (RAS, Backbone-Router, Switches)
Vorfallkurzbeschreibung			
Mindestens eine Person verschaffte sich durch einen Schacht Zutritt zu einer Transformatorenstation in San Jose (USA), durchtrennte mehrere Glasfaserkabel, feuerte mit einem Gewehr zahlreiche Schüsse auf Transformatoren ab und zerstörte diese. Ein großer Telekommunikationsanbieter hatte mehrere Glasfaserkabel in der Transformatorenstation untergebracht. Die Hintergründe und Ziele des Attentäters sind nicht bekannt. Da über die Glasfaserkabel unter anderem Mobilfunkstationen an das Datennetz angebunden waren, kam es zu einem Ausfall des Mobilfunks in der Region.			
Einfluss auf Versorgungsdienstleistung			
Die Dienstleistung konnte nicht mehr in vollem Umfang erbracht werden. Durch die Beschädigung der Glasfaserkabel fielen zudem die Notrufnummern in der Region aus.			
Reaktion Betreiber			
Das Telekommunikationsunternehmen setzte eine Belohnung von 250.000 USD für Informationen aus, die zur Ergreifung des Täters führen. Zusätzlich erhöhte der Betreiber des Geländes seine Sicherheitsmaßnahmen.			
Reaktion beteiligte Behörde			
Das FBI hat die Ermittlungen in dem Fall von der örtlichen Polizei übernommen.			
Auswirkungen Sektor/Branche			
Es sind keine Auswirkungen bekannt.			
Quellen	[CBS 2013]		

ID	7	Virenbefall zentraler Komponenten eines Datennetzes	
DL	1	**Aktualität**	16.09.2013
PS	2	**Herkunft**	international
BP	2, 3	**Grad der Auswirkung auf die kritische DL**	Mittlere Auswirkung
Betroffene Anlagen			-
Betroffene Risikoelemente			• Rechenzentren, Serverschränke • Netzwerkelemente (RAS, Backbone-Router, Switches)

Vorfallkurzbeschreibung

Der größte belgische Telekommunikationskonzern Belgacom gab bekannt, dass sein Netzwerk kompromittiert wurde und einige Systeme mit Schadsoftware infiziert wurden. Kundensysteme seien nicht betroffen gewesen. Es konnte nicht genau festgestellt werden, wie lange die Schadsoftware bereits aktiv war, jedoch gab es Anzeichen dafür, dass die Infektion bereits zwei Jahre in der Vergangenheit stattgefunden hat.

Das Unternehmen bietet auch Carrier-Services für internationale Kunden an, darunter die Bereitstellung von Datenverbindungen über Unterseekabel.

Einfluss auf Versorgungsdienstleistung

Die Versorgungsdienstleistung war nicht beeinträchtigt. Die zentrale Position des Unternehmens als Betreiber von Unterseekabeln birgt jedoch das Risiko, dass bei einer Störung großflächig Telekommunikationsdienste ausfallen können.

Reaktion Betreiber

Der Betreiber hat die betroffenen Systeme bereinigt und eine Klage gegen Unbekannt eingeleitet. Das Unternehmen unterstützt die Behörden bei den Ermittlungen.

Reaktion beteiligte Behörde

Die Strafverfolgungsbehörden haben mit Ermittlungen in dem Fall begonnen.

Auswirkungen Sektor/Branche

Es sind keine Auswirkungen bekannt.

Quellen	[Belgacom 2013]

ID	8	Störung einer Transatlantik-Verbindung zwischen Europa und den USA	
DL	1	**Aktualität**	19.05.2014
PS	2	**Herkunft**	international
BP	2	**Grad der Auswirkung auf die kritische DL**	Niedrige Auswirkung
Betroffene Anlagen			-
Betroffene Risikoelemente			• Rechenzentren, Serverschränke • Netzwerkelemente (RAS, Backbone-Router, Switches)

Vorfallkurzbeschreibung
Das Unterseekabel TAT-14, welches zwischen Europa und den USA verläuft, war für mehrere Stunden gestört, sodass kein Datenverkehr auf diesem Wege mehr möglich war. Dies geschah in Folge eines Fehlers bei einem geplanten Updatevorgang zentraler Netzwerkelemente durch den Betreiber TeliaSonera. Der Tier-1-Carrier beteuerte, dass es sich bei dem Fehler um menschliches Versagen gehandelt habe. Verschiedene Internetdienste hatten die Störung bemerkt und unter anderem auf sozialen Netzwerken darauf hingewiesen.
Einfluss auf Versorgungsdienstleistung
Die Versorgungsdienstleistung war teilweise beeinträchtigt. Es gab keinen kompletten Ausfall der Verbindungen, da mehrere alternative Routen vorhanden sind. Durch die Störung sank der weltweite Traffic um 2 Prozent. Der Datenverkehr musste über alternative Routen geleitet werden.
Reaktion Betreiber
TeliaSonera behob den Fehler durch eine Korrektur des Updates.
Reaktion beteiligte Behörde
Es sind keine Reaktionen von Behörden bekannt.
Auswirkungen Sektor/Branche
Es sind keine Auswirkungen bekannt.

Quellen	[Register 2014]; [Telia 2014]

5 Cyber-Sicherheit

Das Kapitel „Cyber-Sicherheit“ beschreibt die sektor- und marktüblichen Maßnahmen zur IT- und Informationssicherheit im Sektor IKT in Deutschland. Diese beziehen sich auf den derzeit umgesetzten Stand der Technik.

Die Erläuterung der IKT-Sicherheit im Sektor IKT, die in Abschnitt 5.1 **„Cyber-Sicherheit im Sektor“** stattfindet, umfasst die Betrachtung vorhandener Standards. Diese erfolgt anhand einer Beschreibung und Kategorisierung der Standards. Zudem beschreibt der Abschnitt aktuelle Trends zur Prävention von Sicherheitsvorfällen, Trends zur Erkennung von Sicherheitsvorfällen und Trends zur verbesserten Reaktion auf Risiken und Sicherheitsvorfälle.

Der darauffolgende Abschnitt 5.2 **„Gesetzliche Anforderungen“** betrachtet die Anforderungen an die IKT-Sicherheit hinsichtlich Normen, Gesetzen und weiterer spezifischer Regularien.

Abschnitt 5.3 **„Umsetzungsgrad der Cyber-Sicherheit“** stellt die praktische Darstellung des Umsetzungsgrads von Standards und Best Practices, aufgeteilt nach kritischen Dienstleistungen, dar. Diese Darstellung erfolgt unter anderem anhand der Auswertung der Betreiberbefragungen. Dabei werden Prozesse zur Identifikation, Analyse und Behandlung von Risiken beschrieben. Ferner behandelt der Abschnitt die aktuellen Trends und Entwicklungen bezüglich Reaktionsfähigkeit, Sensibilisierung und Cyber-Sicherheitsstrategie. Dies berücksichtigt auch die daraus resultierenden bzw. aktuellen Probleme.

Entwicklungen und Herausforderungen, die aktuell oder absehbar Einfluss auf die Cyber-Sicherheit im Sektor IKT nehmen, werden in Abschnitt 5.4 **„Herausforderungen und Trends“** dargestellt. Die Aufbereitung erfolgt aus verschiedenen Perspektiven und wird in den Kategorien „Organisatorisch“, „Technisch“, „Regulatorisch“ und „Marktbezogen“ zusammengefasst.

5.1 Cyber-Sicherheit im Sektor

Die folgende Aufzählung von Standards und bewährten Vorgehensweisen – sogenannte Best Practices – ist aufgrund ihrer Vielzahl und den international unterschiedlichen Ausprägungen ein Auszug der besonders relevanten Elemente. Es erfolgt lediglich die Aufführung von Standards, die für Deutschland bedeutend sind und direkt auf die IKT-Sicherheit bezogen werden können. Die Standards und Best Practices besitzen innerhalb des Sektors, sogar innerhalb der Branchen, einen unterschiedlichen Verbreitungsgrad. Da sich die Anlagen und IKT-Systeme innerhalb der Branchen im Sektor IKT nicht oder nur geringfügig unterscheiden, geht dieser Abschnitt – sofern nicht anders angegeben – von sektorweiten Standards und Best Practices aus. Zum Teil sind diese Standards auch für andere KRITIS-Sektoren oder IKT ohne KRITIS-Bezug anwendbar.

Diese Studie nimmt eine Einteilung der Standards und Best Practices hinsichtlich verschiedener Aspekte vor (siehe Abbildung 19). Im deutschen IKT-Sektor wurden Standards und Best Practices von verschiedenen Institutionen erarbeitet und vorgestellt. Daher unterscheidet die Studie einerseits zwischen nationalem, internationalem sowie verbandlichem Ursprung; andererseits hinsichtlich der technischen und organisatorischen Betrachtung der jeweiligen Veröffentlichung.

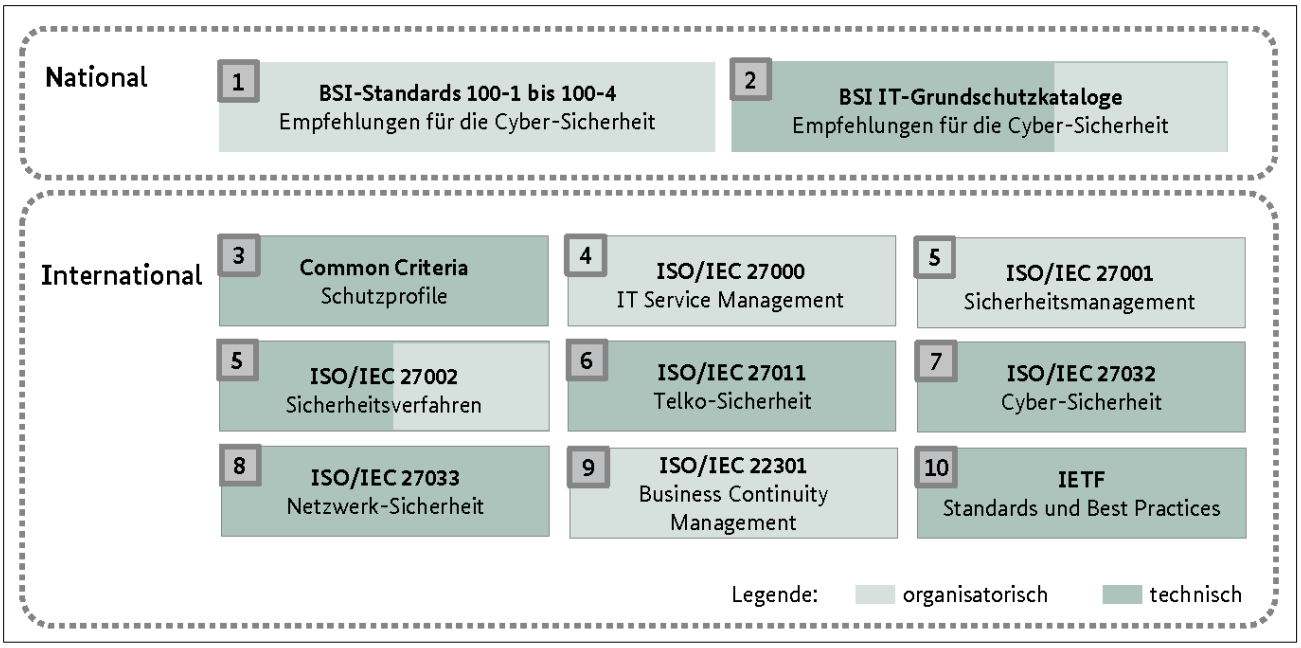

Abbildung 19: Standards und Best Practices für die Cyber-Sicherheit im IKT-Sektor in Deutschland

Quelle: eigene Darstellung

Nachfolgende werden die einzelnen Standards auf und deren Zielstellung vorgestellt. Die in der Übersicht dargestellte Nummerierung dient zur Orientierung und ist daher Bestandteil der Beschreibung der jeweiligen Standards und Best Practices.

Nationaler Ursprung

1. BSI-Grundschutzstandards 100-1 bis 100-4
   Die BSI-Standards enthalten methodische, prozessuale, vorgehens- und verfahrenstechnische Empfehlungen für die Sicherheit von Informationssystemen. Der BSI-Standard 100-1 enthält Empfehlungen zum Informationssicherheitsmanagement-System, 100-2 enthält Vorgehen zum IT-Grundschutz, 100-3 enthält Empfehlungen zum Risiko-Assessment und 100-4 enthält Empfehlungen zum Notfallmanagement.
2. BSI IT-Grundschutzkataloge
   Ein bausteinorientiertes Handbuch auf Grundlage der **BSI-Grundschutzstandards 100-1** bis **100-4** zur Erkennung und Bekämpfung sicherheitsrelevanter Schwachstellen in IKT-Umgebungen. Die Grundschutzkataloge B1 bis B4 umfassen verschiedene Ebenen der gesamten Organisation, von übergreifenden bis hin zu technischen Empfehlungen. Zusätzlich existieren Kataloge zu **Gefährdungen**, Schutzmaßnahmen und geeigneten Hilfsmitteln. Die BSI IT-Grundschutzkataloge sind mit den Best Practices aus der **IEC/ISO 27002** vergleichbar, geben allerdings weiter gehende Handlungsempfehlungen sowie Konfigurationsvorschläge.
3. Common Criteria Schutzprofil(e) (bspw. SM_PP)
   Die Schutzprofile nach Common Criteria (CC) für IT-Produkte legen generische Anforderungen an eine Produktkategorie fest. Sie umfassen Anforderungen an die Funktionalität sowie an die Vertrauenswürdigkeit einer Produktkategorie und decken eine bestimmte Menge von Sicherheitszielen vollständig ab. Die Schutzprofile setzen somit Mindeststandards für bestimmte Produktgruppen. Sie können durch daraus ableitbare Sicherheitsvorgaben auf einen konkreten Gegenstand angepasst werden, sind generell aber implementierungsunabhängig.

Internationaler Ursprung

4. ISO/IEC 20000
   Die Norm legt Anforderungen an ein professionelles IT Service Management (ITSM) fest. Sie kann in Verbindung mit dem **ITIL**- und **COBIT-Framework** auch für Best Practices im Rahmen des ITSM herangezogen werden.
5. ISO/IEC 27001 und ISO/IEC 27002
   Die ISO/IEC 27001 spezifiziert in Verbindung mit der ISO/IEC 27002 Umsetzungsmaßnahmen, unter anderem für die Sicherheit von Rechenzentren und Implementierung von Informationssicherheit. ISO/IEC 27001 kann in Verbindung mit **BSI Standard 100-1** und ISO/IEC 27002 als Best Practice für die Implementierung eines Informationssicherheits-Managementsystem (ISMS) dienen.
6. ISO/IEC 27011
   Die Norm ISO/IEC 27011 deckt den ordnungsgemäßen Betrieb von IKT-Systemen im Sinne von Richtlinien für ein Informationssicherheits-Managementsystem (ISMS) ab. Sie berücksichtigt speziell die Besonderheiten von IKT-Systemen.
7. ISO/IEC 27032
   Die Norm ISO/IEC 27032 enthält Leitlinien für Cyber-Sicherheit und die speziellen Anforderungen aus Internet-/Netzwerk-verbundenen Anlagen und Systemen. Der Fokus liegt auf Informationssicherheit, Netzwerksicherheit, Internetsicherheit und Sicherheit in kritischen Infrastrukturen (CIP). Die Norm beschreibt zusammenfassend Cyber-Sicherheit, besondere Anforderungen und Bedrohungen und will ein Rahmenwerk vorgeben, wie Aspekte der Cyber-Sicherheit von Betreiber adressiert werden können.
8. ISO/IEC 27033
   Die Normen ISO/IEC 27033-1, ISO/IEC 27033-2 und ISO/IEC 27033-1 enthalten Empfehlungen, Definitionen und Best Practices für Netzwerksicherheit. Die Empfehlungen betreffen Hinweise auf Architekturen für Netzwerke, relevante und angemessene technische und nicht-technische Kontrollen sowie deren Implementierung und Umsetzung.
9. ISO/IEC 22301
   Die Normen ISO/IEC 27001 und ISO/IEC 27002 sowie der BSI-Standard 100-1 haben in Verbindung mit der ISO/IEC 22301 die Aufrechterhaltung des Geschäftsbetriebes (Business Continuity Management) zum Gegenstand. Dabei wird ein Managementsystem für die Fortführung beschrieben. Es werden Anforderungen an ein Managementsystem zum Schutz gegen den Geschäftsbetrieb unterbrechende Ereignisse, den Schutz vor diesen sowie die Reaktion und Vorbereitung auf die Ereignisse gegeben.
10. IETF Standards und Best Practices
    In der Internet-Standardisierungsorganisation IETF (Internet Engineering Task Force) gibt es neben technischen Standards und Normen eine Vielzahl an Best Practices und Guidelines für IT-Sicherheit, speziell für Internetprotokolle. Ohne Anspruch auf Vollständigkeit umfasst dies verschiedenste Standards und Protokolle wie IPsec, VoIP-Security, Kryptographie, Betrieblichen Best Practices u. v. m. Ein Versuch der IETF, ein übergreifendes, deskriptives Dokument zu schaffen, das aktuelle und relevante Security Best Practices auflistet (Security Best Practices Efforts and Documents IETF 2013) wurde nicht zum Standard erkoren.

5.2 Gesetzliche Anforderungen

Der folgende Abschnitt greift die verschiedenen Anforderungen an die IKT-Sicherheit in Form von Gesetzen und Verordnungen im Sektor IKT auf und erläutert diese. Hierzu werden die einschlägigen, in Deutschland anwendbaren Gesetze erfasst.

Aufgrund des rechtsverbindlichen Charakters der folgenden Normen besitzen diese im IKT-Sektor (hier jedoch nur für Betreiber von Telekommunikationsdiensten und -netzen) einen sehr hohen Umsetzungsgrad. Diese Studie beschreibt lediglich die Gesetze, die einen direkten Bezug zur Cyber-Sicherheit im Rahmen des Einsatzes von IKT in der Versorgungsleistung besitzen. Allerdings ist zu

berücksichtigen, dass eine scharfe Abgrenzung zwischen unmittelbarem und mittelbarem Bezug zur IKT-Sicherheit nicht immer möglich ist. Eine erschöpfende Aufzählung aller Normen würde den Rahmen dieser Studie überschreiten.

Im Unterschied zu den im vorangegangenen Kapitel beschriebenen Standards und Best Practices betreffen die gesetzlichen Anforderungen primär Betreiber von Telekommunikationsdiensten und -netzen. Unternehmen der Dienstleistung *Datenspeicherung und -verarbeitung* fallen größtenteils nicht unter das TKG.[32] Entsprechend nimmt die Studie im Folgenden bei den sektorspezifischen Gesetzen keine Unterscheidung nach den Branchen vor.

Telekommunikationsgesetz (TKG)

Betreiber von Telekommunikationsdiensten und -netzen fallen in Deutschland unter das Telekommunikationsgesetz (TKG). Betreiber (Anbieter) müssen das Angebot und die Erbringung dieser Leistungen bei der BNetzA anmelden. Das Gesetz befasst sich zum Großteil mit Marktregulierung und verwandten Themen, beinhaltet aber auch Ausführungen zu IT-Sicherheit (vgl. § 109 TKG).

TKG-Meldepflichten (§ 109 Absatz 5 TKG)

Betreiber öffentlicher Telekommunikationsanlagen müssen „Sicherheitsverletzungen einschließlich Störungen“ nach § 109 Absatz 5 TKG an die BNetzA melden. Störungen mit „beträchtlichen Auswirkungen“ liegen nach dem Umsetzungskonzept zu § 109 Absatz 5 TKG mindestens beim Überschreiten von „drei Mio. Nutzerstunden“ vor, aber auch gemäß anderer Kriterien. Die BNetzA kann die Vorfälle an das BSI, andere europäische Regulatoren und auch an die Öffentlichkeit melden. Das BSI, die europäische Kommission und die ENISA (Europäische Agentur für Netz- und Informationssicherheit) erhalten einmal jährlich einen Bericht der BNetzA über Störungen und Sicherheitsvorfälle.

