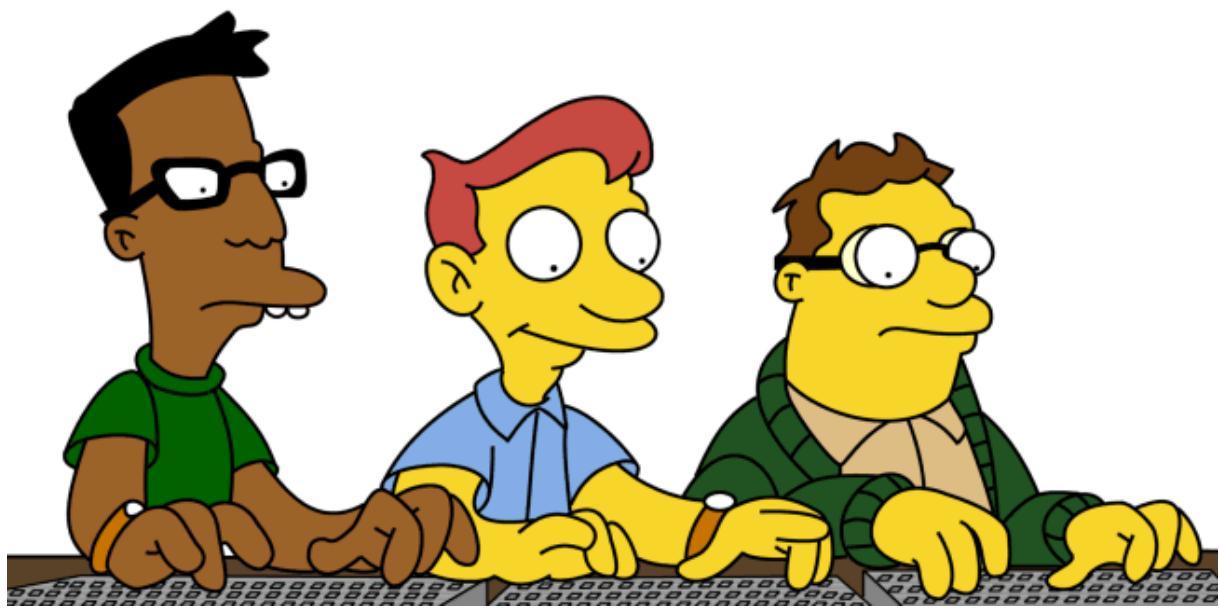


Wirtschaftsinformatik

unter didaktischem Aspekt

Kurs I - WS 18/19
Dr. Franz-Karl Skala

Masterstudium Wirtschaftspädagogik
WU Wien



1	Wirtschaftsinformatik im Unterricht	5
1.1	Wirtschaftsinformatik HAK 2014 im Überblick	5
1.2	Ausbildungsschwerpunkt: Informations- und Kommunikationstechnologie – E-Business..	5
2	Ablauf der Lehrveranstaltung	6
2.1	Aufgabenstellungen.....	6
2.2	Beurteilungskriterien.....	7
3	Hardware.....	8
3.1	Arten von Rechnern	9
3.2	Aufbau eines Desktop PCs.....	12
3.3	Mainboard.....	13
3.3.1	PCI Express (PCIe)	14
3.4	Prozessor (CPU)	18
3.4.1	Architektur eines Prozessors	18
3.4.2	Leistungsmerkmale eines Prozessors	19
3.4.3	Bit/Byte/Mega/Kilo/Giga und Tera & Co. – Grundlagenwissen	22
3.5	Arbeitsspeicher (RAM)	29
3.5.1	Formfaktoren	29
3.6	Das BIOS.....	31
3.7	Festplatte	32
3.7.1	Mechanische Festplatte	32
3.7.2	Solid-state-drive (SSD)	32
3.7.3	Wichtige Leistungsmerkmale.....	34
3.7.4	Partitionen.....	34
3.7.5	Dateisysteme.....	35
3.7.6	RAID.....	37
3.8	Grafikkarte und Monitor.....	38
3.8.1	Grafikkarten	38
3.8.2	IGP - Onboard-Lösungen	38
3.8.3	Auflösungen.....	39
3.8.4	Farbtiefe	40
3.8.5	Anschlüsse	40
3.8.6	Monitor	42
3.9	Gehäuse und Netzteil	43
3.10	Betriebssysteme	45
3.10.1	Funktionen eines Betriebssystems.....	45
3.10.2	Aufbau eines Betriebssystems	46
3.10.3	Marktanteile von Betriebssystemen	47
3.10.4	Wichtige Standardfunktionen unter Windows	48
4	Netzwerke	51
4.1	Klassifizierung von Netzwerken	51

4.1.1	Reichweite von Netzwerken	51
4.1.2	Technologien von Netzwerken	52
4.1.3	Topologien von Netzwerken	52
4.2	Grundlagen der Signal- und Datenübertragung	54
4.3	Träger der Datenübertragung	56
4.3.1	Übertragung per Kabel	56
4.3.2	Übertragung per Funk	57
4.3.3	Wichtige Netzwerkgeräte	58
4.4	Netzwerkkommunikation verstehen	59
4.4.1	ISO/OSI Layer Referenz Modell	59
4.4.2	TCP/IP-Referenzmodell	61
4.5	Der „Aufbau des Internets“	62
4.5.1	Der physische Aufbau	62
4.5.2	Der logische Aufbau	63
4.5.3	Das TCP-Protokoll	64
4.5.4	Das IP-Protokoll	65
4.5.5	Anbindungen an das Internet	68
4.5.6	Das Domain Name System (DNS)	71
4.5.7	Ports	73
4.6	Im Netzwerk zurechtfinden	76
4.6.1	Netzwerkkarte konfigurieren	76
4.6.2	ARP	78
4.6.3	Ports und Firewall	79
4.6.4	Netzwerk unter Windows	80
4.7	WLAN-Verwalten	81
4.7.1	WPS (Wi-Fi Protected Setup)	81
4.7.2	WAN-Setup (Wide Area Network)	82
4.7.3	LAN-Setup (Local Area Network)	82
4.7.4	Wireless-Setup	83
4.7.5	Verschlüsselung (WIFI Security)	84
4.7.6	DHCP-Server	84
4.7.7	Dynamisches DNS - DDNS	85
4.8	Wie sicher ist mein WLAN?	86
4.9	Virtualisierung	90
4.9.1	Das Konzept der Virtualisierung	90
4.9.2	Virtuelle Maschine installieren (VMware-Player)	91
4.9.3	Virtuelle Maschine einrichten	92
4.10	Remote Desktop Verbindung	100
4.10.1	Funktionsweise	100
4.10.2	Remotedesktop-Verbindung einrichten	101
4.10.3	Unterstützte Betriebssysteme	101

4.10.4	Remotedesktop-Verbindung aufbauen	101
4.10.5	Häufige Fehler bei Remotedesktop-Verbindungen.....	104
4.10.6	Remoteunterstützung unter Windows	105
4.11	TeamViewer.....	107
4.11.1	TeamViewer herunterladen.....	109
4.11.2	Fernsteuerung starten	110
4.11.3	Verbindung über IP-Adresse	113
4.11.4	Computer und Kontakte.....	113
5	Web und Server.....	115
5.1	Was ist GNU, UNIX, LINUX?	115
5.2	Debian installieren	121
5.3	Arbeiten mit Linux	128
5.3.1	Shell-Befehle	128
5.3.2	Übersicht wichtiger Bash-Befehle.....	136
5.4	Der Apache2-Webserver	140
5.4.1	Konfigurieren/Warten.....	140
5.4.2	Aufrufen.....	140
5.5	Der MySQL-Datenbank-Server.....	141
5.5.1	Was ist der MySQL-Server?	141
5.5.2	Server installieren	141
5.5.3	Server warten	142
5.5.4	PhpMyAdmin.....	142

1 Wirtschaftsinformatik im Unterricht

1.1 Wirtschaftsinformatik HAK 2014 im Überblick

JG.	Mod.	Tabellenkalkulation	Datenbanken	Informatiksysteme	Informations-technologie, Mensch und Gesellschaft
II.	3				
	4	Dateneingabe, Formatierung, Drucken, Berechnungen, Diagramme			
III.	5	Berechnungen und Entscheidungsfunktionen, Datenaustausch, Datenauswertung, Tabellenentwurf			
	6		Tabellen, Abfragen, Formulare und Berichte	Kaufentscheidung, Fallanalyse	Datensicherheit
IV.	7		Datenauswertung durch Abfragen, Formulare und Berichte, DB-Management, Import und Export		
	8		Datenbankmodellierung	Netzwerk-administration, Netzwerk-konfiguration	
V.	9	Komplexe betriebswirtsch. Aufgabenstellungen			Datensicherheit, Datenschutz und Recht
	10				

1.2 Ausbildungsschwerpunkt: Informations- und Kommunikationstechnologie – E-Business

JG.	Mod.	Lehrstoff	
III.	5	Social Media, Fotografie und Bildbearbeitung	
	6	HTML-Grundlagen, CSS-Grundlagen	
IV.	7	Web-Projekt mit CMS.	
	8	Audio-, Videobearbeitung und Animation	
V.	9	Webserver und Domain, Websites mit dynamischen Elementen, Webseiten mit Datenbankanbindung	
	10	Security, Webseiten mit Datenbankanbindungen	



Wird im Rahmen von Kurs I behandelt



Wird im Rahmen von Kurs II behandelt

2 Ablauf der Lehrveranstaltung

Mo, 01.10.2018 10:00-16:30	HARDWARE <ul style="list-style-type: none"> • Grundlagen von PC-Systemen • Unterschiedliche Hardware-Komponenten • Einführung in Hardware-Verwaltung und Analyse mit Windows
Mo, 08.10.2018 10:00-16:30	NETZWERK <ul style="list-style-type: none"> • Grundlagen von Netzwerken • Aufbauen von Netzwerken • Virtualisierung und Netzwerke • Remoteverwaltung von Rechnern
Mo, 12.11.2018 14:00-19:00	WEB UND SERVER <ul style="list-style-type: none"> • Cloud Computing • Einführung in Linux • Einführung in DB-/Web-/FTP-/SSH-Server
Mo, 19.11.2018 14:00-19:00	WEBANWENDUNGEN <ul style="list-style-type: none"> • Grundlagen HTML und CSS • Content-Management-Systems (Bsp. JOOMLA) • Lern-Management-Systeme (Bsp. MOODLE)
Di, 14.01.2019 14:00-19:00	PRÄSENTATIONEN/SIMULATION <ul style="list-style-type: none"> • 4 Projektpräsentationen • Offene Fragen • Evaluierung/Abschluss

2.1 Aufgabenstellungen

Hausübungen	40 %
<p>Detaillierte Informationen zu allen Hausübungen erhalten Sie noch gesondert. Die Hausübungen 1-3 sind zwischen der zweiten und der vierten Einheit, die vierte Hausübung bis zur fünften Einheit abzugeben. Es sind folgende Hausübungen in Einzelarbeit abzugeben:</p> <ol style="list-style-type: none"> 1. Sie analysieren den Aufbau eines Netzwerkes und halten mehrere relevante Parameter in einer Vorlage fest. Dabei dokumentieren Sie Ihr Vorgehen und halten aufgetretene Probleme fest. Aufgabe in Einzelarbeit. Die Vorlage finden Sie nach der zweiten Einheit auf Learn@WU 2. Installieren Sie TeamViewer (vgl. Abschnitt 4.11) in der aktuellen Version auf Ihrem Rechner. Vereinbaren Sie in Ihrer Projektgruppe ein Teammeeting zu einem bestimmten Zeitpunkt. Versuchen Sie, dieses Teammeeting online durchzuführen. Vereinbaren Sie dabei einen Arbeitsplan für Ihre Projektarbeit oder arbeiten Sie während dieses mindestens 15 Minuten dauernden Projekttreffens an einem Task oder Tauschen Sie Ihre Ideen aus. Nutzen Sie die Kommunikationsmöglichkeiten der Software aus: Webcam, Mikrofon, Bildschirmfreigabe etc. Zeichnen Sie das Meeting auf und stellen Sie die Aufzeichnung dem LV-Leiter zur Verfügung. Dokumentieren Sie Ihre Erfahrungen mit dem Format des Austausches und geben Sie diese auf Learn@WU ab. 3. Installieren Sie auf GOOGLE Cloud eine neue virtuelle Maschine mit dem Betriebssystem DEBIAN 8 (oder ein anderes Betriebssystem) und halten Sie die Installationsschritte in einer Vorlage fest. Dabei dokumentieren Sie Ihr Vorgehen und halten aufgetretene Probleme. Aufgabe in Einzelarbeit. Die Vorlage finden Sie nach der zweiten Einheit auf Learn@WU 	

Projekt	60 %
Im Rahmen der Projekte arbeiten Sie sich eigenständig in einen ausgewählten Themenbereich tiefer ein und bereiten diesen dann für Ihre Kolleg/inn/en didaktisch auf. Die Themenvergabe findet am Ende der zweiten Einheit statt. Folgende Themenvorschläge stehen zur Auswahl:	
1. Erklärungskompetenz mit Animationen	
Es gibt am Markt eine Vielzahl an Produkten, mit denen kleine Lernclips erstellt werden können, die versuchen einen Sachverhalt (hier aus dem wirtschaftlichen Bereich) zu erklären. Ausgehend von einer kurzen Beschreibung der theoretischen Grundlagen (Erklärungskompetenz, Lerntheorie) erstellen Sie ein Drehbuch für die Beschreibung eines wirtschaftlichen Sachverhalts und setzen diesen in einer ersten Version um. In der Lehrveranstaltung geben Sie Ihren Kolleg/innen eine kurze Einführung in eines dieser Animationsprogramme.	
2. Datensicherheit und Datenschutz	
Sie bereiten die Lehrinhalte des Moduls 9 (im Wesentlichen auch Security und Internet aus HAK III) für Ihre Kolleg/inn/en in einem kleinen Skriptum auf und entwickeln exemplarisch didaktische Szenarien, von denen Sie ausgewählte im Rahmen Ihrer Projektpräsentation mit den Kolleg/inn/en ausprobieren können. Der Themenbereich umfasst im Wesentlichen: Datenverlust und Computerviren, Datensicherung, Passwörter, Kryptografie und digitale Signatur und Biometrie und ggf. Firewalls.	
3. Open-Source Office im Unterricht	
Open-Source Software stellt nach unterschiedlichen Aussagen eine reale Alternative zu proprietären Software-Produkten dar. Im Rahmen dieses Projekts analysieren Sie ein Open-Source-Office-Paket für die Eignung für den Unterricht im HAK 2014-Modul 5. Sie Entwickeln ein Skriptum mit allen relevanten Informationen und entwickeln Unterrichtsmaterialien für ausgewählte Themen mit Praxisbeispielen im Umfang von ca. 3 Schulstunden und setzen diese im Lernmanagementsystem MOODLE um.	
4. Datenanalyse und -aufbereitung mit PowerBI	
Das Programm Microsoft PowerBI (www.powerbi.com) erlaubt die einfache Erstellung von Dashboards für die Darstellung umfangreichen Datenmaterials auf Landkarten, in Grafiken und Zeitlinien in Kombination mit statischen und dynamischen Filtern (Stichwort BigData). In einem Skriptum stellen Sie zunächst die Funktionalitäten vor und gestalten auf dieser Basis exemplarisch drei Unterrichtseinheiten (à 50 Minuten) mit Praxisbeispielen für die Zielgruppe betriebliche Weiterbildung (EV: Gute Excel und Access-Kenntnisse).	
5. MS PowerQuery in Excel 2016	
In Excel 2016 wurde mit Power Query eine neue Schnittstelle geschaffen, die es ermöglicht, eine Vielzahl an Daten direkt in einem einzigen Tool zu importieren, nachzubearbeiten und daraus Abfragen/Importe zu erstellen. Sie erstellen eine Kurzeinführung in die relevantesten Funktionen anhand praxisnaher Beispiele und demonstrieren exemplarisch, wie betriebswirtschaftliche Anwendungsbeispiele (zB: ABC/XYZ-Analyse, Berechnung von Kennzahlen, Finanzierung) unter Zuhilfenahme dieses Tools gelöst werden können.	
Sie vereinbaren rechtzeitig mit dem LV-Leiter bitte einen Coaching-Termin spätestens Ende November, wo Sie Ihre ersten Überlegungen vorstellen, sich Anregungen holen und offene Fragen klären, bevor Sie mit der konkreten didaktischen Umsetzung starten!	

2.2 Beurteilungskriterien

Note	Prozent
Sehr Gut	$\geq 90\%$
Gut	$\geq 80\%$
Befriedigend	$\geq 65\%$
Genügend	$\geq 51\%$
Nicht Genügend	$> 51\%$

3 Hardware

In dieser Lehrveranstaltungseinheit beschäftigen wir uns mit dem grundlegenden Aufbau von Computersystemen und ihren Bestandteilen. Zu Beginn werden die grundlegende Struktur und das Zusammenwirken unterschiedlichster Bauteile von Computern beschrieben, bevor die Element der Zentraleinheit sowie Peripheriegeräte vorgestellt werden.

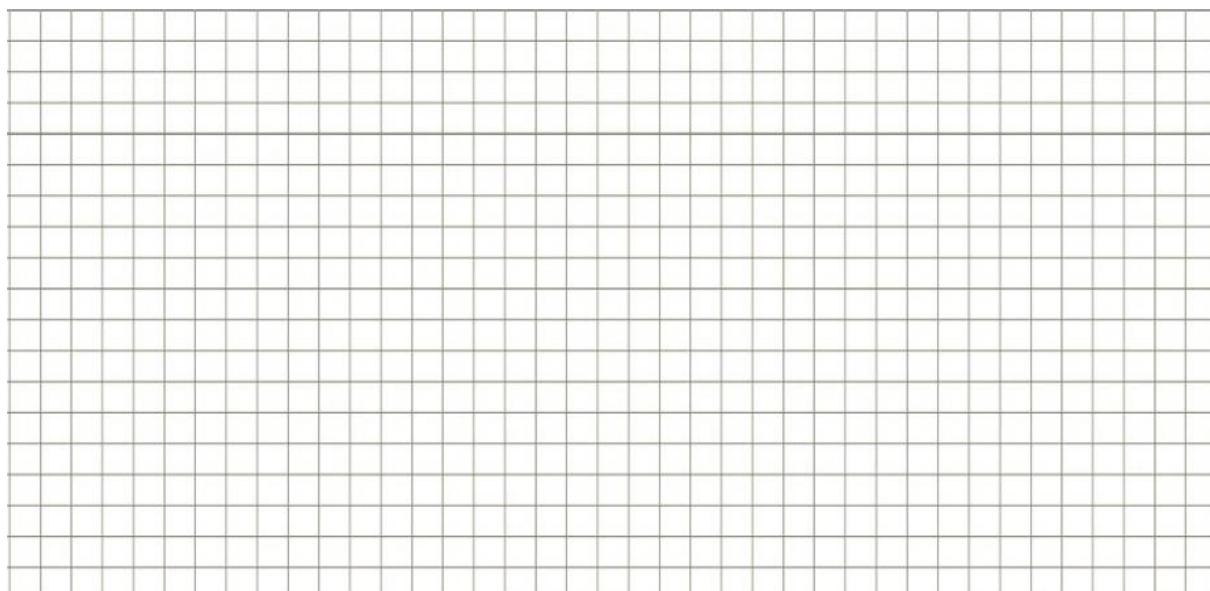
Grundsätzlich setzt sich Hardware aus der Zentraleinheit und der Peripherie zusammen. Die Zentraleinheit umfasst die „lebensnotwendigen“ Bestandteile eines Computers wie den Prozessor, den Arbeitsspeicher, die Anschlüsse und das BIOS (Basic Input Output System), die gemeinsam erst einen Betrieb des Geräts ermöglichen. Unter Betrieb wird in diesem Fall die Verarbeitung von Daten verstanden.

