JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL SCHWICKERT

Schwickert, Axel C.; Müller, Laura; Bodenbender, Nicole; Brühl, Markus W.; Mader, Maria; Kirchhof, Jessica; Himmelsbach, Marina; Falk, Michael; Zakrzewski, Sergiusz; Kießling, Christine; Weil, Tobias

Netzwerke – Grundlagen und Technik – Reader zur WBT-Serie

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 02/2012
ISSN 1613-6667

Arbeitspapiere WI Nr. 2 / 2012

Autoren: Schwickert, Axel C.; Müller, Laura; Bodenbender, Nicole; Brühl, Markus W.; Mader, Maria; Kirchhof, Jes-sica; Himmelsbach, Marina; Falk, Michael; Zakrzewski, Sergiusz; Kießling, Christine; Weil, Tobias

Titel: Netzwerke – Grundlagen und Technik – Reader zur WBT-Serie

Zitation: Schwickert, Axel C.; Müller, Laura; Bodenbender, Nicole; Brühl, Markus W.; Mader, Maria; Kirchhof, Jessica; Himmelsbach, Marina; Falk, Michael; Zakrzewski, Sergiusz; Kießling, Christine; Weil, Tobias: Netzwerke – Grundlagen und Technik – Reader zur WBT-Serie, in: Arbeitspapiere WI, Nr. 2/2012, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2012, 80 Seiten, ISSN 1613-6667.

Kurzfassung: Das vorliegende Arbeitspapier dient als Reader zur WBT-Serie „Netzwerke – Grundlagen und Technik“, die im E-Campus Wirtschaftsinformatik online zur Verfügung steht.

Das Internet wird auch als „Netz der Netze“ beschrieben. Auf dieser Grundlage werden, nach einem historischen Überblick des Internets, Aufbau und Struktur des Internets definiert und erläutert. Anschließend die Differenzierung zwischen Technik und Diensten des Internets. Abschließend wird der Fokus auf Sicherheit und mögliche Schutzmaßnahmen im Internet gelegt.

Schlüsselwörter: Das Internet, Geschichte des Internets, Technik und Dienste, Sicherheit im Internet

A Die Web-Based-Trainings

Der Lernstoff zum Themenbereich „Netzwerke – Grundlagen und Technik“ wird durch eine Serie von Web-Based-Trainings (WBT) vermittelt. Die WBT bauen inhaltlich aufeinander auf und sollten daher in der angegebenen Reihenfolge bearbeitet werden. Um einen Themenbereich vollständig durchdringen zu können, muss jedes WBT mehrfach absolviert werden, bis die jeweiligen Tests in den einzelnen WBT sicher bestanden werden.

WBT-Nr.	WBT-Bezeichnung	Dauer
1	Die Geschichte des Internets	90 Min.
2	Aufbau und Struktur des Internets	90 Min.
3	Technik und Dienste	90 Min.
4	Sicherheit und Schutzmaßnahmen	90 Min.

Tab. 1: Übersicht WBT-Serie

Die Inhalte der einzelnen WBT werden nachfolgend in diesem Dokument gezeigt. Alle WBT stehen Ihnen rund um die Uhr zur Verfügung. Sie können jedes WBT beliebig oft durcharbeiten. In jedem WBT sind enthalten:

- Vermittlung des Lernstoffes,
- interaktive Übungen zum Lernstoff,
- abschließende Tests zum Lernstoff.

Inhaltsverzeichnis

Seite

A Die Web-Based-Trainings I

Inhaltsverzeichnis II

Abbildungsverzeichnis VI

Tabellenverzeichnis VII

1 Die Geschichte des Internets 1

1.1 Die ersten Netze entstehen 1

1.1.1 Der Sputnik-Schock 1

1.1.2 Das ARPANet 1

1.1.3 Das CSNet 2

1.1.4 Ausbau weiterer Netzwerke 2

1.1.5 Netzwerke in Europa 3

1.2 Das Internet entsteht 3

1.2.1 Wechsel zu TCP/IP 3

1.2.2 Backbones entstehen 4

1.2.3 Technische Hürden 4

1.2.4 Der erste Web-Browser 4

1.2.5 Internet ungleich WWW 5

1.2.6 Unternehmen entdecken das Internet 5

1.2.7 Der Internet-Boom 6

1.2.8 Die Dot-com Blase 6

1.2.9 Das Neue Internet 7

1.3 Überblick 7

1.3.1 Die Geschichte des Internets im Zeitablauf 7

2 Aufbau und Struktur des Internets 10

2.1 Das Internet – Das Netz der Netze 10

2.1.1 Das Netz der Netze 10

2.1.2 Verschiedene Übertragungsmedien 10

2.1.3 Verschiedene Rechnernetze 11

2.1.4 Was ist ein LAN? 11

2.1.5 Was ist ein WAN? 13

2.1.6 Backbones und Knotenrechner 13

2.2 Anbieter und Benutzer 14

2.2.1 Der Weg ins Internet 14

2.2.2 Was ist ein ISP? 14
2.2.3 Der Tarifdschungel 15
2.2.4 Aufgaben eines Carriers 16
2.2.5 Private Nutzungsmöglichkeiten 16
2.2.6 Unternehmen im Internet 17
2.2.7 Aktuelle Zahlen zum Internet 17
2.3 Das Client/Server-Konzept 18
2.3.1 Das Internet auf meinem Bildschirm 18
2.3.2 Was ist das Client/Server-Konzept? 19
2.3.3 Client/Server-Konzept im Internet 19
2.3.4 Mehr als ein Server 19
2.3.5 Mögliche Aufgabenverteilung 20
2.3.6 3-Tier-Architektur im Internet 21
2.3.7 Aufruf einer Web Site 21
2.3.8 Verschiedene Server und ihre Aufgaben 22
2.3.9 Eine Alternative: Das Peer-to-Peer-Modell 23
2.4 Abschlusstest 23
2.4.1 Abschlusstest 23

3 Technik und Dienste 25
3.1 Internetdienste 25
3.1.1 Einleitung 25
3.1.2 Elektronische Post 25
3.1.3 Instant Messaging 26
3.1.4 Datentransfer im Internet 26
3.1.5 Der Dienst WWW 27
3.1.6 Was ist ein URL? 28
3.1.7 Wie funktioniert das Domain Name System? 29
3.1.8 Exkurs: Was ist HTML? 30
3.1.9 Ein Beispiel zu HTML 30
3.2 Geräte und Medien 31
3.2.1 Heterogene Systeme im Internet 31
3.2.2 Geräte der Netzwerktechnik 31
3.2.3 Übertragungsmedien 32
3.2.4 Was wird übertragen? 33
3.3 Protokolle und Schichtenmodelle 34
3.3.1 Überwindung einer Sprachbarriere 34
3.3.2 Was ist ein Protokoll? 35
3.3.3 HTTP und HTTPS 35

3.3.4 Die E-Mail-Protokolle 36
3.3.5 Was ist ein Schichtenmodell? 36
3.3.6 Ein Standard für alle Netze 37
3.3.7 Einkapselung von Daten 38
3.3.8 Aufgabenteilung der Schichten 38
3.3.9 Ein weiteres Modell 40
3.3.10 Ein Beispiel 41
3.4 Abschlusstest 42
3.4.1 Abschlusstest 42

4 Sicherheit und Schutzmaßnahmen 44
4.1 Der Begriff Sicherheit um Internet 44
4.1.1 Warum IT-Sicherheit? 44
4.1.2 Definition des Begriffs Sicherheit 44
4.1.3 Privacy versus Security 45
4.2 IT-Risikoanalyse 45
4.2.1 IT-Risikoanalyse 45
4.2.2 Grundschutz kompakt: Leitfaden IT-Sicherheit 46
4.2.3 IT-Grundschutz 46
4.2.4 Detaillierte Risikoanalyse 47
4.3 Gefahren 49
4.3.1 Gefahren: Technische und Menschliche 49
4.3.2 Angreifer: Hacker, Cracker, Skipt Kiddies 50
4.3.3 Eindringlinge: Viren, Würmer und Trojaner 50
4.3.4 Viren 51
4.3.5 Würmer 51
4.3.6 Trojanische Pferde 52
4.3.7 SPAM 52
4.3.8 HOAX (engl.): Falschmeldung 53
4.3.9 Denial of Service (DoS) und Sniffing 53
4.3.10 Social Engineering und Phishing 53
4.4 Schutzsysteme 55
4.4.1 Kryptographie: Verschlüsselung 55
4.4.2 SSL: Secure Socker Layer-Verfahren 55
4.4.3 VPN: Virtual Private Network 56
4.4.4 E-Mail-Sicherheit 56
4.4.5 Firewall 57
4.4.6 Antiviren-Software 57
4.4.7 IDS – Intrusion Detection System 58

4.5 Abschlusstest 59
4.5.1 Abschlusstest 59

Anhang VIII

Abbildungsverzeichnis

Seite

Abb. 1: Bus-Topologie 12
Abb. 2: Ring-Topologie 12
Abb. 3: Stern-Topologie 13
Abb. 4: Der Weg ins Internet 14
Abb. 5: Anteil der Internetnutzer an der Gesamtbevölkerung 18
Abb. 6: Das Client/Server-Konzept 19
Abb. 7: Kaskadierung 20
Abb. 8: Client/Server-Architekturen 20
Abb. 9: Bestandteile eines URLs 28
Abb. 10: Bestandteile eines Domainnamens 29
Abb. 11: Überwindung einer Sprachbarriere 34
Abb. 12: Das TCP/IP Referenzmodell 37
Abb. 13: TCP/IP-Referenzmodell vs. OSI-Schichtenmodell 40
Abb. 14: Vereinfachter E-Mail-Versand 41
Abb. 15: Detaillierte Risikoanalyse 48
Abb. 16: Beispiel Phishing-Mail 54
Abb. 17: SSL-Verbindung in Webbrowser 55
Abb. 18: IDS 58

Tabellenverzeichnis

Seite

Tab. 1: Übersicht WBT-Serie I
Tab. 2: Abschlusstest in WBT 2 24
Tab. 3: Abschlusstest in WBT 3 43
Tab. 4: Abschlusstest in WBT 4 61
Tab. 5: Lösungen zum Abschlusstest in WBT 2 IX
Tab. 6: Lösungen zum Abschlusstest in WBT 3 XI
Tab. 7: Lösungen zum Abschlusstest in WBT 4 XIV

1 Die Geschichte des Internets

1.1 Die ersten Netze entstehen

1.1.1 Der Sputnik-Schock

Im **Oktober 1957** schoss die Sowjetunion den ersten Satelliten (Sputnik 1) ins All. Dieser offensichtliche Technologievorsprung der Sowjets löste in den USA den so genannten **Sputnik-Schock** aus. Das US-Verteidigungsministerium gründete daraufhin im Jahr **1958** die **ARPA** (Advanced Research Projects Agency). Die ARPA war eine Arbeitsgruppe, mit dem Zweck, neue Ideen und Technologien zu erforschen. Die Gründung der ARPA kann als **Grundstein** für die Entwicklung des Internets bezeichnet werden. Das Internet hat sich mittlerweile zu dem "**größten und meistverwendeten Netzwerk**" der Welt entwickelt und ermöglicht u. a. einen weltweiten **Informationsaustausch** in der Wirtschaft, privaten und öffentlichen Bereichen sowie in Bildung und Wissenschaft.

1.1.2 Das ARPANet

Im Jahr **1969** präsentierte die Advanced Research Projects Association (ARPA) das **ARPANet**, ein Computer-Netzwerk, welches ausschließlich Rechner an amerikanischen Universitäten miteinander verband. Die erste Verbindung bestand zwischen den vier Orten Menlo Park, Santa Barbara, Los Angeles und Salt Lake City. **1973** kamen die ersten beiden **internationalen Verbindungen** hinzu: das University College of London und das Royal Radar Establishment in England.

Das ARPANet war ein **dezentrales Netzwerk** und kann als **Vorläufer des heutigen Internets** bezeichnet werden. Ein dezentrales Netzwerk ist nach keinem speziellen Schema aufgebaut. Die einzelnen Knoten sind untereinander mehrfach vermascht, das heißt, dass eine Komponente mit mehreren anderen verbunden ist.

Diese dezentrale Netzstruktur sichert die Funktionsfähigkeit, wenn Teilnetzwerke hinzukommen, entfernt werden oder ausfallen.

In den siebziger Jahren wurde ARPA in **DARPA** (Defense Advanced Research Projects Agency) umbenannt und unterstützte nur noch Projekte, die der Landesverteidigung dienten. **Universitäten** wurde der Zugang zum ARPANet nur gewährt, wenn diese für die **DARPA Forschung** betrieben. Zudem war der Anschluss an das ARPANet sehr teuer und daher für viele Universitäten nicht bezahlbar.

1.1.3 Das CSNet

Der **Computerboom** führte an immer mehr amerikanischen Universitäten zur Bildung von computerwissenschaftlichen Abteilungen. Während das ARPANet weiter expandierte, blieben die meisten Universitäten bei diesem Wachstum außen vor, weil beim Anschluss an das ARPANet einerseits **hohe Kosten** entstanden wären und zudem Forschung für das US-Verteidigungsministerium hätte betrieben werden müssen.

1979 trafen sich Vertreter von mehreren US-Universitäten unter der Leitung von Larry Landweber zu einem Kolloquium, um über die Einrichtung eines neuen Netzwerks - dem **CSNet** (Computer Sciences Network) - zu beraten. Das CSNet sollte **vom ARPANet unabhängig** sein und den computerwissenschaftlichen Abteilungen der Universitäten zugänglich gemacht werden. Das Projekt sollte durch Gebühren der teilnehmenden Universitäten finanziert werden. Die National Science Foundation (US-Regierungsbehörde für Wissenschaftsförderung) **subventionierte** das CSNet-Projekt für die ersten fünf Jahre mit **fünf Millionen Dollar**.

1.1.4 Ausbau weiterer Netzwerke

In den 80er Jahren entwickelten viele amerikanische Institutionen ihre **eigenen**, unabhängigen Netzwerke:

- Das **BITNet** war ein kooperatives Rechnernetzwerk und verband schnell viele Universitäten und wissenschaftliche Institutionen miteinander. Das BITNet benutzte ein einheitliches Kommunikationsverfahren, das auch von Rechnernetzen in Europa und Kanada eingesetzt wurde. Es entstand ein weltweit homogenes Rechnernetz, das auf seinem Höhepunkt rund 3500 Rechner in über 1400 Organisationen miteinander verband.
- Das **Usenet** war ein eigenständiges Netzwerk zur Verteilung von Nachrichten. Eingerichtet wurde das Usenet 1979 zwischen der University of North Carolina und der Duke University. Als Gründer des Usenets gelten Jim Ellis, Steve Bellovin und Tom Truscott.
- Das **SPANet** (Space Physics Analysis Network) war ein Forschungsnetzwerk der NASA, das der Verbindung der NASA-eigenen Forschungseinrichtungen diente.
- Das **FidoNet** wurde 1984 von Tom Jennings gegründet. Es war eines der ersten globalen Netzwerke, das den Nachrichtenaustausch für Privatnutzer ermöglichte.

Alle genannten Netze wurden von ihrer jeweiligen Community sorgsam gepflegt. Allerdings erreichten die meisten Anbindungen nur geringe Übertragungsraten, welche von einem heutzutage handelsüblichen DSL-Anschluss übertroffen werden.

1.1.5 Netzwerke in Europa

1982 gab es erste **Bewegungen in Europa**, die sich das ARPANet als geeignete Basis eines weltweiten Computernetzes zum Vorbild nahmen. Noch im selben Jahr wurde ein eigenständiges Netzwerk namens **EUNet** (European UNIX Network) entwickelt. Auch das EUNet ermöglichte den Nachrichtenaustausch unter den Teilnehmern.

Im Jahre **1986** gründeten europäische Universitäten und Forschungseinrichtungen eine Institution namens **RARE** (Réseaux Associés pour la Recherche Européene). RARE sollte Pläne für ein europäisches Computernetzwerk ausarbeiten und schließlich auch umsetzen. Alle Planungen von RARE liefen in dem Projekt **COSINE** (Cooperation for an Open Systems Interconnection Networking in Europe) zusammen. Als Ergebnis des COSINE-Projekts wurde **1993** das akademische Forschungsnetzwerk **EuropaNet** aufgebaut, das bis heute existiert. Der erste europaweite Backbone namens **Ebone** wurde **1991** aufgebaut. In verschiedenen europäischen Städten wurden **Knoten** über Standleitungen, mit hohen Bandbreiten miteinander verbunden. Knoten dienen als Schnittstellen zwischen Rechnernetzen (LANs und WANs) und als Austauschpunkte für den Datenverkehr des Internets.

1.2 Das Internet entsteht

1.2.1 Wechsel zu TCP/IP

Die Anzahl der Knoten des **ARPANets vergrößerte** sich ständig, denn immer **mehr Rechner** wurden an das ARPANet **angeschlossen**. Gleichzeitig wurde das **Übertragungsprotokoll** immer weiter entwickelt. Ein Protokoll definiert Regeln für den Austausch von Informationen. Im Falle von Übertragungsprotokollen beziehen sich diese Regeln auf den Austausch von Inhalten (z. B. Nachrichten) über Rechnernetze.

Am 1. Januar **1983** fand der **Übergang** vom bisher verwendeten Network Control Protocol (NCP) zum noch heute gültigen Standard **TCP/IP** statt. TCP/IP steht für Transmission Control Protocol/Internet Protocol. Eine erste Spezifikation von TCP gab es schon 1974.

Ab 1978 wurde das Protokoll als TCP/IP weiterentwickelt. Die TCP/IP Protokollfamilie hat ihren Ursprung in einer Entwicklergruppe um Vint Cerf und Bob Kahn. Der Übergang von

NCP zu TCP/IP ermöglichte die Kommunikation zwischen verschiedenen Netzwerken und war eine weitere **Grundlage** für das **Internet**. Durch die Verwendung von TCP/IP konnten nun Computer des ARPANets mit Computern anderer Netzwerke kommunizieren. Der Grundgedanke des ARPANets mit dem NCP-Protokoll war die Verbindung von Computern. Grundgedanke des Internets ist hingegen die Verbindung von Netzwerken.

1.2.2 Backbones entstehen

1985 wurden in den USA fünf Supercomputerzentren eingerichtet. Die **NSF** (die US-amerikanische National Science Foundation) schaffte ein Leitungsverbundsystem, das die bedeutenden wissenschaftlichen Rechenzentren des Landes miteinander verband - das Wort **Backbone** wurde in diesem Zusammenhang geboren. Das von der NSF auf Basis von Supercomputern aufgebaute Netzwerk wurde **NSFNet** genannt. Einzelne Universitätsrechner konnten sich über das eigene Rechenzentrum mit NSFNet verbinden und so in andere Rechnernetze gelangen. Das Backbone-Konzept sollte auch das spätere Internet prägen. Es entstanden viele regionale Netzwerke wie z. B. das **NYSERNet** und das **CERFNet**.

1.2.3 Technische Hürden

Anfang der **90er** Jahre bestand bereits eine **globale Vernetzung**, das Internet. Allerdings war das Internet noch **nicht so einfach** zu benutzen, wie es heute der Fall ist. Es gab zwar **Dienste**, die die Navigation und Informationsgewinnung im Internet ermöglichten, wobei zwischen Basisdiensten, wie z. B. E-Mail; und Informationsrecherchesystemen, wie dem WWW, unterschieden wird. Jedoch gab es keine einfachen, benutzerfreundlichen **Bedienungsoberflächen**. Die verfügbare Software war sehr **komplex**. Der **technische Einstieg** war demnach **schwer** und konnte nur von **Spezialisten** bewältigt werden. Internetnutzern **ohne technisches Know-how** blieb der Internetzugang verschlossen.