Daten für Meldungen liegen laut BNetzA zwischen Sommer 2012 und Sommer 2013 vor; in diesem Zeitraum wurden von 13 Meldungen insgesamt neun als Sicherheitsverletzungen mit „erheblichen Auswirkungen“ auf öffentliche Telekommunikationsnetze bzw. -dienste nach § 109 Absatz 5 TKG eingestuft [BNetzA 2013a].

Die Umsetzung der Meldepflicht ist in einem Umsetzungskonzept der BNetzA beschrieben, welches in der aktuellen Version von 2014 vorliegt [BNetzA 2014b]. Im Umsetzungskonzept werden die folgenden Punkte zu Meldungen und Sicherheitsvorfällen beschrieben:

1. Meldeverfahren
2. Sicherheitsverletzungen im Sinne des Gesetzes, wenn die drei C/I/A-Grundwerte (Vertraulichkeit, Integrität und Verfügbarkeit) von Telekommunikationsnetzen und -diensten betroffen sind.

   Das Gesetz geht bei Sicherheitsverletzungen von mehreren möglichen Störungen aus, die als *Kriterien* für Meldungen und Sicherheitsverletzung für die Betreiber definiert sind:

   - (1) bzw. (2) Eindeutig beträchtliche Auswirkungen bestehen, wenn mindestens 3 Mio. gestörte Nutzerstunden in einem Vorfall für Telefonie- und Datennetze an mobilen und festen Einrichtungen überschritten werden. „Störungen“ bedeuten in diesem Fall, dass Anschlüsse oder Dienste vollständig ausfallen oder nur noch „mit beträchtlich geminderter Qualität“ zur Verfügung stehen.

     Nutzerstunden errechnen sich durch das Produkt der Anschlüsse (bei TK-Netzen) oder Teilnehmer (bei TK-Dienste) und der „Dauer der Leistungsminderung“.

   - (3) Zusammenschaltung von Netzen (Interconnection), falls die Verbindung oder Übertragung zwischen verschiedenen Netzen gestört wird.

32 Im Rahmen dieser Studie wurde kein klares Bild darüber ermittelt, welche Betreiber dem TKG unterliegen und welche nicht. Auskunft darüber kann die Bundesnetzagentur geben, bei der alle Betreiber von Kommunikationsdienstleistungen registriert sind.

- (4) Wirkung im Ausland, falls Störungen in Deutschland Telekommunikationsnetze, -dienste und -systeme im Ausland stören oder beeinträchtigen.
- (5) Ausbreitung/Region, falls Störungen gleich ganze, zusammenhängende geographische oder wirtschaftliche Regionen betreffen (wie Wirtschafts- oder Industriezentren).
- (6) Notruf, falls Elemente, Dienste oder Netze gestört werden, die zur Erkennung und Verarbeitung von Notrufen notwendig sind.
- (7) Sensible Dienste, falls Dienste oder Kunden mit besonderen Sicherheitsanforderungen gestört werden, wie z. B. Krankenhäuser, militärische Bereiche, Regierungsbereiche.

3. Meldungen selbst enthalten Daten zur Störung, den betroffenen Nutzern und eine Übersicht der oben beschriebenen Kriterien. Zuerst sollen Kurzmeldungen per Mail oder Fax an die BNetzA verschickt werden, gefolgt von einer vollständigen Meldung basierend auf einem Formular der BNetzA. Die vollständigen Meldungen sollen per E-Mail oder aber auch per Post oder Fax an die BNetzA übermittelt werden.
4. Auswertung, andere Stellen, Informationen: Nach Auswertung der eingegangenen Mitteilungen kann die BNetzA vom Betreiber einen detaillierteren Bericht verlangen, andere Stellen wie das BSI, deutsche bzw. europäische Regulierungsbehörden unterrichten oder die Öffentlichkeit informieren, falls die Bekanntgabe „im öffentlichen Interesse liegt".

TKG-Schutzmaßnahmen (§ 109 Absatz 1, 2 und 4 TKG)

Nach § 109 Absatz 1 TKG müssen Dienstanbieter das Fernmeldegeheimnis und personenbezogene Daten mit „technischen Vorkehrungen und Maßnahmen" schützen. Betreiber von Telekommunikationsanlagen für die Öffentlichkeit müssen sich nach § 109 Absatz 2 und 4 TKG ebenso mit entsprechenden Maßnahmen vor Störungen schützen, die „zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen" führen, der BNetzA ein Sicherheitskonzept vorlegen sowie einen Sicherheitsbeauftragten benennen.

Die BNetzA hat im Jahr 2012 „50 neue und 22 überarbeitete Sicherheitskonzepte auf die Einhaltung der Vorschriften nach § 109 TKG überprüft." Bei Betreibern von öffentlichen Telekommunikationsnetzen wurden im Jahr 2012 37 Kontrollmaßnahmen durchgeführt [BNetzA 2013a].

Sicherheitskonzepte nach § 109 Absatz 4 TKG müssen vor allem die folgenden Punkte beinhalten:

1. Beschreibung der öffentlichen Telekommunikationsnetze und -dienste;
2. Absehbare Gefährdungen;
3. Technische Vorkehrungen und Schutzmaßnahmen zur Erfüllung von § 109 Absatz 1 und 2 TKG.

Nach § 109 Abs. 1 und 2 TKG muss der Betreiber im Sicherheitskonzept folgende Ziele behandeln:

1. Fernmeldegeheimnis: Schutz des Telekommunikationsverkehrs gegen unerlaubtes Abhören oder Manipulation, Schutz der dabei beteiligten Systeme, Leitungen usw. gegen unbefugten Zutritt oder Zugriff.
2. Personenbezogene Daten: BDSG-konforme Verarbeitung und Speicherung von personenbezogenen Daten in der Telekommunikation, die im Rahmen von Verkehrsdaten, Zahlungssystemen und auch Betrugsabwehr erhoben werden können. Das umfasst den Schutz von Akten, Systemen und Archiven, in denen diese Daten gespeichert, verarbeitet oder erhoben werden.
3. Ordnungsgemäßer Betrieb der Telekommunikationsnetze oder -dienste: Schutz gegen Manipulation oder absichtliche und unabsichtliche Schädigung der Systeme und Leitungen, die Telekommunikation abwickeln. Das beinhaltet Zutrittskontrollen zu den entsprechenden Einrichtungen, Störungsmeldungen etc.

Das Sicherheitskonzept muss unverzüglich nach der Aufnahme des Betriebs der BNetzA vorgelegt werden, zusammen mit einer Erklärung, dass die beschriebenen Maßnahmen umgesetzt oder in Umsetzung sind. Bei

Änderungen an betrieblichen Gegebenheiten muss das Sicherheitskonzept angepasst und aktualisiert werden; die BNetzA kann die Beseitigung von Mängeln im Konzept und dessen Umsetzung verlangen.

TKG-Sicherheitskatalog (§ 109 Absatz 6 TKG)

Als Grundlage und Unterstützung für TKG-Sicherheitskonzepte stellt die BNetzA nach § 109 Absatz TKG einen Sicherheitskatalog mit Vorschlägen und Anforderungen zur Verfügung. Der Katalog soll Betreiber bei der Auswahl und Umsetzung von Maßnahmen unterstützen.

Die folgenden Umsetzungshinweise lassen sich ableiten:

1. Netzstrukturplan: Festlegung des TK-Systems, der Verbindungen und relevanten Anlagen für Geschäftsprozesse.
2. Teilbereiche und Sicherheitsanforderungen: Festlegung und Bildung sinnvoller Teilbereiche der IKT-Infrastruktur zur Festlegung von Sicherheitszielen und Zuordnung von Schutzmaßnahmen.
3. Schutzmaßnahmen: Für Teil- und Gesamtsysteme sollen Maßnahmen für organisatorische, personelle, technische Gefährdungen etc. abgeleitet und definiert werden. Für Schutzmaßnahmen werden z. T. Vorgehen und Bausteine nach BSI IT-Grundschutz empfohlen; Gefährdungen orientieren sich teilweise an den Elementargefährdungen nach BSI IT-Grundschutz.
4. ISMS: Ein Management-System für Informationssicherheit wird nicht gefordert, ISO 27000 und BSI IT-Grundschutz werden erwähnt.
5. Risikomanagement: Ein Risikomanagement-System wird nicht gefordert, jedoch im Rahmen einer Notfallvorbereitung empfohlen.
6. BCM: Ein vollwertiges Business Continuity Management wird nicht gefordert, jedoch ebenfalls im Rahmen einer Notfallplanung und -vorsorge empfohlen.
7. Organisatorische Rahmenbedingungen: Erstellung und Abnahme des Sicherheitskonzepts, Ernennung eines Sicherheitsbeauftragten.
8. Internetsicherheit: Für Verbindungen oder Verkehrsaustausch mit dem Internet werden Vorschläge zur Sicherung des Verkehrs an Übergängen und vor Angriffen gemacht. Die aktuellen Sicherheits- und Technikprobleme des Internets werden dabei kurz aufgegriffen und Betreiber angeregt, sich damit zu befassen.

Überprüfungen

Die BNetzA hat das Recht, Betreiber einer Überprüfung zur Einhaltung dieser Regelungen zu unterziehen (§ 109 Absatz 7 TKG).

PTSG

Mit dem Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen (PTSG) werden Betreiber von (u. a.) Telekommunikationsdiensten verpflichtet, bei „erheblichen Störungen“ eine Mindestversorgung für bestimmte Empfänger sicherzustellen (§ 1 PTSG).

Die Vorkehrungen gelten für Betreiber mit mehr als 100.000 Teilnehmern sowie für Betreiber von „Verbindungsnetzen“, die durch Telekommunikationsunternehmen genutzt werden (§ 1 Absatz 1 PTSG). Unter die nach § 5 TKG sicherzustellenden Dienste fallen „Datenübermittlungsdienste, einschließlich Internetzugangsdienste“ und Unternehmen, die Anschlüsse für diese Dienste bereitstellen.

Bei „erheblichen Störungen“ der Versorgung, u. a. „Naturkatastrophen, besonders schweren Unglücksfällen, Sabotagehandlungen, terroristischen Anschlägen [...] im Spannungs- oder Verteidigungsfall“ (§ 1 Absatz 2 TKG), müssen Unternehmen sogenannten „Telekommunikationsbevorrechtigten“ Anschlüsse und Übertragungswege „unverzüglich und vorrangig bereitstellen [...] und entstören“ (§ 6 Absatz 1 TKG). Die

Bevorrechtigten sind u. a. Verfassungsorgane, Behörden, Gerichte, Bundeswehr, Katastrophen- und Zivilschutz, Hilfs- und Rettungsdienste (§ 6 Absatz 2 TKG).

5.3 Umsetzungsgrad der Cyber-Sicherheit

Der Umsetzungsgrad der Maßnahmen zur Cyber-Sicherheit ist in diesem Kapitel vereinfacht in den folgenden Kategorien zusammengefasst:

1. **Sicherheitsorganisation und -management:** Prozesse, Managementsysteme und Sicherheitsorganisation bei Betreibern, um das Sicherheitsniveau zu erhöhen, Sicherheitsvorfälle und -angriffe zu erkennen und abzuwehren.
2. **Technische IT-Sicherheit:** Vorkehrungen an einzelnen Anlagen oder Risikoelementen, um deren Schutz gegen Ausfälle, Manipulationen oder Angriffe zu erhöhen (Prävention).
3. **Detektion und Reaktion:** Fähigkeiten, Angriffe und Unregelmäßigkeiten zu erkennen und darauf angemessen reagieren zu können.
4. **Externe Abhängigkeiten:** Vorkehrungen für externe Verträge und Schnittstellen zu anderen Organisationen und Betreibern.
5. **Security Awareness**: Sensibilität der Betreiber und Akteure im Sektor für die Risiken, Bedrohungen und Auswirkungen beim Einsatz von IKT.

Wie in Kapitel Fehler: Verweis nicht gefunden muss auch hier berücksichtigt werden, dass diese Aussagen einen teils abstrahierten und zusammenfassenden Ausschnitt der gesamten Praxis im Sektor darstellen. Je nach Größe, Art und Praxis der Betreiber existieren unterschiedlich starke Ausprägungen, auf die nur in bedingtem Maße eingegangen werden kann.

Die festgehaltenen Erkenntnisse basieren auf den Ergebnissen aus den Gesprächen mit den befragten Betreibern. Eine Ableitung auf den Zustand des gesamten Sektors ist daher nur begrenzt möglich.

Basierend auf Expertenwissen der Studienautoren und als Resultat der Betreiberbefragung im KRITIS-Sektor IKT können die nachfolgenden Aussagen zum Stand der Cyber-Sicherheit getroffen werden. Sie beziehen sich auf Sicherheitsthemen, die besonders für den Schutz Kritischer Infrastrukturen relevant sind. Die Betreiberbefragung wurde sektorweit durchgeführt, wobei knapp 20 Interviews mit verschiedenen Betreibern geführt wurden. Allerdings nahm die Mehrheit der großen Betreiber und Konzerne (Telkos), die in der Sprach- und Datenübertragung (DL1) tätig sind, nicht an der Befragung teil. Die direkten Erkenntnisse für diese Dienstleistung basieren daher vor allem auf Interviews mit Betreibern einzelner Prozessschritte oder betriebsinterner Prozesse. Es fehlen somit möglicherweise allgemeingültige Aussagen für die Dienstleistung „Sprach- und Datenübertragung“.

5.3.1 Sprach- und Datenübertragung (DL1)

In diesem Abschnitt werden zunächst allgemeine Beobachtungen zum Umsetzungsgrad der Cyber-Sicherheit in der Dienstleistung „Sprach- und Datenübertragung“ beschrieben. Diese werden durch dedizierte Feststellungen für die einzelnen Themenschwerpunkte der Informationssicherheit in den nachfolgenden Unterkapiteln genauer erläutert und bewertet.

- Die Vorkehrungen im Bereich **Sicherheitsorganisation und -management** sind sektorweit sehr umfangreich, wobei der Grad der Ausgestaltung von der Unternehmensgröße abhängig ist. Ein Großteil der Betreiber unterhält eigene Sicherheitsbereiche, Managementsysteme (BCM für Notfallmanagement, ISMS für Sicherheitsmanagement), Lagezentren (CERT, SOC) und Notfallvorkehrungen. Die entsprechenden Prozesse und Abteilungen bestehen in der Regel seit längerer Zeit und werden in den letzten Jahren zunehmend erweitert.

Viele Betreiber bzw. KRITIS-relevante Unternehmensteile sind nach dem Standard ISO 27001 zertifiziert. BSI IT-Grundschutz oder andere Standards werden nur selten zur Zertifizierung genutzt.

- Das Niveau der **technischen Cyber-Sicherheit** kann über den gesamten Sektor hinweg als hoch angesehen werden. Entsprechende technische Schutzmaßnahmen sind sehr verbreitet und bewährt, können jedoch durch die steigende Komplexität der IKT-Infrastrukturen, speziell des Internets, meist nicht alle Bedrohungen abwehren oder alle Schwachstellen minimieren. Die Komplexität wird durch die schnelle technologische und organisatorische Entwicklung im Sektor begünstigt, wodurch Infrastrukturen vielen Änderungen unterworfen sind. Das führt zu der Notwendigkeit immer neuer technischer Sicherheitsmaßnahmen, die ebenfalls komplexer und damit auch ressourcenintensiver in Anschaffung und Unterhalt werden.

  Unter die genannten Sicherheitsmaßnahmen fällt auch der Bereich **Detektion und Reaktion**, der, basierend auf speziellen IT-Systemen und technischen Vorkehrungen, eine Analyse des Datenverkehrs und die Erkennung von Angriffsmustern und -versuchen fokussiert. Entsprechende Systeme sind im Sektor weit verbreitet und erfahren in den letzten Jahren eine zunehmende Weiterentwicklung, um Angriffen nicht nur vorzubeugen, sondern sie auch angemessen festzustellen und abzuwehren. Ein Großteil der Betreiber setzt solche Systeme und Vorkehrungen ein.

- Größere Unternehmen und Konzerne weisen ein hohes Bewusstsein (**Awareness)** und notwendiges Verständnis für Cyber-Sicherheit und die daraus resultierenden Anforderungen und Notwendigkeiten auf. Kleinere Betreiber entwickeln häufig ebenfalls eine hohe Security Awareness, können hingegen aufgrund geringerer Ressourcen nicht immer alle entsprechenden Maßnahmen ergreifen. Diese Aussage kann aber nicht pauschalisiert werden.

- Das Bewusstsein für **externe Abhängigkeiten** im Sektor und entsprechende Vorkehrungen für Cyber-Sicherheit sind vorhanden, jedoch mit unterschiedlicher Ausprägung. In der Regel werden die KRITIS-relevanten IKT-Komponenten durch die Betreiber selbst oder durch eigene Tochterunternehmen bereitgestellt und betrieben. Einige Unternehmen vertrauen jedoch zunehmend auf die Kenntnisse externer Dienstleister und lagern ihre IKT-Komponenten teilweise (z. B. Konfiguration und Wartung durch Externe) oder vollständig aus. Bei einer vollständigen Auslagerung ist zu beachten, dass die Dienstleister zwar die operative Verantwortung für die technische Umsetzung der definierten Sicherheitsanforderungen übernehmen, die eigentliche Management-Verantwortung jedoch beim Betreiber verbleibt und regelmäßige Überwachungsmaßnahmen erfordert.

  Entsprechende Vorkehrungen für Cyber-Sicherheit beim Outsourcing und dem Einkauf von Dienstleistungen werden zunehmend vertraglich gesichert, haben in der Vertrags- und Dienstleistungsgestaltung allerdings nicht immer oberste Priorität.

5.3.1.1 Sicherheitsorganisation und -management

1. **Zentrale CERTs:** Die Betreiber unterhalten größtenteils zentrale Meldeorganisationen für Sicherheitsvorfälle als Security Operations Center (SOC), Computer Emergency Response Team (CERT), Security Incident Response Team (SIRT) oder generell als Incident Response oder Handling Team. Häufig gibt es in den einzelnen Betriebseinheiten separate Incident Response Teams, die jedoch zu einem zentralen CERT zusammengefasst sind. Diese CERTs erfassen als Querschnitts- oder Stabsfunktion Sicherheitsvorfälle im IT-Betrieb/-Produktion der Betreiber, sammeln und bewerten diese und übernehmen teilweise auch die Nachverfolgung und den Austausch mit Dritten.

   Nicht alle Betreiber haben formalisierte oder gleichartige CERTs; Titel und Ausbaustufe sind sehr unterschiedlich, ebenfalls eine zentrale oder verteilte bzw. in IT-Abteilungen integrierte Struktur.

2. **Advanced Cyber-Defense**: Vor allem größere Betreiber errichten zunehmend fortschrittlichere Cyber-Abwehr-Organisationen, die als zentrale Schnittstellen- und Koordinierungsstellen die verschiedenen Sicherheitsfunktionen zusammenfassen. Dort werden Gegenmaßnahmen bei Angriffen,

Nachuntersuchungen bei Vorfällen und generell Vorbereitung, Detektion und Prävention für Cyber-Sicherheit betrieben.