In der Datenverarbeitung wird die Einteilung zwischen den zentralen Bestandteilen und Peripheriegeräten oft mit dem **EVA-Prinzip** beschrieben. Ähnlich wie der Computer arbeitet auch der Mensch nach dem Prinzip der **Eingabe-Verarbeitung-Ausgabe** (EVA):



	EINGABE (I)	VERARBEITUNG	AUSGABE (O)
MENSCH	Augen (Lesen) Ohren (Hören)	Gehirn (Ordnen, Prüfen, Vergleichen, Speichern)	Hände (Schreiben) Mund (Sprechen) Füße (Laufen)
COMPUTER	Tastatur Maus Scanner Mikrofon Touchpanel Festplatte (I/O) usw.	Zentraleinheit (Prozessor, Arbeitsspeicher, I/O-Schnittstellen)	Monitor Drucker Lautsprecher Festplatte (I/O) usw.

Die Eingabe (I=Input) und Ausgabe (O=Output) erfolgt über I/O-Controller oder über I/O-Prozessoren. Diese leiten die Daten zur Verarbeitung an die Zentraleinheit weiter und dienen auch der Weiterleitung von Daten aus der Zentraleinheit an diverse Ausgabegeräte. Diese Kommunikation wird in der Regel von einem Betriebssystem gesteuert, da es den Systembus (der Datenfluss zur und vom Prozessor) und die Gerätetreiber verwaltet. Da sich diese Komponenten (Eingabe, Ausgabe als auch die Elemente der Zentraleinheit) in ihrer Architektur oder in ihren Protokollen und Standards stark unterscheiden können, ist nicht jedes Hardwareelement mit einem anderen kompatibel.



3.1 Arten von Rechnern

In der heutigen technologisch hochgerüsteten Informationsgesellschaft ist die Übersetzung des Begriffs Computer mit Rechner oder Personal Computer (PC) kaum mehr wirklich auf einen speziellen Gerätetypus zutreffend. Zu sehr hat die Miniaturisierung dazu geführt, dass in vielen Geräten wie Smartphones, Videokameras, Fotoapparaten und sogar in Waschmaschinen oder Kühlschränken bereits Mikroprozessoren und sogar I/O-Schnittstellen und Peripheriegeräte wie Monitore oder Netzwerkanschlüsse integriert sind.

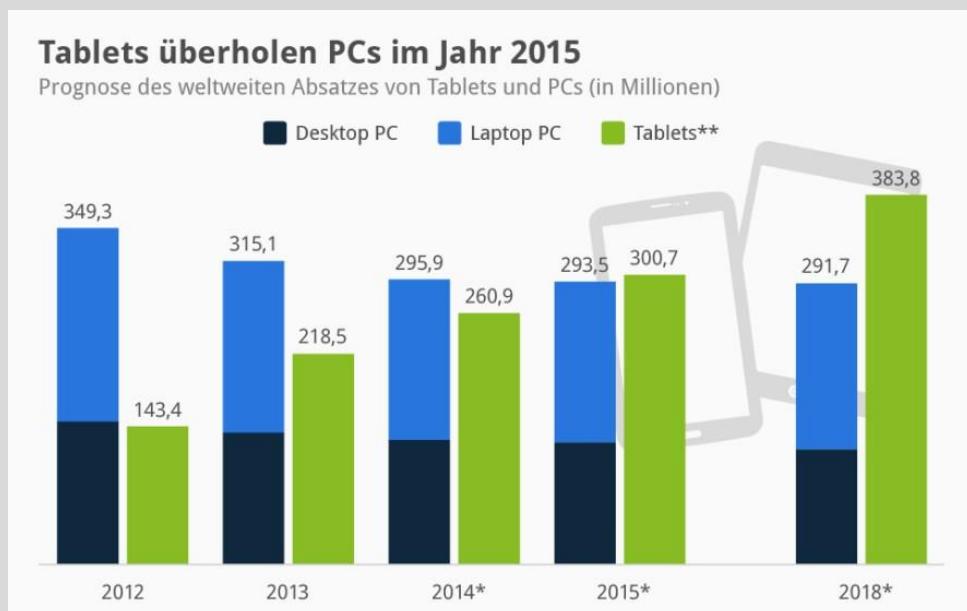
Nachfolgend sind einige Geräte angeführt, die man gemeinläufig unter „Computer“ subsumieren kann:



Tablet-Verkäufe werden PC-Absatz 2015 überholen (Infografik)

Statista hat aktuell wieder eine interessante Infografik veröffentlicht, die einen Ausblick darauf gibt, wie sich die Verkäufe von PCs und Tablets in Zukunft verändern könnten.

Die Daten stammen dabei vom IDC, gegenübergestellt werden die Verkäufe von Tablets und klassischen PCs in den letzten Jahren. Diese Gegenüberstellung zeigt, dass die PC- und Laptop-Verkäufe in den letzten Jahren stetig nach unten gingen, während der Absatz von Tablets die entgegengesetzte Richtung nahm. 2013 ging der Absatz von PCs und Laptops beispielsweise um zehn Prozent zurück.



Aufgrund dieser Daten prognostiziert die IDC darüber hinaus, dass Tablet-Verkäufe (zu denen die IDC auch Hybrid-Geräte, wie das Surface RT, zählt) die von PCs und Laptops im Jahr 2015 erstmals überholen werden. Dann werden die Hersteller voraussichtlich 300 Millionen Tablets verkaufen, während der PC-Markt 294 Millionen abgesetzte Geräte verzeichnen wird.

Ich persönlich kann mir das durchaus sehr gut vorstellen, schon heute kenne ich überraschend viele, denen ein gutes Tablet ausreicht. Darüber hinaus sind Tablets wohl auch eher Geräte, die man jährlich durch neue Geräte ersetzt, während das bei Notebooks und PCs eher nicht der Fall ist. PCs und Notebooks werden zwar natürlich nicht von der Bildfläche verschwinden (immerhin benötigen z.B. Content-Ersteller jeglicher Art die Vorteile dieser Geräte), für einen Großteil der Nutzer werden die immer besser werdenden Tablets aber wohl immer mehr ausreichen. Was meint ihr zu dieser Grafik und zu der prognostizierten Entwicklung?

2013 ging der Absatz hier um rund 10 Prozent zurück. Ein Trend der sich weiter fortsetzen wird. Laut Prognose werden sich die Flachrechner 2015 erstmals besser verkaufen als Desktop-PCs und Laptops. Über 300 Millionen iPads und Android-Tablets werden die Hersteller dann absetzen können gegenüber 294 Millionen PCs.

Quelle: <https://www.mobiflip.de/tablet-verkaeufe-werden-pc-absatz-2015-ueberholen-infografik/>

Trendwende im PC-Markt

13.07.2018 18:33 Uhr Christian Hirsch

Erstmals seit Anfang 2012 nahm die Zahl der weltweit verkauften Rechner wieder zu. Das liegt unter anderem am Umstieg von Unternehmen auf Windows 10.

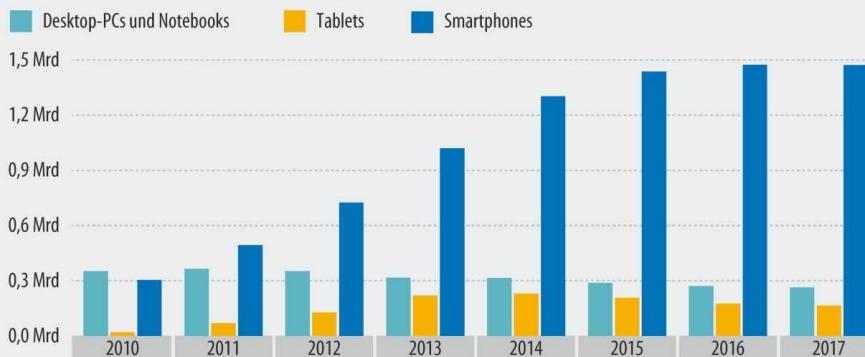


Im zweiten Quartal 2018 konnten die PC-Hersteller nach Angaben der Marktforscher von Gartner und IDC 1,4 beziehungsweise 2,7 Prozent mehr Desktop-Rechner, Notebooks und Workstations verkaufen als im Vorjahreszeitraum. Damit ist der seit Anfang 2012 anhaltende Abwärtstrend [1] gestoppt. Insgesamt fanden von April bis Juni 2018 weltweit rund 62 Millionen neue PCs einen Abnehmer.

Die gestiegene Nachfrage erzeugen vor allem Unternehmen, die anderthalb Jahre vor dem Support-Ende von Windows 7 [2] ihre vorhandenen Geräte durch aktuelle Desktop-PCs und Notebooks mit Windows 10 ersetzen. Der Absatz wuchs gleichermaßen bei preiswerten Rechnern mit Chrome OS wie bei teuren Premium-Notebooks. Private Käufer interessierten sich nach den überwundenen Lieferengpässen und dem folgenden Preisrutsch bei Grafikkarten vor allem für Gaming-PCs. Die zum Jahresanfang bekannt gewordenen Sicherheitslücken in Prozessoren Meltdown und Spectre [3] scheinen keinen Einfluss auf das Kaufverhalten zu haben.

Verkaufszahlen

Die PC- und Notebookverkäufe stabilisieren sich langsam nach den hohen Rückgängen der letzten Jahre. Zudem stagniert der Smartphone-Absatz – allerdings auf sehr hohem Niveau.



In der Region Europa, Naher Osten und Africa (EMEA) wurden laut Gartner 17,4 Millionen Rechner verkauft, wobei in Deutschland vor allem Business-PCs gefragt waren. Trotz des Trends zu Mobilgeräten spielten Desktop-PCs hier eine wichtige Rolle bei den Zuwächsen.

Kopf-an-Kopf-Rennen zwischen HP und Lenovo

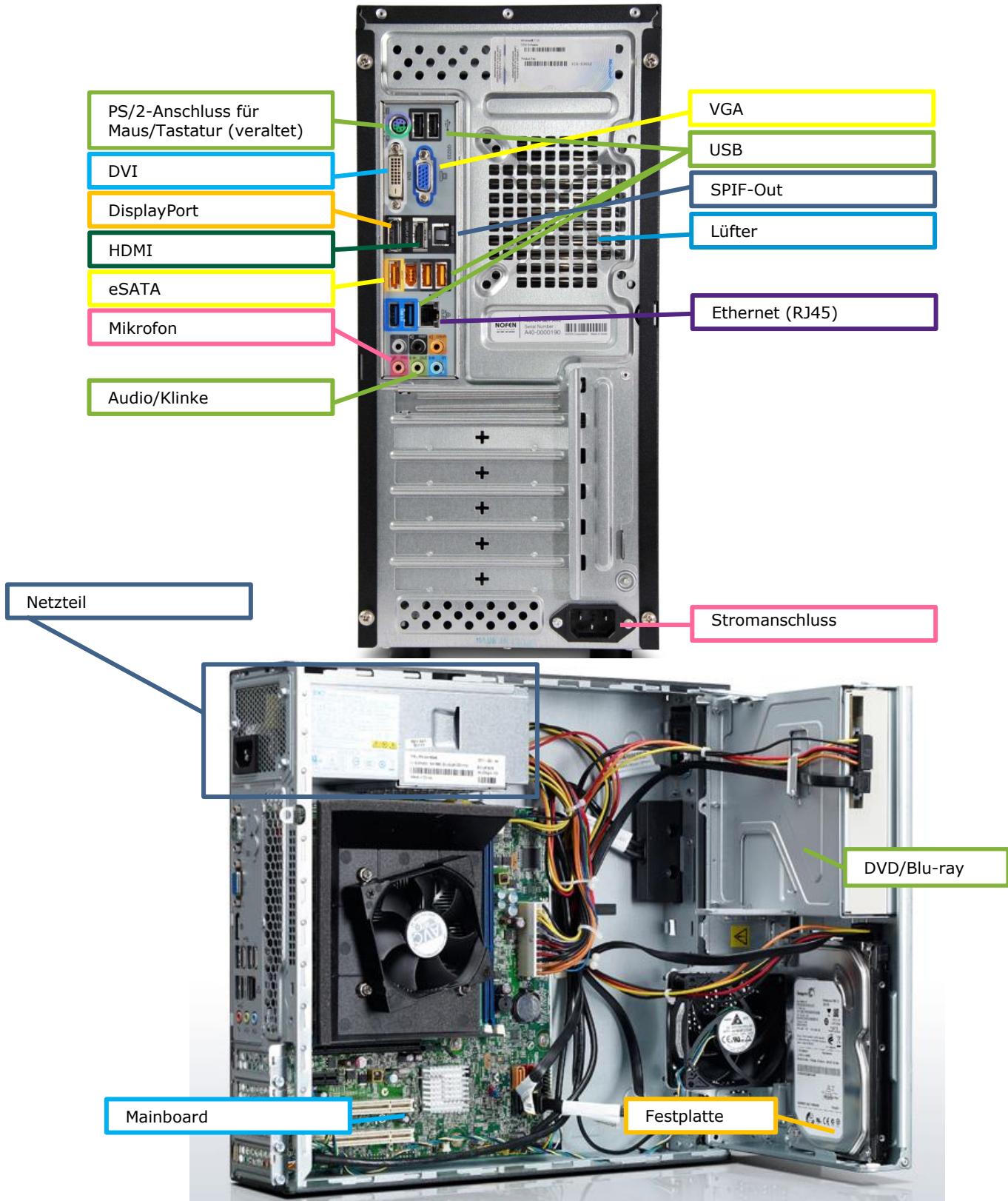
Mit je 21,9 Prozent Marktanteil und je 13,6 Millionen verkauften Rechnern liefern sich Lenovo und HP nach den Angaben von Gartner einen Zweikampf um Platz 1. IDC zählt etwas anders und sieht HP mit 23,9 Prozent knapp vor Lenovo (22,1 Prozent). Hinter Dell auf dem dritten Platz folgen nach Stückzahlen gerechnet mit größerem Abstand Apple und Acer.

Die Marktkonzentration nimmt weiterhin zu: Die Top-5-Hersteller machen inzwischen 78 Prozent der PC-Verkäufe unter sich aus. Die verbleibenden PC-Hersteller haben unterdessen im Vergleich zum Vorjahr mit Rückgängen von 12,9 (Gartner) beziehungsweise 7,3 Prozent zu kämpfen.

Quelle: <https://www.heise.de/newsticker/meldung/Trendwende-im-PC-Markt-4110128.html?view=print>

3.2 Aufbau eines Desktop PCs

Ein klassischer Desktop PC ist in ein Gehäuse mit einem bestimmten Formfaktor eingepasst. Dieses lässt sich meist seitlich durch einen Hebel und ggf. dem Lösen einiger Schrauben leicht öffnen. Die beiden Abbildungen zeigen die wichtigsten Komponenten und Anschlüsse eines PCs.



3.3 Mainboard

Das Mainboard (auch Motherboard bzw. Hauptplatine) ist das Kernstück eines jeden Computers. Sie dient mit ihren Steckplätzen, Schnittstellen und ihrer integrierten Firmware, die sich auf dem BIOS-Chip befindet, als „Heimat“ für alle anderen Komponenten des PCs.

Bei der Auswahl eines Mainboards sind zwei wesentliche Faktoren bei der Kaufentscheidung zu berücksichtigen:

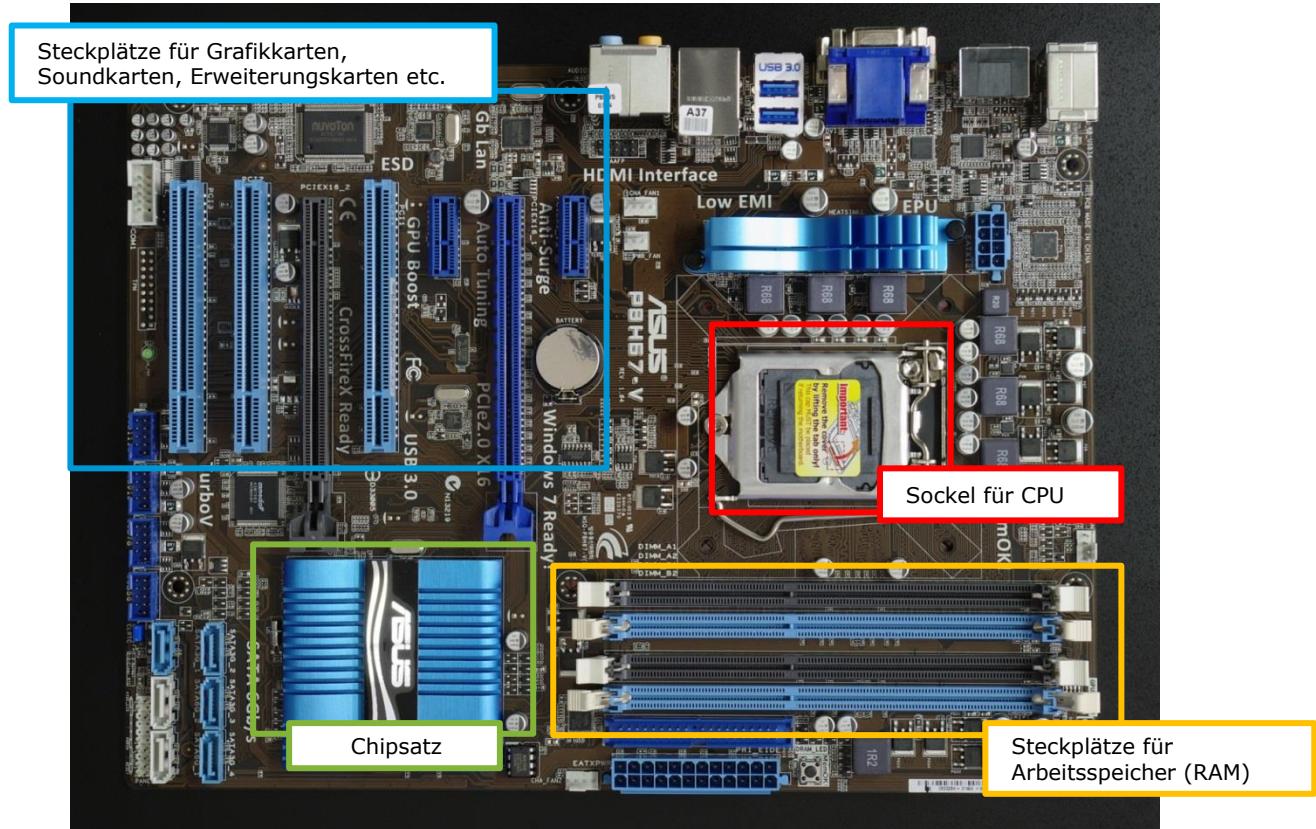
- Der **Formfaktor** des Gehäuses, in das es eingebaut werden soll (zB: ATX, MicroATX etc.)
- Der Typ des **Sockels**, auf dem die CPU (Prozessor) platziert werden soll (zB: Intel Sockel 2011-3, AMD Sockel AM3+ etc.) bzw. korrekter der **Chipsatz** auf dem Mainboard.