1.2.4 Der erste Web-Browser

Ein weiterer Meilenstein in dieser Zeit war die des **World Wide Web** (WWW). Die Nutzung des World Wide Web (WWW) erfolgt auf der Anwenderseite über einen **Web-Browser**. Web-Browser ermöglichen die Darstellung von Inhalten des WWW. Gängige Browser sind Microsoft Internet Explorer oder Mozilla Firefox.

Der **erste Web-Browser** wurde **1990** durch den Physiker Tim Berners-Lee am Kernforschungszentrum CERN in Genf entwickelt. Damit untrennbar war die Entwicklung von HTML und des HTTP-Protokolls verbunden, welches die Übertragung von HTML-Dokumenten ermöglicht und somit die Basis für das WWW darstellt.

Die **Hypertext Markup Language** (HTML) ist eine Seitenbeschreibungssprache zur Beschreibung und Darstellung von Inhalten im WWW. HTML legt durch vordefinierte Markierungen (Tags) die Anordnung und das Format der übertragenen Inhalte fest. Vorteile von HTML liegen u. a. in der Betriebssystemunabhängigkeit sowie der starken Verbreitung.

Das WWW basiert auf dem **Hypertext Transmission Protocol** (HTTP). Dieses Protokoll wird für die Übertragung von Seiten im Web verwendet.

1.2.5 Internet ungleich WWW

Die Begriffe **Internet und WWW** werden oft gleichgesetzt, es bestehen jedoch wesentliche **Unterschiede**. Das Internet ist ein **physisches Netzwerk**. Es ist der "greifbare" Teil der globalen Vernetzung, bestehend aus Rechnern und Verbindungen zwischen diesen einzelnen Rechnern. Die Verbindungen können entweder drahtgebunden (z. B. über Kupferkabel) oder drahtlos (z. B. per Funkverbindung) realisiert sein.

Das **WWW** hingegen ist kein physisches Netz, sondern ein Dienst, der sich eines physischen Netzes (des Internets) bedient. **WWW und Internet** sind vergleichbar mit **Sprachübertragung** und dem **Telefonnetz.** Das physische Netz ist das drahtgebundene oder drahtlose Telefonnetz, der Dienst ist die Sprachübertragung. Weitere Dienste, die über das Telefonnetz in Anspruch genommen werden können, wären bspw. **Fax-Übertragung** oder SMS. Die große Aufmerksamkeit, die das Internet in den letzten Jahren in der **Öffentlichkeit** und der **Wirtschaft** erfahren hat, ist in erster Linie auf den Dienst WWW zurückzuführen.

1.2.6 Unternehmen entdecken das Internet

Bis **1995** wurde das Internet als wirtschaftlich relevanter Faktor nicht ernst genommen. Laut Fachzeitschriften konnte das **Internet keinen wirtschaftlichen Nutzen** erzeugen bzw. in einem Wirtschaftsgefüge nicht nützlich eingesetzt werden.

Mitte der **90er Jahre** wagen die ersten Unternehmen den Schritt im Internet. In dieser Zeit wird der Begriff **E-Business** geprägt. E-Business beschreibt alle geschäftlichen Aktivitäten von

Martktteilnehmern, Unternehmen und Organisationen, die über Informations- und Kommunikationstechnologien ausgeführt werden. E-Commerce ist ein Teil des E-Business und beschreibt den An- und Verkauf (Handel) über elektronische Systeme, wie z. B. das Internet.

Die Möglichkeit, **Geschäfte über das Internet** zu betreiben, gab den Unternehmen Raum für neue Ideen. Das zeigt u. a. das seitdem ständig wachsende **Umsatzvolumen** des Online-Handels mit Endkunden. In Deutschland betrug dieses im Jahr 2006 ca. **23 Mrd. Euro**.

1.2.7 Der Internet-Boom

Im **April 1993** wurde die **WWW-Technologie** vom CERN-Institut **freigegeben**. Die Technologie war somit **für alle zugänglich**. Durch die **rapide "Computerisierung"** in Unternehmen und Haushalten war der "Internet-Boom" nicht mehr zu bremsen. Laut statistischem Bundesamt nutzten im Jahr 2006 **zwei Drittel** der Personen ab 10 Jahren (65%) das Internet. Der **Anteil der Internetnutzer** ist damit im Vergleich zu 2005 (61%) um vier Prozentpunkte **gestiegen.** 2019 nutzen 89% der Deutschen das Internet, etwa 71% nutzen es täglich. 10,7 Millionen Deutsche nutzen das Internet fast rund um die Uhr.

Auch im Vergleich mit anderen **technischen Neuerungen** des letzten Jahrhunderts kann das Internet überzeugen: Für die ersten 50 Millionen Nutzer weltweit benötigte das **Radio** 38, das **Fernsehen** 13 und das **Internet** nur 5 Jahre.

1.2.8 Die Dot-com Blase

Die steigende **Begeisterung** der Internetnutzer sowie neue **technologische Entwicklungen** führten immer mehr Unternehmen auf den "neuen Markt" Internet. Zwischen 1995 und 2001 entstanden viele sogenannte **"Dot-coms".** Dot-Com- Unternehmen betreiben ihr **Geschäft** hauptsächlich über das Internet. Die Web-Adressen (URLs) endeten meist auf ".com", wodurch sich die Bezeichnung "Dot-Com- Unternehmen" etablierte.

Die **hohen Gewinnerwartungen** der Branche führten zu vielen **Unternehmens-Gründungen**. Dem großen Anlegerinteresse an diesen "Zunkunftsunternehmen" folgten zahlreiche Börsengänge. Das große Interesse vieler Neuanleger führte ab 1999 zu hohen Börsenbewertungen bei zahlreichen Unternehmen. Im Jahr 2000 führten **sinkende Kurse** zu einer Panik, in der die Anleger alles verkauften, um ihre Verluste in Grenzen zu halten. Dies brachte die Kurse zum endgültigen Absturz und damit die **Dot-Com Blase zum Platzen**.

1.2.9 Das Neue Internet

Mittlerweile ist das Internet um **Funktionen** erweitert worden, die beim **ursprünglichen** Entwurf keine Berücksichtigung fanden. Aspekte wie Mobilität, Dienstgüte oder Sicherheit waren in der damaligen **Planung nicht enthalten** oder **technisch noch nicht möglich**. Wie Sie wissen, war die **Grundidee** des Internets der Informationsaustausch zu Forschungszwecken. Daher wurde bei der Entwicklung auch darauf der **Fokus** gelegt. Doch das heutige Internet bietet viel **mehr** Möglichkeiten, wie z. B. das **Einkaufen über das Internet** oder E-Mails mit einem Mobiltelefon zu versenden und zu empfangen. Diese **neuen Funktionen** müssen in die bestehende Technik des Internets implementiert werden.

Die nachträgliche **Integration** entsprechender **Lösungen** gestaltete sich allerdings teilweise sehr **schwierig**. Um bspw. den Einkauf im Internet sicher für den Kunden zu machen, muss eine technische Lösung geschaffen werden, die dies ermöglicht und gleichzeitig mit den technischen Voraussetzungen des Internets **kompatibel** ist. Auch der Empfang bzw. Versand von E-Mails über ein Mobiltelefon bedarf einer Lösung, die die wesentlich neuere Mobilfunktechnologie mit der Internettechnologie **verbinden** kann. So gibt es immer häufiger Überlegungen in Richtung eines komplett **neuen Lösungsansatzes**, der keine Rücksicht auf Kompatibilität zum **existierenden Internet** nimmt.

Unter dem Begriff "Future Internet" werden Forschungsinitiativen verstanden, deren Ziel es ist, ein Internet der Zukunft zu entwickeln. Dabei soll versucht, werden die oben genannten Aspekte von Beginn in den Entwurf einer neuen Netzarchitektur mit einzubeziehen. Als Hilfestellung dienen dabei zwei **zentrale Fragen**:

1. Welche Anforderungen bestehen an ein globales Netz in 15 Jahren?
2. Wie sollte das Netz von morgen aus heutiger Sicht entwickelt werden, wenn es von Grund auf neu entworfen werden kann?

1.3 Überblick

1.3.1 Die Geschichte des Internets im Zeitablauf

Die folgende chronologische Auflistung gibt eine Übersicht über die Geschichte des Internets:

1957: Die Sowjetunion sendet den ersten Satelliten "Sputnik 1" ins All. Dies ist der Auslöser für den "Sputnik-Schock".

1958: Die Arbeitsgruppe ARPA (Advanced Research Projects Agency) wird vom US-Verteidigungsministerium im Auftrag des damaligen US-Präsidenten Dwight D. Eisenhower eingerichtet.

1969: Im Dezember 1969 werden die Unis in den vier Orten Menlo Park, Santa Barbara, Los Angeles und Salt Lake City durch ein funktionsfähiges Netzwerk verbunden. Das sogenannte ARPANet entsteht. Dies ist die Geburtsstunde des Internets.

1979: Die Planungen am CSNet beginnen. Ziel ist ein vom ARPANet unabhängiges Netzwerk für die computerwissenschaftlichen Abteilungen der beteiligten Universitäten.

1983: ARPANet wird auf das neue Übertragungsprotokoll TCP/IP (Transmission Control Protocol/Internet Protocol) umgestellt. Damit war die Kommunikation zwischen verschiedenen Netzwerken möglich. Das Internet nutzt auch heute noch dieses Protokoll.

1985: In den USA werden 5 Supercomputer erstmals durch ein "Rückgrat" (Backbone) verbunden. Die NSF betreibt das NSFNet als Backbone für die Verbindung von neuen, regional entstehenden Netzen.

1990: Der Physiker Tim Berners-Lee entwickelt am CERN-Forschungszentrum den ersten Web-Browser. Zu Weihnachten stellt Berners-Lee die ersten HTML-Web-Seiten der Welt zur Verfügung.

1993: Aufbau des akademischen Forschungsnetzwerks EuropaNet. Die WWW-Technologie wir durch das CERN-Forschungszentrum frei zur Verfügung gestellt. Der Siegeszug des WWW beginnt.

1994: Die Suchmaschine Yahoo und das Unternehmen Amazon werden gegründet.

1995: IBM prägt den Begriff E-Business. Das Online-Auktionshaus eBay geht online.

1998: Die Suchmaschine Google wird von den Stanford-Studenten Larry Page und Sergey Brin gestartet. Täglich werden über eine Milliarde Suchanfragen bei Google gestellt.

2001: Die Börsenkurse, der seit 1999 steigenden "Dot-Coms", fallen rapide. Die Dot-com-Blase platzt.

2005: Die Video-Plattform YouTube wird gegründet.

2006: Es sind 92.615.362 Web Sites online. Zwei Drittel der Deutschen nutzen das Internet.

2007: Es Mit Apples iPhone und dem Betriebssystem iOS wird die **mobile Internetnutzung** komfortabel. Google kontert ein Jahr später mit Android.

2010: Zum ersten Mal wird ein PC im Weltraum mit dem Internet verbunden.

2018: 81% der Menschen in den Industriestaaten haben Internet-Zugriff. In Entwicklungsländern liegt die Quote bei 41%.

2019: In Deutschland werden für 6,55 Milliarden Euro Frequenzen für den 5G-Datenfunk versteigert, der unter anderem die Vernetzung in der Industrie einen Schub geben soll.

2 Aufbau und Struktur des Internets

2.1 Das Internet – Das Netz der Netze

2.1.1 Das Netz der Netze

Das Internet wird auch "**Netz der Netze**" genannt. Dieser Beiname beruht auf der **weltweiten Verbreitung** des Internets: Jeder angeschlossene Rechner kann mit jedem anderen angeschlossenen Rechner verbunden werden.

Allerdings führt der Beiname "**Netz der Netze**" leicht in die Irre, denn:

- Das Internet ist **nicht** ein einziges **homogenes Netz**, sondern ein Verbund aus vielen kleinen, territorial oder organisatorisch begrenzten Netzen.
- Diese begrenzten Netze sind **kein fester Bestandteil** des Internets, sie werden von ihrem jeweiligen Besitzer zum Gebrauch freigegeben oder gesperrt.
- Dadurch **ändert sich** die **Struktur** dieses Netzwerkverbunds permanent.

Was diese Punkte genau besagen, erfahren Sie im Folgenden.

2.1.2 Verschiedene Übertragungsmedien

Bevor Sie verschiedene Rechnernetze kennenlernen, erhalten Sie eine kurze Übersicht über **mögliche Wege**, auf denen Daten übertragen werden können. Ein Übertragungsweg ist die physische Verbindung zwischen zwei Datenstationen durch ein **Übertragungsmedium**, das Informationen durch elektrische bzw. optische Signale oder durch elektromagnetische Wellen übermittelt. Diese physischen Verbindungen lassen sich unterscheiden in:

Kabelverbindungen:

- **Kupferkabel** übertragen elektrische Signale. Die Verlegung ist zwar einfach, allerdings sind sie nicht abhörsicher.
- **Glasfaserkabel** übertragen optische Signale. Dazu müssen elektrische Signale vor der Übertragung in optische Signale umgewandelt werden. Glasfaserkabel bieten hohe Übertragungsgeschwindigkeiten und sind weitgehend abhörsicher. Allerdings ist das Verbinden der Kabel aufwendig und ihre mechanische Belastbarkeit ist gering.

Funkverbindungen:

- **Terrestrischer Funk** bezeichnet die drahtlose Verbindung von erdgebundenen Sendern zu Empfängern. Diese Verbindungen haben eine hohe Reichweite. Ein Beispiel hierfür ist das Mobilfunknetz, das über Sendemasten betrieben wird.
- **Satelliten-Funk** ist ebenfalls drahtlos. Die Übertragung erfolgt durch Satelliten, die über eine noch höhere Reichweite als der terrestrische Funk verfügen.

Optische Verbindungen

Bei optischen Verbindungen werden Daten per Licht übertragen. Im Gegensatz zu Glasfaserkabeln sind hier keine Kabel notwendig. Allerdings muss eine direkte Sichtverbindung zwischen Sender und Empfänger bestehen. Eine bekannte optische Verbindung ist die Übertragung per Infrarot (z. B. in Fernbedienungen). Diese ist allerdings in puncto Übertragungsgeschwindigkeit und Reichweite nicht sehr leistungsfähig. Deutlich leistungsfähiger ist bspw. die Übertragung per Laser.

2.1.3 Verschiedene Rechnernetze

Rechnernetze ermöglichen die **gemeinsame Nutzung von Ressourcen** innerhalb der Netze. Solche Ressourcen können Daten (z. B. Kundendaten), Anwendungen (z. B. Termin- oder Auftragsverwaltung) oder allgemein Hardware (z. B. Drucker oder Scanner) sein. In Rechnernetzen werden Rechner oder Peripheriegeräte über Datenleitungen miteinander verbunden. Rechnernetzwerke können in ihrer Gestaltung (Vernetzung und Komponenten) sehr unterschiedlich sein. Eine Unterscheidung nach der räumlichen Ausdehnung in Local Area Networks (LAN) und Wide Area Networks (WAN) ist üblich.

Ein LAN ist begrenzt z. B. auf ein Firmen- oder Campusgelände, ein Gebäude oder einen Raum. Die Ausdehnung eines LAN beträgt **maximal einen (1) km.**

Bei einem WAN hingegen ist die **Ausdehnung unbeschränkt.**

2.1.4 Was ist ein LAN?

In einem **LAN** werden Rechner über ein Übertragungsmedium (Kabel-, Funk- oder optische Verbindungen) zu einem Netzwerk zusammengeschlossen. Zweck eines LANs ist es**, verfügbare Ressourcen** (Daten, Anwendungen, Hardware) jedem berechtigten Benutzer des Netzwerks zugänglich zu machen. Dadurch ergeben sich **Einsparpotenziale** und **Effizienzvorteile**.

Beispielsweise kann innerhalb einer Unternehmensabteilung ein zentraler Drucker von jedem Mitarbeiter genutzt werden. Des Weiteren können Daten **einfacher** und **schneller** zur Verfügung gestellt werden, was die Arbeitsabläufe verbessern kann.

Die Anordnung der Elemente eines LANs (die sog. **Topologie**) kann in drei Grundformen unterschieden werden:

Bus-Topologie:

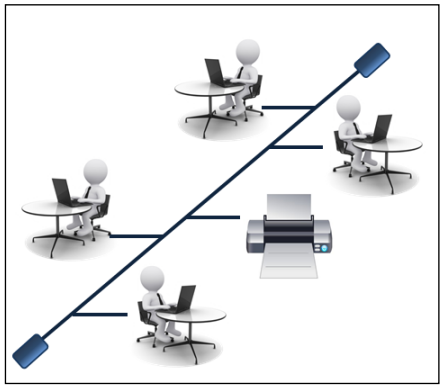

Abb. 1: Bus-Topologie

Bei der Bus-Topologie ist jedes beteiligte Gerät an eine zentrale Datenleitung angeschlossen.

Ring-Topologie:

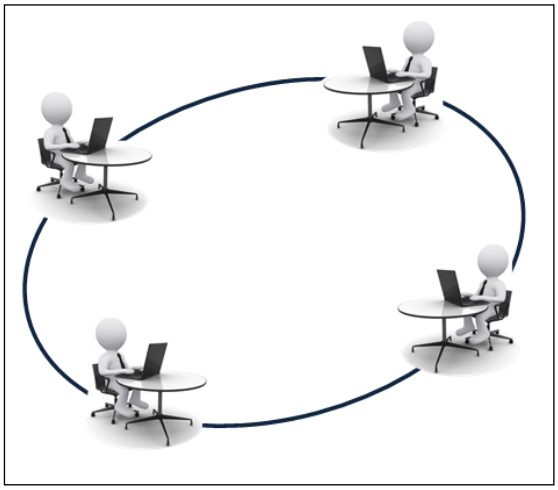

Abb. 2: Ring-Topologie

In der Ring-Topologie ist jedes beteiligte Gerät mit einem linken und einem rechten Nachbarn verbunden.

Stern-Topologie:

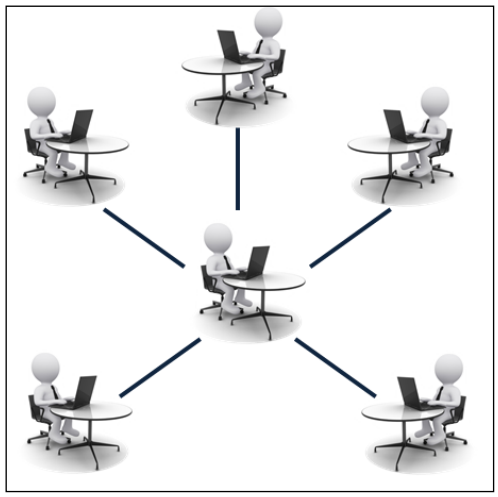

Abb. 3: Stern-Topologie

Bei einer Stern-Topologie sind alle beteiligten Geräte über ein zentrales Gerät miteinander verbunden.

2.1.5 Was ist ein WAN?

Ein **Wide Area Network** (WAN), auch Weitverkehrsnetz genannt, ist ein Netzwerk, welches geografisch entfernte und voneinander **unabhängige Rechner** miteinander **verbindet**. Übrigens: Ein Ihnen sicher bekanntes WAN ist das Telefonnetz der Deutschen Telekom.