3. **Sicherheitsmanagement und Sicherheitsstandards:** Vor allem größere Betreiber unterhalten formalisierte Sicherheitsmanagement-Systeme (ISMS) in ihrer Organisation. Die Management-Systeme betrachten Risiken strukturiert und kontrollieren mit Prozessen und Rollen das Sicherheitsniveau der IT-Landschaft. Im IKT-Sektor sind strukturierte ISMS vor allem gemäß ISO/IEC 27001 und nach BSI IT-Grundschutz verbreitet. Betreiber oder deren Betriebe sind teilweise ebenfalls zertifiziert. Gründe für Zertifizierung sind einerseits interne Bestrebungen für eine formalisierte Behandlung von Sicherheit mit interner und externer Vorbereitung, andererseits eine Außendarstellung der Sicherheitsbemühungen. Die Betreiber der Branche messen dem Standard ISO/IEC 27001 zumindest in der Kommunikation meist eine größere Rolle zu als dem BSI IT-Grundschutz, vor allem aus Gründen der Internationalität des Geschäfts und Marktes. Auffallend ist, dass industriespezifische Standards, wie die ISO/IEC 27011 speziell für Telekommunikationsorganisationen oder die ISO/IEC 27032 für Cybersicherheit, bei den befragten Betreibern keine Anwendung finden.
4. **Notfallübungen**: Viele Betreiber führen Notfallübungen durch, um die Abläufe bei Ausfall oder Störung von zentralen IKT-Infrastrukturen oder auch Rechenzentren und Betriebsgebäuden zu testen. Die Übungen sind meist papierbasierte Simulationen oder auch das kontrollierte Abschalten oder Herunterfahren von einzelnen Komponenten oder Infrastrukturen. Es gibt wenig systematisierte Vorgehensmodelle für diese Notfallübungen.

5.3.1.2 Technische IT-Sicherheit

1. **Redundante IXPs**: Die zentralen IXPs in Deutschland (meist auch europaweit) verfügen über eine redundante Infrastruktur und sind selbst redundant aufgebaut. Wichtige Betriebs-, aber auch Verwaltungsfunktionen verteilen sich über mehrere Standorte, Rechenzentren, Leitungen und Systeme. Die Standorte der IXPs sind in Metropolregionen geographisch verteilt und nutzen zur Vernetzung untereinander und zu Kunden meist mehrfach redundante Leitungen, um den Ausfall einzelner Komponenten abzufedern.
2. **Redundante Backbone-Leitungen**: Die zentralen Backbone-Leitungen großer Betreiber sind meist mehrfach redundant, um gegen Ausfälle einzelner Leitungen, Trassen und Knotenpunkte zu schützen. In der Regel sind diese Netze entweder (doppelte) Ringe oder mehrfach vermascht, sodass Verkehr auf diesen Ebenen der Netztechnologie mehrere Routen zwischen Sender und Empfänger nehmen kann. Neuralgischen Punkten im Netz wird so entgegengewirkt.
3. **Redundante WAN-Verbindungen**: Betreiber nutzen für den Austausch von Verkehr über weite Strecken oder zwischen Metropolregionen oder Ländern entweder eigene oder gemietete WAN-Verbindungen. In der Regel werden hierfür mehrere separate WAN-Verbindungen zwischen Standorten oder Rechenzentren von unterschiedlichen Betreibern oder Trassen genutzt, um Ausfälle einzelner Leitungen überbrücken zu können. Bei Standorten mit verschiedenen Trassen werden zudem redundante Hausanschlüsse genutzt, um die Redundanzen zu erhöhen.
4. **Redundanz des Internets**: Neben der Redundanz der zugrundeliegenden Netzwerke und Leitungen ist das Internet auf Schicht von IP inhärent redundant. Durch die sehr vermaschte Vernetzung der Betreiber, Carrier und (Geschäfts-)Kunden mit meist mehr als zwei separaten Internetanschlüssen kann „das Internet“ auf IP-Ebene Ausfälle zentraler Knotenpunkte und Infrastrukturen meist durch Anpassung des Routings abfangen. Fallen Provider oder Knotenpunkte aus, können Betreiber ihren Verkehr durch Peering an IXPs, bilateral oder über Transit-Verbindungen mit entsprechenden Providern austauschen.
5. **Redundante NMCs**: Systeme und Anlagen zur Netzsteuerung sind zumeist mindestens einfach redundant aufgebaut, Netzwerke und Verkehr können von mehr als einem NMC/NOC überwacht werden. Diese befinden sich bei redundanten Strukturen meist in unterschiedlichen Teilen oder Metropolregionen Deutschlands.

6. **Sicherheitssysteme:** Ein Großteil der eingesetzten Sicherheitssysteme und -software sind stark angepasste Spezialsysteme für Firewalls, IDS, IPS, SIEM und Netzwerkmonitoring. Diese überwachen und kontrollieren Netzwerkverkehr. Die Systeme werden vor allem bei größeren Betreibern in enger Zusammenarbeit mit den Herstellern angepasst oder selbst entwickelt.
7. **Isolierung und Segmentierung**: Systeme, Netze und Infrastrukturen werden von den Betreibern oftmals nach Schutzniveau segmentiert oder isoliert. Im Normalfall versuchen Betreiber, Systeme unterschiedlicher Schutzbedarfe getrennt voneinander zu betreiben.
8. **Sicherung von Peering**: IP-Routing und Peering wird teilweise durch Schutzmaßnahmen wie Hashes und RPKI gesichert. Die Technologien sind noch nicht verbreitet und befinden sich noch in Entwicklung oder Einführung.
9. **Mobile Verschlüsselung**: Der Mobilfunkverkehr wird auf der Funkstrecke zwischen Endgeräten und Basisstationen mittels A5-Chiffren verschlüsselt. In Deutschland sind dies vor allem die Chiffren A5/1 und A5/3 für GSM, die in ursprünglicher oder abgewandelter Form in GPRS als GEA3 und als KASUMI in UMTS integriert sind. Allen Chiffren ist gemein, dass theoretische und teils auch praktische Angriffsmöglichkeiten demonstriert wurden; Mobilfunkverkehr kann also als mit entsprechenden Ressourcen angreifbar angesehen werden.

5.3.1.3 Überwachung und Monitoring (Detektion und Reaktion)

1. **Zentrale Netzüberwachung:** Die gesamte IT-Infrastruktur wird von Betreibern in der Regel sowohl zentral als auch dezentral überwacht und gesteuert. IKT-Betreiber haben so meist eine auf mehrere Orte verteilte Überwachung und Information über das eigene Weitverkehrs-, Backbone- und weitere Netze. Die Überwachungszentren (NMCs) sind durchgängig redundant aufgebaut, meist überwachen mehrere NMCs das oder die Netzwerke.
2. **Überwachung**: Der Stand von Systemen zur Überwachung von Netzwerken und Infrastrukturen ist im IKT-Sektor generell sehr hoch und verbreitet. Infrastrukturen werden meist auf mehreren Schichten und von mehreren Stellen aus überwacht. So sind Ausfall oder Störungen schnell feststellbar. Ebenfalls überwachen Betreiber Netze und Systeme meist, je nach Schutzniveau, hinsichtlich Sicherheitsverstößen oder Angriffsversuchen.
3. **Anomalieerkennung** im Netzwerk, auf Systemen und Anwendungen: Zusätzlich und angelehnt an Überwachung setzen Betreiber vermehrt Systeme zur Anomalieerkennung im Netzwerk und in Systemen ein. Diese meist sehr stark angepassten Speziallösungen untersuchen auftretenden Netzwerkverkehr und Nutzerverhalten nach Mustern, die auf irreguläre Nutzung deuten. In vielen Fällen stellen sie intelligente Systeme dar, die anpassbare Filter bieten und aus Vorfällen für die Zukunft lernen.
4. **Automatisierte Abwehr**: Mit zunehmender Verbreitung befinden sich Systeme zur automatisierten Abwehr von Schadsoftware und Angreifern in Netzen und Systemen in Einführung. Diese Lösungen unterstützen, parallel zur Anomalieerkennung, die Abwehr von Angriffen durch Eingriffe oder Maßnahmen in Netzwerken oder auf Systemen. Dies kann eine Änderung von Routing in Internetanschlüssen umfassen, Blacklisting von IP-Bereichen oder einzelnen Netzen/Hosts, Beschränkung oder Drosselung des Verkehrs u. v. m.

5.3.1.4 Externe Abhängigkeiten

1. **Vertragliche Vorkehrungen**: Vereinzelt wird, vor allem bei größeren und zentralen Betreibern, durch Vorkehrungen und Maßnahmen in Verträgen zwischen IT-Dienstleistern und IKT-Betreibern ein Fokus auf Verfügbarkeitsanforderungen gesetzt. Einzelne Betreiber lassen sich so Knoten- und Kantendisjunktheit von Trassen und Leitungen, geographische Trennung und Sicherung von Rechenzentren und Anlagen etc. garantieren.

2. **Zusammenarbeit**: Betreiber tauschen sich untereinander und mit staatlichen Stellen wie dem BSI und nationalen und internationalen Organisationen (DENOG, IETF, IEEE, NANOG, Euro-IX) regelmäßig und je nach Branche unterschiedlich tief aus. Die Zusammenarbeit ist je nach Betreiber unterschiedlich ausgewachsen, vor allem für Angriffe und Bedrohungen gibt es jedoch Austauschforen.

5.3.1.5 Security Awareness

Sowohl Management als auch IT-Betrieb und Sicherheitsabteilungen zeigen eine sehr ausgereifte Awareness für Sicherheitsthemen. Das ist zum einen auf Anforderungen bereits bestehender Regulierungen wie dem TKG oder BDSG zurückzuführen, die Sicherheitsmaßnahmen in regulierten Infrastruktursektoren fordern. Andererseits reagieren Kunden der Dienstleistung „Sprach- und Datenübertragung“ sehr empfindlich bezüglich des Schutzes ihrer Kommunikation. Dies führt zu einer hohen Awareness und Sensibilität bei Betreibern für die Notwendigkeit von Cyber-Schutzmaßnahmen, um die Verfügbarkeit und auch Vertraulichkeit der Dienstleistung sicherzustellen.

Das Sicherheitsbewusstsein des Top-Managements der Betreiber zeigt sich in der bereits praktizierten Verankerung von IT-Sicherheitsaspekten in der Unternehmensstrategie sowie deren Platzierung in der Bewerbung des Unternehmens bzw. dem Marketing. Auch wird die Bereitstellung entsprechender Ressourcen weiter verstärkt und eigene IT-Sicherheitsbereiche aufgebaut (siehe Abschnitt 5.3.1.1).

5.3.2 Datenspeicherung und -verarbeitung (DL2)

In diesem Abschnitt werden zunächst allgemeine Beobachtungen zum Umsetzungsgrad der Cyber-Sicherheit in der Dienstleistung „Datenspeicherung und -verarbeitung“ beschrieben. Diese werden durch dedizierte Feststellungen für die einzelnen Themenschwerpunkte der Informationssicherheit in den nachfolgenden Unterkapiteln genauer erläutert und bewertet.

- Die Vorkehrungen im Bereich **Sicherheitsorganisation und -management** sind umfangreich, jedoch nicht immer so stark ausgebaut wie bei Betreibern der Dienstleistung „Sprach- und Datenübertragung“. Viele Betreiber unterhalten Sicherheitsbereiche, Managementsysteme (BCM für Notfallmanagement, ISMS für Sicherheitsmanagement) und Lagezentren (CERT, SOC). Oft sind diese Funktionen aber in andere Bereiche (IT-Betrieb, Überwachung) integriert und nicht immer explizit mit eigenem Personal und Funktionen besetzt.

  Betreiber bzw. KRITIS-relevante Unternehmensteile sind häufig nach dem Standard ISO 27001 zertifiziert. BSI IT-Grundschutz oder andere Standards werden nur selten zur Zertifizierung genutzt.

- Das Niveau der **technischen Cyber-Sicherheit** kann über den gesamten Sektor als hoch angesehen werden. Entsprechende technische Schutzmaßnahmen sind stark verbreitet und bewährt. Dabei muss berücksichtigt werden, dass ein Großteil der angebotenen Produkte sehr homogene technische Plattformen nutzt (Monokultur), weshalb einige Angriffe und Bedrohungen schnell einen sehr breiten Kreis an Betroffenen umfassen können. Aus diesem Grund legen Betreiber viel Wert auf die möglichst schnelle **Detektion** neuer Angriffe und Angriffsmuster sowie eine angemessene **Reaktion** darauf.

  Entsprechende Systeme zur Detektion und Reaktion sind bei Betreibern ebenfalls weit verbreitet, werden durch die Preisintensität des Marktes jedoch nicht immer für alle Produkte oder Dienstleistungen angeboten.

- Ein Großteil der Betreiber zeigt ein hohes Bewusstsein und Verständnis für Cyber-Sicherheit, das teilweise jedoch aufgrund von Marktdruck und Kundenwünschen (Preisgestaltung) nicht in konkrete Maßnahmen mündet. Dies ist der Tatsache geschuldet, dass einem Großteil der (Privat-)Kunden Preis und Funktionalitäten der angebotenen Produkte wichtiger sind als Hochverfügbarkeit oder umfassende Schutzmaßnahmen.

- Das Bewusstsein für **externe Abhängigkeiten** im Sektor und entsprechende Vorkehrungen sind vorhanden, jedoch mit unterschiedlicher Ausprägung. Die IKT-Systeme in der Dienstleistung werden

größtenteils von den Betreibern selbst betrieben, die Erbringung der Dienstleistung hängt aber stark von weiteren Betreibern ab, vor allem den Betreibern der entsprechenden Internet- und Weitverkehrsanbindungen (DL1) sowie Betreibern von Rechenzentren bzw. entsprechender Flächen oder Gebäude.

Entsprechende Vorkehrungen für Cyber-Sicherheit beim Outsourcing und dem Einkauf von Dienstleistungen werden zunehmend vertraglich gesichert, haben in der Vertrags- und Dienstleistungsgestaltung allerdings nicht immer oberste Priorität.

5.3.2.1 Sicherheitsorganisation und -management

1. **Verteilte CERTs:** Incident Response Teams und CERTs sind bei den Betreibern meist entweder im (übergreifenden) Konzern koordinierend tätig oder in übergreifende Systeme wie ISMS integriert. In vielen Organisationen finden sich jedoch noch keine oder nur wenig formalisierte CERT-Strukturen, die im eigentlichen Sinne als eigenes Team arbeiten; häufig sind die CERT-Funktionen auf verschiedene Fachabteilungen und IT-Teams verteilt.
2. **Sicherheitsorganisation**: Hoster betreiben häufig Management-Systeme für Informationssicherheit, die eine geregelte Sicherheitsorganisation bereitstellen, oder bauen diese aktuell auf. Die ISMS sind bei Hostern zum Großteil an ISO/IEC 27001 angelehnt, teilweise auch danach zertifiziert. Mit diesen Sicherheitsorganisationen wollen die Betreiber ihre Bemühungen für IT-Sicherheit in formalisierte Kanäle lenken und sich bei den mit Zertifizierung verbundenen Audits prüfen lassen.
3. **Notfallübungen**: IT-Hoster führen in der Regel praktische und theoretische Notfall- und Wiederanlaufübungen durch, teils praktisch oder als Simulation. Das Spektrum betrifft dabei den Ausfall einzelner Netzkomponenten, Server, Verbindungen, Stromversorgungen und Prozesse. Der Ausfall kompletter Rechenzentren und Standorte wird in der Regel selten durchgespielt. Mit diesen Notfallübungen soll die Vorbereitung auf reale Ausfälle verbessert und formalisiert werden. Notfallkonzepte und Pläne lehnen sich teils an Best Practices wie ISO 22301 und BSI IT-Grundschutz 100-4 an, sind jedoch häufig sehr stark angepasst oder Eigenentwicklungen.
4. **Austausch und Zusammenarbeit**: Betreiber nutzen zum Schutz vor koordinierten (Massen-)Angriffen durch Bots, DDoS, Reflektorangriffe etc. häufig Koordinierungsforen und Austauschmöglichkeiten mit anderen Betreibern und staatlichen Stellen. Dort werden aktuelle Angriffe, Quellen und Best Practices zum Schutz ausgetauscht.

5.3.2.2 Technische IT-Sicherheit

1. **Redundanz**: IT-Hoster haben in der Regel redundante, räumlich und technisch getrennte Rechenzentren. Bei Ausfall eines Rechenzentrum können Server und Dienste (abhängig von der Größe des Rechenzentrums) zeitnah in die Ausfallzentren migriert werden. Im Endkundenmarkt gibt es aus Kostengründen meist keine hundertprozentige Redundanz. Server und Dienste in den Rechenzentren selbst sind zwar redundant, müssen beim Ausfall des Rechenzentrums jedoch teilweise wiederhergestellt und erneut gestartet werden.

   Rootserver von Endkunden sind in der Regel nicht vollständig redundant, sondern nutzen redundante Komponenten (Netzteile, Stromversorgung, Festplatten).

   Die Hoster nutzen durchweg mehrere Internetprovider zum Anschluss ans Internet. Teilweise sind die Betreiber auch an mehrere IXPs zum Peering angeschlossen.
2. **Schutz in Internetanbindungen**: Hoster schützen sich vor Massenangriffen von außen häufig durch Maßnahmen in den Internetanbindungen oder durch Lösungen ihrer Carrier (BGP-Blackholing, Anomalieerkennung, Blacklisting etc.). Diese Systeme oder Maßnahmen auf dem Leitungs- oder Vermittlungsweg erlauben es Carriern, Verkehr von aktuellen Angriffen nicht an ihre Kunden

weiterzuleiten, ganze Länder, Adressbereiche oder Netzwerke zeitweise oder dauerhaft zu sperren. Der maliziöse Verkehr kann in diesem Fall Hoster und deren Kunden im Ansatz schon nicht erreichen.

5.3.2.3 Überwachung und Monitoring (Detektion und Reaktion)

1. **Zentrale Netzüberwachung**: Der Verkehr innerhalb des Servernetzwerk und insbesondere an der Netzgrenze zum Internet wird in der Regel durch entsprechende netzbasierte Systeme überwacht. Ebenso filtern entsprechende Geräte Malware aus der Datenübertragung (Internet, Proxy, Mail).
2. **Anomalieerkennung:** Betreiber überwachen mithilfe von Angriffserkennungssystemen (IDS) und/oder Systemen zur Vorfalls- und Eventkorrelation (SIEM) den Netzwerkverkehr im Netzwerk und auch die Vorgänge auf einzelnen Systemen auf Anomalien. So sollen Angriffe, Übernahmen und Störung entdeckt und später behoben werden. Teilweise können auf diese Weise einzelne, störende Systeme vom Computer- oder Stromnetz getrennt werden.

5.3.2.4 Externe Abhängigkeiten

Die externen Abhängigkeiten sind analog zu DL1 (siehe Abschnitt 5.3.1.4).

5.3.2.5 Security Awareness

Analog zur Dienstleistung „Sprach- und Datenübertragung“ (DL1) zeigen Betreiber der Dienstleistung „Datenspeicherung und -verarbeitung“ ein hohes Bewusstsein (Awareness) für Themen der Cyber-Sicherheit. Kunden (vor allem Privatkunden) von IT-Hosting-Angeboten betrachten Sicherheitsaspekte wie die Schaffung von Redundanzen im Vergleich zur Preisgestaltung des Angebots häufig jedoch als nachrangig. Daher existiert zwar ein hohes Verständnis und Bewusstsein für Sicherheit, daraus resultierende Maßnahmen rücken für die Betreiber vor dem Gedanken des Marktdrucks und der Wettbewerbsfähigkeit aber eher in den Hintergrund und können nur selten entsprechend ihrer Relevanz umgesetzt werden.