Man muss daher schon beim Kauf eines Mainboards ganz genau wissen, welchen Prozessortyp man in seinem PC einbauen möchte. Später kann man nur einen neuen Prozessor mit der gleichen Bauart einbauen. Adapter zum Platzieren eines anderen Prozessors auf dem Mainboard gibt es nicht, da es in seiner Gesamtheit genau auf diese eine Prozessorarchitektur abgestimmt ist.

Eine Suche bei <http://geizhals.at/?o=9> ordnet Ihnen alle verfügbaren Mainboards zum Beispiel gleich nach dem Sockel der CPU:

Subkategorien in Mainboards:		
Intel Sockel 1150	Intel Sockel 2011-3	Intel Sockel 2011
Z97, ATX, µATX, ASUS, Mini-ITX, H97, 4x DDR3, Gigabyte ...	ASUS, 8x DDR4, ATX, µATX, Gigabyte, ASRock, M.2 32Gb/s, E-ATX (SSI EEB) ...	ASUS, ATX, µATX, Gigabyte, 8x DDR3, ASRock, E-ATX (SSI EEB), MSI ...
Intel Sockel 1155	Intel Sockel 1366	Intel Sockel 1156
Z77, µATX, Mini-ITX, 4x DDR3, ATX, ASUS, ASRock, Gigabyte ...	ASUS, 6x DDR3, Gigabyte, 7.1, Intel, X58, ab 2x, ab 1x ...	Gigabyte, 4x DDR3, P55, µATX, Mini-ITX, ASUS, ab 2009, Intel ...

Der **Chipsatz** (eng. chipset) auf dem Mainboard ist der wesentlichste Helfer des Prozessors. Er stellt die Kommunikation zwischen den diversen Bussen (Arbeitsspeicher, Grafikkarte etc) und den Input/Output-Controllern (IDE, SATA, USB, Ethernet etc) mit dem Prozessor sicher und sorgt somit dafür, dass die Daten gezielt und schnell weiterverarbeitet werden können.

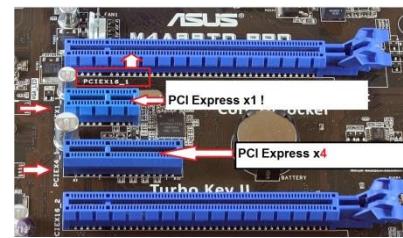


Wesentliche Faktoren beim Kauf eines Mainboards sind neben der indirekten Wahl für den Prozessor auch die Anzahl und die Typen der unterschiedlichen Anschluss- und Erweiterungsbereiche. Dabei sollte man vor allem folgendes beachten:

3.3.1 PCI Express (PCIe)

PCIe verbindet interne Peripheriegeräte – wie zum Beispiel Grafikkarten, Steuerungskarten, Videoschnittkarten, Soundkarten etc. – mit dem Chipsatz eines Prozessors. PCIe wurde 2003 eingeführt und liegt momentan in der Version PCIe 3.0 vor.

Der Standard schafft eine sehr hohe Übertragungsrate von bis zu 15.754 MB/s (PCIe 3.0 x16), was vor allem bei durchsatzintensiven Anwendungen wie Spiele oder Videoschnitt/Rendering etc. notwendig ist. Da es relativ viele (Unter)Versionen von PCIe gibt, empfiehlt es sich, zuerst im Handbuch des Mainboards nachzusehen, welche Anschlüsse sich nach welchem Standard darauf befinden und erst danach ein entsprechendes Peripheriegerät (zB: Grafikkarte) zu kaufen.



PCIe 2.0 kann über eine 32 Bit breite Verbindung (Lane) pro Taktzyklus 500 MB/s senden und empfangen. Durch die Verwendung mehrere Lanes kann diese Verbindungsbreite erhöht werden. Dadurch können pro Taktzyklus bei PCIe 2.0 mit 8 Lanes 4000 MB/s übertragen werden. Je nach Standard (1.0, 2.0, 3.0, 4.0, 5.0) werden durch unterschiedliche Taktungen unterschiedliche Übertragungsraten erreicht:

	PCIe 1.0/1.1	PCIe 2.0/2.1	PCIe 3.0	PCIe 4.0	PCIe 5.0
Erschienen	2003	2007	2012	2017	2019
Taktrate	1,25 GHz	2,5 GHz	4,0 GHz	8,0 GHz	16,0 GHz
Lanes (Breite)	X1	250 MB/s	500 MB/s	985 MB/s	1969 MB/s
	X2	500 MB/s	1000 MB/s	1969 MB/s	3938 MB/s
	X4	1000 MB/s	2000 MB/s	3938 MB/s	7877 MB/s
	X8	2000 MB/s	4000 MB/s	7877 MB/s	15752 MB/s
	X16	4000 MB/s	8000 MB/s	15754 MB/s	31504 MB/s

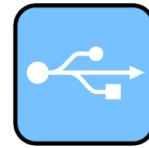
Auf vielen Mainboards finden sich aufgrund der Kompatibilitätsproblematik unterschiedliche PCIe-Steckplätze. Das wird dann meist wie folgt angegeben:

Erweiterungsslots: 4x PCIe 3.0 x16 (2x x16, 2x x8), 3x PCIe 2.0 x1

Das bedeutet, dass hier 2 PCIe 3.0 x16, 2 PCIe 3.0 x8 und 3 PCIe 2.0 x1-Anschlüsse auf dem Mainboard verbaut sind (insgesamt also 7 Anschlüsse mit drei unterschiedlichen Standards).

3.3.1.1 USB

USB (Universal Serial Bus) dient dazu, Daten (und Energie) zwischen Computerbestandteilen oder innerhalb eines Computers zu übertragen. Ein USB-Bus ist im Wesentlichen wie ein Netzwerk innerhalb des PCs aufgebaut. Der USB-Controller (meist auf dem Mainboard fest verbaut) sorgt dafür, dass die Datenpakete zwischen den Peripheriegeräten richtig und schnell verteilt werden.



Je mehr Anschlüsse auf dem Mainboard zur Verfügung stehen, desto besser. Gängige Mainboards haben bis zu 8 Anschlüsse. Sollten die Anschlüsse nicht ausreichen, muss zusätzlich ein USB-Hub erworben und an einen freien USB-Anschluss angedockt werden.

Eine wichtige Entscheidung ist, welcher Standard unterstützt wird. Gängig sind derzeit USB 2.0 (aus dem Jahr 2000) und USB 3.0 (aus dem Jahr 2008). Dabei gibt es vorwiegend die folgenden Unterschiede:

- USB 3.0 überträgt Daten mit 4,8 GBit/s bis zu 10x schneller als USB 2.0 mit 480 MBit/s. Das bedeutet, dass USB 2.0 theoretisch 60 MB pro Sekunde von einem USB-Stick auf die interne Festplatte kopieren kann. USB 3.0 schafft in der gleichen Zeit 600 MB (also eine ganze CD-ROM).
- USB 3.0 unterstützt im Gegensatz zu USB 2.0 Vollduplex. Das heißt, dass Daten in beide Richtungen gleichzeitig übertragen werden können. Halbduplex (USB 2.0) bedeutet, dass Daten zwar in beide Richtungen fließen können, jedoch nicht gleichzeitig (ähnlich dem Taxi-Funk).
- Die maximale Stromstärke beträgt bei USB 3.0 900 mA¹, bei USB 2.0 waren das noch 500 mA. An USB 3.0 können daher leistungsfähige externe Festplatten ohne zusätzliche Stromversorgung angeschlossen werden.
- USB 3.0-Kabel sind maximal 3 Meter lang. USB 2.0 Kabel können bis zu 5 Meter lang sein.
- USB 3.0 ist abwärtskompatibel. Ein USB 2.0-Stick funktioniert auch an einem USB 3.0-Port, jedoch nicht zwingend schneller. Ein USB 3.0-Stick funktioniert auch auf einem USB 2.0-Port jedoch langsamer.
- Unterschiede gibt es jedoch bei den Kabel Mini und Micro; diese sind zwar abwärtskompatibel, USB 3.0-Geräte können aber nicht mehr an USB 2.0-Ports betrieben werden.
- USB 3.0-Ports sind genormt in blauer Farbe zu halten.

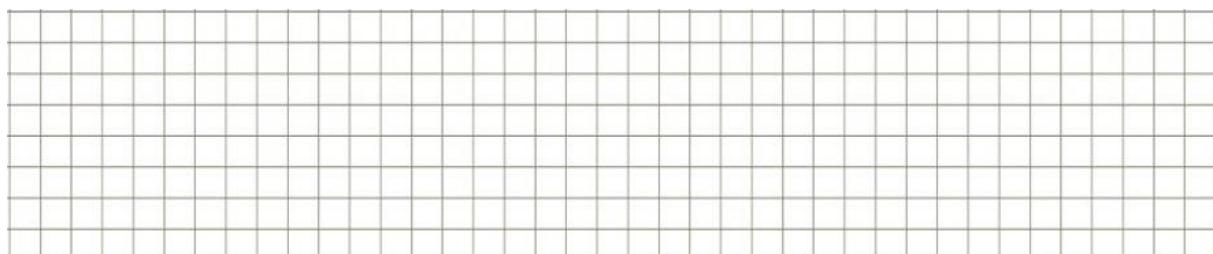


Mittlerweile liegt der Standard USB 3.1 vor, der einen Datentransfer von ca. 10 GBit/s (900 MB/s) ermöglicht und theoretisch wiederum einen doppelt so hohen Datendurchsatz schafft wie der Standard 3.0. Außerdem schafft der neue Standard eine Stromversorgung von bis zu 100 Watt, weshalb auch größere externe Geräte mit Strom versorgt werden können.

AN OVERVIEW OF
USB-C™



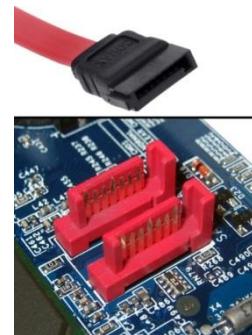
Als Stecker-Verbindung liegt als neuer Standard USB C vor, der auf den Parametern von USB 3.1 basiert, die Steckrichtung jedoch obsolet macht.



¹ mA=Milliampere; Ampere (Stromstärke) ergibt sich durch Watt (Leistung): Volt (Spannung). Ein Gerät mit 50 Watt Leistungsaufnahme bei einer Spannung von 12 V benötigt daher rund 4,17 Ampere.

3.3.1.2 SATA und eSATA

An SATA-Anschlüssen (Serial Advanced Technology Attachment) werden vorwiegend Festplatten aber auch optische Laufwerke oder Bandlaufwerke angeschlossen. SATA sorgt vorwiegend für den schnellen Datenaustausch zwischen der Festplatte und dem Prozessor. Je mehr SATA-Anschlüsse das Mainboard aufweist, desto besser, da in diesem Fall mehr Geräte angeschlossen werden können. Auch bei diesem Anschlusstyp gibt es wiederum mehrere Generationen, die jedoch abwärtskompatibel sind. Während SATA I eine Übertragungsrate von theoretisch 1,2 Gbit/s aufweist, schafft SATA II 3 Gbit/s und SATA III gar 6 Gbit/s.



Externer Anschluss

SATA ist eine interne Anschlussart. Die Form des Steckers hat eine L-Form. Ein neuerer Anschlusstyp ist eSATA (external SATA). Dieser erlaubt den Anschluss von SATA-Geräten extern am Gehäuse, ähnlich wie zB: USB.

Damit interne Geräte (die meist nicht speziell geschirmt sind) nicht versehentlich extern angeschlossen werden, hat eSATA einen geraden Anschlusstyp mit tiefer sitzenden Kontakten. Eine interne SATA-Platte kann daher nicht an einem eSATA-Port angeschlossen werden!



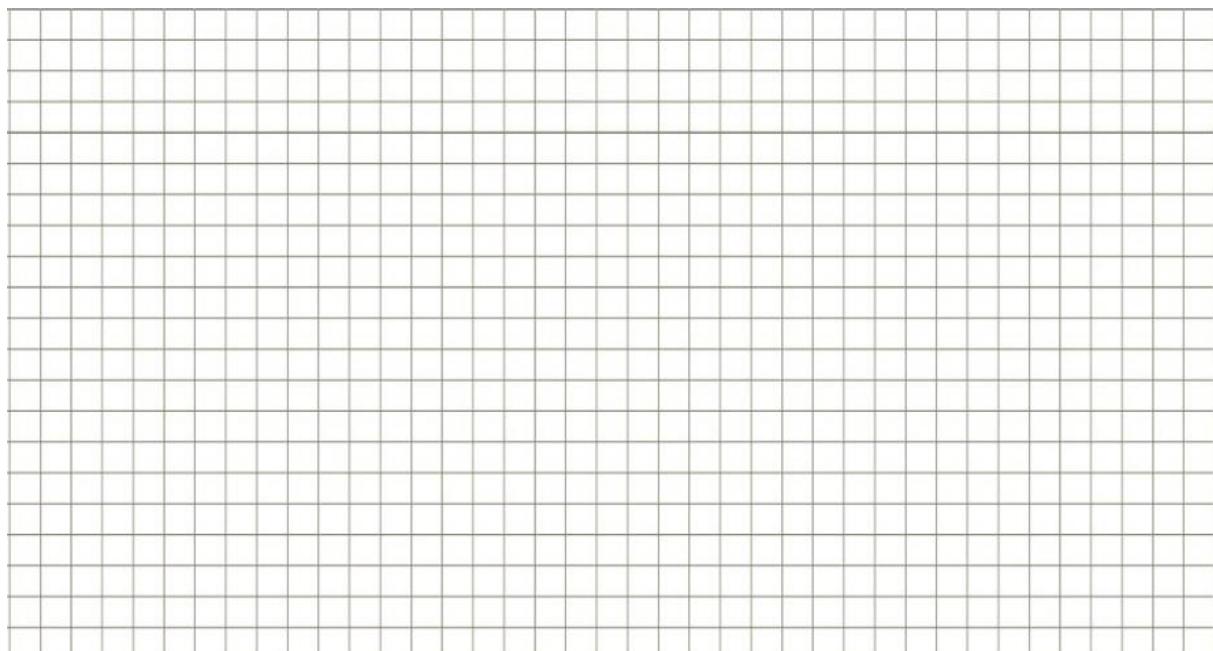
SATA als Steckkarte

Für mobile Geräte wie Laptops und Tablets gibt es mittlerweile auch eine mini-SATA (mSATA) sowie eine micro-SATA Version. Diese verwenden entweder die Revision I (1,5 Gbit/s), II (3,0 Gbit/s) oder III (6,0 Gbit/s).



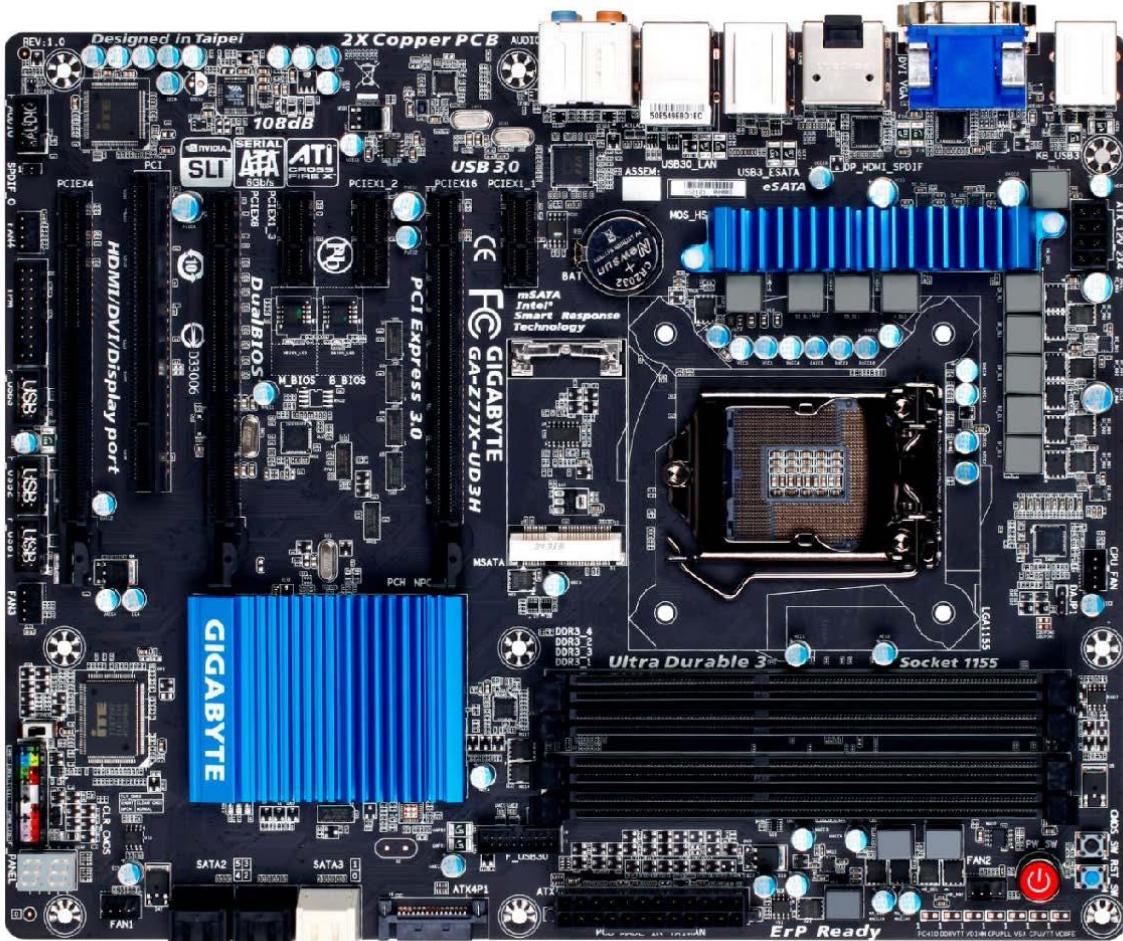
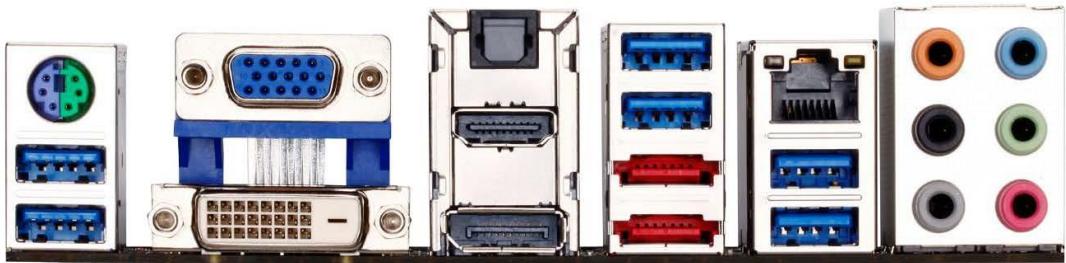
3.3.1.3 Weitere Peripherie

Typischerweise ist auf dem Laufwerk auch eine Soundkarte mit zumindest analogen Klinken (für Mikrofon und Lautsprecher) oder ein **SPDIF-Anschluss** (optisches Lautsprecherkabel) integriert. Außerdem sollte eine GB-LAN (1000 MB/s)-**Netzwerkkarte** integriert sein. Wenn mit dem PC nicht exzessiv gespielt werden soll, reicht die meistens bereits verbaute Grafikkarte vollends aus. Gängige **Grafikkartenanschlüsse** (HDMI, DisplayPort ggf. DVI oder VGA) sollten vorhanden sein.