Neben einzelnen Rechnern können auch komplette LANs, wie z. B. das der **Universität Gießen**, über ein WAN mit anderen LANs und Rechnern verbunden werden. Im Ge-gensatz zu den Strukturen eines LANs sind Weitverkehrsnetze häufig **vermascht**. Das heißt, dass möglichst viele Punkt-zu-Punkt Verbindungen geschaffen werden. Umso mehr von diesen Verbindungen bestehen, desto größer ist die **Ausfallsicherheit**, weil bei Ausfall einer Verbindung die Daten über einen anderen Weg an ihr Ziel gelangen. Die **Übertragung** der Daten im WAN erfolgt entweder **drahtgebunden** (z. B. Glasfaser oder Kupferdraht) oder **drahtlos** (z. B. Satellitenverbindungen). Die eigentlichen Verbindungen werden **Backbones** genannt und im Folgenden näher vorgestellt.

2.1.6 Backbones und Knotenrechner

Die **Vernetzung** eines WAN erfolgt über sog**. Backbones**. Ein Backbone, wie z. B. eine Datenleitung zwischen mehreren deutschen Städten, kann folgende Eigenschaften haben:

- Ein öffentlich zugängliches Netz, das von jedem genutzt werden kann.

- Ein privater Übertragungsweg, der ausschließlich vom Betreiber und berechtigten Nutzern genutzt werden kann. Diese müssen bei der Regulierungsbehörde gemeldet werden.

An den Knotenpunkten der Backbones kommen sog. **Knotenrechne**r zum Einsatz. Dabei handelt es sich um Rechner, die die Netzaktivitäten **überwachen** und **steuern**. Der **Zugang** zu einem **WAN** und damit auch zum Internet ist nur über einen solchen Knotenrechner möglich. Im folgenden Kapitel werden Sie erfahren, wie dieser Zugang hergestellt wird.

2.2 Anbieter und Benutzer

2.2.1 Der Weg ins Internet

Sie haben bisher erfahren, dass das Internet ein Zusammenschluss von verschiedenen Rechnernetzen ist. Doch was bedeutet dies für den Internetnutzer? Ist der Internetnutzer direkt über ein Kabel "mit der Welt" verbunden oder liegt möglicherweise noch etwas dazwischen?

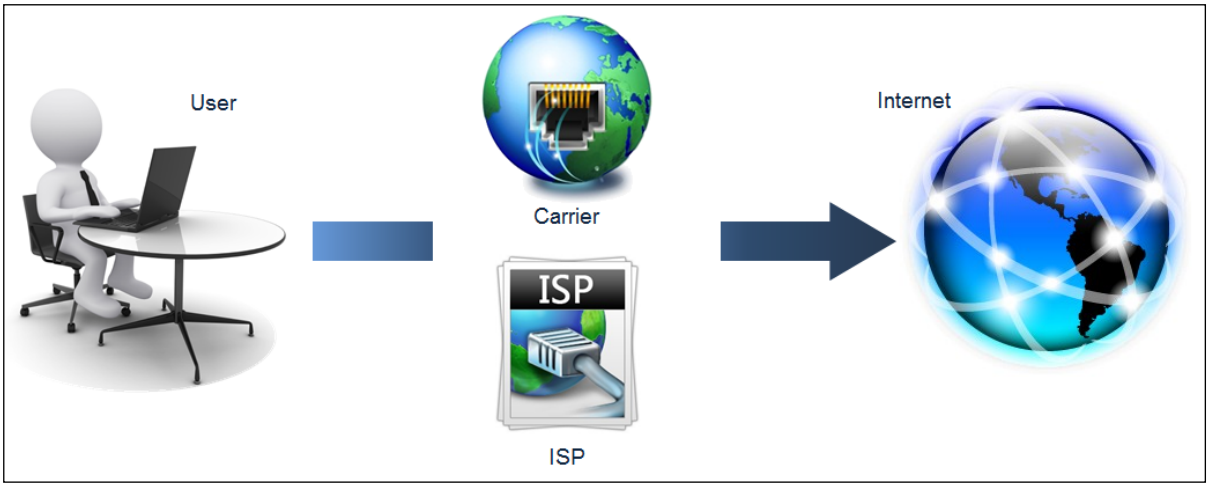

Abb. 4: Der Weg ins Internet

Der Weg ins Internet führt über Internet Service Provider (ISP) und Carrier.

2.2.2 Was ist ein ISP?

Internet Service Provider (ISP) sind Dienstleister mit einem permanenten Internetanschluss (z. B. Telekom, Arcor, 1&1). Für einen **Internetzugang** benötigen Internetnutzer einen ISP, der ihnen **gegen Entgelt** einen Zugang bereitstellt (vergleichbar mit einem Telefonanschluss der Telekom).

Beim Zugang selbst gibt es zwei Möglichkeiten:

1. Die Verbindung zum ISP wird über ein Modem (Analog-, ISDN- oder DSL-Modem) per Einwahl aufgebaut. Bei den sog. **Einwahlverbindungen** (diese sind unter privaten Internetnutzern am meisten verbreitet) muss sich der Nutzer vor dem Verbindungsaufbau mit seinem Benutzernamen und seinem Passwort identifizieren. Einwahlverbindungen sind zeitlich begrenzt, bspw. erfolgt bei einer DSL-Modem-Verbindung nach 24 Stunden eine automatische Zwangstrennung.
2. Bei einer **Standleitung** ist die Verbindung zum ISP, und damit auch zum Internet, permanent aktiv. Standleitungen sind hauptsächlich für Unternehmen interessant, die zum einen eine höhere Bandbreite ("Geschwindigkeit") und zum anderen den permanenten Zugang zum Internet benötigen, weil sie bspw. eigene Server betreiben.

Neben verschiedenen Zugangsmöglichkeiten bieten die zahlreichen Internet Service Provider auch verschiedene Leistungen zu unterschiedlichen Tarifen an. Ein Vergleich der Tarife und Leistungen lohnt sich!

2.2.3 Der Tarifdschungel

Die Vorlieben der Internetnutzer sind sehr **unterschiedlich**. Während die einen nur ab und zu im Internet "surfen" wollen, sind andere ständig im Internet, um große Datenmengen zu versenden und zu empfangen. Dabei legen die "Viel-Surfer" großen Wert auf eine hohe Übertragungsgeschwindigkeit.

Die ISP bieten **verschiedene Tarife**, um möglichst viele Kunden zu erreichen. Anfangs wurden Tarife angeboten, die abhängig von der Einwahlzeit waren. Später kamen Volumentarife hinzu, die entweder Minuten- oder Datenpakete zu einem Pauschalpreis beinhalteten. Mittlerweile ist die sog. **Flatrate**, das am meisten beworbene Angebot. Mit einer Flatrate kann der Internetnutzer für einen festen monatlichen Betrag (**Pauschaltarif**) auf unbegrenzte Zeit im Internet sein und unbegrenzte Datenmengen versenden und empfangen. Je nach Tarif werden unterschiedliche Übertragungsgeschwindigkeiten angeboten. ISP werben ständig mit neuen Tarifen und **Angeboten**. Durch den **Fortschritt** der Internet-Technologie ist mittlerweile auch das Telefonieren und Fernsehen über das Internet möglich, so dass einige ISP versuchen, über sog. Triple-Play-Produkte (Internet, Telefonieren und Fernsehen) zusätzliche Kunden zu akquirieren.

Um eine möglichst große Menge an Internetnutzern zu bedienen, benötigen die Internet Service Provider selbst eine sehr leistungsfähige Internetanbindung, welche Sie von sog. Carriern anmieten. Die Internetanbindung eines ISP muss in der Lage sein die gesamte Datenmenge der

Kunden die von den Kunden des ISP verursacht wird, mit einer hohen Übertragungsgeschwindigkeit weiterzuleiten.

2.2.4 Aufgaben eines Carriers

Carrier sind private Netzbetreiber mit einer **eigenen Netzinfrastruktur**. Sie installieren, betreiben und warten Backbones und Knotenrechner. Bei diesen Netzen handelt es sich um sehr leistungsfähige Netzwerke, die große Datenmengen bewältigen und hohe Übertragungsgeschwindigkeiten realisieren können.

Diese **Carrier-Netzwerke** und deren Verbindungen untereinander **bilden** die eigentliche **Grundlage für das Internet**, weil es ihre Leitungen sind, die die Daten über große Entfernungen transportieren.

- **Private Carrier**, wie z. B. Akamai oder Verizon, verkaufen Zugänge zu ihren Netzen an die ISP. Die ISP wiederum können die leistungsfähigen Verbindungen der Carrier auf möglichst viele Endnutzer "verteilen". Ein einzelner Endnutzer wäre sicher nicht in der Lage, eine Carrierverbindung voll auszuschöpfen oder zu bezahlen.
- **Öffentliche Carrier**, wie bspw. die Deutsche Forschungsgemeinschaft, unterstützen Nachwuchswissenschaftler mit der Bereitstellung eines Netzwerks bzw. der finanziellen Mittel zur Einrichtung eines solchen. Finanziert wird die DFG von Bund und Ländern.

2.2.5 Private Nutzungsmöglichkeiten

Mit den steigenden Nutzerzahlen ist auch das **Informationsangebot** im Internet rasant gestiegen. Dem Internetnutzer stehen zahlreiche Informationen zu fast allen Themen zur Verfügung. **Am häufigsten nutzen Privatanwender** ihren Internetanschluss für:

- die Informationsbeschaffung in der Vorkaufphase (z. B. Produktrecherche, Alternativensuche und Preisvergleich),
- den Kauf von Produkten,
- die Informationsbeschaffung in der Nachkaufphase (Handbücher, Support und Service) und
- die Kommunikation mit Freunden, Bekannten, Behörden und Unternehmen via E-Mail, Foren, Chat, Instant Messaging oder Video-Telefonie.

Neben den genannten Möglichkeiten treten regelmäßig neue Trends im Internet auf. So sind mit dem sog. **Web 2.0 Blogs** und **Podcasts** sehr populär geworden. Ein Weblog (abgekürzt: Blog) ist ein auf einer Web Site geführtes und damit öffentlich einsehbares Tagebuch oder Journal. Bei einem Podcast handelt es sich um eine Audio-Datei, die über das Internet bezogen wird. Ähnlich wie in Blogs, behandeln Podcasts verschiedene Themen.

2.2.6 Unternehmen im Internet

Im Zusammenhang mit Unternehmen im Internet wird häufig von **E-Business** gesprochen. Wichtig ist, dass E-Business alle geschäftlichen Aktivitäten eines Unternehmens umfasst, die über das Internet oder mit Hilfe von Internet- Technologie durchgeführt werden.

E-Business vollzieht sich dabei im **Intranet, Extranet** oder **Internet** - je nachdem, welche User-Gruppen beteiligt sind:

- Das **Intranet** ist nur für bestimmte Personen, in der Regel für Mitarbeiter des Unternehmens, zugänglich. Es ist ein **geschlossenes Netzwerk**, das von berechtigten Personen für Kommunikation und Aufgabenerfüllung genutzt werden kann.
- Über das **Extranet** erfolgt die Kooperation und Kommunikation zwischen Unternehmen. **Geschäftspartnern** wird ein Zugang zum Unternehmen gewährt. So können deren Tätigkeiten besser in die Prozesse des eigenen Unternehmens integriert werden.
- Über das **Internet** kann sich das Unternehmen **öffentlich** präsentieren. Kunden und andere Interessierte können Informationen über Produkte, Dienstleistungen und das Unternehmen selbst erhalten oder einen Kauf tätigen.

2.2.7 Aktuelle Zahlen zum Internet

In der Altersgruppe der 16- bis 24-Jährigen ist das Internet bereits heute das **wichtigste** Kommunikations- und Informationsmedium. Aber auch andere Altersgruppen holen auf, so ist bspw. die Zahl der sogenannten "silver surfer" (Internetnutzer über 55 Jahre) im letzen Jahr um über ein Drittel gestiegen.

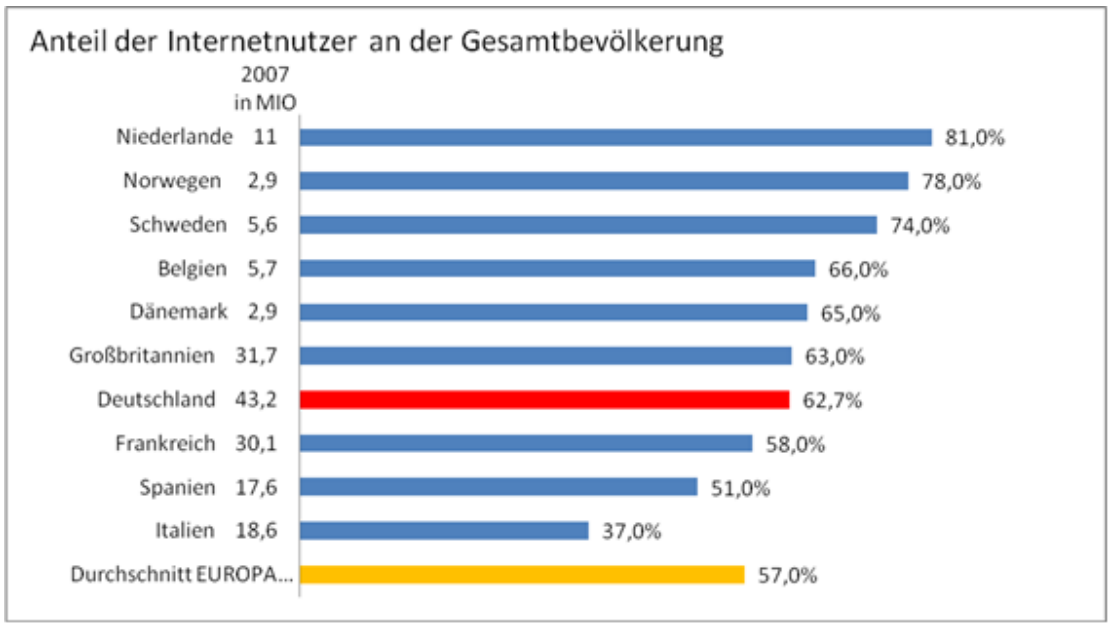

Abb. 5: Anteil der Internetnutzer an der Gesamtbevölkerung

Während in den Beneluxländern und Skandinavien die Sättigungsgrenze beinahe erreicht ist, **steigt** der Anteil der deutschen Internetnutzer an der Gesamtbevölkerung weiter an.

Hauptaktivitäten sind die Informationsbeschaffung per **Suche** und die Kommunikation über **E-Mail**. Immer größere Bedeutung bekommen Online-Netzwerke, wie z. B. Xing oder studiVZ.

2.3 Das Client/Server-Konzept

2.3.1 Das Internet auf meinem Bildschirm

Sie haben erfahren, wie das Internet aufgebaut ist. Sie wissen, über **welche** Verbindungen Daten im Internet übertragen werden und was für einen Internetanschluss notwendig ist. Sie haben auch erfahren, dass über das Internet Informationen bzw. Daten übermittelt werden. Es wird also über das Internet **kommuniziert**, aber

- wie funktioniert diese Kommunikation und
- woher kommen die Daten, die auf dem Bildschirm angezeigt werden?

Im Folgenden werden Ihnen die Grundlagen für die Kommunikation im Internet nähergebracht.

2.3.2 Was ist das Client/Server-Konzept?

Das grundlegende Konzept für die Kommunikation im Internet ist das Client/Server-Konzept. Die Kommunikationspartner werden dabei immer in **Client** (Klient) und **Server** (Lieferant) unterschieden.

Zunächst soll geklärt werden, wie Client und Server miteinander kommunizieren. Die zwei **Kommunikationsschritte** sind dabei immer gleich:

1. "Client fragt Server"

2. "Server antwortet Client"

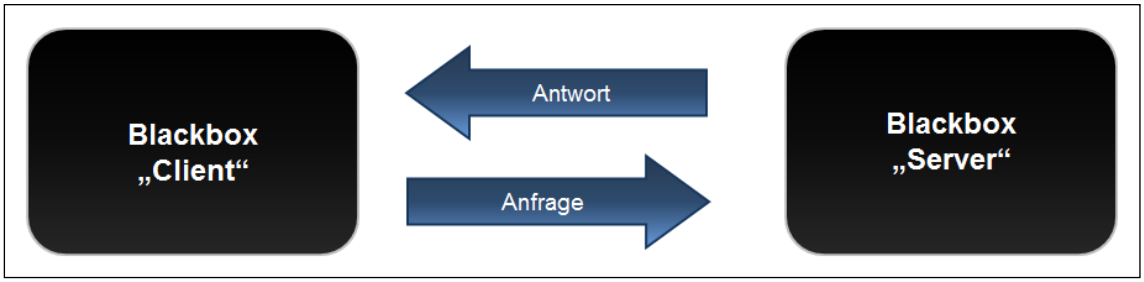

Abb. 6: Das Client/Server-Konzept

2.3.3 Client/Server-Konzept im Internet

Im Internet wird die Rolle von Client und Server durch **Rechner** eingenommen, die **verschiedene Funktionen** erfüllen.

Auf einem **Server** sind Daten und Anwendungen gespeichert, die bei Anfrage zur Verfügung gestellt werden. Wenn die nachgefragten Informationen nicht auf dem Server vorhanden sind, wird eine Fehlermeldung als Antwort gegeben.

Der Server ist passiv, das heißt, dass der Server ständig darauf wartet, dass ein **Client eine Anfrage** stellt. Auf die Anfrage des Clients reagiert der Server, indem er die **gewünschten Informationen zurückmeldet**. Es findet also erst durch die Anfrage eines Clients eine Kommunikation zwischen Server und Client statt.

2.3.4 Mehr als ein Server

Bisher wurde von **einem (1) Client** gesprochen, der an einen **(1) Server** eine Anfrage stellt. Nun kann es aber sein, dass der eine Server nicht selbst über die angeforderten Informationen verfügt, sondern die Informationen auf einem **weiteren (zweiten) Server** "liegen".

In diesem Fall wird der erste **Server selbst zum Client**, indem er die angeforderten Informationen bei dem anderen Server nachfragt und anschließend an den Client weiterleitet.

Dieses Konzept, bei dem ein Server auch gleichzeitig Client ist, wird **Kaskadierung** genannt

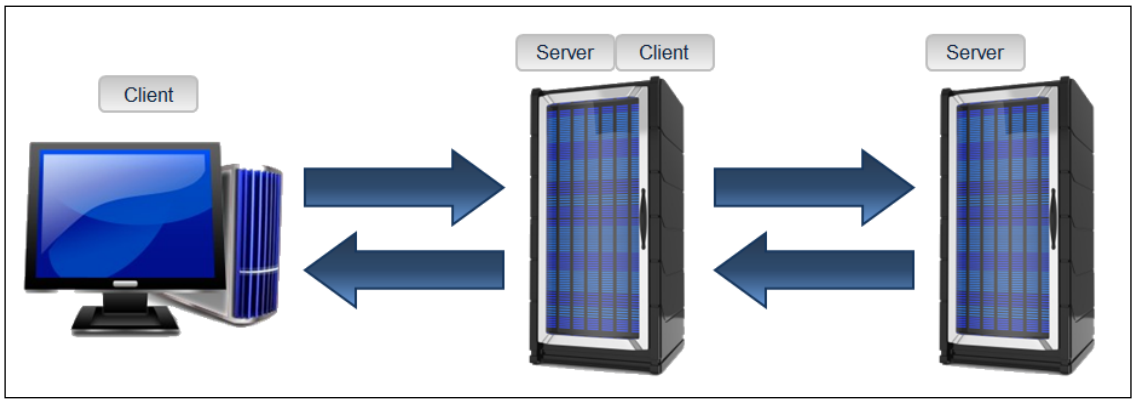

Abb. 7: Kaskadierung

2.3.5 Mögliche Aufgabenverteilung

Das Client/Server-Konzept ist zunächst nur aus **organisatorischer Sicht** zu betrachten. Das heißt, dass die Teilaufgaben (Präsentation, Verarbeitung und Speicherung von Daten), die bei einer Problemstellung anfallen, unterschiedlich auf Client und Server verteilt werden können. Je nach Aufgabenverteilung sind verschiedene sog. Client/Server-Architekturen möglich:

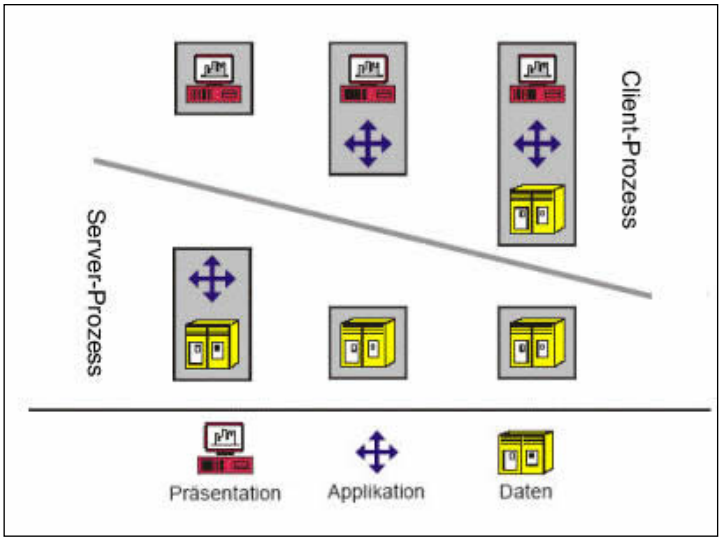

Abb. 8: Client/Server-Architekturen

- **Entfernte Präsentation**: Daten werden auf dem Client lediglich präsentiert. Zum Beispiel der Aufruf einer Web Site im Internet. Eine Anwendung auf dem Server wandelt die Daten des Servers in HTML-Code um. Dieser HTML-Code muss vom Client (hier der Web-Browser) lediglich empfangen, umgewandelt und angezeigt werden.