5.4 Herausforderungen und Trends

Die Herausforderungen und Trends im vielschichtigen IKT-Sektor lassen sich aus vielen Perspektiven betrachten. Die Studie versucht, angelehnt an vorige Abschnitte, Trends und Herausforderungen jeweils zusammengefasst in den folgenden Kategorien zu beschreiben:

1. **Organisatorisch**: Herausforderungen und Trends, die die interne Struktur der Betreiber und deren Sicherheitsorganisationen betreffen. Besonders multinationale Konzerne stehen in Deutschland vor der Herausforderung, dass sich die KRITIS-relevanten Infrastrukturen und Organisationen teilweise nicht in Deutschland befinden. Als Trend lässt sich im Sektor ein auf hohem Niveau steigendes Bewusstsein für Cyber-Sicherheit und weitere Investitionen in organisatorische Managementsysteme wie ISMS, SOCs und CERTs erkennen. Ebenfalls wandelt sich der organisatorische Schutz vor Cyber-Angriffen von der reinen Prävention hin zu einer Verstärkung der Detektion und der reaktiven Fähigkeiten, um Angriffe besser erkennen und bekämpfen zu können.
2. **Technisch**: Änderungen und Entwicklungen eingesetzter Technologien in Bezug auf Betrieb, Produktion oder Schutz von IKT. Der IKT-Sektor und die Betreiber in beiden Dienstleistungen stehen vor den Herausforderungen eines zunehmenden Wandels der eingesetzten Technologien, der einerseits sehr homogene Systeme und Netze hervorbringt und damit Massenangriffe ermöglicht und fördert, wie etwa bei Monokulturen im Hosting und der Verlagerung zu IP-Netzen. Andererseits lässt der technologische Umbruch Systeme komplexer und anfälliger für auch fortschrittliche Angriffe werden (APTs, Nachrichtendienste), vor allem durch die zunehmende (fast vollständige) Vernetzung und Digitalisierung, die hier im Sektor einen höheren Schutz von Weitverkehrsnetzen und mobiler Kommunikation und Geräten fordert.

3. **Regulatorisch**: Auswirkungen und Herausforderungen an und durch nationale Regulierung. Die Unternehmen der Dienstleistung *Sprach- und Datenübertragung* unterliegen der Regulierung (über das TKG), die speziell für das „Internet“ im KRITIS-Kontext jedoch vor Herausforderungen steht. Einerseits unterliegt ein Großteil des Internets einer Selbstregulierung der jeweiligen Betreiber, andererseits besteht das Internet aus einer Vielzahl an unterschiedlichen Technologien, Betreibern und Infrastrukturen auch unterschiedlicher Länder, die schwierig national zu regulieren (und zu schützen) sind. Unternehmen der Dienstleistung *Datenspeicherung und -verarbeitung* fallen größtenteils nicht unter das TKG.
4. **Marktbezogen**: Entwicklungen und Marktbewegungen, die Auswirkungen auf eingesetzte Technologien, Verfahren und Schutzniveaus der Dienstleistungen haben. Im IKT-Sektor bedeutet eine Zunahme mobiler Nutzer und die zunehmende Umstellung auf IP-basierte Kommunikation eine weitere Erhöhung der Kritikalität des Internets und der beteiligten Infrastrukturen. Das Bewusstsein für die Verwundbarkeit von internetbasierter Kommunikation steigt zwar, der Wille von Endkunden, entsprechende Redundanzen oder Schutzmaßnahmen mitzutragen, steigt jedoch nicht in gleichem Maße. Eine Herausforderung im IKT-Sektor sind die teilweise mehrfach verschachtelten Zuständigkeiten für Infrastrukturen wie Leitungen, Trassen oder auch Rechenzentren, die ein durchgängiges Schutzniveau erschweren.

Organisatorisch

1. **Multinationale Konzerne**: Große Betreiber, vor allem in Bereichen der DL1, haben meist hierarchische und zentralisierte Sicherheitsorganisationen, die relevante Funktionen überwachen und steuern. Diese Organisationen sind teilweise nicht in Deutschland angesiedelt und steuern Sicherheitsbelange der deutschen Konzernteile/Tochterfirmen/Infrastrukturen aus dem Ausland. Speziell für das IT-Sicherheitsgesetz könnte für die zunehmend international organisierten Betreiber (NMC/NOC, SOCs, CERTs im nahen osteuropäischen Ausland) bedeuten, dass Sicherheitsstrukturen, Prozesse und Meldewege in Deutschland dupliziert oder abgebildet werden müssten.
2. **Detektion/Reaktion/Prävention**: Der Trend bei der Behandlung und dem Schutz vor Angriffen und Sicherheitsvorfällen geht zunehmend hin zu einer Stärkung der Detektions- und Reaktionsfähigkeiten. Wurde in den letzten ein bis zwei Jahrzehnten primär auf einen starken Perimeterschutz zur Abwehr von Angriffen gesetzt, zeigt sich in den letzten Jahren ein vermehrter Einsatz von zusätzlichen, über den Bereich der Prävention hinausgehenden Systemen zur Detektion von Angriffen und Reaktion auf durchgeführte oder aktive Sicherheitsvorfälle. Das umfasst die Stärkung und Integration bestehender technischer Schutz- und Überwachungsmaßnahmen wie Netzwerkmonitoring, Anomalieerkennung, Auswertung von Logdateien etc. Ziel ist es, Angriffe nicht nur (statisch) abzuwehren, sondern umfassend zu erkennen und Reaktionsmöglichkeiten zu schaffen.
3. **ISMS und BCM(S)**: In der Branche steigt das Bewusstsein dafür, dass (zertifizierte) Informationssicherheit- und Business Continuity Management Systeme (ISMS und BCMS) einen Beitrag zum Unternehmenserfolg leisten. Das lässt sich bei einer Bandbreite von Betreibern beobachten, von kritischen bis weniger kritischen, die aber alle zumindest aus Eigenmotivation und Marktpositionierung ein Interesse an organisierten Sicherheitsprozessen haben.

Technisch

1. **Angreifbares Internet-Routing**: Die Struktur und Funktionsweise von Internet-Routing und (globalem) Peering haben sich zwar als widerstandsfähig erwiesen, bleiben technisch jedoch fragil. Angriffe wie Prefix-Hijacking, more-specific Prefix-Angriffe, Fehlkonfigurationen von Peering/BGP und Re-Announcements von Routen/Prefixen bleiben weiterhin möglich. Einzelne Angriffe oder Fehlkonfigurationen können so zeitweise die Internetversorgung ganzer Netzbereiche, Dienste oder Länder stören oder für missbräuchliche Zwecke gebraucht werden (wie Angriffe, Spam, DDoS).

2. **Monokulturen:** Durch die zunehmende Vereinheitlichung von Kommunikationsnetzen und auch Serversystemen nehmen die Verwundbarkeiten dieser technologischen Monokulturen zu. Kommunikationsnetze konvergieren zu IP-basierten Netzen, Serversysteme für Massen- und Standarddienste basieren zu einem zunehmenden Teil auf LAMP (Linux, Apache, MySQL, PHP) und Endsysteme auf wenigen, standardisierten Plattformen und Programmen.
3. **Verschlüsselung auf Leitungsebene:** Trotz des zunehmenden Bewusstseins, dass Daten bei der Übertragung über Weitverkehrsnetze auf den unteren Schichten der Übertragungstechnik vor Abhören und Manipulation geschützt werden sollten, wird dies aufgrund der aufwendigen Technik noch nicht weitreichend praktiziert. Verschlüsselungen auf Layer 2 von WAN- oder Backbone-Verbindungen ist technisch und mit aktuellen Produkten möglich, jedoch vor allem für hohe Datenraten und Kapazitäten prohibitiv teuer. Die notwendige Verschlüsselung muss daher derzeit primär auf höheren Schichten (ab Layer 3, z. B. durch IPSec) vorgenommen werden.
4. **Trassen:** Die Wegstrecken von in der Erde verlegten Leitungen von Zugangs- und Backbone-Netzen können mit überschaubarem Aufwand ermittelt und angegriffen werden. Einzelne Trassen können und werden so mit entsprechendem Wissen mutwillig zerstört, manipuliert und abgehört. Das umfasst die Trassen und Leitungen an sich, aber ebenfalls passive und aktive Netzwerktechnik wie Repeaterstationen, Weichen etc., die mit entsprechendem Wissen beschädigt werden (können). Durch die Abgelegenheit und Vielzahl dieser physikalisch angreifbaren Elemente kommen entsprechende Beschädigungen wiederholt vor und können nicht immer zeitnah behoben oder verhindert werden.

   Aus Effizienzgründen vor allem in spärlich oder sehr dicht bebauten Gebieten oder aufgrund von Trassenengpässen werden häufig Trassen oder Repeaterstationen durch mehrere Provider geteilt. Dadurch können (unbewusst) Single Points of Failure bei vermeintlich redundanten Leitungen entstehen. Die Konsolidierung von eigentlich separaten Leitungen, Trassen und Räumlichkeiten kann ebenso durch Marktkonsolidierung, Unteraufträgen usw. erfolgen, wenn Marktteilnehmer Teile ihres Betriebs auslagern, verkaufen oder teilen.
5. **Made in Germany:** Durch die Kontroversen über Tätigkeiten ausländischer Nachrichtendienste und deren mögliche Verstrickungen mit IT-Herstellern gibt es den zunehmenden Wunsch nach alternativen Anbietern für Netzwerk- und Verschlüsselungstechnik „Made in Germany“ oder zumindest von Herstellern mit transparenten und ggf. auditierbaren Herstellungsprozessen. Neben Spezialprodukten für Hochsicherheitsanforderungen gibt es wenig marktdurchdringende Angebote, die weitflächig bezogen und genutzt werden können.
6. **Mobile Verschlüsselung**: Die in Mobilfunknetzen genutzten Verschlüsselungen gelten teilweise als angreifbar oder gebrochen (A5/1, A5/3, KASUMI). Vertraulicher oder schützenswerter Verkehr in mobilen Netzen muss demzufolge auf anderen Schichten durch kryptographische oder andere Maßnahmen geschützt werden.
7. **Advanced Persistent Threats**: Neben Massenangriffen auf Monokulturen ließen sich verstärkt auch öffentlichkeitswirksame, sehr gezielte Angriffe über IT- und Internetinfrastruktur in den letzten Jahren beobachten. Die sogenannten Advanced Persistent Threats (APTs) sind sehr gezielte, sorgfältig geplante und durchgeführte Angriffe von Akteuren mit entsprechenden Ressourcen. Es ist davon auszugehen, dass es bei APTs eine sehr hohe Dunkelziffer gibt und sowohl staatliche, halbstaatliche als auch kriminelle Organisationen mit entsprechend komplexen und zeitaufwändigen Attacken auch KRITIS-Betreiber angreifen. Das Bedrohungsniveau steigt also nicht nur durch Standardisierung der Systeme und Angriffe, sondern auch durch extreme Spezialisierung und Komplexität von bestimmten Angriffen.
8. **IPv6**: Die nächste Version des Internetprotokolls wird weiterhin nur langsam eingeführt; durch die zunehmende Adressknappheit der bisherigen Protokolls IPv4 und neue Nutzungsszenarien (Multicast, mobile Nutzer, Heimvernetzung usw.) nimmt der Antrieb für eine weitergreifende Einführung von IPv6 aber zu. Dabei sind technische Hürden für die Einführung bei Betreibern und Kunden abzusehen; auch wird durch den wahrscheinlich sehr langen Parallelbetrieb von IPv4 und IPv6 die Komplexität und

Fehleranfälligkeit der beteiligten Systeme zunehmen. Hinzu kommen teils weitgreifende, notwendige technische und organisatorische Änderungen in Systemen (software- und verfahrensseitig), die möglicherweise neue Angriffsflächen und Schwachstellen bieten. Dies betrifft alle Bereiche der Verbindung von Client-Systemen, über die Zugangs- und Backbonenetze bis zu zentralen Systemen und Diensten.

Regulatorisch

1. **Internetregulierung**: „Das Internet" ist ein Patchwork-Konstrukt und in nationalen Alleingängen oder Regulierung nur sehr schwer regulierbar. In Deutschland wird zum einen sehr viel internationaler Internetverkehr ausgetauscht (mittels Peering, Transit), zum anderen wird ein Großteil des deutschen Internetverkehrs gar nicht in Deutschland ausgetauscht, gespeichert oder verarbeitet. Es ist damit sehr schwer, „Internet" in Deutschland außerhalb der Zugänge (TKG, PTSG) überhaupt zu regulieren, wenn ein Großteil der Leistungen außerhalb Deutschland stattfindet oder geographisch nicht deterministisch lokalisierbar ist.

   Weiterhin besteht die Schwierigkeit, „deutschen" Internetverkehr fest zu definieren. Austausch über das Internet zwischen zwei Kommunikationspartnern in Deutschland kann häufig zum Großteil außerhalb Deutschlands stattfinden, Content und Dienste sind teilweise geographisch nur mit erheblichem Aufwand lokalisierbar (CDNs, Cloud etc.), und damit nur sehr schwer als „deutscher" Internetverkehr definier- und regulierbar.

Marktbezogen

1. **Mobile Nutzer**: Die Kunden- und Nutzungsprofile von Telekommunikation und Internet wandeln sich von ortsgebundener zu mobiler Kommunikation. Die Penetrationsrate mobiler Telekommunikation in Deutschland steigt seit Jahren stetig (im Jahr 2013 auf 143 Prozent), während die Zahl der Festnetzanschlüsse sinkt. Die Nachfrage von Dienstleistungen im Mobilfunk wird daher weiter zunehmen, während die von ortsgebundenen Zugangsnetzen sinkt. Die IKT-Abhängigkeit bleibt davon unberührt, da sie sich in beiden Fällen bereits auf einem sehr hohen Niveau befindet.
2. **Zunahme von IP-basierter Kommunikation**: Telekommunikation und Sprachübermittlung verschieben sich zunehmend auf IP-basierte Kommunikationswege. VoIP-Kommunikation machte 2013 laut BNetzA bereits einen Umfang von 30 Prozent am Gesamtvolumen aus, mit steigender Tendenz. So will beispielsweise die Telekom bis 2018 komplett auf VoIP umstellen. Damit einhergehend verschieben sich die Abhängigkeiten und Verwundbarkeiten der Telekommunikation weiter von denen separater Netze zu jenen der IP-Kommunikation in Datennetzen.

   Analog wächst die Abhängigkeit der Telefoniedienste von der Verfügbarkeit des Internets, der Backbone-Netze und der IP-Vermittlungsinfrastruktur. Durch die Zunahme der IP-basierten Telekommunikation werden Sprachverbindungen vermehrt über herkömmliche Internetverbindungen und Daten-Backbones übertragen. Die Kritikalität des Internets und seiner Komponenten (in den Bereichen Zugang, Vermittlung und Übertragung) für Betreiber sowie die Kritikalität der Internetanbindungen für Kunden steigen damit weiter an.
3. **Bewusstsein von Abhörmöglichkeiten**: Durch die Berichterstattung der letzten zwei Jahre zu den Abhörmöglichkeiten und Tätigkeiten von (ausländischen) Nachrichtendiensten an Internet-Infrastrukturen und Diensten, steigt bei Kunden das Bewusstsein der Verwundbarkeit und Notwendigkeit zum Schutz von Internet- und IKT-basierter Telekommunikation.
4. **Subunternehmer**: Nutzen Unternehmen (ausgelagerte) IT-Leistungen, ist nicht immer feststellbar, ob die Leistungen nur durch den eigentlichen Auftragnehmer erbracht werden oder ob weitere Subunternehmer involviert sind. Unternehmen schließen Verträge und SLAs mit den eigentlichen Auftragnehmern, die gegebenenfalls nicht von allen Subunternehmen eingehalten und beachtet werden müssen. Zum Teil fehlt Transparenz für Subaufträge, welche Subunternehmer konkret beteiligt sind und ob Leistungen z. B. ins Ausland verlagert oder dort erbracht werden. Die Qualität und Sicherheit der Leistungserbringungen muss dadurch nicht immer steigen.

5. **Private WAN-Leitungen**: Unternehmen und Betreiber nutzen für Fernverkehrsstrecken häufig „private“ WAN-Verbindungen wie Dark-Fiber oder andere exklusiv genutzte Produkte. Dabei lässt sich jedoch nicht immer garantieren, dass diese Leitungen für den Kunden von Anfang bis Ende privat und exklusiv sind, ohne weitere, aktive und geteilt genutzte Technik.

   Beim Kauf von WAN-Strecken ist häufig nicht bekannt oder bewusst, dass selbst private Leitungen nicht nur durch Technik und Aufsicht der WAN-Betreibers gehen, sondern möglicherweise Infrastrukturen durch mehrere Betreiber genutzt und geteilt werden.

6. **Preis für Redundanz**: Aus Befragungen verschiedener Betreiber ergibt sich, dass sowohl Kunden als auch der Markt generell an einer hohen Ausfallsicherheit interessiert sind. Im Gegenzug mangelt es jedoch an der Bereitschaft, für möglicherweise ausfallsichere(re) Produkte und Dienstleistungen entsprechend höhere Preise zu zahlen.

6 Schlussfolgerungen und Ausblick

6.1 Notwendiger Handlungsbedarf

Der Handlungsbedarf im Sektor IKT umfasst für die öffentliche Hand vor allem die Schaffung übergreifender sektorweiter Standards und Austauschplattformen für Cyber-Sicherheit.

Sektorweite Standards könnten in Form von Umsetzungshilfen wie KRITIS-Best-Practices oder auch BSI-Grundschutzbausteinen für KRITIS-Organisationen mit Betreibern und Verbänden diskutiert werden. Mit solchen Umsetzungshilfen könnte das BSI Standards und Maßnahmen empfehlen, um Betreibern den Aufbau von Strukturen für KRITIS oder Cyber-Sicherheit zu erleichtern. Eine Sammlung von Best Practices im Sektor könnte Betreibern als Orientierungshilfe für den Aufbau von KRITIS-Organisationen, CERTs oder Lagezentren dienen und beim Schutz einzelner systemischer oder neuralgischer Komponenten wie Weitverkehrsnetzen oder der Internetsignalisierung unterstützen.

Bestehende Kommunikationsplattformen und Austauschmöglichkeiten zwischen Betreibern selbst und mit dem BSI sollten gestärkt und ausgebaut werden, um sowohl den Austausch zwischen Wirtschaft und öffentlicher Hand zu vertiefen als auch kleineren oder aktuell noch nicht im UP KRITIS organisierten Betreibern eine Möglichkeit zur Mitarbeit oder Information zu schaffen sowie generell die Transparenz auch im Hinblick auf Meldewesen, Statistiken und gemeinsame Lagebilder zu erhöhen. Der UP KRITIS verfolgt diese Ziele bereits, jedoch hat sich in der Betreiberbefragung gezeigt, dass eine Vertiefung der Kommunikationsstrukturen und Erweiterung des Teilnehmerkreises wünschenswert ist. Ferner würde eine stärkere Internationalisierung und vorsichtigere Einstufung sowohl von Advisories als auch von Meldungen an entsprechende Behörden die Einbindung internationaler Betreiber und deren Sicherheitsorganisationen erleichtern.

Handlungsempfehlungen an die KRITIS-Betreiber im Sektor beziehen sich auf eine bessere Information der Kunden zu Kritikalitäten und Verfügbarkeiten von IKT-Dienstleistungen, eine stärkere Sicherung vor allem von Weitverkehrsstrecken und Zugangsgeräten beim Kunden. Mit mehr Transparenz in Verträgen und Informationen könnte das Bewusstsein für IKT-Abhängigkeiten bei Kunden erhöht werden. Speziell Weitverkehrsstrecken und deren Anlagen sind für den Sektor neuralgisch und könnten sektorweit oder -übergreifend besser geschützt werden.

BSI Grundschutz-Baustein „KRITIS-Organisation“: Für Betreiber, die unter die KRITIS-Definition oder Regelungen des in Entstehung befindlichen IT-Sicherheitsgesetzes fallen, könnten ein BSI IT-Grundschutzbaustein oder adäquate Cyber-Sicherheitsempfehlungen bei der Schaffung der entsprechenden Sicherheits- und Meldeorganisationen sehr hilfreich sein. Betreiber stehen aktuell vor der Herausforderung, die zum Teil verteilten Sicherheitsorganisationen, Incident Response Abteilungen (CERTs), Sicherheitsverantwortlichen etc. gemäß den voraussichtlichen Vorgaben des IT-SiG abzubilden sowie Schnittstellen zur BNetzA zu schaffen oder zu schärfen.