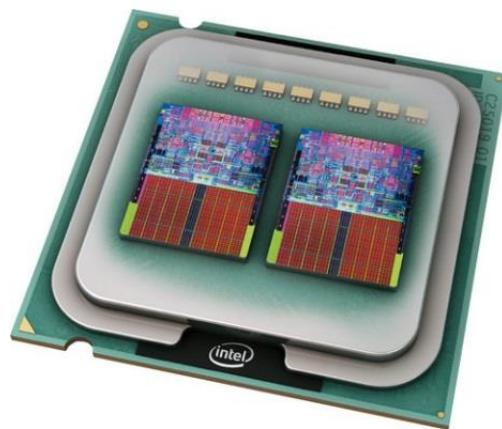
Aufgabenstellung

Formfaktor: ATX • 1 Chipsatz: Intel Z77 • 2 RAM: 4x DDR3 DIMM, dual PC3-22400U/DDR3-2800 (OC), max. 32GB (UDIMM) • Erweiterungsslots: 3 2x PCIe 3.0 x16 (1x x16, 1x x8), 4 1x PCIe 2.0 x16 (x4), 5 3x PCIe 2.0 x1, 1x PCI • Anschlüsse extern: 6 1x VGA, 7 1x DVI-D, 8 1x HDMI 1.4, 9 1x DisplayPort 1.1, 10 6x USB-A 3.0 (Z77/VIA VL800), 11 2x eSATA 6Gb/s (88SE9172), 12 1x Gb LAN (Atheros), 13 6x Klinke, 1x S/PDIF (optisch), 14 1x PS/2 Combo • Anschlüsse intern: 15 2x USB 3.0 (Z77), 16 6x USB 2.0, 17 2x SATA 6Gb/s (Z77), 18 4x SATA 3Gb/s (Z77), 19 1x mSATA 3Gb/s (Z77), 20 1x CPU-Lüfter 4-Pin, 21 4x Lüfter 4-Pin • 22 Audio: 7.1 (VIA VT2021) • RAID-Level: 0/1/5/10 (Z77), 0/1 (88SE9172) • Multi-GPU: NVIDIA 2-Way-SLI (x8/x8), AMD 2-Way-CrossFireX (x8/x8), Lucidlogix Virtu MVP • 23 Stromanschlüsse: 1x 24-Pin ATX, 24 1x 8-Pin EPS12V • Grafik: IGP (via CPU/APU)



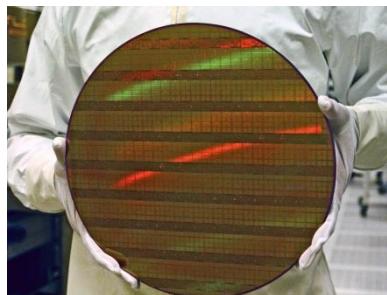
3.4 Prozessor (CPU)

Der Prozessor (Mikroprozessor, CPU=Central Processing Unit) ist das Herz eines Computers. Es ist für die Ausführung der Programme und für die zentrale Steuerung und Verwaltung der Hardware zuständig. Typischerweise befindet sich in einem Rechner nur ein Prozessor. Viele neue Prozessoren haben jedoch zwei, vier, sechs oder sogar acht Kerne. Der Vorteil davon ist, dass diese parallel zueinander rechnen können und somit (bei entsprechender Programmierung) Multitasking-Anwendungen unterstützt werden.

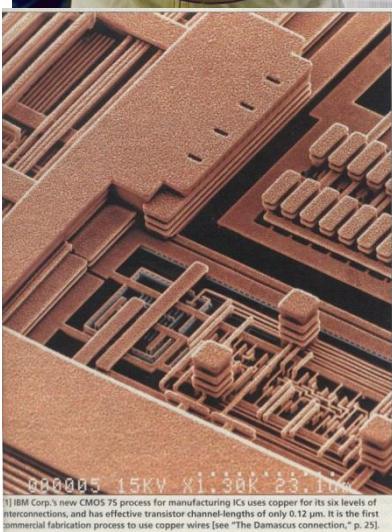


3.4.1 Architektur eines Prozessors

Mikroprozessoren sind nichts Anderes als Schaltkreise, die aus mehreren Millionen Transistoren bestehen. So bestehen neuere Intel Core i7-Prozessoren aus über 2.000.000.000 Transistoren, die jeweils die Werte 0 oder 1 annehmen können.



Heutzutage werden Chips auf Silizium-Wafer durch spezielle Verfahren (fotolithografisch) aufgebracht. Dies geschieht einerseits durch Diffusion (Das Silizium wird mit Bor und Phosphor versetzt), Metallisierung (Aufdampfen von leitfähigem Aluminium oder Kupfer) und dem Aufdampfen von Chrom/Kupfer/Gold-Legierungen als Leiterbahnen gefertigt.

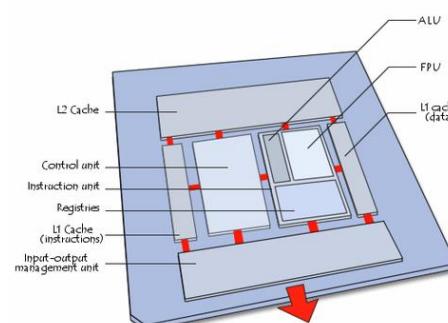


Ein typischer Prozessor besteht aus den folgenden Bestandteilen:

Die **ALU** (Arithmetisch-logische Einheit) ist das Rechenwerk. Es führt mathematische Operationen und logische Verknüpfungen durch. Diese Rechenwerke können heutzutage sowohl Ganzahlberechnungen als auch Fließkommaoperationen berechnen (Floating Point Unit = FPU).

Mit dem **Register** verfügt der Prozessor über spezifische Speicherstellen, wo Werte für die aktuelle Berechnung zwischengelagert werden. Dieser Register wird von der ALU verwendet.

Das **Steuerwerk** (Control Unit) Das Steuerwerk gibt nicht nur an, welcher Rechenbefehl ausgeführt werden soll sondern auch, welche Register ausgelesen oder geschrieben werden sollen (Stack Pointer). Heutzutage sind viele Befehle bereits auf Prozessorebene verankert und Steuerwerke daher weitaus komplexer und nicht mehr rein linear und somit (je nach nachzuvollziehen).



Busse (Datenleitungen)
Über den Datenbus
Arbeitsspeicher
überträgt die
(wo werden die Daten
Steuerbus ist für die
Peripherieanschlüssen

Architektur) kompliziert

Prozessoren sind über spezielle mit der Außenwelt verbunden. werden Dateninhalte mit dem ausgetauscht. Der Adressbus zugehörigen Speicheradressen hin geliefert) und der Ansteuerung von (PCIe, USB etc.) zuständig.

Ganz wesentlich für die Prozessoren sind die sogenannten **Caches**. Das sind extrem schnelle Zwischenspeicher (weit

Leistungsfähigkeit eines

schneller als der Arbeitsspeicher), in dem Befehle oder Daten zwischengespeichert werden, die bald wieder benötigt werden.

Der **Level1-Cache** ist in der Regel sehr klein und unmittelbar im Prozessorkern untergebracht. Er wird daher mit derselben Taktrate wie der Prozessor selbst betrieben. In diesem schnellen Speicher werden Daten für kurze Schleifen bzw. wenige Befehle abgelegt. Bei aktuellen Prozessoren (zB: Intel i7) hat jeder Kern einen L1-Cache von 64 KByte.

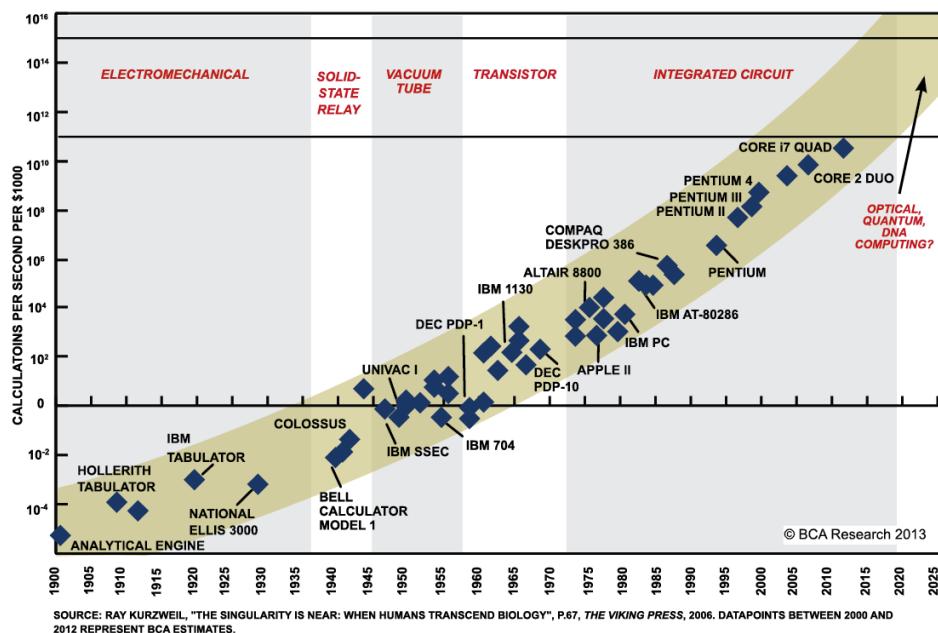
Der **Level2-Cache** beträgt meist ca. 256 KByte pro Kern. Er wird mit einer geringeren Taktrate wie der Prozessor betrieben aber noch immer weitaus schneller als der Arbeitsspeicher. Generell gilt: Je höher der Cache, desto teurer der Prozessor und desto höher der Stromverbrauch.

Manche Prozessoren haben einen Level3-Cache, der wiederum etwas langsamer ist als der L2-Cache. Alle weiteren Daten werden dann im Arbeitsspeicher abgelegt. Dieser ist wiederum viel schneller als die Festplatte und wird meist mit einer Taktfrequenz von über 2000 MHz betrieben. Reicht dieser Speicher ebenfalls nicht mehr aus, werden Daten in einer **Auslagerungsdatei** (SWAP-File oder PAGE-File) auf der Festplatte ausgelagert (unter Windows ist das die Datei pagefile.sys).

Die Größe dieser Auslagerungsdatei wird vom Betriebssystem selbst verwaltet. Man kann die Größe dieses virtuellen Speichers aber auch selbst definieren. Dafür sucht man am besten in der *Systemsteuerung* nach „Erweiterte Systemeinstellungen anzeigen“. Im Dialogfeld Systemeigenschaften klickt man im Register *Erweitert* auf die Schaltfläche *Einstellungen* im Bereich *Leistung*. Im Dialogfeld *Leistungsoptionen* wechselt man wieder in die Registerkarte *Erweitert* und kann dann im Bereich *Virtueller Arbeitsspeicher* die Gesamtgröße der Auslagerungsdatei ändern.

3.4.2 Leistungsmerkmale eines Prozessors

Nach dem **Mooreschen Gesetz** (Gordon Moore, ein Gründer von Intel) verdoppelt sich die Anzahl der Transistoren alle 18 bis 24 Monate. Das Gesetz wurde schon öfters als nicht mehr gültig erklärt, hat sich jedoch immer wieder bestätigt. Durch immer bessere Architekturen und Fertigungsgrößen von ca. 14nm wird eine enorme Dichte auf engstem Raum ermöglicht.



Die wichtigste Information über einen Mikroprozessor ist die **Wortbreite**. Damit wird angegeben, wie groß ein Wort ist, das während eines Durchgangs (Taktzyklus) verarbeitet werden kann. Eine Wortbreite von 4 Bit würde 16 mögliche Zustände zulassen (2^4). Eine Wortbreite von 16 Bit erlaubt schon 65.536 (2^{16}) und 32 Bit bereits 4.294.967.296 (2^{32}) Zustände. Die Verdoppelung auf 64 Bit erlaubt dann sogar ca. 18 Trillionen verschiedene Zustände.

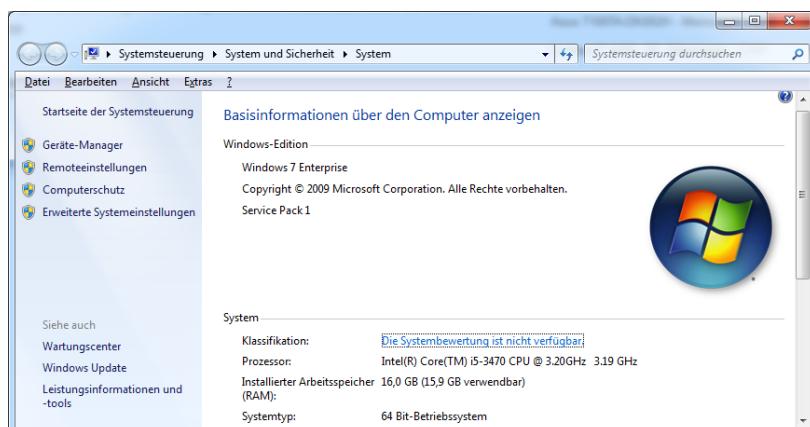
Ein weiteres Leistungsmerkmal ist die Anzahl der verwendeten **Kerne** (Cores). Gerne „matchen“ sich die Hersteller damit, dass ihre neuen Prozessoren mehr Kerne haben als die Konkurrenz. Dabei gilt gemeinhin, dass mehr Kerne gleichzeitig rechnen können und somit Multitasking besser möglich wird. Dafür muss Software jedoch spezifisch ausprogrammiert werden um diesen Vorteil auszuschöpfen! Neuere Prozessoren für Desktop-PCs haben meist 4 bis 8 Kerne.

Die **Taktfrequenz** (Clock Rate) gibt an, wie viele Rechenschritte die CPU pro Sekunde berechnen kann. Dabei bedeuten zB 3 GHz, dass der Prozessor prinzipiell 3.000.000.000 Rechenschritte pro Sekunde durchführen kann. Wie schnell der Prozessor aber tatsächlich arbeitet ergibt sich durch den Multiplikator, der am Mainboard gesetzt wurde. Ist die Taktung eines Mainboards zum Beispiel vom Hersteller mit 133 MHz angegeben, dann führt das Setzen des Multiplikators auf 20 dazu, dass die CPU-Taktrate 2,66 GHz beträgt. Früher wurde der Multiplikator über einen „Jumper“ (Drahtbrücke) auf dem Mainboard gesetzt; heute kann man den Multiplikator meist Softwareseitig im BIOS setzen. Der Betrieb eines Prozessors mit einer Taktfrequenz die höher liegt als vom Hersteller angegeben bezeichnet man als Overclocking, was zur Beschädigung durch Überhitzung führen kann.

Ebenso wichtig wie Taktfrequenz, Anzahl der Kerne und Wortbreite (wenn nicht sogar wichtiger) ist die **Architektur von Prozessoren**. Viele Hersteller wie Intel oder AMD entwickeln spezielle Befehlssätze, mit deren Hilfe regelmäßig vorkommende Berechnungen schneller durchgeführt werden können. Benchmark-Tests² und Bestenlisten³ geben Ihnen Auskunft darüber, wie Leistungsfähig die CPU im Vergleich ist. Diese Angaben erfolgen meist in FLOPS (Floating Point Operations per Second), also der durchführbaren Fließkommaoperationen pro Sekunde.

Sehr verbreitete Architekturen sind **i386** (32 Bit von Intel), **AMD64** (64 Bit von AMD und abwärtskompatibel zu x86), ia64 (64 Bit von Intel für den Serverbereich), ARM, PowerPC (Apple) etc. Diese Information ist für die Installation von Software fundamental. So unterstützt Windows 7 32bit nur die i386-Architektur und Windows 7 64bit nur die amd64-Architektur. Windows lässt sich zum Beispiel nicht auf einem Android-Tablet mit ARM-CPU installieren, da das Betriebssystem ganz eng auf die bestimmte CPU-Architektur abgestimmt ist.

Im nachfolgendem Beispiel sehen Sie die Windows-Systemanzeige (WINDOWS-Taste + PAUSE). Diese zeigt an, welcher Prozessor mit welcher Taktfrequenz und mit welcher Architektur im System installiert ist:



² <https://www.cpubenchmark.net/>

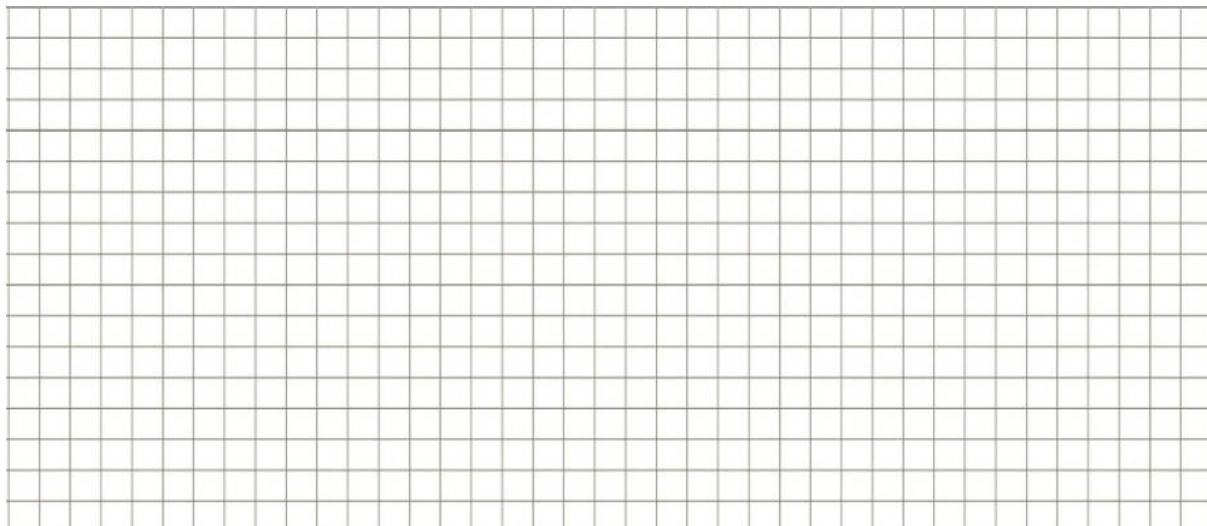
³ <http://www.chip.de/bestenlisten/Bestenliste-Desktop-Prozessoren--index/index/id/693/>

Aufgabenstellung

Entpacken Sie das Freeware-Tool CPU-Z (starten Sie es nicht direkt aus dem ZIP-Ordner!) und ergänzen Sie damit die folgenden Angaben für Ihren Laptop:



Merkmal	Ausprägung
Prozessorname	
Code-Name	
Sockel	
Technologie (Fertigungsgröße)	
Spannung des Kerns in V	
Spezifikation	
Speziell unterstützte Befehlssätze	
Taktfrequenz	
Multiplikator	
Bus Geschwindigkeit	
L1-Cache	
L2-Cache	
L3-Cache	



3.4.3 Bit/Byte/Mega/Kilo/Giga und Tera & Co. – Grundlagenwissen

Ein relativ unbeliebter aber dennoch wichtiger Themenbereich sind die mathematischen Grundlagen, die die Funktionsweise und somit die Reichweiten und Grenzen von Rechnersystemen beschreiben. Es handelt sich dabei um Querschnittswissen, das Sie in vielen Bereichen, von der Digitalfotografie über Bildbearbeitung, Installation von Netzwerken und Hardwarekomponenten etc. bei der Problemlösung zur Hilfe ziehen können. Dementsprechend lohnt sich ein Blick auf die analoge und digitale Datenverarbeitung, das Binär- und Hexadezimalsystem sowie auf die Maßeinheiten, die in der elektronischen Datenverarbeitung geläufig sind.