- **Entfernte Datenbank**: Daten können auf dem Client auch verarbeitet werden. Zum Beispiel das Öffnen eines Videos im Internet. Wenn ein Browser über zusätzliche Funktionen (sog. Plug-Ins) verfügt, können Daten im Browser auch verarbeitet werden. Zum Beispiel können Videos von www.youtube.com mit einem solchen Plug-In betrachtet werden.
- **Verteilte Datenbank**: Daten werden auf dem Client verarbeitet und teilweise gespeichert. Zum Beispiel das Ausfüllen von PDF-Formularen. Auf vielen Web Sites werden PDF-Formulare zum Ausfüllen angeboten z. B. bei Online-Handy-Verträgen. Die Formulare werden temporär auf dem Client gespeichert, bis sie ausgefüllt und ausgedruckt sind.

2.3.6 3-Tier-Architektur im Internet

Im Internet hat sich die 3-Tier-Architektur etabliert, bei der Aufgaben auf mehrere **Schichten** (engl.: **Tiers**) verteilt werden. Die Aufteilung in Schichten ist organisatorisch sowie technisch vorteilhaft, da eine Aufgabe in Teilaufgaben zerlegt werden kann. Dabei wird jede Teilaufgabe von einer Schicht bearbeitet. So müssen bei Änderung einer Aufgabe nur einzelne Schichten angepasst werden, während die anderen von diesen Änderungen unbeeinflusst bleiben.

Die 3-Tier-Architektur im Internet besteht aus Präsentationsschicht, Anwendungs- bzw. Applikationsschicht und Datenschicht.

- Die **Präsentationsschicht** (Tier 1) dient lediglich der Darstellung von Ergebnissen, z. B. in Form einer Präsentationsgrafik.
- Auf der **Applikationsschicht** (Tier 2) liegen die Anwendungen bzw. Programme, die notwendig sind, um das gewünschte Ergebnis zu liefern.
- Die **Datenschicht** (Tier 3) hat Daten gespeichert, die von der Applikationsschicht abgerufen und verarbeitet werden können.

2.3.7 Aufruf einer Web Site

1. Der Internetnutzer gibt zunächst die Adresse der Webseite (z. B. den **URL** http://wiwi.uni-giessen.de/news/top20liste/fb02/ der Top 20 News des Fachbereichs Wirtschaftswissenschaften) in die Adressleiste seines **Web-Browsers** (bspw. Firefox) ein.

2. Der Web-Browser agiert als Client und **sendet** eine **Anfrage** (Request) an den entsprechenden Server auf der Applikationsschicht - in diesem Fall **wiwi.uni-giessen.de**.
3. Da die Top 20 News mit jedem Aufruf neu erstellt werden, müssen die aktuellsten News des Fachbereichs zunächst aus der Datenschicht von einem Datenbank-Server **abgerufen** werden.
4. Die auf der Applikationsschicht laufenden Anwendungen **erzeugen** aus den Daten eine **HTML-Seite** mit den Top 20 News und liefern diese Seite **an den Client**, der die URL der Top 20 News angefordert hatte, aus.
5. Der Web-Browser **generiert** aus dem erhaltenen **HTML-Code** eine entsprechende Ansicht für den User.

2.3.8 Verschiedene Server und ihre Aufgaben

Je nach Aufgabenfeld können im Internet **verschiedene Arten von Servern** betrieben werden, die unterschiedliche Aufgaben erfüllen oder bewältigen:

- **File-Server** verwalten ein lokales Dateisystem und stellen angeschlossenen Rechnern ihre Ressourcen (Daten) zur Verfügung. Die Datenbestände von File-Servern können von allen Netzwerkteilnehmern gemeinsam bearbeitet und für alle zugänglich gemacht werden.
- **Kommunikations-Server** sind Funktionseinheiten, die Kommunikationsaufgaben für angeschlossene Clients leisten. So kann bspw. die Kommunikation zwischen LAN-Stationen und Teilnehmern außerhalb des LANs - z. B. aus dem Internet - ermöglicht werden.
- Auf **Web-Servern** werden Web Sites und andere Online-Informationen bereit gestellt. Diese können beispielsweise von einem Browser angefordert werden. Informationen, die auf Web-Servern bereit gestellt sind, sind u. a. HTML-Seiten, Textdokumente und Grafiken sowie dynamische, datenbankbasierte Seiten.
- Ein **Mail-Server** verarbeitet E-Mails. Die Aufgaben umfassen den Empfang, den Versand, die Speicherung sowie die Weiterleitung von E-Mails.

2.3.9 Eine Alternative: Das Peer-to-Peer-Modell

Anstelle des **Client-Server-Konzepts** kann für kleinere Netze das sog. **Peer-to-Peer-Modell** genutzt werden.

Dabei handelt es sich um eine **Netzkonfiguration**, die ohne Server auskommt. Die Rechner sind, im Gegensatz zu den Rechnern im Client-Server-Konzept, **gleichberechtigt**.

Das bedeutet, dass jedes System im Netz anderen Systemen **Funktionen** und **Dienstleistungen anbieten** und andererseits angebotene Funktionen, Ressourcen und Dienstleistungen **nutzen** kann.

Das Weitergeben von Daten zwischen Benutzern eines Netzes (z. B. Internet) wird durch sogenannte **File-Sharing-Software** ermöglicht. Programme wie z. B. eMule oder Kazaa bauen ein Netzwerk mit gleichberechtigten Benutzern auf, die Daten zur Verfügung stellen. In diesem Netzwerk kann jeder Benutzer auf die Daten der anderen Benutzer zugreifen und diese auf seinen eigenen Rechner kopieren.

2.4 Abschlusstest

2.4.1 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	Die Aufgabe eines Mail-Servers sind der Empfang und die Speicherung von E-Mails.		
	Richtig		
	Falsch		
2	Web-Server verwalten das lokale Dateisystem und stellen angeschlossenen Rechnern ihre Ressourcen zur Verfügung.		
	Richtig		
	Falsch		
3	Internet Service Provider verkaufen Übertragungsleistungen an Carrier.		
	Richtig		
	Falsch		
4	Je mehr Schichten in einer Multi-Tier-Architektur, umso besser.		
	Richtig		

	Falsch		
5	Ergebnisaufbereitung, Verarbeitung und anteilige Datenhaltung sind typisch für welche Client/Server-Architektur?		
	Entfernte Präsentation		
	Entfernte Datenbank		
	Verteilte Datenbank		
6	Das Client/Server-Konzept ein theoretisches Konstrukt, das in der Praxis Anwendung findet.		
	Richtig		
	Falsch		
7	Das Client/Server-Konzept ist ein wichtiges Kommunikationskonzept im Internet.		
	Richtig		
	Falsch		
8	Einer Unternehmensabteilung steht nur ein Drucker zur Verfügung. Wäre ein Zusammenschluss der vorhandenen Rechner zu einem LAN sinnvoll?		
	Ja, der Drucker ist eine Ressource, die im LAN von allen genutzt werden kann.		
	Nein, Ressourcen in einem LAN sind ausschließlich Daten und Anwendungen. Hardware ist lediglich ein Medium für diese Ressourcen.		
9	Ergebnisaufbereitung und Verarbeitung sind typisch für welche Client/Server-Architektur?		
	Entfernte Präsentation		
	Entfernte Datenbank		
	Verteilte Datenbank		
10	Unternehmen sehen keine Notwendigkeit in der Internetnutzung.		
	Richtig		
	Falsch		
11	Die Grundtopologien einer LAN-Netzwerkstruktur sind Stern-, Bus- und Ringtopologie.		
	Richtig		
	Falsch		
12	Die Multi-Tier-Architektur ist im Vergleich zur Client/Server-Architektur effizienter.		
	Richtig		
	Falsch		

Tab. 2: Abschlusstest in WBT 2

3 Technik und Dienste

3.1 Internetdienste

3.1.1 Einleitung

Sie haben erfahren, dass sich hinter den Begriffen **WWW** und **Internet nicht dasselbe** verbirgt. Während es sich beim Internet um ein **physisches Netzwerk** handelt, handelt es sich beim WWW um einen sog. **Dienst**.

Das WWW ist **nur ein Dienst** im Internet, der dem Internetnutzer das "Surfen" im Web ermöglicht. Daneben gibt es noch **weitere** Dienste, die bspw. das Verschicken von E-Mails und den Austausch von Daten ermöglichen.

Es entstehen auch **regelmäßig** weitere, **neue Dienste**, die sich das Internet zu Nutze machen, wie z. B. Instant Messaging und Internettelefonie.

Im weiteren Verlauf, lernen Sie die bekannten Dienste **E-Mail**, **Datentransfer**, **Instant Messaging** und **WWW** sowie deren Funktionsweise kennen.

3.1.2 Elektronische Post

Der Austausch von Nachrichten unter Netzwerkteilnehmern sei "kein wichtiger Beweggrund, um ein Netzwerk von wissenschaftlichen Rechnern aufzubauen". Mit dieser Annahme lag Lawrence Roberts, einer der ARPANET-Initiatoren, im Jahre 1967 weit daneben. E-Mail wird heutzutage als wichtigster und meistgenutzter Dienst des Internets angesehen.

In vielerlei Hinsicht unterscheidet sich eine E-Mail nicht von einem traditionellen Brief. Genauso wie ein Brief, muss eine E-Mail geschrieben, adressiert und verschickt werden.

Eine E-Mail wird über das Internet verschickt. Das Schreiben und Adressieren wird entweder über die Web Site des entsprechenden **E-Mail-Anbieters** oder mit einem sog. **E-Mail-Client** durchgeführt.

Zu den E-Mail-Anbietern gehören u. a. die Freemail-Anbieter GMX oder Web.de, die kostenlose E-Mail-Accounts anbieten. Mit einem E-Mail-Account erhält der Nutzer eine E-Mail-Adresse. Diese besteht aus **zwei Teilen**. Zum einen dem Namen, den der Benutzer selbst wählt (z. B. MaxMuster), zum anderen dem Adressnamen des E-Mail-Anbieters (z. B. gmx.de oder web.de). Beide Teile werden durch das Zeichen "@" (steht für engl. at und wird auch Klammeraffe genannt) miteinander verbunden bspw. maxmuster@emailanbieter.de.

Bei E-Mail-Clients, wie z. B. Thunderbird oder Outlook Express, handelt es sich um ein Programm mit dem E-Mails empfangen, gelesen, geschrieben und versendet werden können. Der E-Mail-Client muss mit den Daten des E-Mail-Anbieters **konfiguriert** werden, da aus- und eingehende E-Mails immer über den Mail-Server des E-Mail-Anbieters geleitet werden. Dieser übernimmt die Rolle von Postannahme und Briefkasten **zugleich**.

3.1.3 Instant Messaging

Ein weiterer Dienst, der die Kommunikation über das Internet ermöglicht, ist der Nachrichtensofortversand (engl.: Instant Messaging). Dabei handelt es sich um einen Dienst, der eine **textbasierte Kommunikation** in **Echtzeit** ermöglicht. Daher wird beim Instant Messaging von synchroner Kommunikation gesprochen, während u. a. die E-Mail als asynchrones Kommunikationsmedium gilt.

Zur Nutzung dieses Kommunikationsmediums wird eine spezielle Software ein sog. **Instant Messenger** benötigt. Der bekannteste und älteste Vertreter ist ICQ, der im Jahre 1996 entwickelt wurde.

Mit ICQ lässt sich eine **Kontaktliste** erstellen und an die Personen in der Kontaktliste können **Textnachrichten** versendet werden. Normalerweise benötigt der Empfänger einer Textnachricht ebenfalls Software ICQ. Mittlerweile gibt es jedoch auch Instant-Messenger-Programme, die mit mehreren verschiedenen Instant Messengern kommunizieren können (z. B. Trillian).

Ein wenig beachteter Aspekt bei Instant Messengern ist die Sicherheit bei der Übertragung der Inhalte. So werden bspw. bei ICQ die Sofortnachrichten unverschlüsselt versendet. Andere Instant Messenger wie z. B. **Skype** versenden die Sofortnachrichten verschlüsselt.

Mit der ständigen Weiterentwicklung von Instant Messengern ist auch der **Funktionsumfang** gestiegen. Beispielsweise unterstützt mittlerweile fast jeder Instant Messenger den Versand von Daten oder ermöglicht Videokonferenzen.

3.1.4 Datentransfer im Internet

Neben Nachrichten können über das Internet auch Daten jeglicher Art übertragen werden - hiermit ist eine Datenübertragung gemeint, die nicht vornehmlich der Kommunikation mit anderen dient. Für den Dienst "Datentransfer" werden i. d. R. spezielle Clients verwendet. Es können bspw. Programme, Dokumente, Grafiken oder Audio-Dateien übertragen werden.

Beim Datentransfer wird unterschieden zwischen:

Download:

Beim **Herunterladen** (engl.: Download) werden Daten von einer Gegenstelle, wie z. B. ein File-Server, angefordert und zum Rechner übertragen. Mit den gängigen Web-Browsern ist es ebenfalls möglich, Dateien herunterzuladen. Einige Web-Browser beinhalten hierzu einen sog. Download-Manager.

Upload:

Hochladen (engl.: Upload) bedeutet, dass Daten vom eigenen Rechner zu einem entfernten Rechner bzw. Speichermedium über das Internet übertragen werden. Beim Hochladen von Daten können sog. FTP-Clients, wie z. B. FileZilla, dem Internetnutzer die Arbeit erleichtern. Diese Programme bieten eine leicht verständliche Benutzeroberfläche, mit der die Daten bspw. per "Drag&Drop" auf einen entfernten Rechner oder File-Server hochgeladen werden.

3.1.5 Der Dienst WWW

Das World Wide Web (WWW) ist ein populärer **Dienst** im Internet. Irrtümlicherweise wird dieser Dienst häufig mit dem **physischen Netzwerk** Internet gleichgesetzt. Die Popularität des WWW beruht auf der Verwendung von grafischen Benutzeroberflächen sog. Web Sites. Zur Darstellung einer Web Site wird ein **Web-Browser** benötigt. Web Browser werden in verschiedenen Formen von unterschiedlichen Anbietern zur Verfügung gestellt, wie z. B.:

- Der **Internet Explorer** ist ein Web-Browser, der von der Firma **Microsoft** entwickelt und vertrieben wird. Seit Windows 95 ist der Internet Explorer ein **Bestandteil** der Microsoft Betriebssystem-Serie **Windows**. Die derzeit aktuelle Version ist der Internet Explorer 7.
- **Opera** ist ein **frei** erhältlicher Web-Browser, der neben dem Web-Browser noch **weitere** Funktionen zur Internetnutzung (z. B. einen E-Mail-Client) enthält. Trotz der Konkurrenz zum ebenfalls kostenlosen Internet Explorer, konnte Opera mit seinen vielen Funktionen zahlreiche Anwender für sich gewinnen.
- **Mozilla Firefox** ist ein freier Web-Browser, der aus dem Mozilla-Projekt entstanden ist. Eine **Besonderheit** ist die Fokussierung auf die Web-Browser-Funktion an sich. Entwickler haben **bewusst** auf zusätzliche Funktionen verzichtet, um **schnellere Ladezeiten** sowie **geringere Speicherauslastung** und Rechenzeit zu realisieren.

Wesentliche Elemente des WWW sind Adressierung per URL und Hypertext Markup Language (HTML). Diese werden Sie im Folgenden kennenlernen.

3.1.6 Was ist ein URL?

Zum Aufrufen einer Web Site im WWW wird eine Adresse benötigt, diese Adresse wird als Uniform Resource Locator (URL) bezeichnet. URLs werden in die Adresszeile eines Web-Browsers eingegeben und bestehen aus:

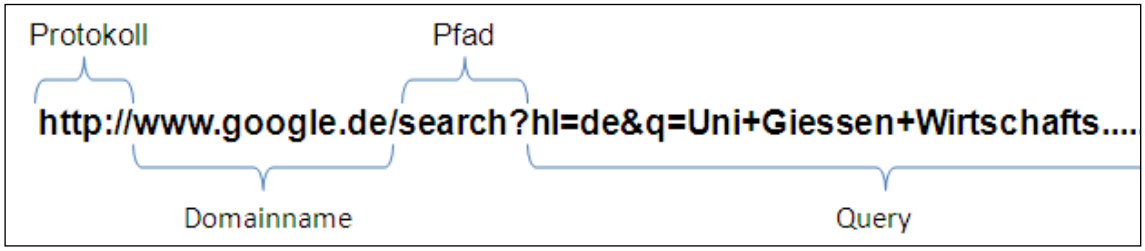

Abb. 9: Bestandteile eines URLs

Protokoll:

Die Protokolle HTTP oder HTTPS sind für die Übertragung von Web Sites zuständig.

Domainname:

Jedes Endgerät, welches mit dem Internet verbunden ist, hat eine eindeutige IP-Adresse (z. B. 134.176.85.27). Die IP-Adresse ist mit einer Telefonnummer vergleichbar. Bei der Eingabe von wiwi.uni-giessen.de wird der Domainname durch einen Domain-Name-System-Server (DNS–Server) in die entsprechende IP-Adresse umgesetzt. Probieren Sie es doch einfach mal aus und tippen Sie die IP-Adresse (134.176.85.27) in die Adresszeile Ihres Browsers.

Pfad:

Eine Web Site besteht aus einzelnen Web Seiten. Für die Navigation zwischen den einzelnen Web Seiten ist ein Pfad nötig. Der Pfad beschreibt eine bestimmte Datei oder ein bestimmtes Verzeichnis auf dem Server, auf dem die Web Site gespeichert ist. Pfade können im Browser eingegeben werden oder öffnen sich automatisch beim Anklicken von Links.

Query:

Getrennt durch ein Fragezeichen können zusätzliche Parameter im Query übertragen werden. Diese werden vom Server empfangen und verarbeitet. Beispielsweise werden bei einer Suchmaschine, wie z. B. Google, die gesuchten Begriffe im Query der URL übermittelt.