BSI Grundschutz-Baustein oder Best Practice „Peering für KMU oder kleine Carrier“: Aus verschiedenen Gründen werden kleine und mittlere IT-Betreiber zunehmend zu Carriern im Sinne von RIPE. Aus Gründen der IPv4-Knappheit haben sie sich beim RIPE als Local Internet Registry (LIR) registriert, um IPv4-Bereiche (und ggf. IPv6-Bereiche) zu erhalten, und haben durch die Zuteilung einer Autonomous System Number (ASN) die Möglichkeit, mit anderen Carriern direkt oder über IXPs zu peeren. Um dabei das Sicherheitsniveau und grundlegende Sicherheitsmaßnahmen beim Peering umzusetzen, könnte die verpflichtende oder empfehlende Umsetzung von BGP/Peering Best Practices mit einem BSI IT-Grundschutzbaustein hilfreich sein.

BSI Grundschutz-Baustein oder Best Practice „Schutz von WAN-Strecken“: Erstellung von Richtlinien für Nutzer von WAN-Strecken oder „outsourced Backbones“, um die Weitverkehrsstrecken zu schützen und das Sicherheitsniveau bei vermuteten Private Lines oder Dark-Fibers zu erhöhen. Das umfasst Verschlüsselung auf Layer2 (oder Layer3) bei Weitverkehrsstrecken und genauere Betrachtungen bei der

Wahl von WAN-Providern mit Fokus auf SPOFs bei redundanten Anbindungen (Überland-Trassen oder Verteilern) und möglichen nachgelagerten Subunternehmer-Kaskaden.

BSI-Empfehlungen oder nationaler Standard für CERTs: Für die Einrichtung von CERTs, Notfall- oder Lageorganisationen könnten Empfehlungen des BSI oder ein Standard sehr hilfreich sein. Aktuell gibt es unterschiedlichste Vorgaben für die Einrichtung von CERTs/SIRTs auf europäischer und internationaler Ebene (z. B. ENISA, cert.org, NIST 2013), jedoch mit unklaren Handlungs- und Vorgehensempfehlungen. Ein einheitlicher Satz von Vorgaben oder Empfehlungen für Einrichtung, Aufbau und Weiterentwicklung von CERTs könnte die Qualität und Effektivität dieser Organisationen erhöhen.

Zusammenarbeit BSI und Community: Betreiber haben den Wunsch nach mehr Abstimmungen und Austausch zwischen den Betreibern und dem BSI auf Fachebene geäußert. Foren dafür sind teilweise nicht vorhanden bzw. unklar. Der gewünschte Austausch könnte in KRITIS-Arbeitsgruppen oder auch außerhalb erfolgen. Ebenso wünschen sich viele Betreiber mehr Transparenz und Feedback vom BSI bei Meldungen, Statistiken oder Bedrohungen, wenn möglich als direkter Dialog. Da der UP KRITIS genau diese Ziele bereits adressiert und weiterführende Branchenarbeitskreise (BAK) anbietet, ist es möglicherweise ausreichend, dies an die Betreiber zu kommunizieren und zu einer aktiven Mitarbeit aufzufordern. Darüber hinaus können die behandelten Inhalte vertieft und die Arbeitskreise um weitere Teilnehmer erweitert werden. Ein Austausch mit weiteren Betreibern, die an einem Austausch zu Themen der Cyber-Sicherheit teilhaben wollen, könnte über alternative Foren initiiert werden.

Englische Meldungen an betreffende Behörden (BSI, BNetzA): Zurzeit ist noch unklar, ob Meldungen zu Sicherheitsvorfällen von KRITIS-Betreibern an betreffende Behörden (BSI, BNetzA) ausschließlich in deutscher Sprache erfolgen können. Vor allem bei größeren KRITIS-Betreibern oder Konzernen sind die verteilten oder im Ausland zentralisierten Sicherheitsorganisationen nicht in jedem Fall mit deutschsprachigen Mitarbeitern besetzt. Betreiber, deren CERT oder zentrale Sicherheitsorganisation im Ausland angesiedelt ist, können möglicherweise nicht immer garantieren, deutschsprachige Meldungen an betreffende Behörden (BSI, BNetzA) zu senden. Es sollte in Betracht gezogen werden, englischsprachige Meldungen an die entsprechenden Regulierungsbehörden oder Stellen in Deutschland zuzulassen.

Englische und VS/TLP-Advisories von betreffenden Behörden (BSI, BNetzA): In Zusammenhang mit englischsprachigen Betreibermeldungen an betreffende Behörden (BSI, BNetzA) stehen vor allem große und verteilte KRITIS-Betreiber vor dem Problem, mit deutschsprachigen und eingestuften Advisories der betreffenden Behörden (BSI, BNetzA) umzugehen. Solche Betreiber nutzen häufig verteilte Sicherheitsorganisationen oder CERTs, die teilweise oder vollständig mit nicht-deutschsprachigen Mitarbeitern besetzt sind und die meist nicht für die Behandlung von eingestuften Informationen ermächtigt sind. Das führt zu Koordinierungs- und Kommunikationsproblemen in großen Konzernen, in denen entsprechende Advisories der betreffenden Behörden (BSI, BNetzA) nicht innerhalb der Sicherheitsorganisation verteilt oder kommuniziert werden können. Es ist zu evaluieren, ob ggf. zusätzlich englischsprachige und nicht-eingestufte Advisories an Betreiber mit entsprechendem Bedarf verschickt werden können.

Sicherung von Trassen und Repeater-/Verteilerstationen: Die Absicherung vor unbefugtem Zugang und Manipulation von Infrastrukturen kann durch zusätzliche Sicherungsmechanismen der Netzbetreiber und Carrier erhöht werden. Es ist zu prüfen, welche Maßnahmen einen wirkungsvollen Schutz insbesondere unter Berücksichtigung des Standorts der Stationen mit angemessenem Aufwand bieten und umgesetzt werden können.

Aufklärung und Information von Kunden: ISPs und Anbieter von Hostingdiensten können weiterführende Informationen zu BCM und Notfallmanagement sowie zu möglichen Ausfallszenarien und deren Konsequenzen für Verfügbarkeiten der angebotenen Dienstleistungen bereitstellen und so das Bewusstsein ihrer Kunden schärfen. Derzeit sind sowohl Privat- als auch Geschäftskunden nur unzureichend über die genaue Bedeutung von SLAs und darin vereinbarten Verfügbarkeitsangaben informiert, sodass die Risiken mangelnder Redundanzen oft falsch eingeschätzt werden.

Transparenz in Verträgen zwischen Providern und Geschäftskunden: Durch die Abfrage der Kritikalität der in Anspruch genommenen Dienstleistung für den Kunden, besonders im Geschäftskundenbereich, kann mehr Transparenz geschaffen werden. Sicherungsmaßnahmen könnten dann entsprechend der Kritikalität der Verfügbarkeit vereinbart werden.

Sichere Default-Konfiguration von CPE durch Access-Provider: Teilnehmer-Endgeräte (Customer Premises Equipment, CPE), wie DSL-Modems, Router etc. sollten standardmäßig „sicher" konfiguriert werden, wobei sowohl Provider-abhängige als auch übergreifende Sicherheitsstandards und Konfigurationsparameter berücksichtigt werden sollten. Das betrifft auch die SNMP-Konfiguration, die Einschränkung von Telnet/HTTP-Zugriffen aus dem Internet, verwendete Betriebssystem-Images etc. Zum Schutz der Privatsphäre und für den Datenschutz der Endanwender sollte die Verwendung von TR-069 (Protokoll zum Datenaustausch zwischen Provider und Teilnehmer-Endgerät, z. B. zur Fernkonfiguration) deaktiviert werden. Ist der Einsatz dennoch notwendig, sollte der Endkunde zuvor über Einsatzzweck und Funktionsweise des Protokolls sowie datenschutzrechtliche Auswirkungen informiert und ggf. sein Einverständnis eingeholt werden.

6.2 Weiterer Untersuchungsbedarf

Weiterer Untersuchungsbedarf richtet sich vor allem an die öffentliche Hand zur Untersuchung von methodisch sowie betreiberspezifisch und sektorweit noch ungeklärten Fragestellungen.

Im Umgang mit den in der Telekommunikationsbranche vorhandenen großen, internationalen Konzernen gibt es noch ungeklärte Sachverhalte. So können Steuerungs- und Sicherheitsorganisationen für in Deutschland betriebene Netze und Infrastrukturen teilweise außerhalb Deutschlands angesiedelt sein. Der Schutz dieser Infrastrukturen ist dabei für die (deutsche) öffentliche Hand schwierig, was auch auf europäischer Ebene weiter untersucht werden sollte.

Innerhalb Deutschlands ist eine Feststellung der Kritikalität einzelner Betreiber oder auch Anlagen im IKT-Sektor mitunter ebenfalls schwierig. Dass manche Anlagen für den Internetverkehr in Deutschland neuralgisch sind, ist für einzelne Betreiber und auch die öffentliche Hand teils nur schwer feststellbar, sei es durch mangelndes systemisches Wissen über Trassen von Weitverkehrsleitungen, Knotenpunkte und Rechenzentren in Deutschland, aber auch durch eine Kaskade von Unterauftragnehmern und Dienstleistern.

Forschungsbedarf für KRITIS speziell im IKT-Sektor besteht bei einer Definition und Abgrenzung von „deutschem Internetverkehr" und auch dem „deutschen Internet". Beides sollte teilweise innerhalb des KRITIS-Sektors IKT untersucht und geschützt werden. Eine allgemeine Definition des Begriffs „deutscher Internetverkehr" und eine Eingrenzung, wo genau dieser stattfindet, sowie welche Komponenten und Leitungen zum deutschen (schutzbedürftigen) Internet gehören, ist jedoch sehr schwierig.

„Deutsches" Internet: In den KRITIS-Befragungen im IKT-Sektor und speziell mit Internet-Betreibern hat sich schnell gezeigt, dass sich „das Internet in Deutschland" sehr schwer definieren und damit auch regulieren lässt. Telefonnetze lassen sich geographisch sehr exakt eingrenzen, mit Leitungen und Knotenpunkten in Deutschland und Übergabepunkte in Fremdnetze und das Ausland. Es ist jedoch äußerst schwierig zu definieren, was „deutscher Internetverkehr" ist und welche Strukturen das „deutsche Internet" ausmachen, das innerhalb des KRITIS-Sektors IKT untersucht und geschützt werden soll. Das Internet als technologisches Konstrukt basiert stark auf Selbst- und Marktregulierung und lässt sich innerhalb von Staatsgrenzen nur schwer schützen, da selbst Kommunikation über Verbindungen, die sowohl in Deutschland starten als auch terminieren, ohne Weiteres über Staats- oder Kontinentgrenzen ausgetauscht werden kann, „deutsche" Server oder Internetdienste geographisch nur sehr schwer auf Deutschland einzugrenzen sind (Clouddienste, CDNs) und somit die Handhabe von nationalen Regulierungsvorhaben möglicherweise mangels Zuständigkeit gar nicht greifen kann. Beispiele sind die internationale (oder US-amerikanische) IP-Adressverwaltung, Sicherheitsorganisationen oder Infrastrukturen von Betreibern im Ausland etc.

Kritikalität von Backbone-Netzen: Die Kritikalität von Infrastrukturen, die nur mittelbar Endkunden bedienen, ist sehr schwer mess- und quantifizierbar. Betreiber von Backbone-Netzen, aber auch IXPs und PoP, bedienen fast ausschließlich Geschäftskunden, die als zwischengeschaltete Stelle Endkunden oder weitere Geschäftskunden versorgen. Für die Betreiber der zugrundeliegenden Infrastrukturen ist nicht feststellbar, welche Art und Masse von Verkehr die eigenen Backbones durchläuft („Layer-2 Traffic“) und wie schützenswert oder kritisch dieser ist.

Kritikalität von „unsichtbaren“ Anlagen im Backbone: Einige Anlagen oder Risikoelemente in Backbones oder Weitverkehrsnetzen sind sehr schwer ermittelbar. Das umfasst Repeaterstationen oder weitere aktive Netzwerktechnik in der Fläche. Diese Anlagen sind teilweise sehr abgelegen, somit nur schwer erreich- und überwachbar, und werden teilweise zwischen mehreren Betreibern geteilt. Die Ermittlung der Kritikalität und das mögliche Vorhandensein von neuralgischen Punkten innerhalb dieser Studie war nicht möglich.

Verwundbare WANs/Backbones: Trassen, insbesondere in ländlichen Gegenden, bilden häufig Single Points of Failure. Ebenfalls sind WANs, vor allem in Szenarien mit mehreren kaskadierten Betreibern, möglicherweise leichter abhörbar als es die Bezeichnung „Private Line“ oder „Dark Fiber“ vermuten lässt. Das ist für einzelne Kunden schwer bis gar nicht überprüf- oder beherrschbar. Mögliche Handlungswege sind Methoden zur Ermittlung und Vermeidung von Single Points of Failure wie z. B. Unterstützungsdienstleistungen bei der Erarbeitung von Ausschreibungen zur Vermeidung von Subunternehmer-Kaskaden mit geringerem Sicherheitsniveau. Jedoch tritt zusätzlich das Problem auf, dass Betreiber nicht notwendigerweise einen systemischen Überblick über alle Trassen und Knotenpunkte in Deutschland haben und einzelne Lösungsansätze somit nicht unbedingt zielführend sind.

Verteilte Betriebsorganisationen: Die Betriebsorganisationen von Infrastrukturen, wie vor allem WANs und Backbones, befinden sich teilweise nicht in Deutschland. Da Teile oder manche Backbones in Gänze von multinationalen oder ausländischen Konzernen in Deutschland betrieben werden, befinden sich manche der Betriebs- und Überwachungsorganisationen (wie NMC und OMC) im Ausland. Wie diese Anlagen und Organisationen unter die KRITIS-Definition oder spätere Vorgaben für z. B. Schutzmaßnahmen fallen, ist zurzeit noch unklar.

Verteilte Sicherheitsorganisationen: Große Infrastrukturen wie WANs und Backbones in Deutschland werden teilweise von multinationalen (ausländischen) Konzernen betrieben, die jedoch analog zum Betrieb auch die Sicherheitsorganisationen (CERTs, ISMS) nicht notwendigerweise in Deutschland unterhalten. Bei Regelungen durch KRITIS oder das IT-SiG müssten die jeweiligen Betreiber diese Sicherheitsorganisationen möglicherweise in Deutschland replizieren oder lokale Kontakt-/Verbindungsorganisationen für KRITIS einrichten. Die Auswirkungen und Herausforderungen dabei sind zurzeit noch unklar.

Handlungsmöglichkeiten des BSI bei Internetausfällen: Bei weitreichenden Ausfällen des Internets oder zentraler Knotenpunkte könnte ein „Öffnen“ des Peerings zwischen Carriern in Deutschland das Internet stabilisieren und die Erreichbarkeit trotz einzelner Ausfälle unterstützen. Denkbar wäre eine Hotline oder Meldewege zwischen BSI und Betreibern wie Carrier oder IXPs, damit diese in fest definierten Notfall- oder Katastrophenfällen ihr (BGP-)Peering zeitweise komplett für alle angeschlossenen Carrier freischalten, um so mehr Redundanz und Verbindungsmöglichkeiten im deutschen Internet zu schaffen. Die Möglichkeiten dafür sowie für die Einbindung ausländischer Providern mit Anschlüssen in Deutschland (und deutscher Provider mit Anschlüssen im Ausland) sollten eruiert werden.

„Made in Germany“ für Netzwerk- und Verschlüsselungskomponenten: Im Rahmen der Diskussionen über das weitreichende Abhören von Internetverkehr durch ausländische Nachrichtendienste besteht eine zunehmende Nachfrage und Interesse an Netzwerkhardware und Verschlüsselungssystemen „Made in Germany“. Die bereits bestehenden Initiativen (teils mit jedoch anderer Zielrichtung oder Zielgruppen) könnten für den zunehmenden Bedarf von Betreibern und Carriern an solchen Systemen aus Deutschland überprüft und möglicherweise erweitert werden.

Externe Abhängigkeiten: Die KRITIS-Sektoren unterliegen weiteren Abhängigkeiten, die nicht IKT-spezifisch sind. Im volkswirtschaftlichen Kontext sind die Infrastruktur-betreibenden Sektoren, vor allem die sogenannten „Leitungsunternehmen", auf funktionierende Genehmigungsprozesse bei

Bauvorhaben von Leitungen und Netzen angewiesen. Diese Bauvorhaben, vor allem in Städten hängen von Genehmigungen, Baubehörden und Verkehrslenkung ab, die unmittelbaren Einfluss auf Terminierung und Durchführung von Infrastrukturarbeiten haben. Genehmigen diese Behörden weitere Vorhaben wie in den letzten Jahren nur verzögert, ist dies zwar nach der engen Definition nicht KRITIS-relevant, stellt die Kapazitätsplanung und den Netzaufbau von Betreibern jedoch vor große Schwierigkeiten. Ein möglicher Untersuchungsbedarf ist die geminderte Widerstandsfähigkeit (Resilienz) bei Störungen durch Engpässe oder verzögerte Bauvorhaben.

Eine weitere indirekte Abhängigkeit besteht bei der Verfügbarkeit von entsprechend ausgebildetem und qualifizierten Personal für KRITIS-Betreiber. Dass umfasst vor allem (informations-)technische Berufe für Installation, Wartung, Betrieb und Planung von spezialisierten Infrastrukturnetzen einschließlich der Leit- und Kontrolltechnik. Arbeitgeber (große KRITIS-Betreiber eingeschlossen) suchen sowohl Hochschulabsolventen der IT, Hochtechnologie und Ingenieurstechnik als auch Facharbeiter und Spezialisten. Dieser Mangel wirkt sich teilweise auf Wachstum, Innovationskraft aber auch auf den regulären Betrieb aus.

Auswirkungen DNSSEC: Durch die langsame, aber zunehmende Einführung von DNSSEC, den Domain Name Security Extensions zum Schutz von DNS-Records und -Antworten, steigt die Komplexität des gesamten DNS. Die Auswirkungen dieser Veränderungen auf die Internetinfrastruktur in Deutschland und die zunehmende Komplexität und mögliche Fehleranfälligkeiten sind noch nicht vollständig absehbar und sollten genauer untersucht werden.

6.3 Fazit und Zusammenfassung

Die vorliegende Studie untersucht die KRITIS-Branchen des IKT-Sektors. Sowohl durch die technische als auch die marktwirtschaftliche Konsolidierung und Konvergenz der beiden Branchen Telekommunikation und Informationstechnik sowie deren Dienstleistungen erfolgt eine gemeinsame Betrachtung in dieser Studie als einheitliche KRITIS-Branche IKT. Innerhalb dieser KRITIS-Branche werden die folgenden Dienstleistungen als KRITIS-relevant (kritisch) definiert und behandelt:

- **Sprach- und Datenübertragung** (DL1)
- **Datenspeicherung und -verarbeitung** (DL2)

Betrachtet werden alle Teile dieser Branche, die direkt oder indirekt an der Erbringung der zwei kritischen Dienstleistungen des Sektors beteiligt sind.

Die Kritischen Infrastrukturen, d. h. die Anlagen und Einrichtungen dieser Dienstleistungen, sind in diesem Sektor fast ausschließlich in der Hand privater Unternehmen, den Betreibern. Viele Betreiber des IKT-Sektors sind in mehreren Branchen und verschiedenen Prozessen gleichzeitig aktiv. Zudem bestehen Branchenverbände, die die Interessen der Betreiber vertreten. Staatliche Instanzen, wie die Bundesnetzagentur oder die Bundesregierung, machen regulatorische Vorgaben und kontrollieren gleichzeitig deren Einhaltung.

Die Besonderheit des IKT-Sektors besteht in der geringen Anzahl von Betreibern mit großem Marktanteil in der Dienstleistung Sprach- und Datenübertragung (DL1). Es dominieren vier, teils multinationale Konzerne einen Großteil des Marktes und sind maßgeblich an fast allen Prozessen innerhalb der Dienstleistung beteiligt.