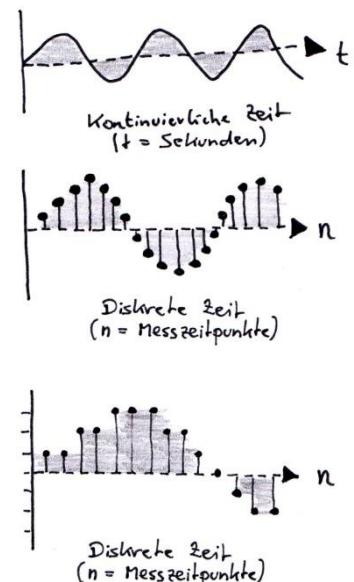
3.4.3.1 Analog vs. Digital

Ausgangspunkt für die folgenden Unterscheidungen sind **Signale**. Signale dienen der Informationsübertragung, sind meist zeitabhängig und können mit Sensoren gemessen werden, da sie in physikalischen Formen vorkommen, wie zum Beispiel der elektrischen Spannung, dem Druck, der Temperatur etc. Typische Signale sind Töne wie Sprache und Musik, Bilder und Videos, Datenströme in Leitungen, Abstandsmessungen wie GPS, Echolot, Radar etc.

Als **Analog** bezeichnet man generell Signale mit einem stufenlosen Verlauf ohne Unterbrechungen. Beispiele dafür sind die elektrische Spannung, Frequenzen elektromagnetischer Wellen etc. Diese können entweder zeitkontinuierlich verlaufen oder zeitdiskret nach bestimmten Messzeitpunkten.

Als Beispiele für analoge Geräte kennen Sie Schallplatten, Verstärker, Rundfunk (UKW; MW, LW), analoge Telefonanschlüsse, das analoge Fernsehsignal, das Echolot etc.

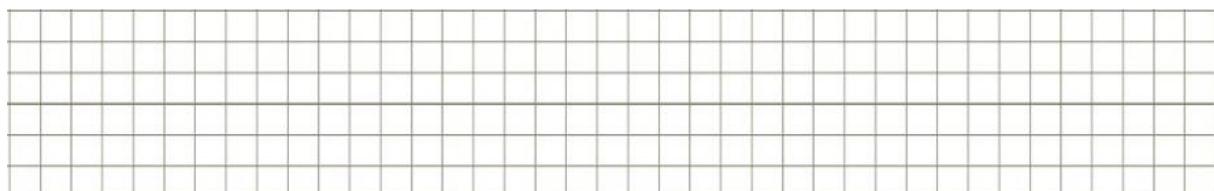
Als **Digital** bezeichnet man ein Signal, das in einen abgegrenzten gestuften Bereich eingeordnet werden kann. Digitale Signale werden durch das Quantisieren eines analogen Signals oder einer physikalischen Größe gewonnen. Zuerst wird ein zeitkontinuierliches Signal in ein zeitdiskretes Signal umgewandelt (Messzeitpunkte). Danach wird ein wertkontinuierliches Signal in ein wertdiskretes umgewandelt. Somit liegen Messzeitpunkte vor, denen jeweils ein konkreter Messwert zugeordnet ist. Digitale Werte werden in Binärzahlen kodiert, so dass sie in Bits angegeben werden können.



3.4.3.2 Das Bit als kleinste Informationseinheit

Ein Bit (**binary digit**) ist die kleinste Informationseinheit in der elektronischen Datenverarbeitung. Diese Informationen sind durch Informationsträger repräsentiert, die genau zwei Zustände darstellen können, da ein Bit nur zwei Zustände, also 0 und 1 oder Ja und Nein oder geschlossen/offen darstellen kann.

Am besten kann man sich ein Bit durch eine Glühbirne vorstellen. Die Glühbirne an sich ist der Informationsträger. Wird der Strom eingeschaltet, dann leuchtet die Glühbirne und hat damit ihren Zustand geändert. Man könnte den leuchtenden Zustand mit JA oder TRUE oder auch 1 bezeichnen. Stellt man den Strom wieder aus, dann leuchtet die Glühbirne nicht mehr und es tritt genau ein einziger anderer Zustand ein. Diesen kann man mit NEIN oder FALSE oder auch 0 bezeichnen. **Wichtig** zu wissen ist, dass ein Bit niemals mehr als 2 Zustände repräsentieren kann.



Informationsträger, die ein Bit repräsentieren können sind sehr vielfältig:

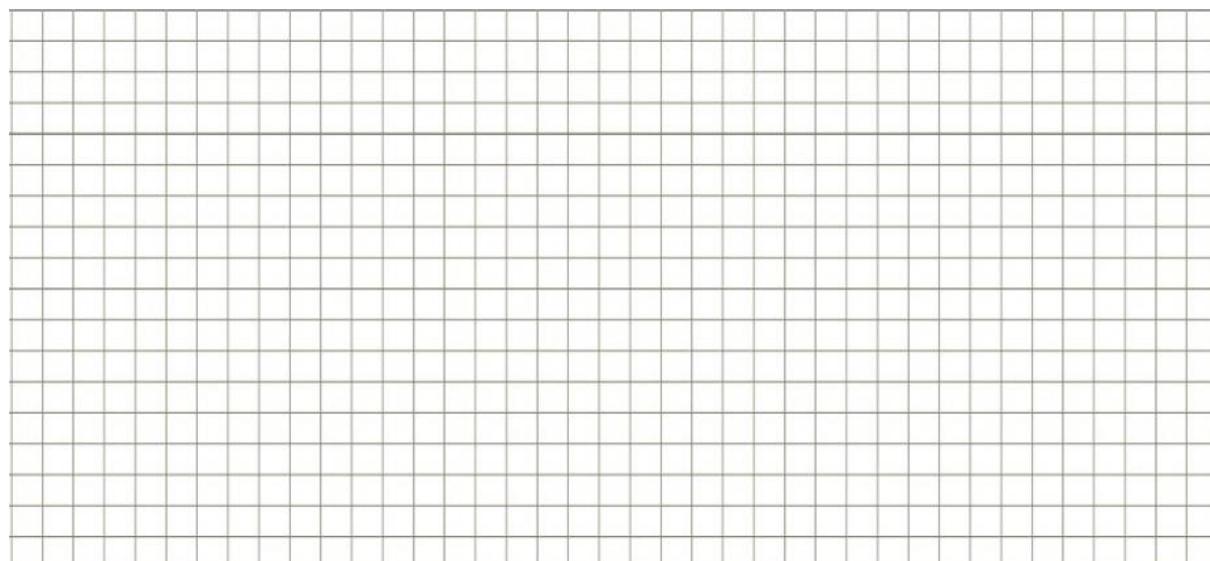
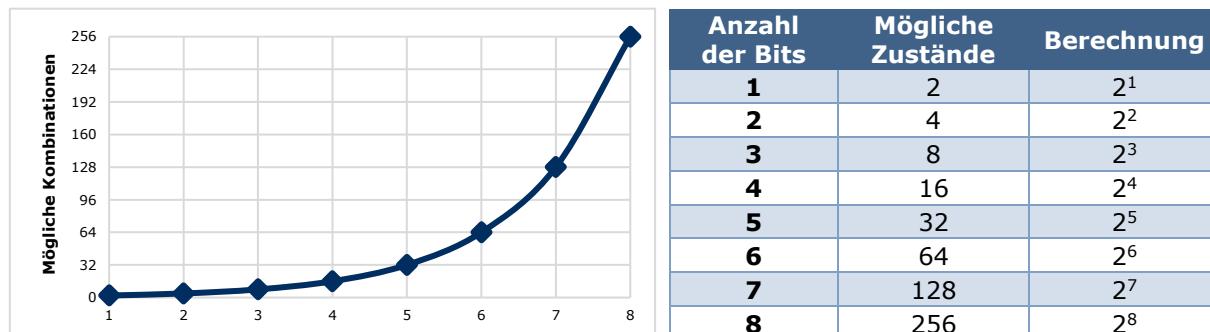
- Die Stellung eines Schalters mit zwei Zuständen.
- Ein Qubit als Zweizustands-Quantensystem.
- Die Stelle auf einem Magnetband ist magnetisch oder nicht.
- Die Stelle auf einem optischen Medium (zB: CD) reflektiert Licht oder nicht.
- Über einen Lichtwellenleiter wird ein Licht gesendet oder nicht.
- Der Schaltzustand eines Transistors (geringer oder hoher Widerstand).
- Elektrische Spannung, die *größer* oder *kleiner* als ein bestimmter Wert ist.
- Eine Variable, die logische Wahrheitswerte (Wahr, True, High, On etc. oder Falsch, False, Low, Off etc.) enthalten kann.

Mehr als 0 und 1 darstellen

Spannend wird es dann, wenn man mehrere Bits kombiniert. Dadurch kann dann eine größere Anzahl an Informationen dargestellt werden. Mit zwei Lichtschaltern und zwei Glühbirnen kann man daher vier verschiedene Zustände darstellen:

1. Beide Glühbirnen leuchten (1 1)
2. Glühbirne A leuchtet, Glühbirne B ist ausgeschaltet (1 0)
3. Glühbirne A ist ausgeschaltet, Glühbirne B leuchtet (0 1)
4. Beide Glühbirnen sind ausgeschaltet (0 0)

Nichts anderes könnte man darstellen, wenn man zwei Transistoren oder zwei Stellen auf einem optischen Medium etc. miteinander kombiniert. Jeweils genau vier verschiedene Zustände. Je mehr kleinste Informationseinheiten (Bits) man also miteinander kombiniert, desto mehr Information können diese repräsentieren.



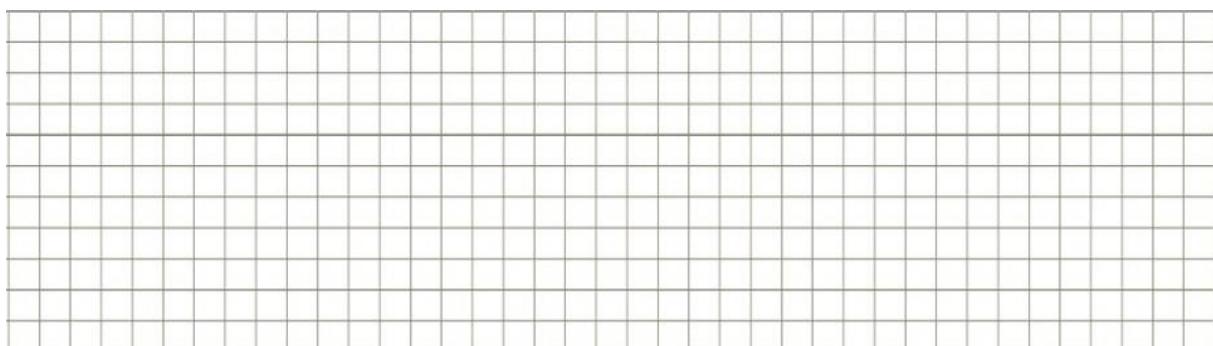
3.4.3.3 Das Binärsystem

Für die Darstellung dieser Informationen ist das Binärsystem geläufig. Während das Dezimalsystem aus 10 Ziffern besteht (0,1,2,3,4,5,6,7,8,9) gibt es im Binärsystem nur 2 Ziffern (0,1). Welcher Dezimalwert durch welche Bit-Zustände repräsentiert werden kann ist relativ einfach nachvollziehbar, wenn man die Bit-Folgen von rechts nach links liest.

Binär	Dezimal						
0000	0						
0001	1						
0010	2						
0011	3						
0100	4						
0101	5						
0110	6						
0111	7						
1000	8						
1001	9						
1010	10						
1011	11						
1100	12						
1101	13						
1110	14						
1111	15						

Vereinfacht wird diese Berechnung durch das folgende 8-Bit-Schema. Dafür überlegen Sie zuerst, wie viele verschiedene Zustände mit einer bestimmten Anzahl an Bits dargestellt werden können. Betrachtet man zum Beispiel das vierte Bit (die fünfte Stelle von der linken Seite gelesen), dann weiß man, dass man mit 5 Bit $2^5=32$ Kombinationen dargestellt werden können. Die Hälfte dieser Kombinationen ist 16, was im Binärsystem der folgende Wert wäre: 10000. Jetzt muss man nur noch dort, wo der Zustand 1 angezeigt wird, die Hälfte der Anzahl der möglichen Zustände je Bit addieren und erhält den Wert im Dezimalsystem.

Binär	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Dezimal
	Die Hälfte der mit der Anzahl dieses Bits darstellbaren Kombinationen ist								
	128	64	32	16	8	4	2	1	
00000101	0	0	0	0	0	1	0	1	5
11000000	1	1	0	0	0	0	0	0	192
01000011	0	1	0	0	0	0	1	1	67
11111111	1	1	1	1	1	1	1	1	255
									188
									39
									14
01100111	0	1	1	0	0	1	1	1	
10110110	1	0	1	1	0	1	1	0	
10111101	1	0	1	1	1	1	0	1	



Aufgabenstellung

- 1) Berechnen Sie die gelb hervorgehobenen leeren Felder in der obigen Tabelle.
- 2) Wie viele unterschiedliche Kombinationen können mit 32 Bit, 128 Bit und 256 Bit dargestellt werden? Notieren Sie im Dezimalsystem! Verwenden Sie einen Taschenrechner, Excel oder den GOOGLE-Rechner (zB: [https://www.google.de/search?q=2³](https://www.google.de/search?q=2^3)).

- 3) Welche Uhrzeit wird auf dieser Binär-Uhr dargestellt, wenn die oberen LEDs die Stunden und die unteren die Minuten repräsentieren?



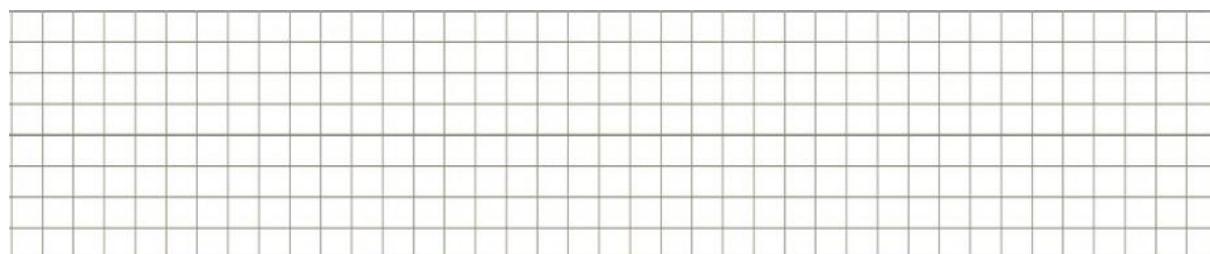
Maßeinheiten in der Datenverarbeitung

Neben der Informationseinheit Bit ist vor allem die Maßeinheit Byte, die aus einer Kombination von 8 Bit besteht. Mit einem Byte können daher 256 (2^8) verschiedene Kombinationen dargestellt werden. Ausgehend davon werden große Datenmengen mit spezifischen Vorsilben

Bedeutung	Zahl	Vorsilbe	Beispiel
Tausend	1.000	Kilo	15 Kilobyte (15 kB)
Million	1.000.000	Mega	15 Megabyte (15 MB)
Milliarde	1.000.000.000	Giga	15 Gigabyte (15 GB)
Billion	1.000.000.000.000	Tera	15 Terabyte (15 TB)
Billiarde	1.000.000.000.000.000	Peta	15 Petabyte (15 PB)
Trillion	1.000.000.000.000.000.000	Exa	15 Exabyte (15 EB)

Wesentlich ist, dass man hier von 10er-Potenzen ausgeht. Dh. eine Milliarde sind im Dezimalsystem 10^9 . Tausend wären 10^3 usw. Man kann sich jetzt berechtigterweise die Frage stellen, warum das Binärlahlensystem gerade hier durchbrochen wird und auf das Dezimalsystem zurückgegriffen wird. Tausend müssten daher im Binärsystem 2^{10} , Million 2^{20} und die Milliarde folglich 2^{30} sein.

Größeneinheit	Dezimalsystem		Binärsystem	
Tausend	10^3	1.000	2^{10}	1024
Million	10^6	1.000.000	2^{20}	1.048.576
Milliarde	10^9	1.000.000.000	2^{30}	1.073.741.824
Billion	10^{12}	1.000.000.000.000	2^{40}	1.099.511.627.776
Billiarde	10^{15}	1.000.000.000.000.000	2^{50}	1.125.899.906.842.620

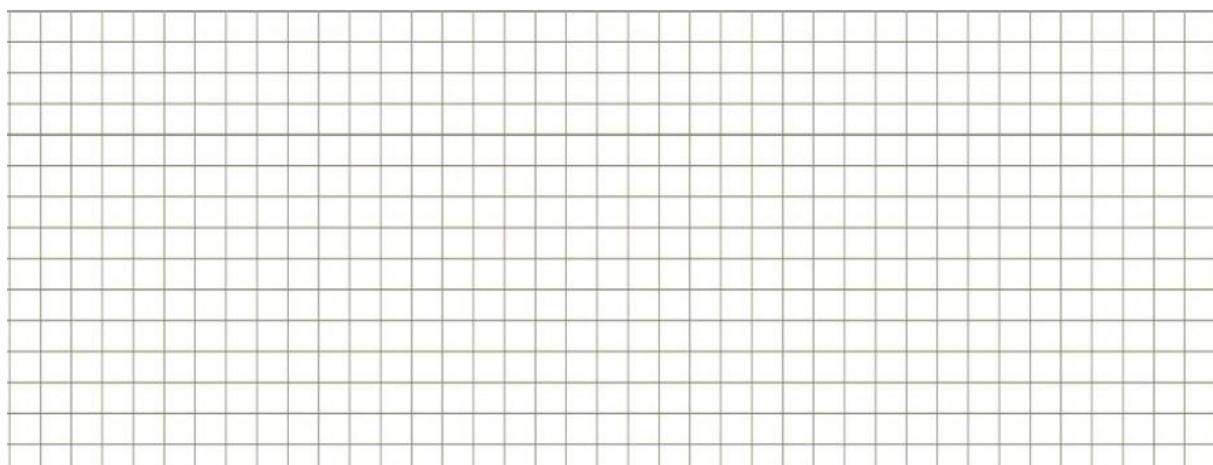
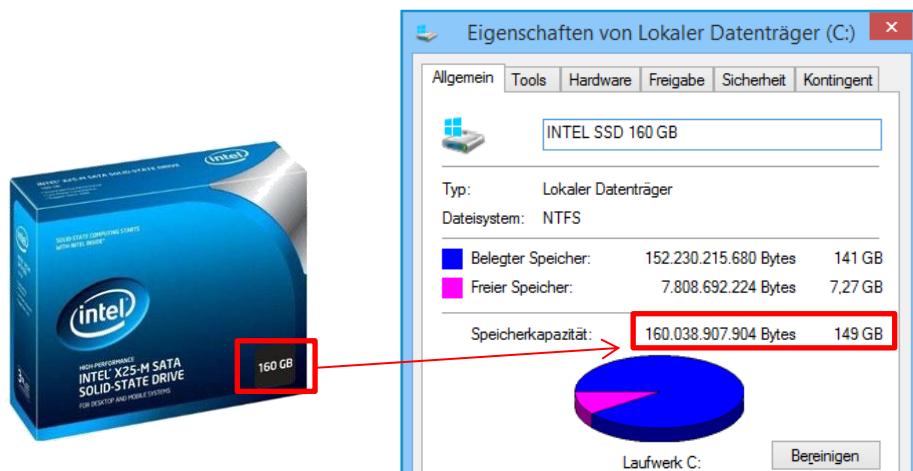
A large grid of squares, likely for handwritten calculations or notes.