3.1.7 Wie funktioniert das Domain Name System?

Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. Hauptsächlich wird das DNS zur Umsetzung von Domainnamen in IP-Adressen benutzt. Dies ist vergleichbar mit einem Telefonbuch, das die Namen der Teilnehmer in die jeweilige Telefonnummer übersetzt.

Jeder Domainname besteht aus einer **Folge** von Zeichen, die durch Punkte voneinander **getrennt** werden. Ein Domainname wird bei der **Auflösung** in eine IP-Adresse immer von rechts nach links gelesen.

Abb. 10: Bestandteile eines Domainnamens

- Die **Top-Level-Domain** bezeichnet entweder das Land, in dem der Domainname registriert wurde (z. B. ".de" für Deutschland), einen Staatenverbund (z. B. ".eu" für die Europäische Union) oder einen anderen organisatorischen Bereich (z. B. ".org", ".com" oder ".biz").
- Die **Second-Level-Domain**, meist auch nur Domain genannt, bezeichnet die Web Site an sich. Die Domainbezeichnung sollte vom Web-Site-Betreiber so gewählt werden, dass sie den Inhalt der Web Site beschreibt und für den Internetnutzer leicht zu merken ist.
- Weitere, hierarchisch untergeordnete Domains werden als **Subdomains** bezeichnet. Im Bsp. "wiwi.uni-giessen.de" handelt es sich bei "wiwi" um eine sog. Host-Domain. Damit wird der Rechner bzw. Server bezeichnet, auf dem die einzelnen Web Seiten vorgehalten werden (i. d. R. werden diese Rechner "WWW" genannt).

3.1.8 Exkurs: Was ist HTML?

Die grafische Oberfläche des Dienstes WWW wird verbreitet mit der Seitenbeschreibungssprache HTML (**Hypertext Markup Language**) gestaltet. Diese dient der Strukturierung von Texten, wobei aber auch die Möglichkeit besteht, Grafiken und multimediale Inhalte einzubinden und in den Text zu integrieren.

Auf HTML basierende Web Sites enthalten sog. **HTML-Code**. In diesem HTML-Code wird bspw. **festgelegt**, wo eine Überschrift auf dem Bildschirm platziert wird, welche Farbe die Überschrift hat und welche Schriftart und -größe für die Überschrift verwendet werden soll.

Neben den im Web-Browser angezeigten Inhalten kann HTML auch zusätzliche Angaben (sog. **Metainformationen**) enthalten. In Meta-Angaben können verschiedene nützliche **Anweisungen** z. B. für Web-Server oder Web-Browser notiert werden. Es können u. a. Angaben zum Autor und zum Inhalt gemacht werden. Metaangaben werden beim Öffnen einer Web Seite nicht im Browser angezeigt.

Seit der HTML Version 4.01 gibt es Bestrebungen, HTML durch **XHTML** (Extensible Hypertext Markup Language) zu ersetzen. Wie der Name bereits andeutet, ist XHTML eine **erweiterte** Version von HTML, die sich bisher nicht als Standard durchgesetzt hat.

3.1.9 Ein Beispiel zu HTML

Beispielsweise führt folgender Quelltext zu weißem Text auf schwarzen Hintergrund:

```
<html>
<head>
  <title>Text</title>
</head>
<body text="#FFFFFF" bgcolor="#000000">
  <h1>Die Textfarbe ist weiß</h1>
  <p>Der Hintergrund ist schwarz</br>
.....
```

Durch Veränderungen im Quelltext kann der Seiteninhalt verändert werden. Zum Beispiel könnten folgende Veränderungen durchgeführt werden:

Die Eingabe von:

```
bgcolor="#0000FF"
```

verändert die Farbe des Hintergrunds in Blau.

```
body text="#FF0000"
```

verändert die Schriftfarbe in Rot.

Mit HTML können noch **weitaus mehr** Veränderungen erreicht werden, die das Aussehen einer Web Seite beeinflussen. Daher auch die Bezeichnung **Seitenbeschreibungssprache** (nicht zu verwechseln mit dem Begriff Programmiersprache).

3.2 Geräte und Medien

3.2.1 Heterogene Systeme im Internet

Sie kennen nun verschiedene Dienste. Um diese Dienste nutzen zu können, ist ein Rechner und eine Internetverbindung erforderlich. Allerdings gibt es eine **Vielzahl** unterschiedlicher Geräte und Systeme, die über das **Internet** miteinander kommunizieren und Daten austauschen.

Verschiedene **Hardware-Geräte** können über das Internet miteinander verbunden werden: Beispielsweise kann ein Notebook mit einem Handy über das Internet kommunizieren und Daten austauschen. Es können auch verschiedene Programme auf den Rechnern installiert sein, die miteinander kommunizieren. So wird bspw. auf einem Rechner die E-Mail mit Microsoft Outlook geschrieben, während die E-Mail auf einem anderen Rechner mit Mozilla Thunderbird gelesen wird. Ebenso ist es möglich, dass auf einem Rechner das Betriebssystem Windows Vista und auf einem anderen Endgerät das Betriebssystem Linux installiert ist. Aber wie ist es möglich, dass mit unterschiedlicher Hard- und Software, die gleichen Internetdienste genutzt werden können? Dazu ist zunächst eine Übersicht über verschiedene Hardware-Geräte und Übertragungsmedien notwendig. Diese werden benötigt, um überhaupt im Internet kommunizieren zu können.

3.2.2 Geräte der Netzwerktechnik

Neben dem PC selbst existieren verschiedene Hardwarekomponenten, die zum Netzwerkbetrieb und zur Internetnutzung beitragen. Beispielsweise gibt es neben den Endgeräten auch Hubs, Router und Gateways, welche für den Betrieb eines Netzwerks benötigt werden.

Netzwerkkarte:

Die Netzwerkkarte ermöglicht den Anschluss eines Endgerätes (PC, Notebook, Drucker etc.) an ein Netzwerk. Moderne PC oder Notebooks haben Netzwerkkarten bereits fest auf der Hauptplatine installiert.

Router:

Ein Router ist eine Vermittlungsstelle zwischen mehreren Netzwerken. Zentrale Aufgabe des Routers ist die Wegwahl für Daten, die über Netzwerke versendet werden. Daten werden empfangen, analysiert und zum vorgesehenen Zielnetz weitergeleitet.

Gateway:

Ein Gateway kann unterschiedliche Netzwerksysteme miteinander verbinden. Dazu prüft der Gateway die Inhalte, die verschickt werden sollen, auf "Verständlichkeit". Inhalte, die an andere Netzwerke (z. B. Mobilfunk- oder Telefonnetz) weitergeleitet werden, werden in diesen Netzwerken nicht immer korrekt erkannt. Der Gateway ist deshalb in der Lage, die Inhalte so zu verändern, dass diese im Zielnetzwerk verarbeitet werden können.

3.2.3 Übertragungsmedien

Die Übertragung von Daten zwischen den einzelnen Geräten erfolgt durch eine physische Verbindung. Über diese werden Informationen durch elektrische bzw. optische Signale oder durch elektromagnetische Wellen übermittelt. Die physischen Verbindungen können folgendermaßen unterschieden werden:

Kabelverbindungen:

- **Koaxialkabel** übertragen elektrische Signale über einen (1) metallischen Leiter, der von einer Isolierschicht umgeben wird und ihn so von der Abschirmung (Drahtgeflecht) trennt. Ein Mantel aus Gummi, PVC oder Teflon umgibt das gesamte Kabel.
- **Twisted-Pair-Kabel** verwenden zur Übertragung elektrischer Signale ein oder mehrere, paarweise verdrillte, metallische Leiter. Bei der Übertragung ist für Sender sowie Empfänger mindestens ein Leitungspaar vorgesehen. Twisted-Pair-Kabel sind flexibel und daher einfach zu verlegen.

- **Glasfaserkabel** übertragen optische Signale. Dazu müssen elektrische Signale vor der Übertragung in Lichtsignale umgewandelt werden. Glasfaserkabel können große Datenmengen über hohe Distanz übertragen. Allerdings ist der Aufbau und die Erweiterung von Glasfasernetzen sehr aufwendig und kostenintensiv.

Funkverbindungen:

Bei Funkverbindungen handelt es sich um die drahtlose Übertragung von Signalen mit Hilfe elektromagnetischer Wellen.

- **Terrestrischer Funk** beschreibt ein erdgebundenes Funknetz, wie z. B. ein Mobilfunknetz, das über Sendemasten betrieben wird. Die Reichweite eines solchen Senders kann sehr unterschiedlich sein. Sie ist vor allem von der technischen Ausstattung des Senders abhängig.
- **Satellitenfunk** hingegen ermöglicht interkontinentale Funknetze durch die Verwendung von Satelliten in der Erdumlaufbahn. Dabei fungieren die Satelliten als Reflektor und Verstärker der Funksignale. Auch auf diese Weise können Computernetzwerke realisiert werden.

Optische Verbindungen:

Optische Verbindungen verwenden eine Technik zur drahtlosen Übertragung von Daten mittels Licht, wie z. B. Infrarot oder Laser. **Vorteile** liegen u. a. in hohen Übertragungsraten und hoher Reichweite. Die Reichweite ist allerdings abhängig von der Lichtquelle. Ein Laser kann deutlich höhere Entfernungen überwinden als Infrarot. Allerdings gibt es verschiedene Einflüsse in der Atmosphäre, die die Übertragung beeinflussen können, wie bspw. Witterungseinflüsse oder Umweltverschmutzung.

3.2.4 Was wird übertragen?

Bisher ist immer davon die Rede gewesen, dass Daten, Informationen oder Anwendungen über das Netzwerk übertragen bzw. genutzt werden können. Doch wie funktioniert diese Übertragung? Wie können so unterschiedliche Inhalte durch ein und dieselbe Leitung geschickt werden? Es stellt sich also die Frage: **Was** bei der Übertragung **genau** versendet wird?

Gegenstand der Übertragung ist ein **binärer** Zahlencode. Für diesen Zahlencode werden die Ziffern **Eins** und **Null** verwendet (Binäres Zahlensystem). Bei der Übertragung wird ein Signal (elektrische Spannung oder Lichtsignal) gesendet. Dieses Signal wird als eine Eins interpretiert.

Eine Abweichung des Signals (veränderte Spannung oder Lichtstärke) wird als eine Null verstanden.

Nun wissen Sie, was für eine Übertragung notwendig ist und was genau übertragen wird. Es stellt sich aber weiterhin die Frage, wie sichergestellt werden kann, dass Sender und Empfänger unter diesem Binär-Code das Gleiche verstehen?

3.3 Protokolle und Schichtenmodelle

3.3.1 Überwindung einer Sprachbarriere

Das "Problem" bei der Kommunikation im Internet sind die verschiedenen Systeme, die miteinander kommunizieren wollen. Die Barriere durch unterschiedliche Systeme lässt sich mit der **Sprachbarriere** zwischen zwei Nationalitäten vergleichen.

Wie können zwei Personen, die unterschiedliche Sprachen sprechen und räumlich voneinander getrennt sind, miteinander **kommunizieren**?

Sie **einigen** sich auf eine Sprache, wie z. B. Englisch und beauftragen Dolmetscher, die sich über ein Telefon austauschen. Die Dolmetscher übersetzen die Nachrichten aus bzw. in die englische Sprache und leiten die Inhalte entsprechend weiter.

Abb. 11: Überwindung einer Sprachbarriere

Die Netzwerktechnik bedient sich einer Lösung, die **wesentliche** Elemente aus dem eben genannten Beispiel übernimmt. Dabei handelt es sich um **Protokolle** und **Schichtenmodelle**, die Sie im Folgenden kennenlernen werden.

3.3.2 Was ist ein Protokoll?

Protokolle sind ein wichtiger Bestandteil der Übertragungstechnik. Durch den Einsatz von Protokollen ist eine eindeutige Übertragung von Inhalten möglich.

Ein Protokoll stellt eine Menge von formalen **Regeln** dar, die die Struktur von Daten und den Ablauf des **Datenaustauschs** regeln. Es handelt sich also um Kommunikationsvereinbarungen, die von beiden Seiten eingehalten werden müssen.

Beispiel vorher (Abb. 8): A und Dolmetscher sprechen die gleiche Sprache (verwenden das gleiche Protokoll). Diese Nachricht wird von dem Dolmetscher von A an den Dolmetscher von B weitergeleitet, dabei sprechen beide Dolmetscher die gleiche Sprache (z. B. Englisch). Der Dolmetscher von B übersetzt die Nachricht in die Sprache von B und gibt die Nachricht an B weiter. In jedem dieser Schritte kann die jeweilige Sprache als Kommunikationsvereinbarung bzw. Protokoll verstanden werden.

3.3.3 HTTP und HTTPS

Das **Hyper Text Transfer Protocol** (HTTP) ist dafür zuständig, Web Sites aus dem WWW in den Web-Browser zu übertragen. Die Bekanntheit von HTTP ist darauf zurückzuführen, dass die meisten Internetadressen mit "http://" beginnen. Obwohl fast jeder den Begriff bereits gehört hat, wissen die wenigsten was sich dahinter verbirgt.

Bei der Übertragung über HTTP ist zu beachten, dass die Übertragung im Klartext, d. h. **unverschlüsselt** erfolgt. Dies ist bei der Eingabe von Daten, wie bspw. Benutzernamen mit Passwörtern oder Kreditkarteninformationen, zu beachten.

Während der Einführung des WWW hat das Thema Sicherheit keine Rolle gespielt. Doch dies hat sich mittlerweile **geändert**, da unter anderem viele **Geldgeschäfte** über das Internet vollzogen werden.

Im August 1994 wurde das **HTTPS** (Hyper Text Transfer Protocol Secure) von Netscape entwickelt und im gleichnamigen Browser veröffentlicht.

Über dieses Protokoll werden sowohl Anfragen als auch die Antworten von Web-Server und -Client so **verschlüsselt**, dass die übertragenen Daten nicht mehr ohne Weiteres für einen Dritten lesbar sind.

Bei der Verwendung dieses Protokolls beginnt die Internetadresse mit "https**://**".

3.3.4 Die E-Mail-Protokolle

Der Dienst E-Mail basiert auf **verschiedenen** Protokollen, die für das Versenden und Abholen von elektronischer Post verantwortlich sind. Zunächst noch einmal zur Erinnerung: E-Mails werden von **Mail-Servern** eines E-Mail-Anbieters (z. B. Web.de oder GMX) versendet und empfangen. E-Mail Protokolle werden nach ihren Aufgaben unterschieden, also **Versand** und **Abruf** von E-Mails.

Versand per SMTP:
Das **Simple Mail Transfer Protocol** (SMTP) - frei übersetzt "einfaches E-Mail-Sende-verfahren" - ist ein Protokoll, das dem Versand von E-Mails dient. Dabei kann es sich um den Versand von E-Mail-Client zu Mail-Server oder von Mail-Server zu Mail-Server handeln.

Abruf per POP oder IMAP:
Das **Post Office Protocol** (POP) und das **Internet Message Access Protocol** (IMAP), dienen beide dem Empfang von E-Mails.

Wesentlicher Unterschied ist, dass das POP die E-Mails aktiv vom Mail-Server abholt und an einen E-Mail-Client überträgt. Die E-Mails werden nach der Übertragung auf dem Mail-Server gelöscht (Standardeinstellung im Mail-Client). IMAP ermöglicht eine Verwaltung der empfangenen E-Mails auf dem Mail-Server. Bei der Verwendung von IMAP werden E-Mails zwar im E-Mail-Client bearbeitet und verwaltet, gespeichert bleiben die E-Mails jedoch auf dem Mail-Server.

3.3.5 Was ist ein Schichtenmodell?

Schichtenmodelle können in **allen** Bereichen des Lebens eingesetzt werden. Sie dienen der Aufgliederung von Problemstellungen in **einzelne** Schritte, die **unabhängig** voneinander Teile der Problemstellungen schrittweise und aufeinander **aufbauend** lösen.

Im Beispiel der Sprachbarriere zwischen zwei Personen haben sich die Kommunikationspartner **ebenfalls** eines Schichtenmodells bedient. A redet mit Dolmetscher (Übersetzungsschicht). Der Dolmetscher telefoniert mit dem anderen Dolmetscher (Übertragungsschicht). Der zweite Dolmetscher übersetzt die Nachricht für B (Übersetzungsschicht).

Ein **anderes Beispiel** zur Verdeutlichung eines Schichtenmodells ist der Versand eines Briefs. Auch hierbei kann ein Schichtenmodell zugrunde gelegt werden:

1. Zunächst muss der Brief geschrieben werden.
2. Der geschriebene Brief wird in einem Briefumschlag verpackt.
3. Der Briefumschlag muss mit einer Empfängeradresse und Briefmarke versehen werden.
4. In dieser Form kann der Brief von der Post entgegengenommen und an den Empfänger weitergeleitet werden.

3.3.6 Ein Standard für alle Netze

Im Jahr 1978 hat das amerikanische Verteidigungsministerium das **TCP/IP- Referenzmodell** als **Standard** für heterogene Netze eingeführt. Dieses Modell ermöglicht den Datenaustausch über die Grenzen lokaler Netzwerke hinaus.

Dabei bedient sich das TCP/IP-Referenzmodell des Schichtenmodells und der Protokolle:

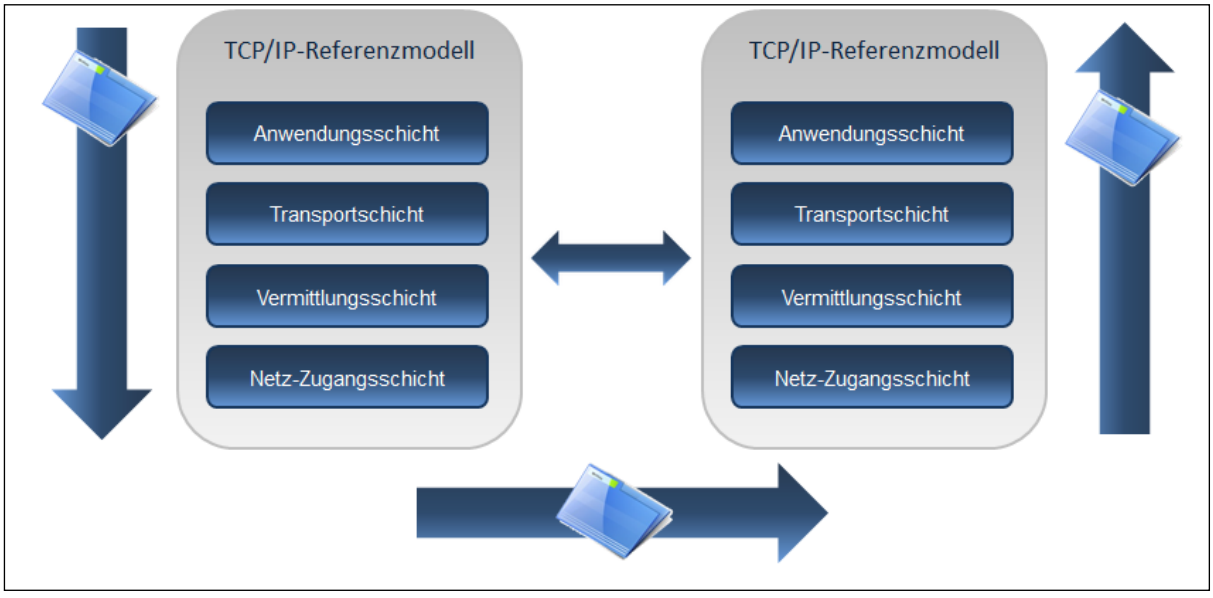

Abb. 12: Das TCP/IP Referenzmodell

Vor dem eigentlichen **Versand** müssen die Daten **nacheinander vier Schichten** durchlaufen.