Jede Dienstleistung und damit auch die Aktivitäten der gesamten Branche werden in dieser Studie als Gesamtprozess modelliert. Dabei nimmt die Studie an, dass die einzelnen Prozesse und Anlagen derart verknüpft sind, dass sie gemeinsam die Erbringung der Dienstleistung ermöglichen. Im Umkehrschluss kann bei einer Störung oder einem Ausfall eines Prozesses die Versorgungssicherheit der gesamten Dienstleitung gefährdet sein.

Dies ist insbesondere in der Sprach- und Datenübertragung der Fall. Fehler im Zugangs-, Übertragungs- oder Vermittlungsnetz können bedeuten, dass eine Nutzung von Internet und Telefonie für viele

Endkunden komplett ausfällt. Die Besonderheit im IKT-Sektor ist zudem, dass durch die Baumstruktur im Zugangsnetz Komplettausfälle für einen Teilbereich denkbar sind, während alle anderen Nutzer den Dienst weiterhin uneingeschränkt nutzen können. Darüber hinaus bestehen im Übertragungsnetz durch die vermaschte Struktur starke Redundanzen, sodass ein Ausfall eines Netzes unter Umständen nur geringe Auswirkungen hat. Eine problematische Entwicklung kann in der zunehmenden Zentralisierung von Knotenpunkten im Übertragungsnetz gesehen werden. Dort laufen verschiedene Netze zusammen und tauschen Daten untereinander aus; ein Ausfall wäre so in mehreren Netzen gleichzeitig bemerkbar.

Die aktuelle Relevanz dieser Studie lässt sich anhand von Vorfällen im IKT-Sektor ablesen. Sowohl nationale als auch internationale Ausfälle der Dienstleistungen haben in der Vergangenheit gezeigt, dass eine Anfälligkeit besteht. Kapitel 4 beschreibt verschiedene Ausfälle des IKT-Sektors, anhand derer die Kritikalität einzelner IKT-Komponenten erkannt werden kann.

Die Umsetzung der Cyber-Sicherheit als Reaktion auf diese Bedrohungen ist im IKT-Sektor teilweise unterschiedlich aber im Vergleich zu anderen Sektoren eher hoch. Die im Zuge dieser Studie durchgeführten Betreiberbefragungen zeigen ein relativ hohes Niveau von umgesetzten Maßnahmen und Bewusstsein für mögliche Bedrohungen. Das mag unter Umständen an der Natur des Sektors selbst liegen. Kapitel 5 befasst sich mit dem Stand der Cyber-Sicherheit und soll sowohl die momentane Situation wiedergeben, als auch mögliche Entwicklungen in der nahen Zukunft aufzeigen.

Bei der Auswertung der Betreiberbefragung waren insbesondere die hohen Redundanzen der eingesetzten IKT-Komponenten (redundante Server, Knotenpunkte, Leitungen, Trassen, Rechenzentren etc.), der weitverbreitete Einsatz von (redundanten) Netzwerküberwachungszentren und die Orientierung und Umsetzung nach internationalen Standards (z. B. ISO/IEC 27001) auffallend. Eine weitere wichtige Erkenntnis ist die eigene „Selbst-Regulierung“ der Betreiber des Sektors. Ein aktiver Austausch und die Kommunikation zwischen den Betreibern ist innerhalb des Sektors durchaus üblich.

Zusammengefasst lässt sich über die Kritische Infrastruktur des IKT-Sektors sagen, dass eine sehr hohe Abhängigkeit von IKT-Komponenten besteht. Einzelne Anlagen, Risikoelemente und IKT-Komponenten können durch gezielte Angriffe die gesamte Dienstleistung für einen begrenzten Personenkreis ausfallen lassen. Dennoch ist ein großflächiger und langanhaltender Ausfall in der Bundesrepublik Deutschland als eher unwahrscheinlich anzusehen, falls nicht ganze zentrale Metropolregionen ausfallen. Dies ist insbesondere durch die große Redundanz im Übertragungsnetz und bei zentralen IKT-Komponenten gegeben. Wichtig in diesem Zusammenhang ist die Abhängigkeit vom Energiesektor, insbesondere von der Stromversorgung. Zwar kann dieser Abhängigkeit durch entsprechende Maßnahmen entgegengewirkt werden, meist jedoch nur über einen kurzen Zeitraum hinweg.

Durch die weiter ansteigende Technologisierung fast sämtlicher Wirtschaftsbereiche bestehen auch in Zukunft große Abhängigkeiten der Wirtschaft von der Dienstleistungserbringung des IKT-Sektors. Hier ist es insbesondere wichtig, dass staatliche Stellen Rahmenbedingungen schaffen, die den Betreibern dabei helfen, ihre Infrastrukturen angemessen zu schützen und weitere Untersuchungen und Anstrengungen unternehmen.

Der in dieser Studie identifizierte Handlungsbedarf wurde in Form von Vorschlägen an den Gesetzgeber und die Betreiber in Abschnitt 6.1 beschrieben. Weiterer Untersuchungsbedarf, der sich aus der KRITIS-Studie und der Betreiberbefragung ergeben hat, wurde in Abschnitt 6.2 dargestellt.

Anhänge

Abkürzungsverzeichnis

Abkürzung	*Begriff*	*Beschreibung*
AuC	Authentication Center	Element des GSM-Funknetzes zur Authentifizierung von SIM-Karten im Netz des Betreibers.
BK-Verstärkerstelle	Breitbandkabel-Verstärker-stelle	Netzwerkelement des Kabelnetzes zur Verstärkung des Signals über große Entfernungen.
BSC	Base Station Controller	(deutsch *Basisstations-Steuereinrichtung*) Netzelement des digitalen GSM-Funknetzes zur Steuerung von mehreren BTS.
BTS	Base Transceiver Station	(deutsch *Basissendeempfängerstation*) Netzelement des digitalen GSM-Funknetzes zur Anbindung von mobilen Endgeräten.
CMTS	Cable Modem Termination System	Netzwerkelement im Kabelnetz um Endnutzern Datendienste über das Kabelnetz bereitzustellen.
DOCSIS	Data Over Cable Service Interface Specification	Übertragungsstandard in Kabelfernsehnetzen.
DSL-Splitter	Digital Subscriber Line Splitter	Netzwerkelement der DSL-Technologie zur Datenübertragung über die TAL. DSL-Splitter befinden sich einerseits auf der Endkundenseite und andererseits in der Ortsvermittlungsstelle.
DSLAM	Digital Subscriber Line Access Multiplexer	(deutsch *DSL-Zugangskonzentrator*) Netzwerkelement der DSL-Technologie zur Datenübertragung über das PSTN. Befindet sich meistens in den Kabelverzweigern.
E-UTRAN	Evolved Universal Terrestrial Radio Access Network	Name der LTE-Zugangstechnologie.
EIR	Equipment Identity Register	Netzwerkelement des GSM-Funknetzes. Enthält Informationen über die eindeutige Identifikationsnummer (die IMEI) der im Netz angemeldeten Mobilfunkgeräte, um zum Beispiel bestimmte Geräte sperren zu können.

Abkürzung	*Begriff*	*Beschreibung*
eNode B	Evolved Node B	Element des digitalen LTE-Funknetzes zur Anbindung von mobilen Endgeräten.
EWSD	Elektronisches Wählsystem Digital	Netzwerkelement zur digitalen Vermittlung im analogen Festnetz der Firma Siemens AG.
GERAN	GSM EDGE Radio Access Network	Name der zweiten Generation der GSM-Zugangstechnologie.
GGSN	Gateway GPRS Support Node	Netzelement des digitalen GSM-Funknetzes, das als Schnittstelle von Datenverkehr der GPRS-Technologie in andere Datennetze dient.
GPRS	General Packet Radio Service	Technologie zur Datenübertragung im GSM-Funknetz.
HLR	Home Location Register	Netzwerkelement des GSM-Funknetzes. Enthält verschiedene Teilnehmerinformationen zum Beispiel zum Einwählen des Nutzers und regelt, welche Dienste er nutzen darf.
HSS	Home Subscriber Server	Zentrales Netzwerkelement des LTE-Funknetzes zur Steuerung der Teilnehmer und deren Standorte (vgl. HLR in GSM/UMTS-Funknetzen).
HÜP	Hausübergabepunkt	Übergabepunkt des Kabelnetzes an das Gebäudenetzwerk.
HVt	Hauptverteiler	Zentrales Netzwerkelement des PSTN-Zugangsnetzes. Siehe auch Ortsvermittlungsstelle (VE:O).
KVz	Kabelverzweiger	Netzwerkelement des PSTN-Zugangsnetzes zur Zusammenführung mehrerer TAL für die Anbindung an die Ortsvermittlungsstelle.
LNP	Local Number Portability	Lokale Rufnummermitnahmedatenbank. Ermöglicht die Mitnahme von lokalen Rufnummern beim Wechsel des Telefonanbieters.
MGW	Media Gateway	Netzwerkelement, das den Übergang zwischen verschiedenen Datennetzen ermöglicht.

Abkürzung	*Begriff*	*Beschreibung*
MNP	Mobile Number Portability	Rufnummermitnahmedatenbank. Ermöglicht die Mitnahme von mobilen Rufnummern zu anderen Mobilfunkanbietern.
MSC	Mobile-services Switching Center	(deutsch: *Vermittlungsstelle in Mobilfunknetzen*) Netzelement des digitalen GSM-Funknetzes, das als Schnittstelle zum Festnetz dient.
NMC	Network Management Center	Zentrale Einrichtung zur Überwachung der Funktionalität von Datennetzen. In großen Netzen sind einem NMC mehrere OMC hierarchisch untergeordnet.
NOC	Network Operation Center	Synonym zu NMC.
Node B		Element des digitalen UMTS-Funknetzes zur Anbindung von mobilen Endgeräten.
OLT	Optical Line Terminal	Übergabepunkt der Glasfaserleitung in das Gebäudenetzwerk.
OMC	Operation and Maintenance Center	Einrichtung zur Überwachung der Funktionalität von Sprach- und Datennetzen. Oft auf einen bestimmten regionalen Bereich begrenzt.
ONT	Optical Network Terminal	Übergabepunkt der Glasfaserleitung an die Endgeräte.
OSS	Open Source Software	Software, deren Quelltext offenliegt.
RAS	Remote Access Server	Netzwerkelement von Datennetzen zur Anbindung von entfernten Verbindungen in das eigene Netzwerk.
RNC	Radio Network Controller	Netzelement des digitalen UMTS-Funknetzes zur Steuerung von mehreren Node B.
S12	System 12	Netzwerkelement zur digitalen Vermittlung im analogen Festnetz der Firma Alcatel.
SCP	Service Control Point	Netzwerkelement des Signalisierungssystems. Ermöglicht die Nutzung verschiedener erweiterter Funktionen.
SCTP	Stream Control Transmission	Verbindungsorientiertes

Abkürzung	*Begriff*	*Beschreibung*
	Protocol	Netzwerkübertragungsprotokoll, ursprünglich eingesetzt um Nachrichten aus dem Signalisierungsnetz des analogen Festnetzes in IP umzuwandeln.
SG	Signalling Gateway	Netzwerkelement des Signalisierungssystems. Regelt die Vermittlung in andere Datennetze (z. B. Internet).
SGSN	Serving GPRS Support Node	Netzelement des digitalen GSM-Funknetzes, das als zentrales Element zur Ermöglichung von Datenverkehr im GSM-Funknetz dient.
SPOF	Single Point of Failure	Bestandteil eines technischen Systems, dessen Ausfall den Ausfall des gesamten Systems nach sich zieht, da keine Absicherung durch Redundanzen besteht.
SSP	Service Switching Point	Netzwerkelement des Signalisierungssystems. Regelt die Orts- und Fernvermittlungen in andere Datennetze (nur VoIP) und zu anderen Betreibern von analogen Telefonnetzen.
STP	Signaling Transfer Point	Netzwerkelement des Signalisierungssystems. Vermittelt Signalisierungsnachrichten zwischen den Netzwerkelementen des Signalisierungsnetzes.
UTRAN	Universal Terrestrial Radio Access Network	Name der UMTS-Zugangstechnologie.
VE:A	Vermittlungseinheit Ausland	Netzwerkelement des analogen Festnetzes (PSTN) zur Vermittlung von Anrufen ins Ausland.
VE:F	Vermittlungseinheit Fernnetz	Netzwerkelement des analogen Festnetzes (PSTN) zur Vermittlung von Anrufen im Fernnetz.
VE:N	Vermittlungseinheit mit Netzübergangsfunktion	Netzwerkelement des analogen Festnetzes (PSTN) zur Vermittlung von Anrufen in andere Netze (PSTN oder Datennetze).
VE:O	Vermittlungseinheit Ort	(auch Ortsvermittlungsstelle) Netzwerkelement des analogen Festnetzes (PSTN) zur Vermittlung von Anrufen aus dem Ortsnetz in das Fernnetz.

Abkürzung	*Begriff*	*Beschreibung*
VLR	Visitor Location Register	Netzwerkelement des GSM-Funknetzes. Enthält Informationen über den momentanen Standort des Mobilfunkteilnehmers.
VoIP	Voice-over-Internet-Protocol	Bezeichnet Methoden und Technologien die eine Sprachübertragung über das Internet Protokoll erlauben.
zMNP	zentrale Mobile Number Portability	Zentrale Rufnummermitnahmedatenbank deutscher Mobilfunkanbieter.

Glossar

Begriff	*Beschreibung*
Anpassbarkeit	Mögliche Reaktion auf eine Verschärfung von Bedrohungen durch - Beheben einer Schwachstelle, Vernetzung/Entnetzung; - Bezug zu Abhängigkeit von Herstellern; - Standardsoftware vs. Individualsoftware. Anpassbarkeit beschreibt die Möglichkeit, IKT-Komponenten in ihrer Konfiguration oder Ausprägung zu verändern. Je besser IKT-Komponenten des betriebsinternen Prozesses angepasst werden können, desto geringer ist grundsätzlich die Abhängigkeit des Prozesses von diesen Komponenten. Auf Veränderungen kann reagiert und somit die Wahrscheinlichkeit eines erfolgreichen Angriffs oder Ausfalls reduziert werden.
Backbone	System von Übertragungsnetzwerken, die einen Großteil der Daten zwischen Computernetzwerken transportieren.
Co-Location	Bereitstellung von Räumlichkeiten in Rechenzentren zur Unterbringung und Betrieb von IT-Hardware durch Dritte.
Diversifizierungsgrad	Homogenität, spezifische Soft-/Hardware, Lieferanten-Abhängigkeiten. Der Diversifizierungsgrad bezeichnet die Ausprägung der IKT-Systeme. Diese können bspw. homogen von einem einzigen Hersteller und Typ, gemischt homo- und heterogen (Multi-Vendor-Strategie) oder heterogen sein. Vollständig homogene und vollständig heterogene Landschaften haben Einfluss auf die Fähigkeit, auf Ausfall und Beeinträchtigung zu reagieren.
Ersatzversorgung	Möglichkeit zur Aufrechterhaltung des Prozesses bei Ausfall von IKT durch entsprechende Kompensationsmöglichkeiten. Ersatzversorgung bezeichnet die Fähigkeit, IKT-Komponenten durch manuelle Ersatzmaßnahmen ohne wesentlichen IKT-Einsatz zu ersetzen. Der Prozess kann bspw. weitestgehend, eingeschränkt oder kaum durch manuelle Maßnahmen aufrechterhalten werden. Die Ersatzversorgung ist ein Kriterium für die IKT-Abhängigkeit des gesamten Prozesses.
Ganzheitlicher Betreiber	Idealtypischer Informations- und Telekommunikationsbetreiber, der einen Großteil der Dienstleistungen des Sektors selbständig erbringt.
Housing	Siehe Co-Location.
Kabelnetzbetreiber	Idealtypischer Kabelnetzbetreiber, der Dienstleistungen anbietet, die über das Fernsehkabelnetz übertragen werden. Hierzu zählen Zugang zur Sprach- und Datenübertragung durch Kabelanschlüsse

Begriff	*Beschreibung*
	und Betrieb eines eigenen Kabelnetzes.
Mobilfunkprovider	Idealtypischer Mobilfunkbetreiber, der ausschließlich Mobilfunkdienstleistungen anbietet. Hierzu zählen Zugang durch mobile Endgeräte und Betrieb eines eigenen Funknetzes.
Tier-1-, Tier-2-, Tier-3-Netz	Klassifizierung von Datennetzen nach funktionaler Ausprägung. Tier-1-Netze haben die größte Ausprägung und sind alle untereinander verbunden (globale Ausdehnung - siehe Backbone). Tier-2-Netze haben nationale und regionale Ausdehnung und sind über Tier-1-Netze verbunden. Tier-3-Netze haben nur begrenzte regionale bzw. lokale Ausdehnung und sind mit Tier-2-Netzen verbunden.
Übertragungsnetz	Netzwerk mit großer geographischer Ausdehnung zur Übertragung von Daten und Sprache zwischen verschiedenen Zugangsnetzen.
Zentralität	IT-Zentralisierung z. B. durch Auslagerung an IT-Dienstleister. Zentralität bezeichnet den Grad der Konzentration wesentlicher IKT-Komponenten und Prozesse an einzelnen Standorten oder auf einzelne Dienstleister. Die IKT-Komponenten des Prozesses können bspw. vollständig zentralisiert oder vollständig dezentral betrieben werden. Je zentraler die IKT-Komponenten realisiert sind, desto wahrscheinlicher ist bei Ausfall oder Beeinträchtigung der zentralen Komponente auch ein negativer Einfluss mit stärkerer Wirkung auf den Prozess.
Zugangsnetz	Netzwerk, das abhängig von der technischen Zugangsart Daten und Sprache vom Endgerät zu den Übertragungsnetzen und von dort wieder zurück überträgt.