Das heißt, dass eine Berechnung von einem Terabyte nach dem Dezimalsystem zu einem um 99.511.627.776 Byte geringeren Wert führt als nach dem Binärsystem. Das sind bei der Berechnung eines Terabytes immerhin 92,68 GB Differenz (binär gerechnet)!

Bis vor einigen Jahren wurden die Größeneinheiten nach dem Binärsystem berechnet. Aus Simplifizierungsgründen wurde das jedoch geändert. Seitdem werden gemeinhin SI-Präfixe (Dezimal) verwendet. Die Binärpräfixe – die mit der Norm IEC 60027-2) geregelt werden sollen nicht mehr verwendet werden. Um Missverständnisse zu vermeiden, wurde auch gleich die Vorsilbe von Binärpräfixen geändert:

Größeneinheit	Dezimalpräfix	Binärpräfix
Tausend	Kilo	Kibi
Million	Mega	Mebi
Milliarde	Giga	Gibi
Billion	Tera	Tebi
Billiarde	Peta	Pebi

Was hier wahrscheinlich wie eine eher formalistische Problemlage klingt hat in der Realität – zumindest unter Windows-Systemen – erhebliche Auswirkungen. Wenn Sie Beispielsweise eine 1-TB-Festplatte kaufen und diese einbauen, dann zeigt Windows statt 1 TB nur 0,909 TB an, also um 92,68 GB weniger.



Aufgabenstellung

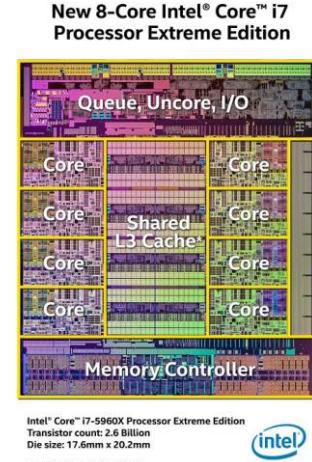
Sehen Sie sich die folgenden Informationen zu einem Prozessor an und beantworten Sie danach die folgenden Fragen:

Octa-Core • Intel Core i7-5960X Extreme Edition, 8x 3.00GHz: "Haswell-E" • Taktfrequenz: 3.00GHz, Turbo: 3.50GHz • TDP: 140W • Fertigung: 22nm • Interface: DMI, 5GT/s • L2-Cache: 8x 256kB • L3-Cache: 20MB shared • Stepping: R2 • Grafik: N/A • PCIe-Lanes: 40x PCIe 3.0 • Sockel: 2011-3, max. 1 CPU • Memory Controller: Quad Channel PC4-17000U (DDR4-2133), 68GB/s, max. 64GB • Features: SSE4.1, SSE4.2, AVX2, Turbo Boost 2.0, Hyper-Threading, VT-x EPT, VT-d, Intel 64, Idle States, EIST, Thermal Monitoring, IPT, AES-NI, XD Bit, Multiplikator frei wählbar

1. Über wie viele Kerne verfügt dieser Prozessor?
2. Wie hoch ist die angegebene Taktfrequenz der Kerne?
3. Welcher CPU-Sockel muss auf dem Mainboard vorhanden sein?
4. Wie viel L2-Cache ist verbaut?



5. Wie viel L3-Cache ist verbaut?
6. Mit wieviel Arbeitsspeicher welcher Bauart kann der Prozessor maximal arbeiten?
7. Kann man den Prozessor übertakten? Begründen Sie!



IBM meldet Durchbruch bei Quantencomputern

IBM vermeldet einen Durchbruch auf dem Weg zum Bau eines Quantencomputers: IBM-Forscher konnten die Leistung wesentlicher Bauteile so weit verbessern, dass es fast möglich ist, einen praktisch nutzbaren Quantencomputer in nennenswerter Größe zu bauen.

Die Forscher in den IBM Labs haben einige dort entwickelte Technologien kombiniert und drei wesentliche Fortschritte auf dem Weg zum Bau eines Quantencomputers erzielt. Es gelang ihnen, die Zahl der Fehler bei elementaren Berechnungen so weit zu reduzieren, dass Fehlerkorrekturverfahren effektiv eingesetzt werden können. Zudem konnten sie die Integrität der quantenmechanischen Eigenschaften von Qubits deutlich steigern.

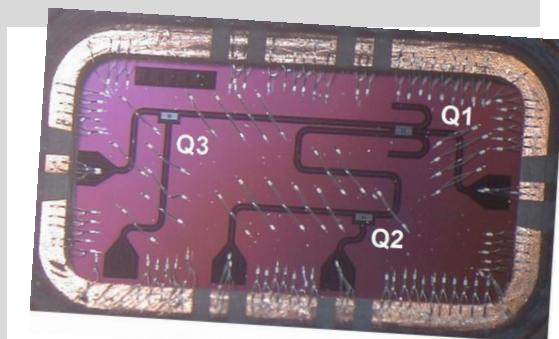
Während ein Bit in klassischen Computern nur zwei Zustände haben kann - 0 oder 1 -, können Qubits diese beiden Werte auch gleichzeitig enthalten, was in der Quantentheorie als Superposition beschrieben wird. Qubits, als kleinste Informationseinheit in einem Quantencomputer, ermöglichen es so, mehrere Millionen Berechnungen parallel auszuführen. Herkömmliche Computer können nur eine kleine Zahl von Berechnungen gleichzeitig abwickeln. So enthält laut IBM ein Quantencomputer mit 250 Qubits mehr Bits an Information, als es Atome im Universum gibt.

Diese Eigenschaften haben große Auswirkungen für Verschlüsselungstechniken, die in erster Linie darauf basieren, dass es mit herkömmlicher Technik sehr aufwendig ist, sehr große Zahlen in ihre Faktoren zu zerlegen. Quantencomputer können dies deutlich schneller erledigen. Aber auch bei Datenbanken unstrukturierter Informationen und Optimierungsaufgaben sehen die IBM-Forscher Einsatzgebiete für Quantencomputer. Diese könnten helfen, bislang unlösbare mathematische Probleme zu lösen.

Um die Möglichkeiten von Quantencomputern zu nutzen, ist es aber notwendig, die sogenannte Dekohärenz - die durch Faktoren wie Hitze, elektromagnetische Strahlung und Materialdefekte hervorgerufenen Rechenfehler - zu kontrollieren oder zu eliminieren. Ein wichtiger Ansatzpunkt dafür ist es, die Zeit zu verlängern, über die Qubits ihre quantenmechanischen Eigenschaften behalten. Ist diese Zeitspanne lange genug, lassen sich Fehlerkorrektursysteme effektiv einsetzen, so dass sich lange und komplexe Berechnungen durchführen lassen.

Quantencomputer rückt in greifbare Nähe

Nun gibt es verschiedene Ansätze, um einen funktionierenden Quantencomputer zu entwickeln. IBM konzentriert sich auf supraleitende Qubits. Dabei experimentiert IBM mit einem dreidimensionalen supraleitenden Qubit (3D Qubit), einer Idee, die an der Universität Yale entstand. Damit konnte IBM die Zeitspanne, für die ein Qubit seinen Quantenstatus behält, im Vergleich zu den bisherigen Rekorden um das Zwei- bis Vierfache verlängern. Damit sei gerade so das Minimum erreicht, um Fehlerkorrektursysteme effektiv einzusetzen, erklärte IBM. So könnten sich Ingenieure um Fragen der Skalierbarkeit kümmern.



"Unsere Arbeiten im Bereich Quantencomputer zeigen, dass es hierbei nicht länger um ein rein physikalisches Experiment geht. Es ist Zeit, damit zu beginnen, Systeme auf Basis dieser wissenschaftlichen Erkenntnisse zu entwickeln, die die Computerei an neue Grenzen heranführen", sagt der Leiter von IBMs Quantencomputer-Forschungsteams, Matthias Steffen.

In einem weiteren Experiment konnten die IBM-Forscher ein eher traditionelles, zweidimensionales Qubit präsentieren und eine logische Operation - Controlled-NOT (CNOT) - mit zwei Qubit umsetzen, ein wichtiger Baustein beim Bau eines Quantencomputers. Die Operation war in 95 Prozent aller Fälle erfolgreich. Das wurde durch eine lange Kohärenzzeit von 10 Mikrosekunden ermöglicht. Damit werde fast die für den Einsatz von Fehlerkorrektursystem notwendige Grenze erreicht, so IBM. Quelle: <http://www.golem.de/news/3d-qubit-ibm-meldet-durchbruch-bei-quantencomputern-1202-90080.html>

3.5 Arbeitsspeicher (RAM)

Im Arbeitsspeicher werden alle Daten von den Programmen zwischengespeichert die aktuell verarbeitet werden. Wenn ein Programm das erste Mal gestartet, wenn der PC eingeschaltet wird, werden die Daten zuerst von der Festplatte in den Arbeitsspeicher übertragen und dann über den Cache an den Prozessor weitergeleitet.



Der Arbeitsspeicher besteht aus mehreren Speicherbausteinen die man als RAM (Random Access Memory; Speicher mit wahlfreiem Zugriff) bezeichnet. Das bedeutet, dass die Inhalte des Speichers sowohl gelesen als auch verändert werden können (im Gegensatz zu ROM; Read-Only Memory). Random bedeutet, dass auf beliebige Speicherzellen in beliebiger Reihenfolge zugegriffen werden kann. Bei optischen Laufwerken muss im Gegensatz dazu oft eine bestimmte Reihenfolge eingehalten werden.

Als Faustregel gilt: Je mehr RAM das System hat, desto besser, da mehr Daten von der Festplatte in den schnellen Speicher geschrieben werden können. Viel RAM benötigt man vor allem dann, wenn man mit speicherintensiven Anwendungen wie Bildbearbeitung oder Videoschnitt etc. arbeitet.

Wichtig zu wissen ist, dass es sich um einen **flüchtigen Speicher** handelt. Das heißt, dass RAM ständig mit Strom versorgt werden muss, da es sonst zu Datenverlust kommt. Wird der PC vom Strom getrennt, dauert das Hochfahren (laden der Daten von der Festplatte in den Arbeitsspeicher) oft einige Zeit.

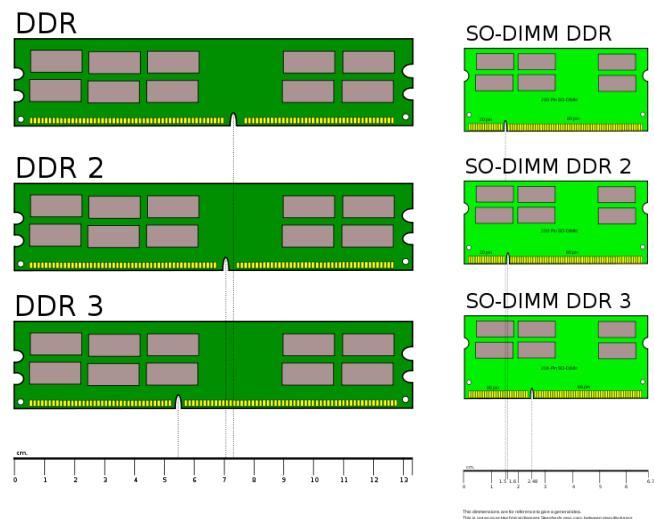
Unter Windows-PCs gibt es die Funktion „Ruhezustand“ (Hibernate). Diese ermöglicht es, dass man den Laptop zuklappen und vom Strom trennen kann und die Daten dennoch nicht verloren gehen. Das passiert durch einen einfachen Trick: Beim Ruhezustand wird der gesamte RAM-Inhalt in die Datei hibernate.sys auf der Festplatte geschrieben. Beim „Aufwecken“ wird der Inhalt wieder in den RAM geschrieben. Somit hat man genau dort weiterarbeiten wo man zuletzt aufgehört hat!

3.5.1 Formfaktoren

Es gibt unterschiedliche Arten von RAM-Bausteinen. Die erste wesentliche Unterscheidung ist die Bauform. Hier unterscheidet man gemeinhin DDR und SO-DIMM DDR-Speicher. SO-DIMM-Bauteile werden meist in Laptops und Micro-PCs eingebaut. Die DDR-Bauform hat 204 PINs, die SO-DIMM-Bauform 204 PINs (Kontakte) und werden direkt in die dafür vorgesehenen Slots auf das Mainboard gesteckt.

Neben dieser Unterscheidung ist außerdem die Version des DDR-Speichers wichtig. Hier unterscheidet man DDR, DDR2, DDR3 und DDR4 (wobei momentan noch DDR3 gebräuchlich ist).

Welcher DDR-RAM auf das Mainboard passt kann man dem Handbuch des Mainboards entnehmen. Dabei ist wichtig, dass DDR3 nicht mit DDR oder DDR2 oder DDR4 kompatibel ist. Aufgrund spezieller Kerben in den Steckplätzen passen nur jene Arbeitsspeicher-Riegel (zB: DDR3) die mit dem Steckplatz (zB: DDR3) kompatibel sind.

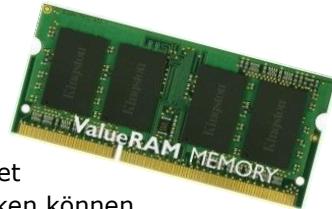


Beispiel

Kingston ValueRAM SO-DIMM 8GB, DDR3-1333, CL9
 Typ: DDR3 SO-DIMM 204-Pin • Modul: 1x 8GB • JEDEC: PC3-12800S • Spannung: 1.50V •
 Besonderheiten: N/A • Herstellergarantie: lebenslang

Bei diesem Angebot handelt es sich um einen DDR3-Speicherbaustein mit 204-Pins. Das heißt, es ist eine SO-DIMM-Bauform die typischerweise in Laptops und Micro-PCs verwendet wird. Die Speicherkapazität beträgt 8 GB. Dabei ist das 1x 8GB eine wichtige Information. Sie bekommen hier nämlich einen Speicherriegel zu 8 GB und nicht zwei Riegel zu jeweils 4 GB geliefert (das wäre dann 8GB (2x4GB)). Die Spannung beträgt 1.5 Volt und die Taktfrequenz bis zu 1333 MHz.

Wenn auf einem Mainboard angegeben ist, dass 4 Steckplätze für DDR3 vorhanden sind und insgesamt 32 GB unterstützt werden, bedeutet das, dass Sie maximal Speichermodule mit 8 GB in die Steckplätze stecken können. Module mit 16 GB werden vom Mainboard dann nicht unterstützt.



Defekte und/oder nicht unterstützte Speichermodule erkennt man leicht, da bei schweren Fehlern das Lautsprechermodul des Gehäuses piepst. Friert der Computer häufig einfach ein und reagiert nicht mehr, dann deutet das auch meist auf einen defekten Speicherbereich am RAM-Modul hin.

Hinweis

32-Bit-Systeme arbeiten mit 32 Bit langen Adressen. Das bedeutet, dass es eine rechnerische Obergrenze des Arbeitsspeichers gibt, der angesprochen werden kann. Diese Grenze liegt bei 2^{32} Byte. Es können also nicht mehr als 4.294.967.296 Byte (4 GByte) adressiert werden. Windows 7 32-Bit kann daher (ohne Tricksereien) nur 4 GByte verwalten, auch wenn 16 GByte eingebaut sind. Bei 64-Bit-Systemen liegt diese Beschränkung deutlich höher (18.400.000 TeraByte). Hier sind die Limitierungen durch die Versionen des Betriebssystems definiert (Windows 7 Home Premium unterstützt maximal 16 GB; Windows 7 Professional unterstützt 192 GB etc.).

Aufgabenstellung

Finden Sie heraus, wie viel GB-RAM in Ihrem PC verbaut sind. finden Sie weiter mit dem Tool CPU-Z die folgenden Spezifikationen heraus:

Merkmal	Ausprägung
Typ	
Taktfrequenz	
Größe	
Anzahl der Karten	
Größe der Module	

Überprüfen Sie nun mit dem Tool *RAMMap*, welche die fünf Dateien sind, die am meisten RAM belegen (Tipp: Registerkarte File Summary):

#	Dateiname	MB
1		
2		
3		
4		
5		

3.6 Das BIOS

Das BIOS (Basic Input Output System) ist ein Programm auf einem ROM-Modul (Read Only Memory) auf dem Mainboard, das die zentrale Basis-Steuerlogik eines PCs übernimmt. Man erkennt es in vielen Fällen beim Starten des PCs, wenn es diverse Kontrollmeldungen ausgibt. Neuere PCs werden mit UEFI (einer neueren Version) ausgeliefert.



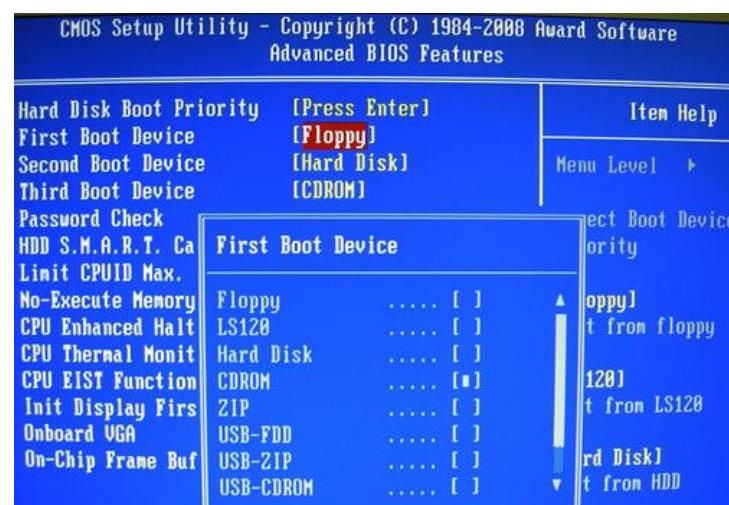
Die Funktionen des BIOS sind die folgenden:

- Beim Starten des Rechners wird die Funktionsweise der wichtigsten Hardware getestet. Zunächst die Grafikkarte, dann der RAM. Anschließend wird überprüft, welche und wie viele Laufwerke am zB: SATA-Bus angeschlossen sind. Gibt es dabei Probleme piepst meist der kleine Lautsprecher, der im PC verbaut ist in einer bestimmten Reihenfolge (die meist im Handbuch beschrieben ist).
- Hat das BIOS den Systemcheck erfolgreich durchgeführt, gibt es die Kontrolle an das Master Boot Record (MBR) der primären Festplatte weiter. Dort befindet sich dann zB: der Bootloader, der das installierte Betriebssystem lädt.