Am Bestimmungsort angekommen müssen die Daten dieselben vier Schichten in **umgekehrter** Richtung durchlaufen.

Um die Daten richtig zu interpretieren, muss der Empfänger das gleiche Schichtenmodell benutzen wie der Sender: Jede Schicht beim Empfänger muss **dasselbe** Protokoll nutzen, wie die gegenüberliegende Schicht des Absenders.

3.3.7 Einkapselung von Daten

Bevor die **Daten** über das Internet verschickt werden, müssen sie die einzelnen Schichten des TCP/IP-Referenzmodells durchlaufen. Bei diesen Schichten wird vom **TCP/IP-Protokollstapel** gesprochen.

Von jeder Schicht werden dabei Kontrollinformationen in Form eines "Protokollkopfes" (sog. **Header**) **angefügt**. Diese Kontrollinformationen dienen der korrekten Zustellung und Interpretation der Daten. Das Hinzufügen von Kontrollinformationen wird als Einkapselung bezeichnet.

Das versendete Datenpaket umfasst also neben den eigentlichen Daten noch **zusätzliche** Informationen.

Bei der Ankunft der Daten können die empfangenden Schichten, die für sie notwendigen Informationen aus dem jeweiligen Header **auslesen**. Das Datenpaket wird sozusagen "**ausgepackt**". Auf diese Weise wird eine **korrekte** Zustellung der Daten sichergestellt.

3.3.8 Aufgabenteilung der Schichten

Die Schichtung im TCP/IP-Referenzmodell beruht auf dem Prinzip, dass jede Schicht eine Aufgabe hat. Jede Schicht kann die darunterliegende Schicht in **Anspruch nehmen**. Dabei muss die Schicht **keine** Kenntnisse darüber zu haben, wie die darunterliegende Schicht ihre Aufgabe erfüllt. Auf diese Art wird folgende Aufgabenteilung der Schichten erreicht:

Anwendungsschicht:
Die Anwendungsschicht ist die Schnittstelle zu Anwendungsprogrammen, die Daten über das Internet verschicken wollen. Die Anwendungsprogramme selbst sind dieser Schicht nicht zugeordnet, sie stehen außerhalb der Modellvorstellung (z. B. Web-Browser zur Nutzung des WWW-Dienstes). Damit ein Anwendungsprogramm das Internet nutzen kann, muss es ein Protokoll der Anwendungsschicht verwenden. Bekannte Protokolle aus dieser Schicht sind:

- HTTP (Hypertext Transfer Protocol) dient der Übertragung von Web Sites.

- FTP (File Transfer Protocol) dient dem Dateitransfer.
- SMTP (Simple Mail Transfer Protocol) dient dem Versand von E-Mails.

Transportschicht:

Die Transportschicht stellt eine End-zu-End-Verbindung über sog. Ports her. Das wichtigste Protokoll dieser Schicht ist das Transmission Control Protocol (TCP), das die Verbindung zwischen jeweils zwei Netzwerkteilnehmern herstellt. Damit wird der zuverlässige Versand von Daten sichergestellt. Ports sind Adressen, die Daten den Protokollen der Anwendungsschicht zuordnen. Unter dem Begriff "Well Known Ports" sind die Ports 0 bis 1023 bestimmten Protokollen zugeordnet. Die Portnummern bei TCP gehen von 0 bis 65535 und werden von der I-ANA (Internet Assigned Numbers Authority) an bestimmte Protokolle vergeben. Bspw. werden Daten des Protokolls SMTP beim Versand über den Port 25 gesendet. Im Gegenzug werden Daten, die mit dem Zusatz Port 25 in der Transportschicht eingehen, dem Protokoll SMTP zugeordnet.

Vermittlungsschicht:

Die Vermittlungsschicht ist für die Weitervermittlung von Daten und deren Wegewahl zuständig. Kern dieser Schicht ist das Internet Protocol (IP), das die Daten in kleine Datenpakete zerlegt, den Weg für jedes Paket bestimmt und diese auf die gewählten Wege verteilt. Der wichtigste Aspekt des Internet Protocols ist die IP-Adresse. Jede im Internet angeschlossene Ressource (Web Site, Server, Drucker usw.) besitzt eine eindeutige IP-Adresse. Dadurch ist es möglich, Computer in größeren Netzwerken zu adressieren und Verbindungen zu ihnen aufzubauen. Die Verwaltung von IP-Adressen erfolgt über das Domain Name System (DNS).

Netz-Zugangsschicht:

Über die Netz-Zugangsschicht wird eine Verbindung zu einem Netzwerkadapter hergestellt. Ein Netzwerkadapter ist eine Hardwarekomponente, die an ein Rechnernetz angeschlossen ist, wie z. B. die bereits erwähnten Geräte der Netzwerktechnik (Netzwerkkarte, Router und Gateway). Für diese Verbindung benötigt die Hardwarekomponente eine sog. MAC-Adresse (Media Access Control), die zur eindeutigen Identifikation des Geräts im Netzwerk dient. Netzwerkgeräte brauchen also eine MAC-Adresse, um Dienste auf höheren Schichten anbieten zu können. MAC-Adressen werden vom Hersteller des jeweiligen Gerätes vergeben. Die Identifikation von MAC-Adressen erfolgt durch das Adress Resolution Protocol (ARP).

3.3.9 Ein weiteres Modell

Die Übertragungstechnik im Internet **basiert** auf Netzwerkprotokollen, die in einem Schichtenmodell nacheinander durchlaufen werden. Mit dem **TCP/IP-Referenzmodell** haben Sie einen **Standard** für die Übertragung im Internet kennengelernt. Das später entwickelte **OSI-Schichtenmodell** (Open Systems Interconnection Reference Model) ist in **sieben Schichten** unterteilt.

Das OSI-Schichtenmodell ist das von der ISO (**Internationale Organisation für Normung**) standardisierte Referenzmodell für Kommunikationssysteme. An diesem Modell lassen sich weitere **Vorteile** eines Schichtenmodells erkennen. Einzelne Schichten können durch eigene Protokolle **angepasst, geändert oder ausgetauscht** werden. Im OSI-Schichtenmodell sind dazu Schichten des TCP/IP-Referenzmodells **weiter unterteilt** worden.

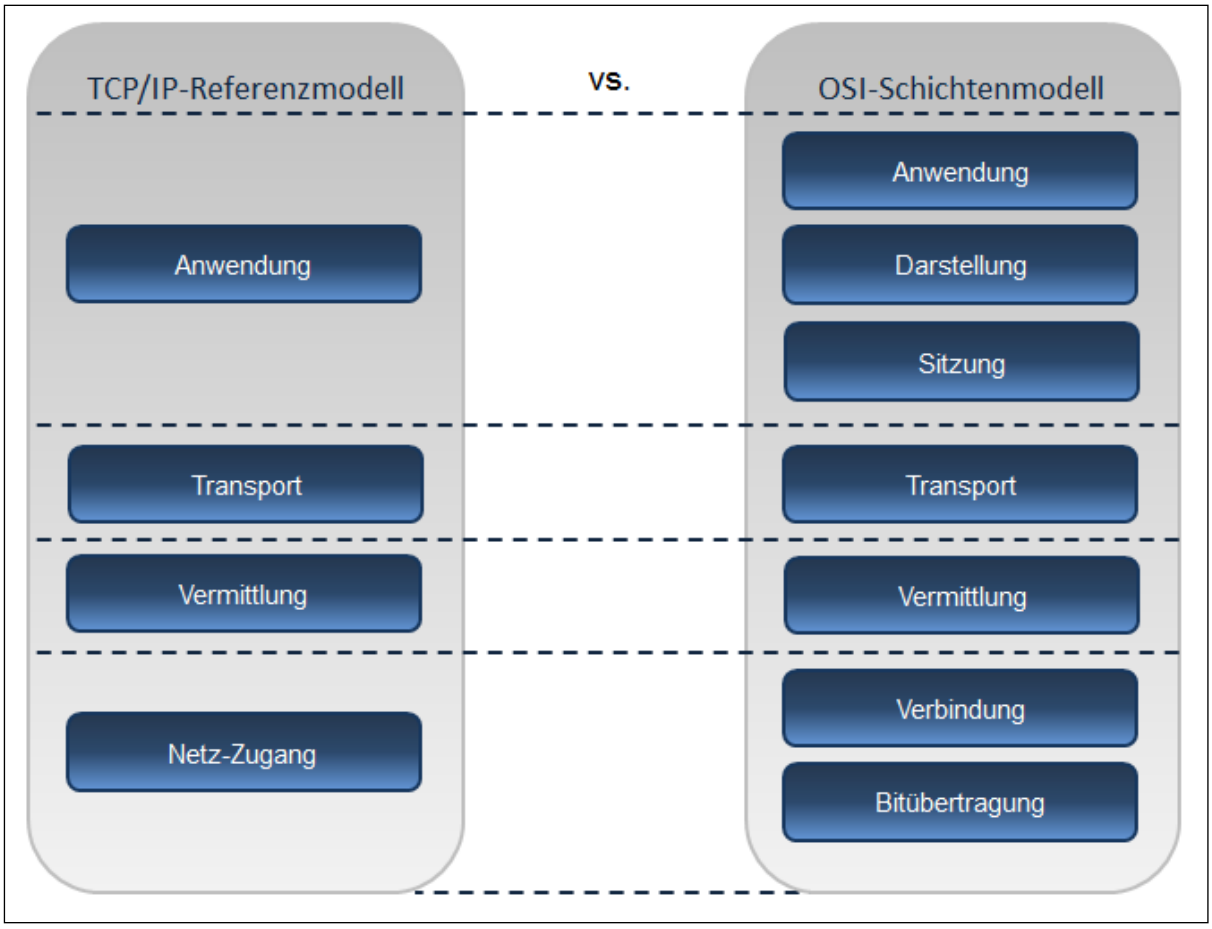

Abb. 13: TCP/IP-Referenzmodell vs. OSI-Schichtenmodell

Trotz der Aufteilung in mehrere Stufen ist auffällig, dass Transport- und Vermittlungsschicht gleich geblieben sind. Dies liegt daran, dass die Protokolle TCP und IP in allen gängigen Netzwerkstrukturen **gut** und vor allem **stabil** funktionieren.

3.3.10 Ein Beispiel

Sie haben bereits den Dienst E-Mail kennen gelernt. Der **Versand** einer E-Mail wird auf der Anwendungsschicht von dem Simple Mail Transfer Protocol (**SMTP**) initialisiert. Den **Abruf** regeln die Protokolle **POP** (Post Office Protocol) oder **IMAP** (Internet Message Access Protocol) auf der Anwendungsschicht.

Hier ein vereinfachtes Beispiel für das Zusammenspiel von Schichtenmodell und Protokollen beim Versand einer E-Mail:

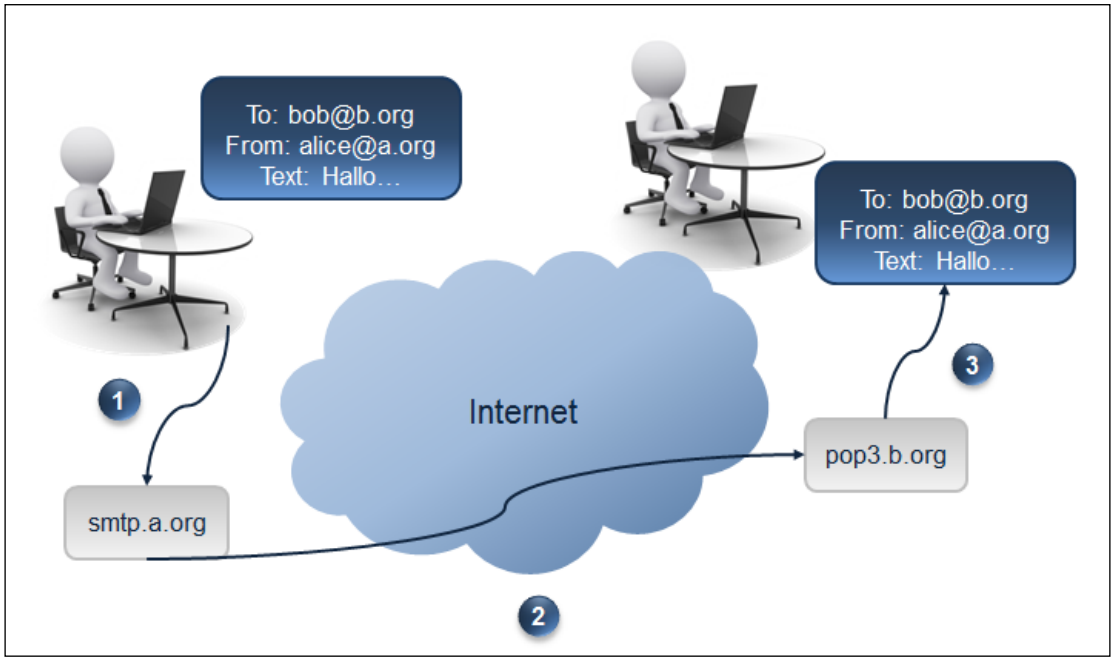

Abb. 14: Vereinfachter E-Mail-Versand

1. Eine Person A versendet eine E-Mail an eine Person B. Der E-Mail-Client kommuniziert über das Protokoll SMTP mit der Anwendungsschicht. Von dort aus durchläuft die E-Mail den Protokollstapel und wird über das Internet an den Mail-Server der Person A (hier smtp.a.org) versendet.
2. Um eine E-Mail zu lesen, muss der Empfänger überprüfen, ob E-Mails auf seinem Mail-Server eingegangen sind, vergleichbar mit dem regelmäßigen Gang zum Briefkasten. Diese Aufgabe übernimmt das Post Office Protokoll. Beim Herunterladen der E-Mail vom Mail-Server wird wieder der Protokollstapel durchlaufen.
3. Der Mail-Server von Person A empfängt die E-Mail. Das heißt die E-Mail durchläuft den Protokollstapel in umgekehrter Richtung (von unten nach oben). Wenn die E-Mail

am Mail-Server der Person A angekommen ist, wird der Empfänger der E-Mail ermittelt. Die E-Mail wird an den Mail-Server (pop3.b.org) des Empfängers gesendet. Dabei wird wieder der Protokollstapel durchlaufen, zunächst von oben nach unten und dann von unten nach oben.

3.4 Abschlusstest

3.4.1 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	Das TCP/IP-Referenzmodell ist lediglich für das Versenden von Daten vorgesehen.		
	Richtig		
	Falsch		
2	Mit welchem Protokoll werden Dateien im Internet übertragen?		
	FTP		
	HTTP		
	HTML		
	POP		
3	Welche dieser Schichten sind TCP/IP-Referenzmodell enthalten?		
	Transportschicht		
	Sicherungsschicht		
	Anwendungsschicht		
	Vermittlungsschicht		
	Netzzugangsschicht		
4	Eine E-Mail, die mit Microsoft Outlook verfasst wurde kann auch von Mozilla Thunderbird geöffnet werden.		
	Richtig		
	Falsch		
5	Wie viele Schichten hat das TCP/IP-Referenzmodell?		
	vier		
	fünf		
	sechs		
	sieben		
6	Informationen können übermittelt werden durch		

	Elektrische Signale		
	Optische Signale		
7	Bei HTTPS wird eine verschlüsselte Verbindung aufgebaut.		
	Richtig		
	Falsch		
8	Mit HTML können nur Schriftgröße und -farbe verändert werden.		
	Richtig		
	Falsch		
9	Optische Verbindungen übertragen elektrische Signale.		
	Richtig		
	Falsch		
10	Daten werden über eine andere Leitung übertragen als Anwendungen.		
	Richtig		
	Falsch		
11	Damit ein Schichtenmodell einwandfrei funktioniert, muss jede Schicht mit der Funktionsweise der anderen Schichten vertraut sein.		
	Richtig		
	Falsch		
12	Kontrollinformationen (sog. Header) werden nur von der Anwendungsschicht zu den Daten hinzugefügt.		
	Richtig		
	Falsch		
13	Die Transportschicht ist für die Verteilung von sog. Ports zuständig.		
	Richtig		
	Falsch		

Tab. 3: Abschlusstest in WBT 3

4 Sicherheit und Schutzmaßnahmen

4.1 Der Begriff Sicherheit um Internet

4.1.1 Warum IT-Sicherheit?

- **C't – Magazin für Computertechnik**
  Für das einzelne Unternehmen kann ein Sicherheitsproblem und damit verbundene Ausfälle der IT dessen Existenz bedrohen: Verschiedene Studien beziffern den Schaden durch einen IT-Ausfall auf durchschnittlich 100.000 US$ pro Stunde.
- **Computerwoche**
  "[...] Auch bei der Schadenshöhe tappen viele Verantwortliche im Dunkeln: Fast die Hälfte (47%) konnte Verluste, die durch sicherheitsbedingte Ausfälle entstanden sind, nicht beziffern. [...] Im Mittel registrierten die deutschen Betriebe im vergangenen Jahr rund 36 sicherheitsbedingte Ausfälle in der IT." (Quelle: Magazin "CIO" und PWC, 2005)
- **Computer Zeitung**
  Der Anteil von Spamnachrichten beträgt zwischen 60 und 90 Prozent aller E-Mails. So bekommt jeder Befragte im Durchschnitt 18,5 Spam-Mails am Tag; 2,8 Minuten verwendet er für deren Löschung. Gemessen an den Löhnen kosten diese 2,8 Minuten pro Arbeitstag die amerikanische Volkswirtschaft 21,6 Milliarden US$ jährlich.

4.1.2 Definition des Begriffs Sicherheit

Das **Konzept der dualen Sicherheit** gliedert sich in die folgenden zwei Sichtweisen, welche sich gegenseitig ergänzen:

1. Verlässlichkeit – Schutz des Systems –

   Der Nutzer muss sich auf die Korrektheit und Verfügbarkeit der Funktionen des Systems und deren Ergebnisse jederzeit verlassen können.

   Die Komponenten der Verlässlichkeit sind:

   - **Vertraulichkeit:** Grad der Nichtausforschbarkeit der zu schützenden Daten (z. B. geheime oder streng geheime Informationen schützen)
   - **Integrität:** Schutzniveau für Daten gegen unberechtigte Veränderung wie z. B. Verfälschung von E-Mails eines Konkurrenzunternehmens

- **Verfügbarkeit:** Grad der zeitlich uneingeschränkten Nutzbarkeit eines IT-Systems oder IT-Dienstes (Bsp.: 99,5% Verfügbarkeit bedeutet ca. 167 Stunden Nutzbarkeit und 1 Stunde Ausfall pro Woche)

2. Beherrschbarkeit – Schutz vor dem System –

   Auch ein perfekt verlässliches System kann eine Gefahr für den Nutzer darstellen. Daher müssen Daten, Vorgänge und Ereignisse nachprüfbar und rechtsverbindlich sein. Dies lässt sich unter folgenden Punkten zusammenfassen:

   - **Authenzität:** Grad der Zurechenbarkeit von Daten und Datenänderungen zu ihrem Urheber (z. B. welcher Mitarbeiter eine finanzielle Transaktion getätigt hat)
   - **Verbindlichkeit (Revisionsfähigkeit):** Niveau der Beweiskraft elektronischer Veränderungen und Willenserklärungen (im Gegensatz zur zwischenmenschlichen Kommunikation eher problematisch; Lösung: elektronische Signatur)

4.1.3 Privacy versus Security

Der im Deutschen unscharfe Begriff Sicherheit wird im Englischen in "Privacy" und "Security" unterschieden:

- **Privacy = Datenschutz**

  ... Schutz der Privatsphäre

  ... regelt das Recht des Bürgers auf informationelle Selbstbestimmung.