Abbildungen

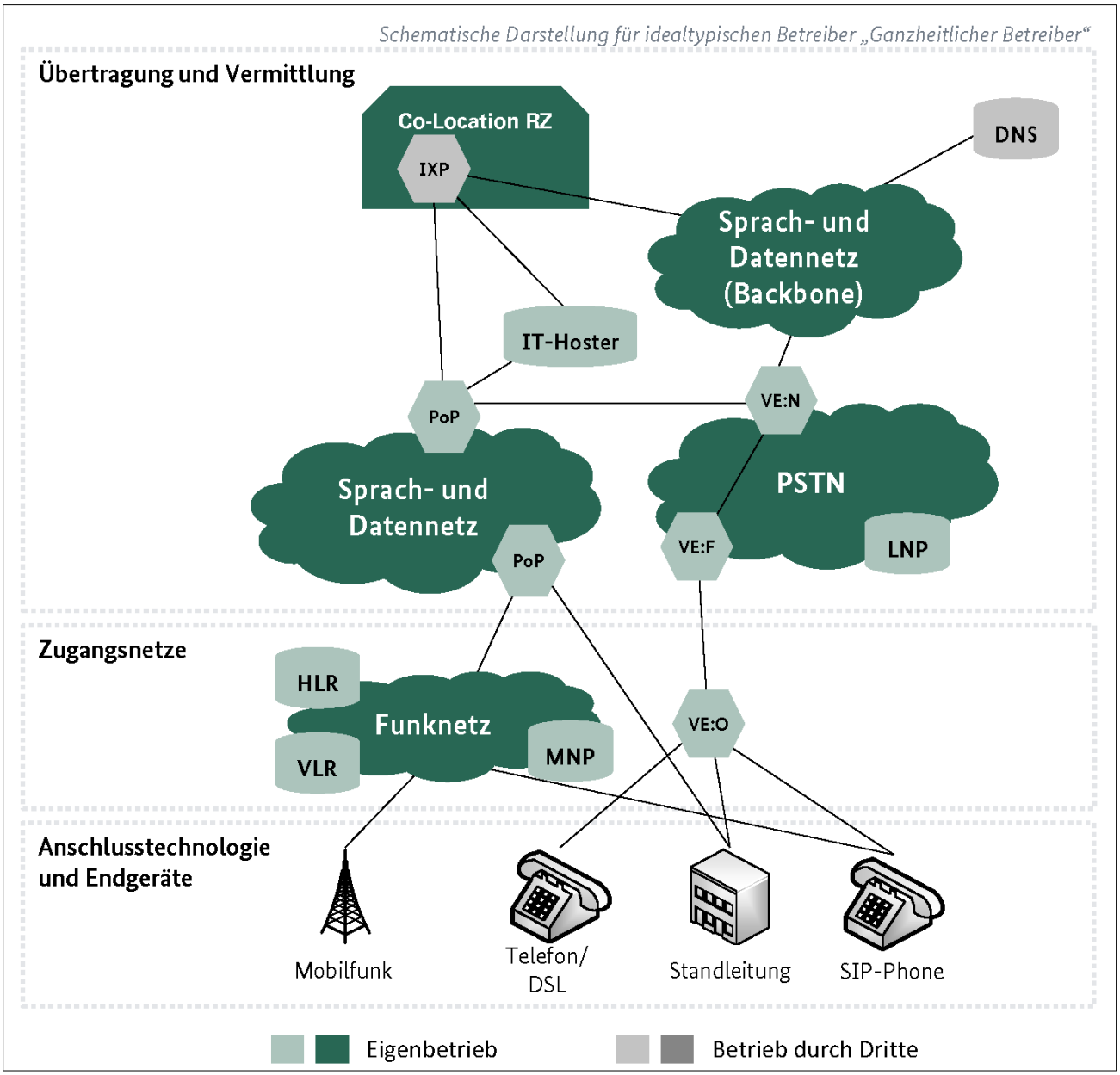

Abbildung 20: Schematischer Aufbau der Struktur der IKT-Branche für einen „ganzheitlichen Betreiber“

Quelle: eigene Darstellung

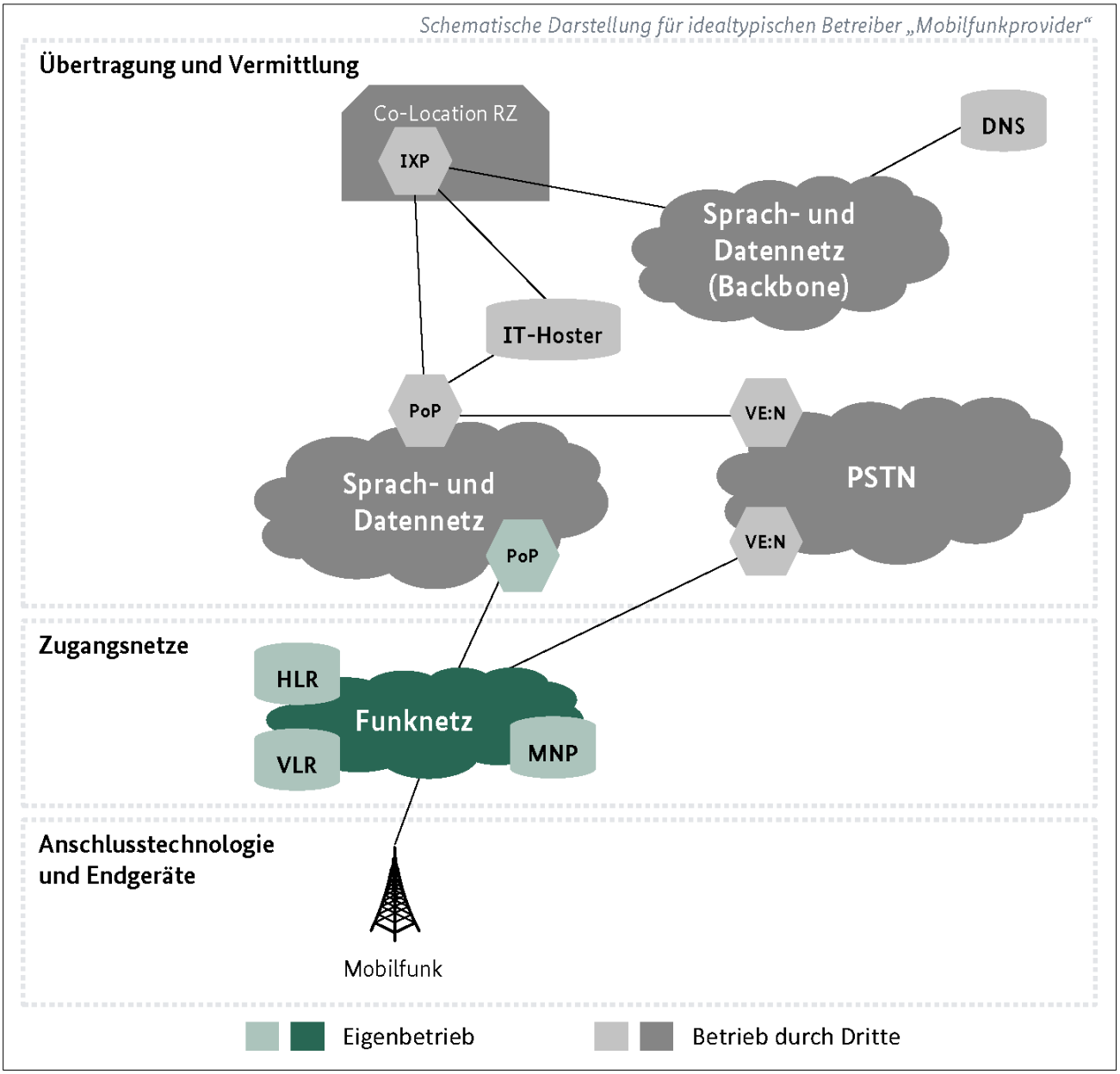

Abbildung 21: Schematischer Aufbau der Struktur der IKT-Branche für Mobilfunkprovider

Quelle: eigene Darstellung

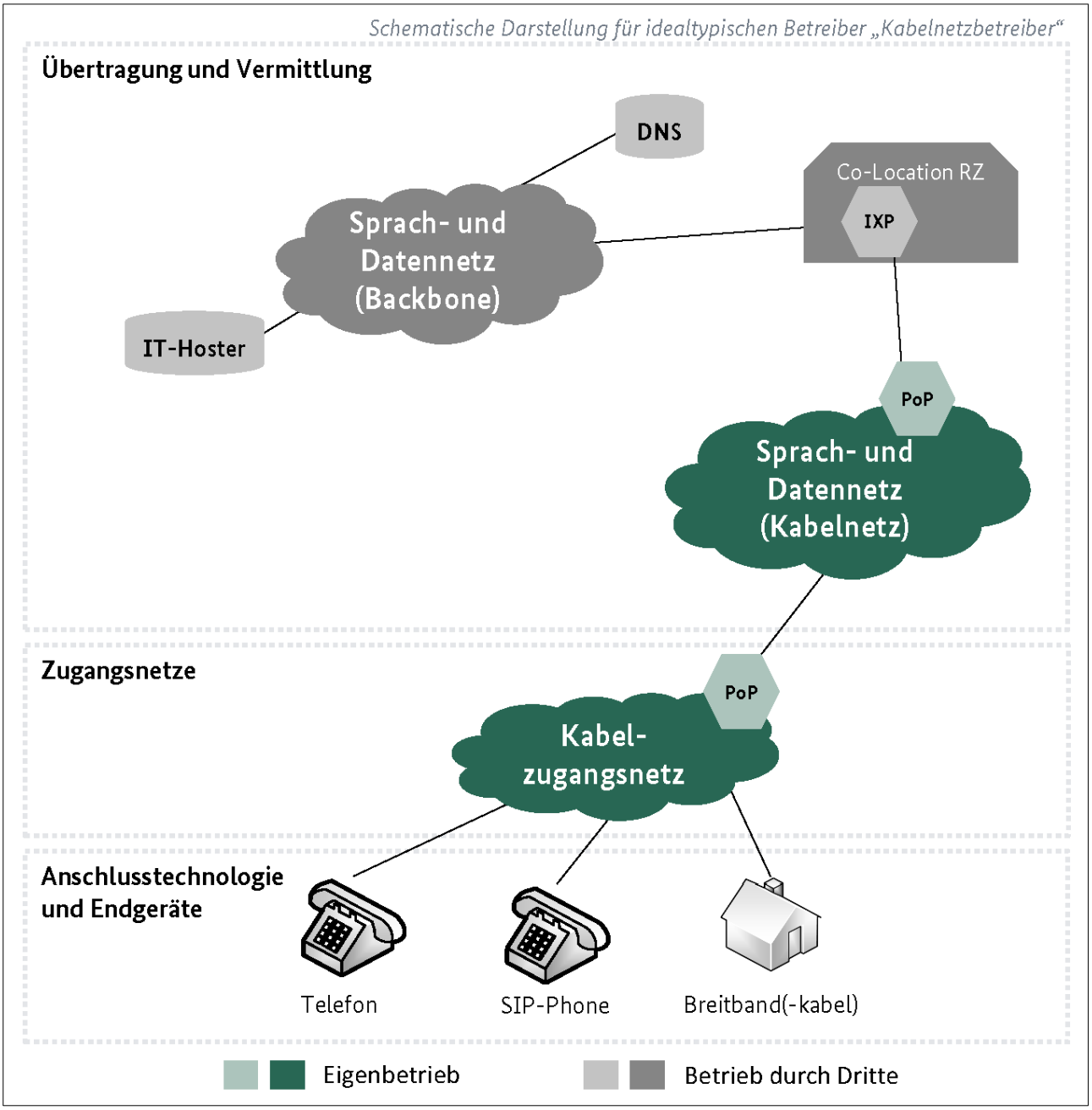

Abbildung 22: Schematischer Aufbau der Struktur der IKT-Branche für Kabelnetzbetreiber

Quelle: eigene Darstellung

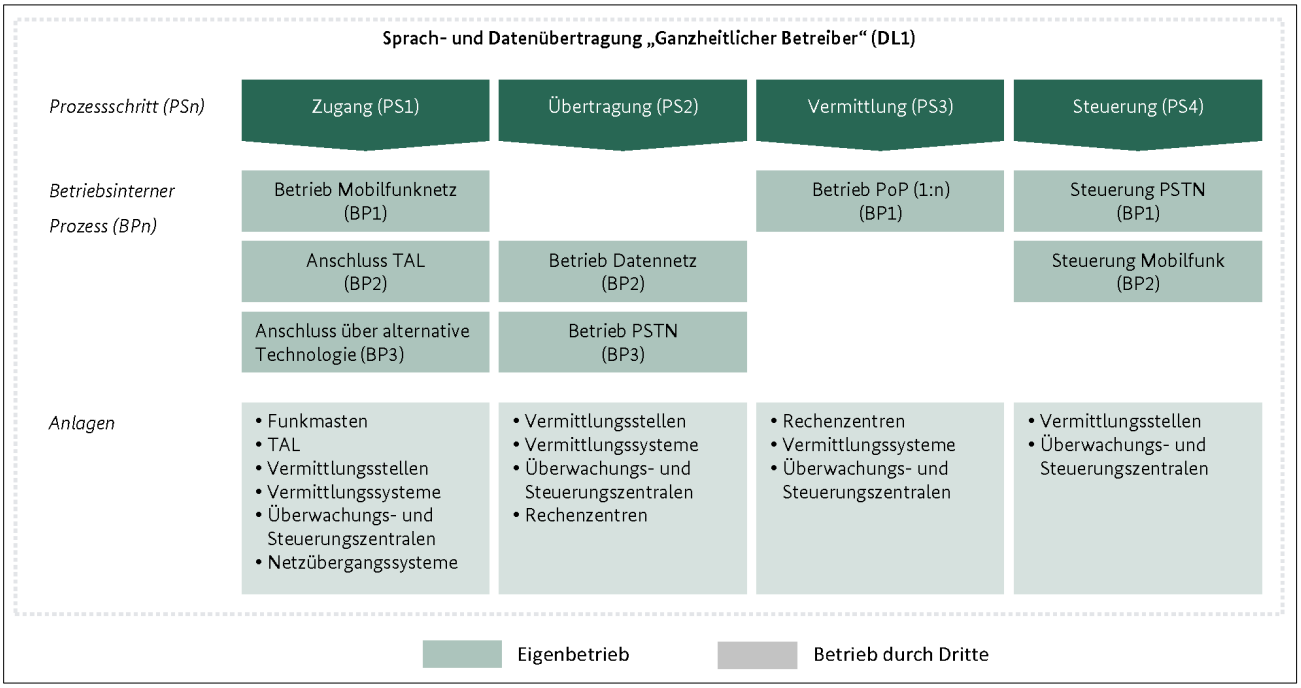

Abbildung 23: DL1 Sprach- und Datenübertragung für den „ganzheitlichen Betreiber“

Quelle: eigene Darstellung

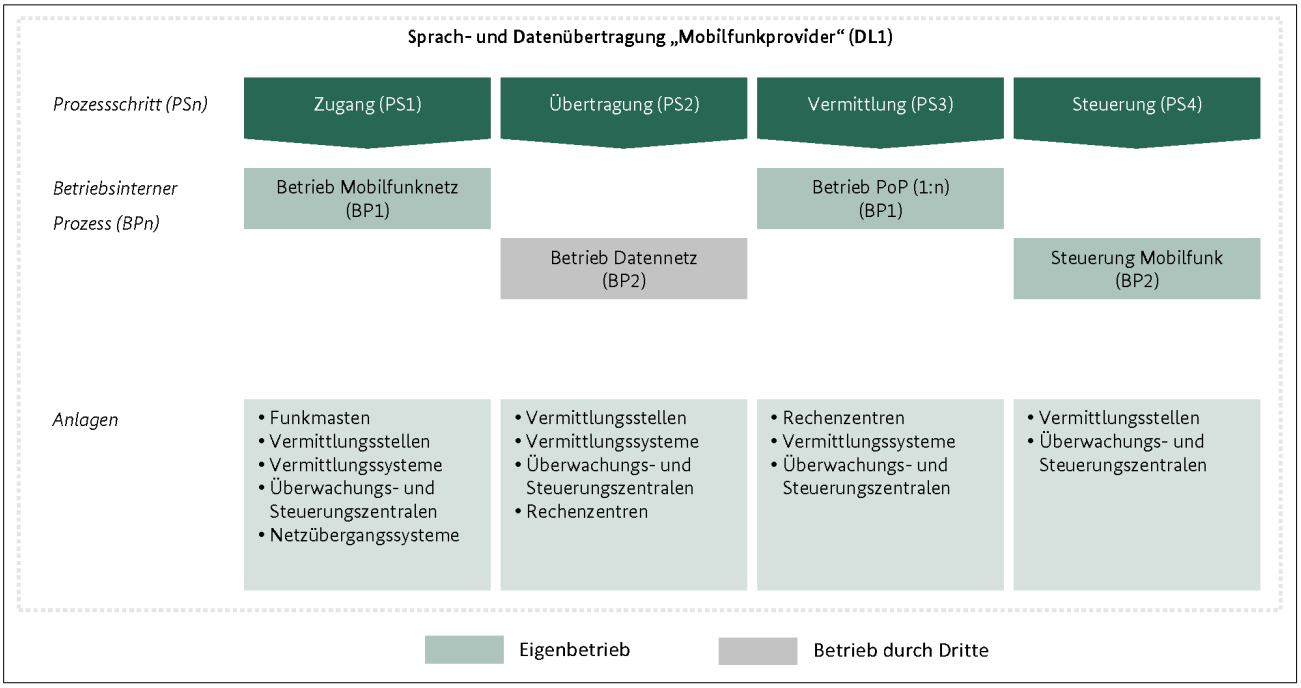

Abbildung 24: DL1 Sprach- und Datenübertragung für den Mobilfunkprovider

Quelle: eigene Darstellung

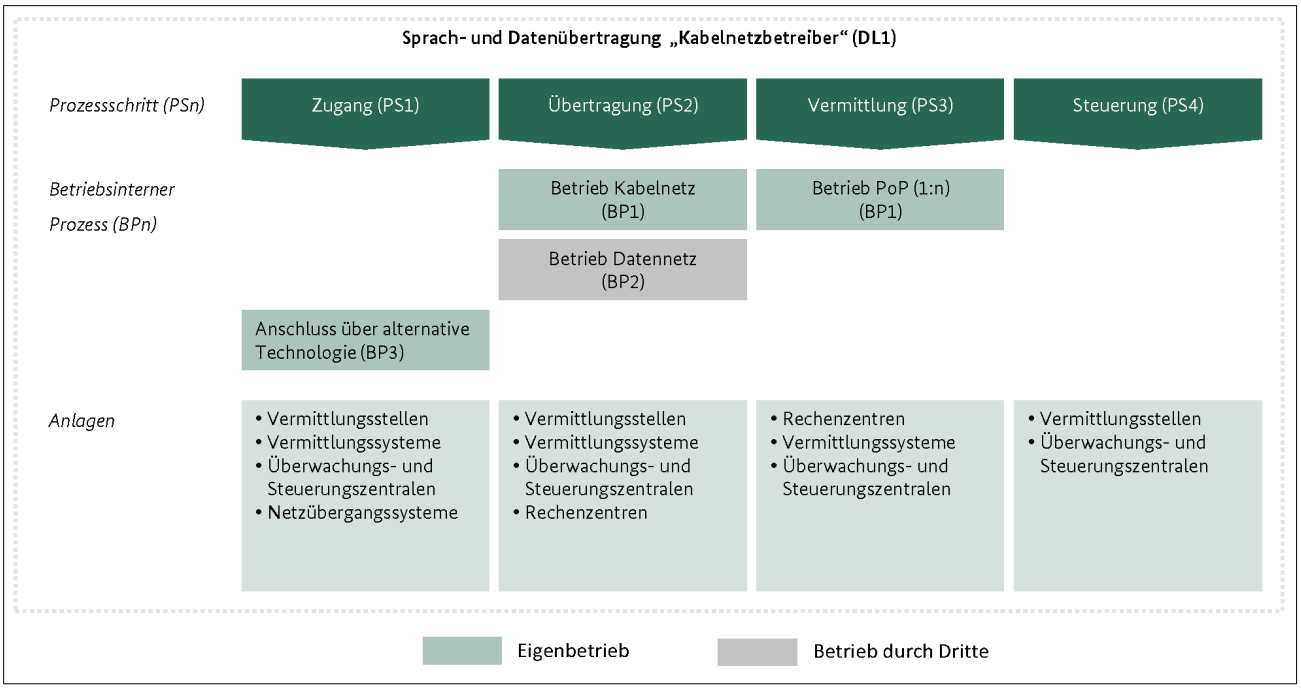

Abbildung 25: DL1 Sprach- und Datenübertragung für den Kabelnetzbetreiber

Quelle: eigene Darstellung

Literaturverzeichnis

2013 National Institute of Standards and Technology: Security and Privacy Controls for Federal Information Systems and Organizations.: National Institute of Standards and Technology 2013.