Das BIOS kann je nach Version direkt beim Starten des PCs durch Drücken der Taste ENTF oder F2 oder F1 aufgerufen werden. Meist wird beim Start eine Meldung wie „Press DEL to enter setup“ ausgegeben. Durch das BIOS navigieren Sie mit den Pfeiltasten der Tastatur. Durch ENTER können Sie einen Wert auswählen und verändern. Über ESC verlassen Sie ein Menü/das BIOS wieder. Teilweise müssen Sie Änderungen bestätigen. Das passiert in der Regel mit der Taste Y. Beachten Sie dabei, dass das BIOS das englische Tastaturlayout lädt und somit Y und Z vertauscht sind!

In der Regel benötigt man das BIOS nur in einem einzigen Fall, nämlich wenn Sie die BOOT-Reihenfolge ändern wollen und zB von einer anderen Festplatte oder von einem USB-Stick ein Betriebssystem starten wollen.

Das klassische BIOS wird in der nächsten Zeit sukzessive von UEFI (Unified Extensible Firmware Interface) ersetzt. UEFI wird einfacher zu bedienen sein, bietet einfachere Wiederherstellungsmöglichkeiten und schützt auch besser vor Rootkits oder Bootkits, also Tools, die bereits vor dem Ausführen des Betriebssystems Schadsoftware laden und somit das Betriebssystem (vom Anwender unerkannt) kompromittieren.



3.7 Festplatte

Festplatten (Hard Discs; HD) sind die mit Abstand wichtigsten Peripheriegeräte. Als Massenspeicher ist die Festplatte zwar nicht fundamental Notwendig für den Betrieb eines Desktop-PCs, das tägliche Arbeiten und das Ablegen von Daten wird durch natürlich enorm vereinfacht. Es werden im Wesentlichen zwei Arten von Festplatten unterschieden: die mechanische Festplatte (HD) und Festplatten, die aus Speicherzellen bestehen (Solid-state-Disks; SSD).

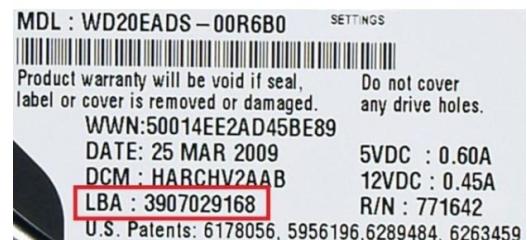
3.7.1 Mechanische Festplatte

Bei mechanischen Festplatten handelt es sich um eine runder Metallplatten, die auf einer gemeinsamen drehenden Achse angeordnet sind (Spindel). Diese Spindel dreht sich – je nach Plattentyp – zwischen 5000 – 15000-mal pro Minute (rpm=rotations per minute).



Über die Platten werden von Schreib-/Leseköpfen abgetastet, die sich auf einem Aktuator-Arm befinden. Köpfe schweben quasi über der Platte, wobei der Abstand zwischen Kopf und Platte nur der Bruchteil eines menschlichen Haars ist. Deshalb ist eine Festplatte auch vakuumverschweißt, damit keine Staubkörner in das Gebilde kommen können und der Widerstand beim Bewegen des Lesekopfs verringert wird.

Auf den Metallplatten werden die einzelnen Spuren (Zylinder) in Blöcke eingeteilt. Gängig ist das LBA-Verfahren (Logical Block Addressing). Hier werden die einzelnen Spuren in feste Blöcke zu jeweils 512 Byte eingeteilt. Je mehr Blöcke auf einer Platte untergebracht werden können, desto größer ist natürlich die Speicherkapazität. Im nebenstehenden Aufdruck einer Festplatte ist zum Beispiel angegeben, dass sich 3.907.029.168 LBA-Sektoren auf der Platte adressieren lassen. Multipliziert man diese Zahl mit 512 Byte ergibt das eine Speicherkapazität von 2.000.398.934.016 Byte. Im Dezimalsystem gerechnet sind das 2000 GB bzw. 1863 GiB.



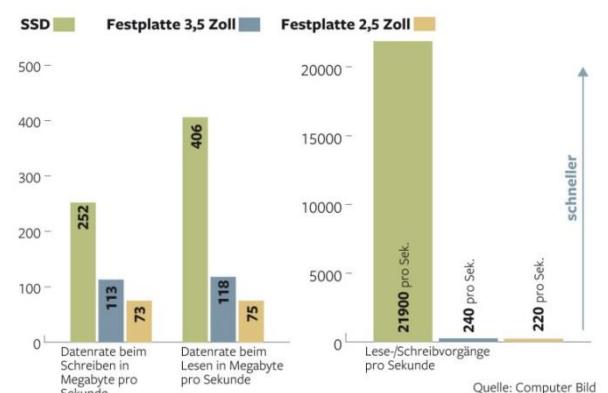
3.7.2 Solid-state-drive (SSD)

Im Gegensatz zu mechanischen HD haben SSDs keine mechanischen Teile. Sie bestehen aus nichtflüchtigen Speicherzellen, die auf Chips untergebracht sind. Man könnte eine SSD umgangssprachlich mit einem großen USB-Stick oder einer großen Speicherkarte beschreiben. Der große Vorteil von SSDs ist, dass die Zugriffszeiten im Vergleich zu HD stark reduziert sind, da jeder Speicherbereich eine eindeutige Adresse hat und dieser nicht erst auf der Platte mit Hilfe eines Lesekopfs gesucht werden muss.



Deshalb schreiben und lesen SSD meist viel schneller als ihre mechanischen Kollegen.

Die Schnelligkeit hat jedoch ihren Preis. Während ein Gigabyte auf einer SSD im Jahr 2014 ca. € 0,40 kostet, bekommt man ein Gigabyte auf einer HD schon um ca. € 0,03.



SSD 960: Samsung bringt neue, flotte Solid State Disks

Im M.2-Format – Pro-Variante soll mit bis zu 3,5 GByte/s lesen

Samsung baut seine Angebot an flotten Solid State Disks aus. Im Rahmen des eigenen SSD Global Summit hat der Hardwarehersteller nun die neue SSD-960-Serie präsentiert. SSD 960 Samsung verweist dabei vor allem auf die Performance seiner neuen SSDs. Demnach erzielt die SSD 960 Evo 3,2 GBbyte/s bei Lesevorgängen, beim Schreiben sind es noch immer bis zu 1,9 GByte/s, wobei das von der jeweiligen Ausführung abhängt. Diese Top-Performance gibt es nur beim größten Modell mit 1 TB Speicherplatz, die Variante mit 256 GB muss sich mit 1,5 GByte/s zufrieden geben.

Die als maßgeblicher Wert für zufällige Zugriffe ermittelnden IOPS-Werte liegen bei maximal 380.000 (Lesen) beziehungsweise 360.000 (Schreiben). Noch flotter geht es bei der 960 Pro zu: Diese kommt auf maximal 3,5 GByte/s beim Lesen und 2,1 GByte/s beim Schreiben. Auch die IOPS-Werte liegen mit 440.000 bzw. 360.000 entsprechend höher. Verfügbarkeit SD 960 Evo und die 960 Pro sind für den M.2-Steckplatz gedacht. Das Evo-Modell soll ab November erhältlich sein, für die Pro-Variante gibt es noch keinen Erscheinungstermin. Preise nennt der Hersteller derzeit ebenfalls noch nicht. (apo, 21.9.2016)

Quelle: derstandard.at/2000044718549/SSD-960-Samsung-bringt-neue-flotte-Solid-State-Disks

Firefox: Ist der Mozilla-Browser ein SSD-Killer?

Sitzungsmanager schreibt täglich Dutzende GByte an Daten auf die SSD und lässt diese so altern

Der Sitzungsmanager des Firefox ist eine nützliche Angelegenheit. Sorgt dieser doch dafür, dass nach einem Absturz des Browsers die vorherige Session wieder genau so hergestellt wird, und der entstandene Datenverlust damit minimiert wird. Doch genau diese Funktion bringt Browserhersteller Mozilla nun schwere Kritik ein. Schreibvorgänge Wie sich nun herausstellt, schreibt der Firefox nämlich selbst wenn er unbenutzt im Hintergrund läuft, laufende massive Mengen an Daten auf das lokale Speichermedium. Grund dafür ist eben jener Sitzungsmanager, der alle 15 Sekunden einen Schnappschuss des aktuellen Browergeschehens erstellt.

Blog-Autor Sergei Bobik hat sich das daraus resultierende Datenvolumen mithilfe des Analysetools SSDLife im Detail angesehen: Daraus erfuhr er, dass sein Firefox im Verlaufe des letzten Tages 12 GB an Daten auf die SSD geschrieben hat. Dies obwohl er den Browser nur wenig genutzt hatte, und keine größeren Dateien heruntergeladen hat. Insofern dürfte es sich bei den 12 GB um einen eher niedrigen Wert handeln, wer den Browser intensiver nutze, und mehr Tabs geöffnet habe, komme schnell auf ein Volumen von 35 GB am Tag, so die Untersuchung von Bobik. Lebensdauer Problematisch ist all dies vor allem deswegen, weil dieses Verhalten SSDs schnell altern lässt. 35 GB pro Tag ergeben im Jahr ein Schreibvolumen von mehr als 12 TB. Vor allem bei billigeren SSDs stellt dies einen bedeutenden Anteil der gesamten Lebenszeitgarantie des Herstellers dar. Trotzdem gibt man sich zummindest bei SSD-Hersteller Samsung gelassen. Das Verhalten des Firefox sei zwar ärgerlich, trotzdem solle man nicht vergessen, dass selbst billige SSDs aus eigener Produktion bei einer Nutzungsdauer von fünf Jahren auf 41 GB pro Tag ausgelegt sind, betont das Unternehmen gegenüber dem Spiegel. Freilich kommt man mit den erwähnten 35 GB hier schon recht nahe an diesen Wert – und das eben ganz ohne andere Aktivitäten am Rechner.

Quelle: derstandard.at/2000045166294/Firefox-Ist-der-Mozilla-Browser-ein-SSD-Killer

3.7.3 Wichtige Leistungsmerkmale

Neben der Speicherkapazität sind natürlich auch bei einer Festplatte weitere Spezifika für die Kaufentscheidung relevant. Allen voran der **Formfaktor**. Während in Desktop-PCs meistens Festplatten mit 3,5" eingebaut werden können, sind in Laptops Schächte für 2,5" vorgesehen. In manchen Netbook-PCs werden die noch kleineren 1,8"-Platten verbaut.

Heutzutage werden die meisten Festplatten über die **SATA-Schnittstelle** angebunden. Aktuell ist momentan die Schnittstelle SATA III mit 6 Gb/s. Vor allem bei SSDs muss darauf geachtet werden, dass eine schnelle SATA-Schnittstelle vorhanden ist, da sonst möglicherweise nicht das volle Potenzial ausgeschöpft werden kann. In mobiles Devices wird immer stärker der M.2-Formfaktor eingesetzt.

Je höher die **Drehzahl** pro Minute desto schneller ist in der Regel auch die Übertragungsrate. Klassische Desktop-Festplatten haben momentan eine Drehzahl von ca. 7200 rpm. Problematisch dabei ist oft, dass schnellere Drehzahlen zu einer höheren **Geräuschenwicklung** führen können. Die Lautstärke beträgt bei so einer Platte ca. 30 Dezibel (das entspricht der Lautstärke von Flüstern).

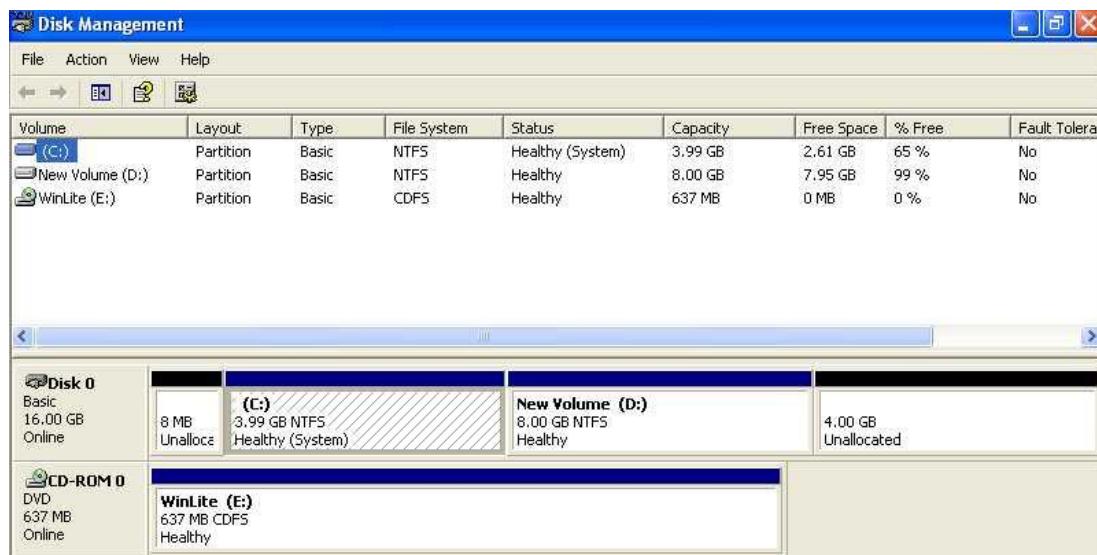
Soll die (HDD)-Platte im **Dauerbetrieb**, zum Beispiel in einem NAS, verwendet werden, sollte eine spezielle Platte für den Server-Betrieb, für NAS-Systeme oder mit speziellem Hinweis für den Dauerbetrieb gekauft werden. In diesem Zusammenhang ist vor allem dann auch der **Stromverbrauch** nicht zu vernachlässigen. Verbraucht eine Platte im Leerlauf 5 Watt und wird dauerhaft betrieben, so sind das bei einem kWh-Preis von ca. € 0,035 pro Jahr ca. € 12,50 pro Jahr.

3.7.4 Partitionen

Es empfiehlt sich sehr, große Festplatten in mehrere Partitionen einzuteilen. Diese Partitionen können mit unterschiedlichen Dateisystemen formatiert werden. Das erlaubt auch die Installation von mehreren unterschiedlichen Betriebssystemen parallel zueinander. Solche Partitionen können unter Windows mit dem Tool *diskmgmt.msc* erstellt, gelöscht, erweitert oder verkleinert werden.

Windows behandelt diese Partitionen dann wie eigene Festplatten, denen Sie Laufwerksbuchstaben und Bezeichnungen zuordnen können, obwohl nur zB eine physische Festplatte im PC eingebaut ist.

In der nachfolgenden Abbildung ist ersichtlich, dass lediglich eine physische Festplatte (Disk 0) verbaut ist, auf der sich zwei Partitionen befinden. Beide sind mit dem File-System NTFS formatiert. 4 GB der Festplatte sind keiner Partition zugeordnet, die von Windows gelesen werden kann.



Ähnlich funktionieren auch virtuelle Festplatten (VHD). Diese sind im Wesentlichen Dateien, die von Windows wie als Festplatte behandelt werden. Oft kann man schon vorinstallierte Betriebssysteme als VHD von der Herstellerseite herunterladen und dann als Laufwerk einbinden und natürlich auch wieder entfernen.

3.7.5 Dateisysteme

Jedes Speichermedium muss mit einem speziellen Dateisystem (file system; FS) formatiert werden. Ein solches Dateisystem definiert die Ablageorganisation auf einem Datenträger. Es regelt genau, wie Dateien gespeichert, gelesen oder gelöscht werden. Außerdem werden neben dem Dateiinhalt auch diverse Attribute wie der Dateiname, Zugriffsberechtigungen, Version etc. mitgespeichert.

Für unterschiedlichste Anwendungsbereiche gibt es unterschiedliche Dateisysteme, die natürlich auch historisch unterschiedlich gewachsen sind und dementsprechend zw. zueinander auch zw. inkompatibel sind.

FAT16 (File allocation table 16bit)

Dieses Dateisystem wurde 1983 von Microsoft veröffentlicht. Daher kann es $65.536 (=2^{16})$ Cluster verwalten. Die Größe einer Datei durfte maximal 2 GiB betragen.

FAT32 (File allocation table 32bit)

1996 wurde eine neuere FAT-Version von Microsoft veröffentlicht. Es arbeitet mit 32 bit, wovon 4 bit reserviert sind und kann somit $258.435.456 (=2^{28})$ Cluster adressieren. Eine Datei darf hier maximal 4 GiB haben.

NTFS (New Technology File System)

Mit Windows XP wurde dieses neue System von Microsoft eingeführt. Es verwaltet die Cluster nicht mehr in einfachen Tabellen sondern verwaltet die Cluster in komplexen Baumstrukturen, was einen schnelleren Zugriff ermöglicht. Somit ist auch ein höherer Schutz vor Fehlern gegeben. Zusätzlich wurden auch Zugriffsrechte für Benutzer und Gruppen eingeführt, die individuell für Ordner und Dateien gesetzt werden können. Die maximale Dateigröße beträgt 16 TiB (Tebibyte) und die maximale Länge der Dateinamen beträgt 255 Zeichen.

ReFS (Resilient File System)

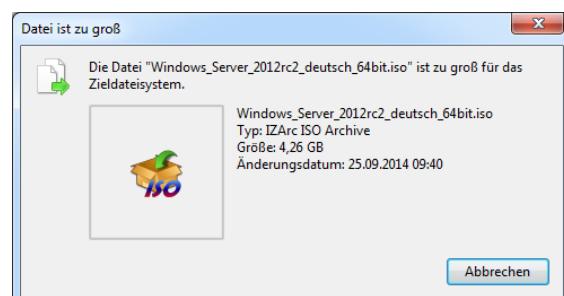
Dieses Dateisystem wurde 2012 eingeführt. Es arbeitet mit 64bit und erlaubt daher Dateigrößen von 2^{64} (18.446.744.073.709.600.000 Byte, also 16 Exabyte). Auch die Länge eines Dateinamens wurde auf 32000 Zeichen erhöht. Es erlaubt eine Vielzahl weiterer Funktionen wie Verschlüsselung, automatische Fehlerkorrektur etc.

Weitere Dateisysteme

Auf Apple-PCs wird das HFS, HFS+ und HFSX-Dateisystem eingesetzt. Unter Linux-Systemen ist ext3 und ext4 geläufig. Daneben gibt es noch eine Vielzahl weiterer Systeme. Unter Unix ist zw. noch das UFS auf Solaris-Servern etc. gängig.

Wichtige Implikationen bei Dateisystemen

- Wenn das Betriebssystem ein bestimmtes Dateisystem nicht unterstützt, kann auf die Festplatte nicht zugegriffen werden. Sind zwei Festplatten im PC eingebaut (oder zwei Partitionen) und auf einer ist Windows und auf der anderen ein Linux-Derivat installiert, so kann Windows (prinzipiell) nicht auf die Linux-Dateien zugreifen.
- Möchte man auf einen USB-Stick, der mit FAT32 formatiert ist, eine Datei kopieren, die größer als 4 GB ist, erscheint eine Fehlermeldung, da die maximale Dateigröße überschritten wurde.
- Im Zweifel sollte bei USB-Sticks etc. FAT32 verwendet werden, da es sowohl von Windows, Apple und Linux-Systemen gut unterstützt wird.



Versuch, eine 4,26 GB große Datei auf FAT32 unter Windows 7 zu speichern

Aufgabenstellung

1. Überprüfen Sie mit Hilfe des Tools **diskmgmt.exe** die folgenden Merkmale Ihres Laptops/PCs:

- a) Wie viele Festplatten sind in Ihrem PC verbaut?
- b) In wie viele Partitionen sind Ihre Festplatten eingeteilt?
- c) Mit welchem Dateisystem sind die vorhandenen Partitionen formatiert?
- d) Wie viel Speicherplatz ist auf den Partitionen belegt (in %)?