  ... bezeichnet den Schutz vor Missbrauch personenbezogener Daten.

- **Security = Datensicherheit**

  ... Sicherheit der Daten

  ... bezeichnet vorwiegend technische Aspekte zur Schadensverhütung.

  ... beinhaltet Maßnahmen zur Datensicherung (WIE ist zu schützen?).

4.2 IT-Risikoanalyse

4.2.1 IT-Risikoanalyse

Die IT-Risikoanalyse dient der Analyse der IST-Situation im Unternehmen: welche Risiken bedrohen die IT-Systeme und wie sind diese Risiken zu bewerten? Oder anders formuliert: wie

wahrscheinlich ist das Eintreten eines bestimmten Schadens und welche negativen Folgen hätte der Schaden?

Diese Fragen beantworten die zwei folgenden grundsätzlich unterschiedlichen Methoden: IT-Grundschutz und detaillierte Risikoanalyse.

Eine Kombination beider Methoden ist **ebenfalls** möglich. Der kombinierte Einsatz von Grundschutz und detaillierter Risikoanalyse vereint die Vorteile beider Methoden: IT-Systeme mit hohem Schutzbedarf werden entsprechend geschützt; für die übrigen Systeme können Maßnahmen schnell und effektiv ausgewählt werden.

4.2.2 Grundschutz kompakt: Leitfaden IT-Sicherheit

Der Grundschutzkatalog des BSI umfasst eine Vielzahl von Gefährdungen, welche sich auf die gesamte IT beziehen. Der Leitfaden zur IT-Sicherheit (herausgegeben vom BSI) bietet daher eine Zusammenfassung des Themas, zugeschnitten auf die Bedürfnisse von kleinen und mittleren Unternehmen. Im Folgenden werden einige darin enthaltene **Sicherheitsmaßnahmen** zum Thema Internet vorgestellt:

- …**Virenschutzprogramme** sollten installiert werden
- …zum Schutz von Netzen muss eine **Firewall** mit bestimmten Mindestanforderungen verwendet werden
- …bei **E-Mail-Anhängen** ist besondere Vorsicht notwendig
- …**Sicherheits-Updates** müssen regelmäßig eingespielt werden
- …es müssen gut gewählte (**sichere**) **Passwörter** eingesetzt werden.
- …alle wichtigen Daten müssen regelmäßig gesichert werden (**Backup**).

4.2.3 IT-Grundschutz

Bei IT-Systemen mit niedrigem bis mittlerem Schutzbedarf sind die Schadensauswirkungen begrenzt und überschaubar. Die Maßnahmen des IT-Grundschutzes reichen in der Regel aus, um die Sicherheit zu gewährleisten.

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** bietet Unternehmen und Behörden Informationen und Hilfestellungen rund um das Thema IT-Sicherheit.

Das Vorgehen nach IT-Grundschutz zusammen mit den IT-Grundschutzkatalogen, konzipiert vom BSI, hat sich als ganzheitliches Konzept für die IT-Sicherheit etabliert. Die Grundschutzkataloge sind eine umfangreiche Sammlung von möglichen Gefährdungen, enthalten im IT-Grundschutzhandbuch. Aus ihnen leiten sich Sicherheitsmaßnahmen ab, mit deren Hilfe der Aufbau einer Sicherheitsorganisation sowie eine Risikobewertung und die Überprüfung des vorhandenen IT-Sicherheitsniveaus angestrebt wird. Unternehmen erreichen dadurch eine grundlegende IT-Sicherheit.

Die Software **Grundschutztool (GSTool)** des BSI Die Software Grundschutztool (GSTool) des BSI bat dem Anwender im Unternehmen bis 2016 Unterstützung bei der Umsetzung des IT-Grundschutzes. Es gibt zahlreiche Software-Lösungen, die die BSI-Standards umsetzen.

4.2.4 Detaillierte Risikoanalyse

IT-Systeme mit hohem oder sehr hohem Schutzbedarf erfordern eine genaue Analyse der bestehenden Werte, Bedrohungen und Schwachstellen. Dieses Vorgehen wird am Beispiel eines W-LAN im Unternehmen vorgestellt:

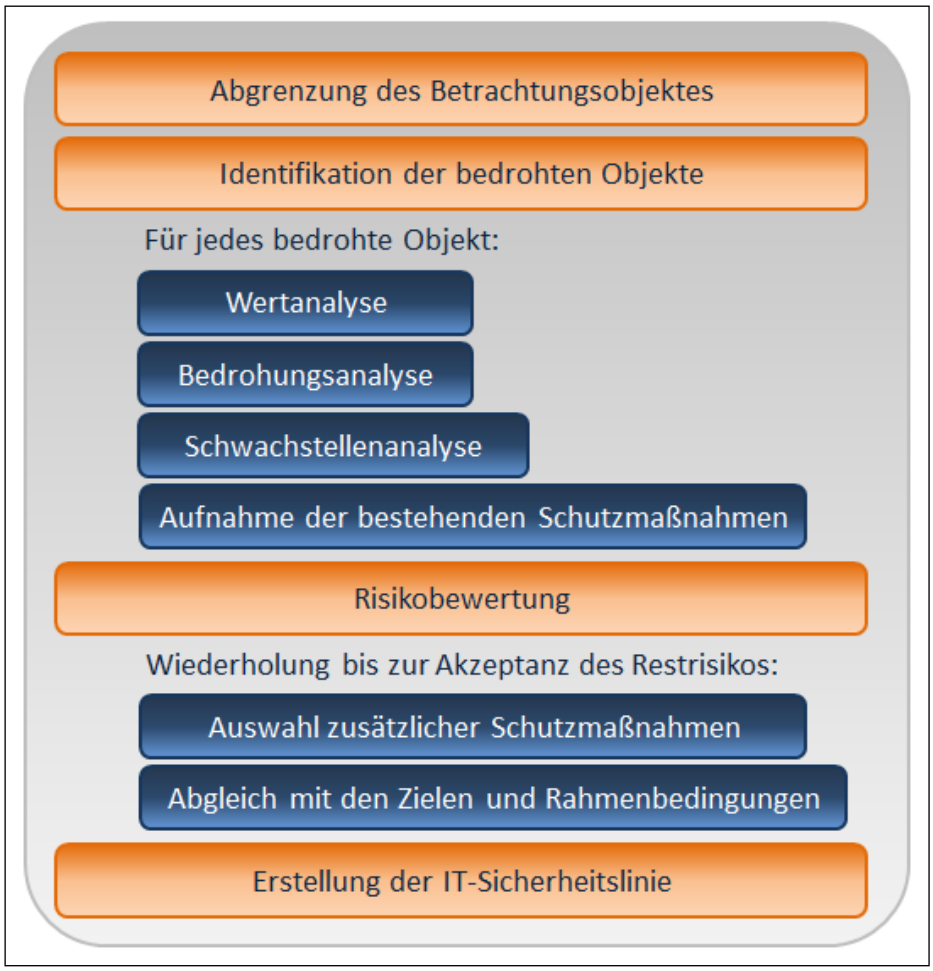

Abb. 15: Detaillierte Risikoanalyse

Abgrenzung des Betrachtungsobjektes:

Wie groß ist die Reichweite des W-LAN? Welche Geräte (z. B. Router) zählen dazu?

Identifikation der bedrohten Objekte:

Bedrohte Objekte können u. a. Unternehmens-Know-how, Software oder Kundendaten sein.

Für jedes bedrohte Objekt:

Wertanalyse: qualitativ (z. B. Imageschaden bei Kundendatenklau) oder quantitativ (z. B. resultierende Umsatzeinbußen)

Bedrohungsanalyse: Mögliche Bedrohungen wie z. B. Eingriffe in das firmeninterne Netzwerk oder Viren identifizieren inkl. Ihrer Eintrittswahrscheinlichkeiten.

Schwachstellenanalyse: Die Schwachstelle (z. B. keine Verschlüsselung des W-LAN) an sich verursacht noch keinen Schade, ermöglicht aber einer Bedrohung wirksam zu werden.

Aufnahme der bestehenden Schutzmaßnahmen: Alle bereits existierenden oder geplanten Sicherheitsmaßnahmen identifizieren und ihre Wirksamkeit prüfen.

Risikobewertung:

Risiko: Wie groß ist die Möglichkeit, dass eine Bedrohung (z. B. Virus) unter Ausnutzung einer Schwachstelle (fehlender Virenscanner) Schaden verursacht?

Wiederholung bis zur Akzeptanz des Restrisikos:

Auswahl zusätzlicher Schutzmaßnahmen: Z. B. Einsatz eines VPN zur Sicherung der übertragenen Daten.

Abgleich mit den Zielen und Rahmenbedingungen: VPN: schützt dies das Netzwerk effektiv und ist auch in der bestehenden Infrastruktur implementierbar.

Erstellung der IT-Sicherheitslinie:

Sicherheitsrichtlinie (Security Policy): sehr allgemein gehaltenes Bekenntnis zur IT-Sicherheit in Unternehmen.

4.3 Gefahren

4.3.1 Gefahren: Technische und Menschliche

Gefahren für IT-Systeme entstehen sowohl durch technisches Versagen als auch durch menschliche Handlungen.

Technisches Versagen:

... entsteht durch Fehlverhalten von Hard- und Software;

... zeigt sich oft im Ausfall von Teilen des Unternehmensnetzwerkes oder Störungen von Kommunikations- und Übertragungswegen. Bsp.: Ausfall von Routern, Störung der Internetverbindung, Ausfall einer Festplatte.

Menschliche Handlungen:

Schäden entstehen entweder:

... durch menschliche Fehlhandlungen, die auf Unwissenheit basieren; Bsp.: unbeabsichtigtes Deaktivieren einer Anti-Viren-Software oder...

... durch vorsätzliche Handlungen, die auf Böswilligkeit beruhen. Bsp.: beabsichtigtes Eindringen eines Unberechtigten in das Firmennetzwerk.

4.3.2 Angreifer: Hacker, Cracker, Script Kiddies

Im Allgemeinen unterscheidet man im Unternehmen zwischen internen und externen Angreifern. Gerade die internen Angreifer können dem Unternehmen großen Schaden zufügen, da sie über betriebsinterne Informationen und Abläufe informiert sind. Ihre Motivation liegt bspw. in Racheakten aufgrund einer Kündigung. Externe Angreifer wollen sich oftmals nur selbst beweisen oder dem Unternehmen Schaden zufügen, weil es bspw. ihren moralischen Vorstellungen widerspricht.

Hacker

... IT-Sicherheitsspezialist
... folgt einer gewissen Hackerethik
... sein Ziel ist es nicht, möglichst viel Schaden anzurichten, sondern verantwortungsvoll mit dem Medium Computer / Internet umzugehen
... die meisten Hacker veröffentlichen die von ihnen entdeckten Sicherheitslücken samt Hilfestellungen, um diese zu beheben
... ihr Ziel ist eine Verbesserung von Sicherheitssystemen

Cracker

... Personen, die ihr Wissen missbrauchen, um Schaden anzurichten
... werden oft mit Hackern verwechselt
... keine grundlegenden ethischen oder ehrenhaften Motive
... handeln mit dem Ziel, Daten zu erbeuten, zu beschädigen oder anderweitig Schäden anzurichten.

Script Kiddies

... Personen, die ohne fundiertes Know-how Cracker-Tools einsetzen, um Schaden anzurichten oder zum Herumexperimentieren
... es handelt sich nicht um Profis, sondern lediglich um Störenfriede, die einen Wettbewerb im Lahmlegen von Computern sehen
... die Zahl der Script Kiddies übersteigt die der Cracker erheblich

4.3.3 Eindringlinge: Viren, Würmer und Trojaner

In vernetzten Systemen besteht ein besonderes Sicherheitsproblem, da Eindringlinge sich oft über E-Mails oder Downloads verbreiten. Ein Virus oder ein Trojanisches Pferd kann auch über

einen Datenträger in ein System eingebracht werden; der Wurm dagegen ist eine typische Netzwerkerscheinung.

Der Begriff Virus wird oftmals als Oberbegriff für Viren, Würmer oder Trojanische Pferde verwendet.

Viren können andere Programme infizieren und sind die bekannteste Bedrohung im Internet.
Würmer funktionieren ähnlich wie Viren, sind allerdings eigenständige Programme.

Trojaner: In einem eigentlich nützlichen Programm versteckt sich ein weiteres jedoch schädliches Programm.

4.3.4 Viren

Der Computervirus benötigt - genauso wie die aus der Biologie bekannten Schädlinge - einen Wirt, um sich auszuführen und zu verbreiten. Der Wirt kann dabei ein einfaches Programm sein, bei dessen Start sich der Virus aktiviert. Von diesem Punkt an infiziert er das Betriebssystem oder andere Programme. Der Virus versteckt sich im Gegensatz zu Würmern in anderen Programmen.

Verbreitung: Früher waren die Hauptverbreitungswege Wechselmedien wie Disketten, heutzutage sind es überwiegend Rechnernetze (z. B. über E-Mail oder Downloads).

Schadenswirkung: Die Beschädigungen reichen von verlorenen oder verfälschten Daten und Programmen bis hin zum Formatieren der gesamten Festplatte.

Boot-Sektor-Viren: Diese besonders "bösartigen" Exemplare können bereits beim Booten des Betriebssystems aktiv werden und verhindern evtl. das Starten des Computers.

4.3.5 Würmer

Diese Schädlingsart wird oft fälschlicherweise auch als Virus bezeichnet. Würmer sind jedoch eigenständige Programme, als ungefährliche Dateitypen getarnt. Daher benötigen sie keinen Wirt, um Schäden anzurichten. Ihre Ausbreitung erfolgt über Computernetzwerke und ist damit sehr rasant.

Verbreitung: Würmer verbreiten sich aktiv, d. h. sie warten im Gegensatz zu Viren nicht passiv darauf, von einem Anwender auf einem neuen System ausgelöst zu werden, sondern versuchen selbst in neue Systeme einzudringen.

Beispiel: I LOVE YOU-Wurm - Der wohl bekannteste Wurm richtete im Jahr 2000 vor allem bei größeren Unternehmen erheblichen Schaden an. Die Verbreitung erfolgte via E-Mail.

4.3.6 Trojanische Pferde

Trojaner verstecken sich in vermeintlich harmloser Software (z. B. in Tools zur Systembeschleunigung). Im Gegensatz zu Viren und Würmern richtet der Trojaner jedoch nicht unbedingt Schaden an, sondern zielt auf die Überwachung und Auskundschaftung des Systems ab und ermöglicht dem Angreifer evtl. sogar die Kontrolle darüber zu erlangen (Backdoor-Trojaner).

Verbreitung: Trojaner sind häufig in Downloads oder E-Mail-Anhängen enthalten, besitzen jedoch meist selbst keine Verbreitungsmechanismen

Abhören von Tastatureingaben ist möglich (Passwort- /PIN-Klau)!

4.3.7 SPAM

... ist die Bezeichnung für vom Empfänger **unerwünschte Massenmails** (meist Werbemails)

... ursprüngliche Abkürzung für "**s**piced **p**ork **a**nd **h**am"

... heute: **s**end **p**henomenal **a**mounts of **m**ail
Der zeitliche Aufwand sowie die Kosten für den SPAM-Versender sind sehr gering: selbst wenn nur jeder 10.000 Empfänger reagiert, übersteigt sein Ertrag die Kosten.

Die Adressen beschafft sich der Versender u. a. bei kostenlosen Diensten, bei denen eine E-Mail-Adresse angegeben werden muss (z. B. Grußkarten).

Zum **Schutz vor SPAM** werden SPAM-Filter verwendet. Dabei können jedoch auch erwünschte Mails fälschlicherweise aussortiert werden.

Hinweis: Auf SPAM-Mails **niemals antworten**!

Zum einen ist die Absenderadresse oft falsch, zum anderen erhält der Versender Gewissheit darüber, dass die Empfängeradresse tatsächlich existiert.

4.3.8 HOAX (engl.): Falschmeldung

Kettenbriefe, die im Internet kursieren und eine gefälschte Meldung verbreiten, funktionieren immer nach demselben Prinzip: Der Empfänger soll die Nachricht möglichst schnell an viele Bekannte weiterleiten.

Typische Themen dieser Hoaxes sind Viruswarnungen, angebliche Hilfe- und Spendenaufrufe (z. B. Knochenmarkspende) sowie Falschmeldungen über aktuelle Geschehen.

Eine umfassende Übersicht zu den aktuell kursierenden Hoaxes finden Sie unter: http://hoax-info.tubit.tu-berlin.de/hoax/.

4.3.9 Denial of Service (DoS) und Sniffing

Denial of Service ist der englische Begriff für Dienst- und Kommunikationsunterbindung: dabei wird an den Server eine **Flut von Anfragen** geschickt, die dieser nur langsam oder gar nicht bearbeiten kann.

Unter **Sniffing** versteht man das **Abhören von Kommunikationsinhalten** in einem Netzwerk mit Hilfe von "Sniffern". Dies sind Programme, die zur Analyse des Datenstroms in LANs dienen. Der Angreifer fängt damit den gesamten Datenstrom ab; durch dessen Auswertung gelangt er an Passwörter, vertrauliche Unternehmensdaten etc.

4.3.10 Social Engineering und Phishing

Social Engineering ist eine der gefährlichsten Angriffsmethoden, da es keine technischen Schutzmaßnahmen gegen diese Art von Datenklau gibt. Hierbei versucht der Angreifer die Unwissenheit des Mitarbeiters ausnutzen: er gibt sich bspw. als Systemadministrator aus und fordert den Mitarbeiter zur Änderung seiner Zugangsdaten in ein von ihm vorgegebenes Passwort auf; damit erhält er Zugang zum Firmennetz.

Beim **Phishing** wird versucht, per E-Mail den Benutzer zur Herausgabe vertraulicher Daten wie Passwörter, PINs und TANs zu bewegen. Die betreffende E-Mail wird im Design des Unternehmens ausgestaltet, sodass der Benutzer die Tricktäuschung auf den ersten Blick nicht erkennen kann. Phishing zielt in den meisten Fällen auf Informationen des Onlinebankings oder von anderen Zahlungssystemen ab. Mit diesen Informationen ist es dem Angreifer möglich, Transaktionen im Namen des Kunden durchzuführen.

Hinweis: Auf keinen Fall sollte auf solche E-Mails geantwortet werden!

Abb. 16: Beispiel Phishing-Mail

4.4 Schutzsysteme

4.4.1 Kryptographie: Verschlüsselung

Unter Kryptographie versteht man die Wissenschaft der Verschlüsselung von Informationen. Unternehmen müssen sicherstellen, dass kein Unautorisierter ihre gespeicherten oder übertragenen Daten lesen kann.

Mit Hilfe von Verschlüsselungsverfahren soll die Vertraulichkeit der Informationen gewährleistet werden.

Public-Key-Verfahren:
Bei dem Public-Key-Verfahren (auch asymmetrisches Verfaheren genannt) wird mit zwei verschiedenen Teilschlüsseln gearbeitet:

Public key: Der öffentliche Schlüssel dient zur Verschlüsselung der Daten.

Private key: Der geheime Schlüssel dient zur Entschlüsselung der Daten und ist nicht öffentlich bekannt.

4.4.2 SSL: Secure Socker Layer-Verfahren

Das von Netscape entwickelte SSL-Verfahren stellt eine Kombination von symmetrischen und asymmetrischen Schlüsseln dar:

Der öffentliche (asymmetrische) Schlüssel wird zuerst zwischen Server und Client beim Verbindungsaufbauausgetauscht. Ist die Sitzung eröffnet, werden im Folgenden symmetrische Schlüssel (Sitzungsschlüssel) zur Verschlüsselung der Nachrichten und Informationen verwendet. Der Sitzungsschlüssel gilt nur für diese eine Sitzung und verfällt nach ihrer Beendigung.