1&1 2012 Alexander Thieme: Informationen zur Netzwerkstörung in unserem Rechenzentrum. 2012. http://blog.1und1.de/2012/11/27/informationen-zur-netzwerkstoerung-in-unserem-rechenzentrum/#page-content (13.06.2014)

451Research 2014 Michelle Bailey: Hosting and Cloud Study 2014: Hosting and Cloud Go Mainstream. Survey Results. 2014. http://www.microsoft.com/en-us/news/download/presskits/cloud/docs/hostingstudy2014.pdf (10.06.2013)

ARD/ZDF 2014 ARD/ZDF: ARD/ZDF-Onlinestudie 2013: Onlinenutzung. 2014. http://www.ard-zdf-onlinestudie.de/index.php?id=422 (04.04.2014)

Bauer 2009 Bauer, Oliver; Tenz, Beate: Informations- und Kommunikationstechnologien in Unternehmen: Ergebnisse für das Jahr 2008. 2009. https://www.destatis.de/DE/Publikationen/WirtschaftStatistik/Informationsgesellschaft/IKTUnternehmen012009.pdf?__blob=publicationFile (26.03.2013)

BCIX 2014 BCIX Berlin Commercial Internet Exchange e. V.: Statistics. 2014. http://www.bcix.de/bcix/statistik/ (23.03.2014)

Belgacom 2013 Belgacom S.A.: Belgacom takes actions related to IT security. 2013. http://www.belgacom.com/be-en/newsdetail/ND_20130916_Belgacom.page (23.07.2014)

BGH 2013 Bundesgerichtshof, vom 24.01.2013, Aktenzeichen III ZR 98/12

BGH 2013 Bundesgerichtshof: Bundesgerichtshof erkennt Schadensersatz für den Ausfall eines Internetanschlusses zu: Mitteilung der Pressestelle. 2013. http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&pm_nummer=0014/13 (04.04.2014)

Bhatti 2000 Bhatti, Nina; Bouch, Anna; Kuchinsky, Allan: Integrating User-Perceived Quality into Web Server Design 2000

BITKOM 2014a Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM): ITK-Marktzahlen: Kurzfassung. 2014. (02.04.2014)

BITKOM 2014b Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM): Wir über uns. 2014. http://www.bitkom.org/de/wir_ueber_uns/99.aspx (26.03.2014)

BITKOM 2013 Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM): BITKOM fordert Nachbesserungen am IT-Sicherheitsgesetz. 2013. http://www.bitkom.org/de/themen/54746_75692.aspx (04.04.2014)

BITKOM 2011a Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM): Netzgesellschaft: Eine repräsentative Untersuchung zur Mediennutzung und dem Informationsverhalten der Gesellschaft in Deutschland. 2011.

http://www.bitkom.org/files/documents/BITKOM_Publikation_Netzgesellschaft.pdf (26.03.2014)

BITKOM 2011b IW Consult GmbH; Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM): Wirtschaft Digitalisiert: Wie viel Internet steckt in den Geschäftsmodellen deutscher Unternehmen? 2011. http://www.bitkom.org/files/documents/Wirtschaft_Digitalisiert_BM2D.pdf (02.04.2014)

BITKOM 2009 Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM): IT Services Made in Germany: Stärken, Erfolgsbeispiele und Strategien deutscher IT-Dienstleister im internationalen Wettbewerb. 2009. https://www.bitkom.org/files/documents/IT_Services_Made_in_Germany.pdf (02.04.2014)

BMBF 2014 Bundesministerium für Bildung und Forschung (BMBF): Zukunftsbild "Industrie 4.0": Hightech-Strategie. 2014. http://www.bmbf.de/pubRD/Zukunftsbild_Industrie_40.pdf (22.04.2014)

BMF 2013 Bundesministerium für Finanzen (BMF): Deutsche Telekom AG: Bundesvermögen. 2013. http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Bundesvermoegen/Privatisierungs_und_Beteiligungspolitik/deutsche-telekom-ag.html?__act=renderPdf&__iDocId=168774 (22.04.2014)

BMI 2011 Bundesministerium des Innern: Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. 2011. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.html (10.06.2014)

BMI 2009 Bundesministerium des Innern (BMI): Nationale Strategie zum Schutz Kritischer Infrastrukturen: KRITIS-Strategie. 2009. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf;jsessionid=FDCE3DD1CBC592D8FBA25EBD1B47F442.2_cid364?__blob=publicationFile (02.04.2014)

BMWi 2013 Bundesministerium für Wirtschaft und Energie (BMWi): Monitoring-Report Digitale Wirtschaft 2013: Digitalisierung und neue Arbeitswelten. 2013. (14.03.2014)

BMWi 2010 Bundesministerium für Wirtschaft und Energie (BMWi): IKT-Strategie der Bundesregierung "Deutschland Digital 2015": Innovationspolitik, Informationsgesellschaft, Telekommunikation. 2010.

BNetzA 2014a Bundesnetzagentur (BNetzA): Anschriften der Zuteilungsnehmer. 2014. http://www.bundesnetzagentur.de/cln_1412/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/Rufnummern/MobileDienste/Anschriften%20Zuteilungsnehmer/AnschriftenZuteilungsnehmer_Basepage.html;jsessionid=57FDB5645609790BC423416E6CD46A20?nn=268384#download=1 (12.05.2014)

BNetzA 2014b Bundesnetzagentur (BNetzA): Umsetzung des § 109 Absatz 5 TKG zur Mitteilung einer Sicherheitsverletzung: Umsetzungskonzept. 2014. http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/mitteilungeinersicherheitsverletzung/Umsetzungskonzept_

%C2%A7_109_(5)_TKG_Mitteilung_Sicherheitsverletzung.pdf?__blob=publicationFile&v=3

BNetzA 2014c Bundesnetzagentur (BNetzA): Über unsere Aufgaben. 2014. http://www.bundesnetzagentur.de/cln_1932/DE/Sachgebiete/Telekommunikation/UeberunsereAufgaben/ueberunsereaufgaben-node.html (04.04.2014)

BNetzA 2013a Bundesnetzagentur (BNetzA): Tätigkeitsbericht: Telekommunikation 2012/2013. 2013. http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2013/131216_TaetigkeitsberichtTelekommunikation2012-2013.pdf?__blob=publicationFile&v=8 (12.03.2014)

BNetzA 2013b Bundesnetzagentur (BNetzA): Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten: nach § 109 Telekommunikationsgesetz (TKG). 2013. (14.03.2014)

BNetzA 2013c Bundesnetzagentur (BNetzA): NGA/NGN. 2013. http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/NGA_NGN/nga_ngn-node.html (04.04.2014)

BNetzA 2010 Bundesnetzagentur (BNetzA): Eckpunkte über die regulatorischen Rahmenbedingungen für die Weiterentwicklung moderner Telekommunikationsnetze und die Schaffung einer leistungsfähigen Breitbandinfrastruktur. 2010. http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/NGA_NGN/NGA_Eckpunkte/NGA_Eckpunkte_Id16268pdf.pdf?__blob=publicationFile&v=2 (02.04.2014)

BREKO 2012 Bundesverband Breitbandkommunikation e.V. (BREKO): Marktdaten 2012: Marktbefragung der BREKO-Mitgliedsunternehmen. 2012. http://www.brekoverband.de/fileadmin/user_upload/Marktdaten/Marktdaten_BREKO_2012_oeffentlich.pdf (01.04.2014)

BSI 2014 Bundesamt für Sicherheit in der Informationstechnik: UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen. 2014. http://www.bbk.bund.de/SharedDocs/Downloads/Kritis/DE/Fortschreibung_Gesamtdokument.pdf?__blob=publicationFile

Bundestag 2013 Bundestag (05.07.2013): Gesetz zur Förderung der elektronischen Verwaltung Ä sowie zur Änderung weiterer Vorschriften g, EGovG. In: Bundesgesetzblatt http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/egovg_verkuendung.pdf;__blob=publicationFile (26.03.2014)

BZ 2011 Berliner Zeitung: Ostkreuz-Brand: Vodafone ohne Saft. 2011. http://www.bz-berlin.de/artikel-archiv/ostkreuz-brand-vodafone-ohne-saft (23.08.2014)

CBS 2013 CBS San Francisco: Shots fired at PG&E substation; Silicon Valley urged to conserve electricity. 2013. http://sanfrancisco.cbslocal.com/2013/04/16/gunshots-cause-oil-spill-at-san-jose-pge-substation/ (04.08.2014)

CIO 2013 Christiane Pütter: IT-Ausfall kostet bis zu 41.000 Euro pro Stunde: Vier Vorfälle pro Jahr. 2013. http://www.cio.de/knowledgecenter/security/2918599/ (04.04.2014)

CIOBund 2014 Die Beauftragte der Bundesregierung für Informationstechnik: Moderne Verwaltungskommunikation. 2014. http://www.cio.bund.de/Web/DE/Strategische-Themen/Moderne-Verwaltungskommunikation/moderne_verwaltungskommunikation_node.html (22.04.2014)

DECIX 2014 DE-CIX Management GmbH: Traffic Statistics. 2014. https://www.de-cix.net/about/statistics/ (23.03.2014)

DECIX 2013 DE-CIX Management GmbH: Nationales Routing: DE-CIX lädt Deutsche Telekom an den Verhandlungstisch. 2013. http://presse.de-cix.net/press-releases/pressemitteilung/article/nationales-routing-de-cix-laedt-deutsche-telekom-an-den-verhandlungstisch/ (27.03.2014)

DENIC 2014 DENIC eG: Der Nameserverdienst der DENIC. 2014. http://www.denic.de/hintergrund/nameservice.html (08.09.2014)

DENIC 2010 Beate Schulz: Background of the Partial Failure of the Name Service for.de Domains. 2010. http://www.denic.de/denic-im-dialog/mailinglisten/public-l.html?url=msg04454.xml (21.08.2014)

DESTATIS 2013a Statistisches Bundesamt (DESTATIS): Unternehmen und Arbeitsstätten: Nutzung von Informations- und Kommunikationstechnologien. 2013. https://www.destatis.de/DE/Publikationen/Thematisch/UnternehmenHandwerk/Unternehmen/InformationstechnologieUnternehmen5529102137004.pdf?__blob=publicationFile (26.03.2014)

DESTATIS 2013b Statistisches Bundesamt (DESTATIS): Dienstleistungen: Strukturerhebung im Dienstleistungsbereich Information und Kommunikation 2011. 2013. https://www.destatis.de/DE/Publikationen/Thematisch/DienstleistungenFinanzdienstleistungen/Struktur/InformationKommunikation2090420117004.pdf?__blob=publicationFile (26.03.2014)

DESTATIS 2013c Statistisches Bundesamt (DESTATIS): IKT-Branche in Deutschland: Bericht zur wirtschaftlichen Entwicklung. 2013. https://www.destatis.de/DE/Publikationen/Thematisch/UnternehmenHandwerk/Unternehmen/IKT_BrancheDeutschland5529104139004.pdf?__blob=publicationFile (02.04.2014)

DESTATIS 2013d Statistisches Bundesamt (DESTATIS): Ausstattung privater Haushalte mit Informations- und Kommunikationstechnik: Einkommen, Konsum, Lebensbedingungen. 2013. https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/AusstattungGebrauchsguetern/Tabellen/Infotechnik_D.html (04.04.2014)

DESTATIS 2008 Statistisches Bundesamt (DESTATIS): Klassifikation der Wirtschaftszweige: Mit Erläuterungen. 2008. https://www.destatis.de/DE/Methoden/Klassifikationen/GueterWirtschaftklassifikationen/klassifikationwz2008_erl.pdf?__blob=publicationFile (01.04.2014)

DTAG 2014a Gero Niemeyer: Wiederholte Einschränkungen in der IP-Telefonie. 2014. http://www.telekom-hilft.de/service-notizen/2014/09/wiederholte-einschraenkungen-in-der-ip-telefonie (08.09.2014)

DTAG 2014b Deutsche Telekom AG: Fragen und Antworten rund um die Teilnehmeranschlussleitung (TAL). 2014. http://www.telekom.com/medien/medienmappen/regulierung/170464 (04.04.2014)

DTAG 2013 Deutsche Telekom AG: Geschäftsbericht 2012: Wir glauben an eine Zukunft voller Möglichkeiten. 2013. http://www.telekom.com/static/-/173410/13/130228-q4-12-pdf-si (04.04.2014)

DTAG 2012 Deutsche Telekom AG: Deutsche Telekom investiert annähernd 30 Milliarden Euro in drei Jahren in die Zukunft der Telekommunikation. 2012. http://www.telekom.com/medien/konzern/164846 (28.03.2014)

EC 2013 European Commission: Digital Agenda Scoreboard 2013. 2013. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/DAE%20SCOREBOARD%202013%20-%20SWD%202013%20217%20FINAL.pdf (02.04.2014)

ECIX 2014 Peering GmbH: Statistics. 2014. http://www.ecix.net/statistics/ (23.03.2014)

eco 2009 Arthur D. Little: Die deutsche Internetwirtschaft 2009-2012: Überblick, Trends und Treiber. 2009. http://www.eco.de/wp-content/blogs.dir/die-deutsche-internetwirtschaft-2009-2012.pdf (02.04.2014)

EU 2009 Europäische Union (18.12.2009): Richtlinienpaket zur Novellierung des Regulierungsrahmens für Telekommunikationsnetze - Richtlinie 2009/140/EG. In: *Amtsblatt der Europäischen Union* 52. Jahrgang (L 337)

GasLine 2014 GasLINE Telekommunikationsnetzgesellschaft deutscher Gasversorgungsunternehmen mbH & Co. KG: Unternehmensdarstellung. 2014. http://www.gasline.de/profil/gesells.htm (08.09.2014)

HA 2013 Hamburger Abendblatt: Hamburger legt Internetportal Sachsen-Anhalts lahm. 2013. http://www.abendblatt.de/hamburg/article120447006/Hamburger-legt-Internetportal-Sachsen-Anhalts-lahm.html (11.06.2014)

Hackbarth 2006 Klaus-D. Hackbarth, Gabriele Kulenkampff: Technische Aspekte der Zusammenschaltung in IP-basierten Netzen unter besonderer Berücksichtigung von VoIP. 2006. (08.09.2014)

IANA 2014a Internet Assigned Numbers Authority (IANA): Root Zone Database. 2014. http://www.iana.org/domains/root/db (08.09.2014)

IANA 2014b Internet Assigned Numbers Authority (IANA): Root Servers. 2014. http://www.iana.org/domains/root/servers (08.09.2014)

IETF 2013 Internet Engineering Task Force (IETF): IETF Security Best Practices Efforts and Documents: draft-ietf-opsec-efforts-20.txt. 2013. https://tools.ietf.org/html/draft-ietf-opsec-efforts-20 (06.09.2014)

KabelD 2014 Kabel Deutschland AG: Das Glasfaser-Koaxialkabel-Netz von Kabel Deutschland: eine leistungsfähige Infrastruktur. 2014. http://www.kabeldeutschland.com/static-com/com/media/documents/downloads/factsheet/Infoblatt_Aufbau_Kabelnetz.pdf (04.04.2014)

Keller 2005 Andres Keller: Datenübertragung im Kabelnetz: DOCSIS über Hybrid-Fibre-Coax. Berlin/Heidelberg: Springer-Verlag 2005.

Level3 2014 Level 3 Communications, Inc.: Global Reach: Germany. 2014. http://www.level3.com/en/global-reach/europe/germany/ (28.03.2014)

MoKo 2013 Monopolkommission: Telekommunikation 2013:: Vielfalt auf den Märkten erhalten. Sondergutachten 66. 2013. (25.04.2014)

Nemat 2013 Nemat, Claudia; Günther, Kerstin: Webinar IP-Transformation. 2013. http://www.telekom.com/webinar-All-IP (26.03.2014)

OECD 2008 Organisation for Economic Co-operation and Development (OECD): Convergence and Next Generation Networks. 2008. http://www.oecd.org/sti/40761101.pdf (02.04.2014)

ONForum 2014 Open Network Alliance: Open Access Networks. 2014. http://www.opennetworkforum.org/what-is-an-open-network (04.04.2014)

Register 2014 Jack Clark: EU phone home! Cloudy transatlantic cable coughs, gags, chokes: Cloudflare, DigitalOcean, hit by big problems. 2014. http://www.theregister.co.uk/2014/05/19/eu_cable_outage/ (23.05.2014)

Ryan 2012 Ryan, Patrick S.; Gerson, Jason: A Primer on Internet Exchange Points for Policymakers and Non-Engineers. 2012. http://dx.doi.org/10.2139/ssrn.2128103 (15.05.2014)

Spiegel 2009 Matthias Kremp: Netzausfall: Störung im T-Mobile-Netz behoben. 2009. http://www.spiegel.de/netzwelt/mobil/netzausfall-stoerung-im-t-mobile-netz-behoben-a-620431.html (03.05.2014)

Spiegel 2008 Matthias Kremp: Mobilfunk-Panne: Wartungsfehler legt Vodafone-Netz teilweise lahm. 2008. http://www.spiegel.de/netzwelt/mobil/mobilfunk-panne-wartungsfehler-legt-vodafone-netz-teilweise-lahm-a-546902.html (04.05.2014)

statista 2014a statista: Umsatzanteil der Deutschen Telekom und von Wettbewerbern im Telekommunikationsmarkt in Deutschland von 1998 bis 2012. 2014. http://de.statista.com/statistik/daten/studie/74071/umfrage/umsatzerloesanteil-im-telekommunikationsmarkt-seit-1998/ (26.03.2014)

statista 2014b statista: Preisindex für Festnetztelefonie und Internet in Deutschland von 1995 bis 2013. 2014. http://de.statista.com/statistik/daten/studie/77783/umfrage/entwicklung-des-preisindex-fuer-festnetz-und-internet-seit-1995/ (04.04.2014)

Telia 2014 Telia: Problemen med internettrafiken mot USA och Asien är nu avhjälpta. 2014. http://www.telia.se/privat/driftinformation/2014/Maj/Problemen-med-internettrafiken-mot-USA-och-Asien--r-nu-avhj-lpta (08.09.2014)

teltarif 2013a Marleen Frontzeck: DSL- und Telefon-Störung bei 1&1 (behoben): Teil der DSL-Kunden mit Anschluss über Partner Vodafone betroffen. 2013. http://www.teltarif.de/1und1-vodafone-dsl-ausfall-stoerung/news/51339.html (22.07.2014)

teltarif 2013b Thorsten Neuhetzki: Leipzig: Vodafone-Kunden mehrere Stunden ohne Festnetz: Störungsursache behoben, Netz wird wieder hochgefahren. 2013. http://www.teltarif.de/vodafone-stoerung-festnetz-leipzig-anschluss-ausfall/news/51096.html (23.07.2014)

UnitedInt 2013 United Internet AG: Geschäftsbericht 2012. 2013. http://www.united-internet.de/fileadmin/extern/2012_annual_report_de/files/assets/common/downloads/publication.pdf (04.04.2014)

Unitymedia 2014 Unitymedia KabelBW GmbH: Unitymedia Fiber Power. 2014. http://www.unitymedia.de/privatkunden/beratung/produktberatung/fiberpower/ (27.03.2014)

VATM 2013 Dialog Consult / VATM: 15. TK-Marktanalyse Deutschland 2013: Ergebnisse einer Befragung der Mitgliedsunternehmen im Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V. im dritten Quartal 2013. 2013. http://www.vatm.de/uploads/media/2013_TK-Marktstudie.pdf (26.03.2014)

VDE 2009 Verband der Elektrotechnik (VDE): Informationstechnik – Breitbandkommunikation. 2009. https://www.vde-verlag.de/normen/0800027/vde-ar-e-2800-901-anwendungsregel-2009-12.html (04.04.2014)

Versatel 2014 Versatel GmbH: Über Versatel. 2014. http://www.versatel.de/unternehmen/profil/unser-profil (04.04.2014)

Vodafone 2014 Vodafone GmbH: Netze: Hohe Leistungsfähigkeit durch zweitgrößtes Transportnetz. 2014. http://www.vodafone.de/unternehmen/innovationen/netze.html (04.04.2014)

Vodafone 2013a Vodafone GmbH: Vodafone kündigt Abgabe eines freiwilligen öffentlichen Übernahmeangebots für Kabel Deutschland Holding AG an. 2013. http://www.vodafone.de/unternehmen/presse/pm-archiv-2013_214322.html (28.03.2014)

Vodafone 2013b Vodafone GmbH: Bundesnetzagentur beschließt höhere Miete für die Teilnehmeranschlussleitung. 2013. http://www.vodafone.de/unternehmen/presse/pm-archiv-2013_212058.html (28.03.2014)

Welt 2013 Die Welt: Stromstöße zerstören Technik in NSA-Rechenzentrum. 2013. http://www.welt.de/wirtschaft/webwelt/article120717405/Stromstoesse-zerstoeren-Technik-in-NSA-Rechenzentrum.html (12.06.2014)