Die gängigsten **Webbrowser** zeigen eine SSL-Verbindung wie folgt an:

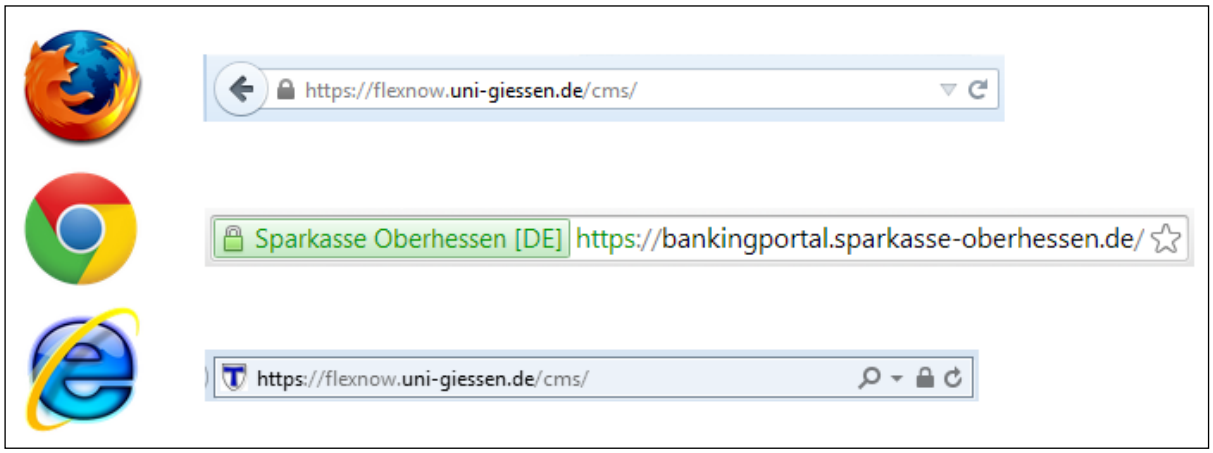

Abb. 17: SSL-Verbindung in Webbrowser

Das SSL-Verfahren findet vor allem Anwendung im E-Commerce Bereich, z. B. zur Verschlüsselung von personenbezogenen Daten und Passwörtern sowie Kreditkartenangaben in Online-Shops und bei Banken.

4.4.3 VPN: Virtual Private Network

Ein VPN soll sicherstellen, dass während der Übertragung über Netzwerke sensible Daten vertrauenswürdig weitergegeben werden; nur die berechtigten Personen sollen darauf zugreifen können.

VPNs nutzen dazu kryptographische Verfahren und andere Sicherheitskomponenten wie digitale Signaturen, Tunneling und Firewalling.

Die Einbettung eines Protokolls (**TCP/IP**) in ein anderes (**VPN-Protokoll**) wird als **Tunnel** bezeichnet; das VPN-Protokoll übernimmt dabei den **sicheren Transport** des TCP/IP-Protokolls.

Man klassifiziert drei verschiedene Arten von VPNs:

1. **Intranet VPNs** zwischen Firmenzentrale und Zweigniederlassungen.
2. **Remote Access VPNs** zwischen Firmennetz und mobilen Mitarbeitern.
3. **Extranet VPNs** zwischen Unternehmen und strategischen Partnern / Kunden / Lieferanten.

4.4.4 E-Mail-Sicherheit

Der Versand von Geschäftsunterlagen in Briefform gewährleistet eine relativ sichere Form der Datenübertragung:

- kommt der Brief unversehrt beim Empfänger an, sind Vertraulichkeit und Integrität sichergestellt;
- die handschriftliche Unterschrift gewährleistet die Identität des Absenders (Authenzität);
- diese Unterschrift macht das Dokument rechtswirksam (Verbindlichkeit).

Durch den Einsatz von digitaler Signatur und digitaler Verschlüsselung wird bei **elektronischer Post** dieselbe Sicherheit erreicht.

PGP = Pretty Good Privacy Programm zur digitalen Verschlüsselung und Signatur von E-Mails.

4.4.5 Firewall

Die Firewall dient der Kontrolle des Übergangs von einem zu schützenden Netz in ein öffentliches unsicheres Netz, wie z. B. das Internet. Das elektronische Firewall-System schottet also einen bestimmten Bereich ab, um diesen vor Gefahren von außerhalb zu schützen. Es wird nur ein einziger sicherer Übergang zwischen den beiden Teilnetzen realisiert, der gesamte Datenverkehr läuft damit nur noch über dieses Firewall-System.

Der Einsatz von **Internet-Firewall-Systemen** dient der sicheren Verknüpfung des Intranets von Unternehmen mit dem Internet. So können Mitarbeiter auf Informationen und Dienste des Internets ungefährdet zugreifen.

Unternehmens-Firewall:
Ein Firewall-Rechner markiert hier die Grenze zwischen Intranet und Internet. Jeglicher Datenverkehr wird dort analysiert und bei Bedarf (z. B.infizierte E-Mail-Anhänge) herausgefiltert.

Personal-Firewall:
Die Personal-Firewall ist dezentralauf dem Mitarbeiter-PC installiert und schützt ihn vor den noch vorhandenen Lücken des zentralen Firewall-Systems sowie Gefahren innerhalb des Intranets. Hier finden Sie ein Beispiel zu der in Windows XP standartmäßig integrierten Firewall.

Hinweis: An dieser Stelle des WBT befindet sich ein Video zur Verdeutlichung der Inhalte.

4.4.6 Antiviren-Software

Die eben beschriebene Firewall soll Schädlingen den Zugang zum PC verweigern. Gelangt Malware (**Viren, Würmer, Trojaner**) trotzdem auf den PC, sorgt ein **Antiviren-Programm** für deren **Erkennung**. Im Optimalfall ist es auch in der Lage, sie zu beseitigen und angegriffene Programme zu reparieren oder verlorene Daten wiederherzustellen.

Virenscanner können allerdings nur ihnen **bekannte Viren** ausfindig machen. Dafür benötigen sie aktuelle Virensignaturen, die Viren anhand ihrer Wirkung (Muster und Regelmäßigkeiten) identifizieren. In der Regel laden Virenscanner Updates mit den neuesten Signaturen über das Internet herunter.

Hinweis: Es empfiehlt sich, das Programm auf automatische Updates einzustellen!

Echtzeitscanner = On-Acess Scanner
Dieser Virenscanner ist dauerhaft im Hintergrund aktiv und untersucht fortlaufend verwendete Daten, Programme, den Arbeitsspeicher etc.

Manueller Scanner = On-Demand Scanner

Dieser Virenscanner wird vom Benutzer von Hand gestartet. In regelmäßigen Abständen sollte damit die Festplatte überprüft werden.

Hinweis: An dieser Stelle des WBT befindet sich ein Video zur Verdeutlichung der Inhalte.

4.4.7 IDS – Intrusion Detection System

Ein **Intrusion Detection System** (Einbruchs-Erkennungs-System) kann man sich vorstellen wie ein System zur **Videoüberwachung** oder auch eine Alarmanlage. Es **erkennt Angriffe** und ist in der Lage, darauf aktiv zu reagieren: es informiert den Systemadministrator (per E-Mail) oder fährt zum Schutz sogar das System herunter. Damit dient es als **Ergänzung** eines **Firewall**-Systems und verhindert Angriffe, die durch dieses nicht gestoppt werden können.

Das IDS erkennt z. B. Anomalien - also untypisches System- und Nutzerverhalten - oder aber auch Angriffe wie Denial of Service-Attacken.

Überdurchschnittliche Fehlerrate bei der Einwahl ins Firmennetzwerk. Möglicherweise verursacht durcheinen unbefugten Mitarbeiter.

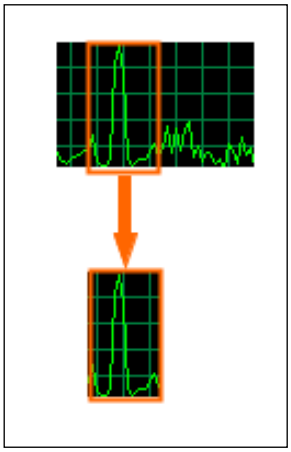

Abb. 18: IDS

Durch die Erkennung von Unregelmäßigkeiten sind Intrusion Detection Systeme sehr wirksam gegen interne Angriffe.

4.5 Abschlusstest

4.5.1 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	Technisches Versagen entsteht immer durch vorsätzliche Handlungen, die auf Böswilligkeit beruhen.		
	Richtig		
	Falsch		
2	Das Ziel von Hackern ist…		
	eine Verbesserung von Sicherheitssystemen.		
	Daten zu erbeuten, zu beschädigen oder anderweitig Schäden anzurichten.		
	Verantwortungsvoll mit dem Medium Computer / Internet umzugehen.		
3	Echtzeitscanner werden vom Benutzer von Hand gestartet.		
	Richtig		
	Falsch		
4	Der Sitzungsschlüssel gilt für mehrere Sitzungen.		
	Richtig		
	Falsch		
5	Die Personal-Firewall ist auf dem Server-Rechner des Unternehmens installiert.		
	Richtig		
	Falsch		
6	Die Verbreitung eines Virus erfolgt über Speichermedien sowie Rechnernetze.		
	Richtig		
	Falsch		
7	Welche Begriffe lassen sich der Sicht der Beherrschbarkeit zuordnen?		
	Vertraulichkeit		
	Verbindlichkeit		
	Verlässlichkeit		
	Integrität		
	Authenzität		

8	Die Grundschutzkataloge sind eine umfangreiche Sammlung von möglichen Gefährdungen und sind im IT-Grundschutzhandbuch enthalten.		
	Richtig		
	Falsch		
9	IT-Systeme mit hohem oder sehr hohem Schutzbedarf erfordern eine detaillierte Risikoanalyse.		
	Richtig		
	Falsch		
10	Folgende Eigenschaften lassen sich dem digitalen Zertifikat zuordnen:		
	Verschlüsselung		
	sichere Übertragung		
	gleiche Funktion wie ein Personalausweis		
	wird von einer Zertifizierungsstelle vergeben		
	ordnet eine E-Mail dem Absender klar zu		
11	Die Sicht der Verlässlichkeit und die Sicht der Beherrschbarkeit schließen sich gegenseitig aus.		
	Richtig		
	Falsch		
12	Sniffing bezeichnet das ..... von Kommunikationsinhalten in einem Netzwerk mit Hilfe von Programmen (Sniffern). Bitte geben Sie den gesuchten Begriff in das unten stehende Feld ein!		
13	Ein Intrusion Detection System erkennt:		
	Viren		
	Anomalien		
	hohe Fehlerraten		
	externe Angriffe		
	interne Angriffe		
14	Die detaillierte Risikoanalyse ist bei IT-Systemen mit niedrigem bis mittlerem Schutzbedarf erforderlich.		
	Richtig		
	Falsch		
15	Technisches Versagen entsteht durch Fehlverhalten von Hard- und Software.		
	Richtig		
	Falsch		

16	Die IT-Risikoanalyse dient der Analyse der ..... -Situtation im Unternehmen. Bitte geben Sie den gesuchten Begriff in das unten stehende Feld ein!		
17	Interne Angreifer sind im Allgemeinen weniger gefährlich als externe.		
	Richtig		
	Falsch		
18	Beim ..... -Key-Verfahren wird mit zwei verschiedenen Teilschlüsseln gearbeitet. Bitte geben Sie den gesuchten Begriff in das unten stehende Feld ein!		

Tab. 4: Abschlusstest in WBT 4

Anhang

Lösungen zum Abschlusstest in WBT 2

Nr.	Frage	Richtig	Falsch
1	Die Aufgabe eines Mail-Servers sind der Empfang und die Speicherung von E-Mails.		
	Richtig		X
	Falsch	X	
2	Web-Server verwalten das lokale Dateisystem und stellen angeschlossenen Rechnern ihre Ressourcen zur Verfügung.		
	Richtig		X
	Falsch	X	
3	Internet Service Provider verkaufen Übertragungsleistungen an Carrier.		
	Richtig		X
	Falsch	X	
4	Je mehr Schichten in einer Multi-Tier-Architektur, umso besser.		
	Richtig		X
	Falsch	X	
5	Ergebnisaufbereitung, Verarbeitung und anteilige Datenhaltung sind typisch für welche Client/Server-Architektur?		
	Entfernte Präsentation		X
	Entfernte Datenbank		X
	Verteilte Datenbank	X	
6	Das Client/Server-Konzept ein theoretisches Konstrukt, das in der Praxis Anwendung findet.		
	Richtig		X
	Falsch	X	
7	Das Client/Server-Konzept ist ein wichtiges Kommunikationskonzept im Internet.		
	Richtig	X	
	Falsch		X
8	Einer Unternehmensabteilung steht nur ein Drucker zur Verfügung. Wäre ein Zusammenschluss der vorhandenen Rechner zu einem LAN sinnvoll?		
	Ja, der Drucker ist eine Ressource, die im LAN von allen genutzt werden kann.	X	

	Nein, Ressourcen in einem LAN sind ausschließlich Daten und Anwendungen. Hardware ist lediglich ein Medium für diese Ressourcen.		X
9	Ergebnisaufbereitung und Verarbeitung sind typisch für welche Client/Server-Architektur?		
	Entfernte Präsentation		X
	Entfernte Datenbank	X	
	Verteilte Datenbank		X
10	Unternehmen sehen keine Notwendigkeit in der Internetnutzung.		
	Richtig		X
	Falsch	X	
11	Die Grundtopologien einer LAN-Netzwerkstruktur sind Stern-, Bus- und Ringtopologie.		
	Richtig	X	
	Falsch		X
12	Die Multi-Tier-Architektur ist im Vergleich zur Client/Server-Architektur effizienter.		
	Richtig		X
	Falsch	X	

Tab. 5: Lösungen zum Abschlusstest in WBT 2

Lösungen zum Abschlusstest in WBT 3

Nr.	Frage	Richtig	Falsch
1	Das TCP/IP-Referenzmodell ist lediglich für das Versenden von Daten vorgesehen.		
	Richtig		X
	Falsch	X	
2	Mit welchem Protokoll werden Dateien im Internet übertragen?		
	FTP	X	
	HTTP		X
	HTML		X
	POP		X
3	Welche dieser Schichten sind TCP/IP-Referenzmodell enthalten?		
	Transportschicht	X	
	Sicherungsschicht		X
	Anwendungsschicht	X	
	Vermittlungsschicht	X	
	Netzzugangsschicht	X	
4	Eine E-Mail, die mit Microsoft Outlook verfasst wurde kann auch von Mozilla Thunderbird geöffnet werden.		
	Richtig	X	
	Falsch		X
5	Wie viele Schichten hat das TCP/IP-Referenzmodell?		
	vier	X	
	fünf		X
	sechs		X
	sieben		X
6	Informationen können übermittelt werden durch		
	Elektrische Signale	X	
	Optische Signale	X	
7	Bei HTTPS wird eine verschlüsselte Verbindung aufgebaut.		
	Richtig	X	
	Falsch		X

8	Mit HTML können nur Schriftgröße und -farbe verändert werden.		
	Richtig		X
	Falsch	X	
9	Optische Verbindungen übertragen elektrische Signale.		
	Richtig		X
	Falsch	X	
10	Daten werden über eine andere Leitung übertragen als Anwendungen.		
	Richtig		X
	Falsch	X	
11	Damit ein Schichtenmodell einwandfrei funktioniert, muss jede Schicht mit der Funktionsweise der anderen Schichten vertraut sein.		
	Richtig		X
	Falsch	X	
12	Kontrollinformationen (sog. Header) werden nur von der Anwendungsschicht zu den Daten hinzugefügt.		
	Richtig		X
	Falsch	X	
13	Die Transportschicht ist für die Verteilung von sog. Ports zuständig.		
	Richtig	X	
	Falsch		X

Tab. 6: Lösungen zum Abschlusstest in WBT 3

Lösungen zum Abschlusstest in WBT 4

Nr.	Frage	Richtig	Falsch
1	Technisches Versagen entsteht immer durch vorsätzliche Handlungen, die auf Böswilligkeit beruhen.		
	Richtig		X
	Falsch	X	
2	Das Ziel von Hackern ist…		
	eine Verbesserung von Sicherheitssystemen.	X	
	Daten zu erbeuten, zu beschädigen oder anderweitig Schäden anzurichten.		X
	Verantwortungsvoll mit dem Medium Computer / Internet umzugehen.	X	
3	Echtzeitscanner werden vom Benutzer von Hand gestartet.		
	Richtig		X
	Falsch	X	
4	Der Sitzungsschlüssel gilt für mehrere Sitzungen.		
	Richtig		X
	Falsch	X	
5	Die Personal-Firewall ist auf dem Server-Rechner des Unternehmens installiert.		
	Richtig		X
	Falsch	X	
6	Die Verbreitung eines Virus erfolgt über Speichermedien sowie Rechnernetze.		
	Richtig	X	
	Falsch		X
7	Welche Begriffe lassen sich der Sicht der Beherrschbarkeit zuordnen?		
	Vertraulichkeit		X
	Verbindlichkeit	X	
	Verlässlichkeit		X
	Integrität		X
	Authenzität	X	

8	Die Grundschutzkataloge sind eine umfangreiche Sammlung von möglichen Gefährdungen und sind im IT-Grundschutzhandbuch enthalten.		
	Richtig	X	
	Falsch		X
9	IT-Systeme mit hohem oder sehr hohem Schutzbedarf erfordern eine detaillierte Risikoanalyse.		
	Richtig	X	
	Falsch		X
10	Folgende Eigenschaften lassen sich dem digitalen Zertifikat zuordnen:		
	Verschlüsselung		X
	sichere Übertragung		X
	gleiche Funktion wie ein Personalausweis	X	
	wird von einer Zertifizierungsstelle vergeben	X	
	ordnet eine E-Mail dem Absender klar zu		X
11	Die Sicht der Verlässlichkeit und die Sicht der Beherrschbarkeit schließen sich gegenseitig aus.		
	Richtig		X
	Falsch	X	
12	Sniffing bezeichnet das ..... von Kommunikationsinhalten in einem Netzwerk mit Hilfe von Programmen (Sniffern). Bitte geben Sie den gesuchten Begriff in das unten stehende Feld ein!		
			Abhören
13	Ein Intrusion Detection System erkennt:		
	Viren		X
	Anomalien	X	
	hohe Fehlerraten	X	
	externe Angriffe		X
	interne Angriffe	X	
14	Die detaillierte Risikoanalyse ist bei IT-Systemen mit niedrigem bis mittlerem Schutzbedarf erforderlich.		
	Richtig		X
	Falsch	X	
15	Technisches Versagen entsteht durch Fehlverhalten von Hard- und Software.		
	Richtig	X	
	Falsch		X

16	Die IT-Risikoanalyse dient der Analyse der ..... -Situtation im Unternehmen. Bitte geben Sie den gesuchten Begriff in das unten stehende Feld ein!		
			Ist
17	Interne Angreifer sind im Allgemeinen weniger gefährlich als externe.		
	Richtig		X
	Falsch	X	
18	Beim ..... -Key-Verfahren wird mit zwei verschiedenen Teilschlüsseln gearbeitet. Bitte geben Sie den gesuchten Begriff in das unten stehende Feld ein!		
			Public

Tab. 7: Lösungen zum Abschlusstest in WBT 4

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: https://wi.uni-giessen.de

Herausgeber: Prof. Dr. Axel Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
https://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungs-, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr-, Vortrags- und Kolloquiumsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Prof. Dr. Axel Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Prof. Dr. Bernhard Ostheimer, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit einem der Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Web-Adresse https://wi.uni-giessen.de/