2. Überprüfen Sie mit dem Tool **WinDirStat** auf Ihrem Laptop/PC:

- e) welche die größte Datei auf Ihrer Partition C:\ ist!
- f) wie hoch die Speichernutzung des Ordners C:\Windows ist!



3. Überprüfen Sie mit dem Tool **Recueva**, ob sich auf dem USB-Stick, den Sie vom LV-Leiter erhalten haben, Dateien befinden, die Sie möglicherweise wiederherstellen können und stellen Sie diese wieder her.



4. Löschen Sie mögliche wiederhergestellte Dateien auf dem Stick dauerhaft mit Hilfe des Tools **Eraser** und versuchen Sie diese danach mit dem Tool Recueva wiederherzustellen.



3.7.6 RAID

Raid steht für „Redundant Array of Independent Disks“ und dient dazu, mehrere physische Laufwerke zu einem logischen Laufwerk zu verbinden. Dadurch wird ein größerer Datendurchsatz ermöglicht, da die Daten auf zwei Festplatten verteilt werden. RAID setzt das Vorhandensein eines speziellen Controllers voraus, der das Management der unterschiedlichen Festplatten übernimmt.

Ein solcher RAID-Controller ist auf vielen Festplatten bereits verbaut. Das erkennt man durch die Angabe des RAID-Levels in der Beschreibung des Mainboards, wie zB: „RAID-Level: 0/1/5/10“. Jede Zahl steht für eine andere Art des Umgangs mit den Festplatten. Ein auf dem Mainboard verbauter RAID-Controller kann direkt im BIOS unter „Integrated Peripherals“ verwaltet werden.

RAID-Level 0 (Striping)

In diesem Modus werden Daten auf zwei Festplatten verteilt. Der Controller verteilt auf jeder Festplatte Blöcke, die dann gemeinsam als ein einziger Block beschrieben werden können. Das heißt, dass zum Beispiel ein Datenpaket von 512 Byte auf zwei Platten zu je 256 Byte gespeichert wird. Dadurch wird sowohl die Lese- als auch die Schreibrate stark verkürzt. Fällt jedoch eine Platte aus kommt es zu Datenverlust. Je nach Raid-Controller können zwei, drei vier oder auch mehr Festplatten eingesetzt werden.



RAID-Level 1 (Mirroring)

Wer auf der sicheren Seite sein möchte wählt am besten den RAID-Level 1. In diesem Modus werden die gleichen Daten einfach auf mehreren Festplatten gespeichert. Somit gibt es zumindest eine oder auch mehrere (je nachdem wie viele Platten eingesetzt wurden) Kopie/n. Fällt eine Platte aus, wird der RAID-Level einfach aufgehoben und die noch fehlerfreie Festplatte nicht mehr im RAID-Modus betrieben. Mirroring sichert vor Datenverlust durch den durch Hardware bedingten Ausfall jedoch nicht durch Datenverlust durch Virenbefall, Benutzungsfehler etc. und ist somit kein reiner Ersatz für die Datensicherung!



RAID-Level 5

Bei diesem RAID-Level benötigt man mindestens drei Festplatten. Ähnlich wie bei RAID 0 werden die Daten auf mehrere Festplatten verteilt. Somit wird die Performance stark erhöht. Gleichzeitig wird jedoch Speicherplatz für die Wiederherstellung reserviert (Parity-Daten). Fällt eine Platte aus, können die Daten wiederhergestellt werden. Das geht jedoch zu Lasten des verfügbaren Speicherplatzes.



RAID-Level 10

Dieser Raid-Level kombiniert die Levels 0 + 1 und benötigt mindestens vier Festplatten. Jeweils zwei Festplatten werden zu einem logischen Laufwerk zusammengefasst. Die Daten sind dann auf einem logischen Laufwerk auf zwei physische Festplatten verteilt. Auf dem zweiten logischen Laufwerk werden die Daten gespiegelt. Somit verbindet RAID 10 die Vorteile des Mirroring und des Striping.

3.8 Grafikkarte und Monitor

Grafikkarten sorgen dafür, das Bild, das vom der GUI (Graphical User Interface) des Betriebssystems auf dem Monitor oder einem anderen Gerät (Beamer, Smartboard etc) wiederzugeben. Grafikkarten können nicht nur einfache 2D-Berechnungen durchführen, also welcher Pixel an welcher Stelle mit welcher Farbe beleuchtet werden soll. Moderne Grafikkarten verfügen über 3D-Beschleuniger, die das Echtzeit-Rendering von 3D-Szenen unterstützen und somit Tiefeninformationen in der dritten Dimension mit Beleuchtungseffekten, Transparenz und Darstellungsgrößen umzurechnen. Eine Grafikkarte besteht im Wesentlichen aus den folgenden Bestandteilen:

- Grafikprozessor – GPU (graphics processing unit)
- Video-RAM – Arbeitsspeicher für GPU
- RAMDAC – Analog/Digital-Konverter (Random Access Memory Digital/Analog Converter)

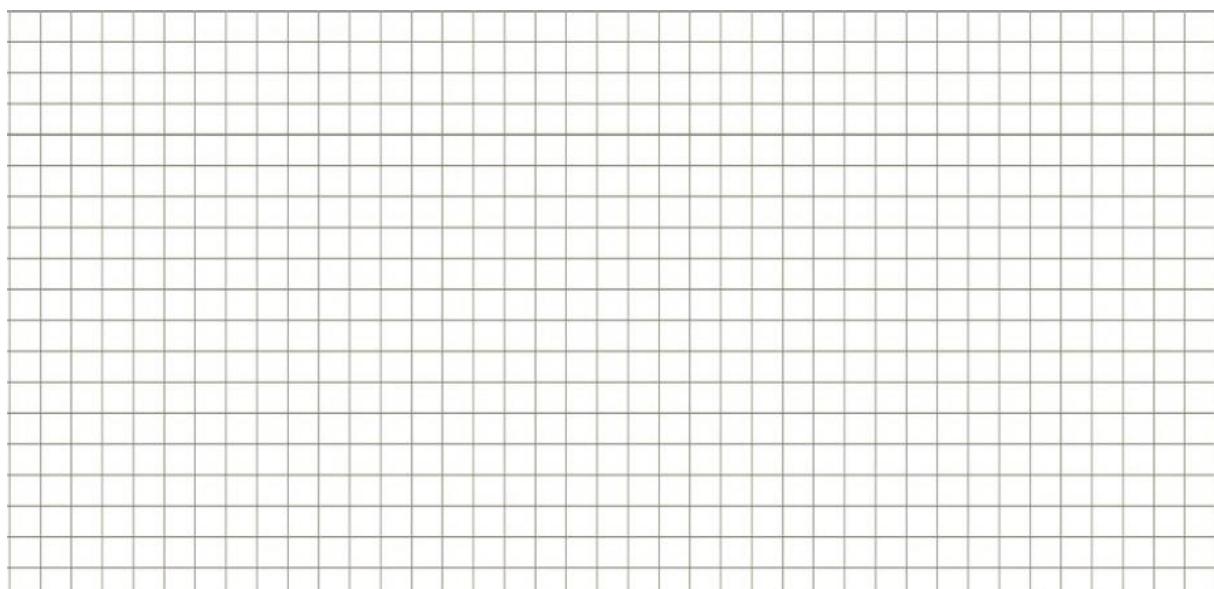
3.8.1 Grafikkarten

Sobald mit dem Desktop-PC komplexe Grafikanwendungen mit 3D-Szenen wie zum Beispiel Spiele oder Rendering-Programme betreiben möchten, ist eine eigene Grafikkarte notwendig. Solche Grafikkarten verfügen teilweise über mehr Transistoren auf der GPU als klassische CPUs, haben mehrere GB eigenes Hochleistungs-RAM und benötigen von ihrer Bauart her mehrere PCIe-Ports, weil sie zusätzliche Anschlüsse für die Stromversorgung für die GPU und die Kühlung benötigen. Teilweise verbrauchen diese spezialisierten Grafikkarten bis zu 250W unter Hochlast, was wiederum das Vorhandensein eines entsprechend leistungsfähigen Netzteils voraussetzt.



3.8.2 IGP - Onboard-Lösungen

Während es bis vor wenigen Jahren noch üblich war, Desktop-PCs mit eigenen Grafikkarten auszustatten, setzen sich immer mehr die Onboard-Lösungen (Integrated Graphics Processor) durch, die die Funktionalität einer Grafikkarte in den Chipsatz des Mainboards integrieren. Diese integrierten Grafiklösungen sind für den Büro- und den einfachen Multimediaterieb durchaus ausreichend. Onboard-Lösungen teilen sich meist den Arbeitsspeicher mit der CPU. Man spricht hier von „Shared Memory“. IGPs sind auf mittlerweile allen handelsüblichen Mainboards verbaut.



3.8.3 Auflösungen

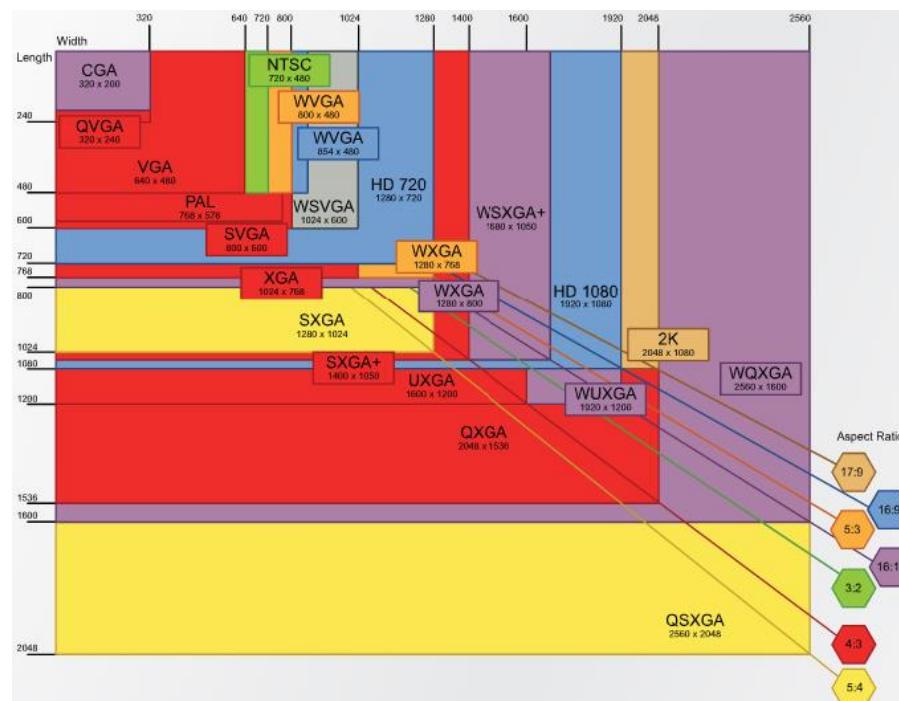
Das Bild des Monitors (natürlich auch des Beamers etc) setzt sich aus tausenden von einzelnen Bildpunkten zusammen. Jeder Bildpunkt (Pixel) kann auf den heute gängigen LED oder OLED-Bildschirmen gesondert angesteuert und mit einem Farbewert versehen werden. Bei der Wahl des richtigen Ausgabegeräts müssen bzgl. der Qualität zwei Faktoren berücksichtigt werden:

- Die **Auflösung** wird durch die Anzahl der Pixel auf der horizontalen und vertikalen Achse angegeben. Eine Auflösung von 800 x 600 bedeutet, dass der Monitor auf der X-Achse 800 Pixel und auf der Y-Achse 600 Pixel darstellen kann. Das sind insgesamt 480.000 Pixel.
- Es kommt bei der Bildqualität aber vor allem auch darauf an, wie groß bzw. klein die Fläche ist, auf der diese 480.000 Pixel untergebracht werden. Das ist die **Pixeldichte**, die in DPI (Dots per inch) angegeben wird. 300 DPI würde bedeuten, dass auf 2,54 cm 300 Pixel untergebracht werden können. Je höher diese Pixeldichte, desto besser ist in der Regel die Bildqualität.

Die Auflösungen sind genormt. In den Spezifikationen von Grafikkarten und Monitoren ist immer genau angegeben, welche Standards unterstützt werden. Beispiele für solche Videoformate als Standard sind:

Format	Technik	Breite	Höhe	Seitenverh.	Pixel
VHS	analog	320	240	4:3	76.800 (0,08 MP)
S-VHS	analog	533	400	4:3	213.200 (0,21 MP)
DVD-Video (PAL)	digital	720	576	4:3 oder 16:9	414.720 (0,41 MP)
HDTV („720p“)	digital	1280	720	16:9	921.600 (0,92 MP)
FullHD („1080p“)	digital	1920	1080	16:9	2.073.600 (2,07 MP)
WUXGA	digital	1920	1200	16:10	2.304.000 (2,3 MP)
UHDV-1	digital	3840	2160	16:9	8.294.400 (8,3 MP)
4K	digital	4096	3072	4:3	12.582.912 (12,58 MP)
UHDV-2	digital	7680	4320	16:9	33.177.600 (33,2 MP)

Diese Standards können wie folgt visualisiert werden:



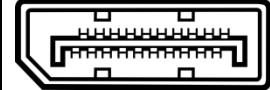
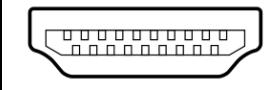
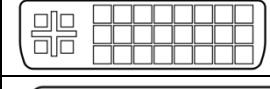
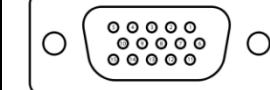
Je höher die Auflösung, desto mehr Datendurchsatz und/oder Speicherplatz wird natürlich benötigt.

3.8.4 Farbtiefe

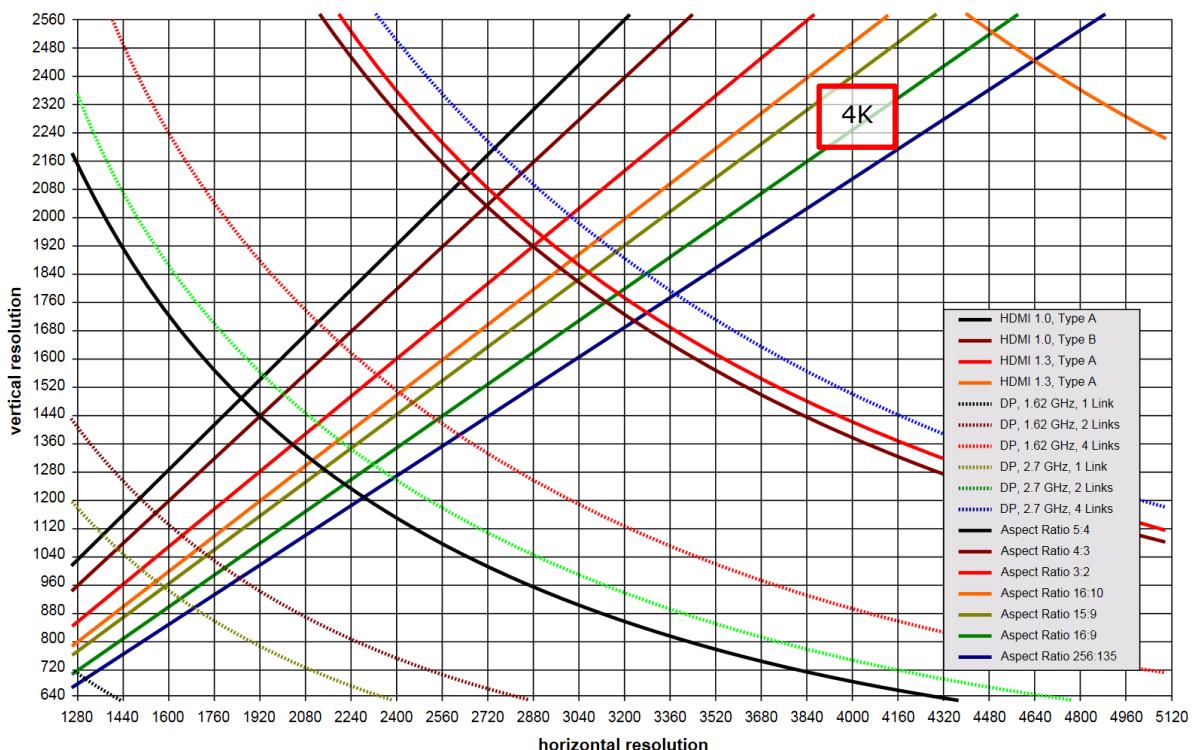
Ein weiterer Faktor der die Bildqualität beeinflusst ist die Farbtiefe. Diese gibt an, in wie vielen verschiedenen Farben ein Pixel leuchten kann. Da die Farbtiefe in Bit angegeben wird, ist es recht einfach diese zu berechnen. Liegt die Farbtiefe bei 4 Bit, können damit 16 unterschiedliche Farben dargestellt werden. Bei 8 Bit sind es schon 256 Farben, bei 16 Bit 65.536 Farben und bei 24 Bit gar 16,7 Millionen unterschiedliche Farben.

3.8.5 Anschlüsse

Es gibt zahlreiche unterschiedliche Standards für den Anschluss von Peripheriegeräten wie Monitoren und Beamer, von denen die wichtigsten folgende sind:

	Display Port	Digital
	HDMI	Digital
	DVI	Digital
	VGA	Analog

Die unterschiedlichen Verbindungstypen – achten Sie hier wieder auf die Versionierungen! – unterstützen unterschiedliche Videoauflösungen. In der folgenden Abbildung stellen die Geraden die Kombination unterschiedlicher Bildschirmauflösungen dar. Die Parabeln zeigen jeweils die theoretisch möglichen Grenzen eines Standards. Eine Auflösung bei 4K (4096x2304 Pixel) setzt bei der Videowiedergabe mindestens den Standard HDMI 1.3 voraus.



Jetzt wird's richtig scharf

Der Pay-TV-Sender Sky geht mit den ersten UHD-Sendern an den Start. Ab Oktober beginnt Sky mit der Ausstrahlung von Sendungen in Ultra-HD-Auflösung. Allerdings ist dafür neue Hardware nötig. Im Video zeigen wir Ihnen, ob sich der Umstieg von Full-HD auf 4K für Sie überhaupt lohnt.

Der Pay-TV-Sender Sky macht endlich ernst und beginnt im Oktober mit der Ausstrahlung von Inhalten in 4K. Dabei will sich der Sender erst auf sein Steckenpferd, die Sportübertragung, konzentrieren. Doch um UHD-Inhalte via Sky zu empfangen, brauchen Sie neue Hardware. CHIP erklärt, worauf es ankommt.

Was Sie brauchen:

Sie sind bereits Kunde bei Sky? Dann die gute Nachricht vorweg: Ab Oktober lassen sich die UHD-Sender von Sky empfangen. Die schlechte: Sie brauchen dafür einen neuen Receiver, der leider gar nicht billig ist. Rund 100 Euro veranschlagt Sky für seinen neuen Empfänger, den man nun online vorbestellen kann. Damit ist der Receiver fast doppelt so teuer, wie das alte Full-HD-Gerät. Dabei sind die Empfangsgeräte stets Leihgeräte und dürfen vom Kunden während der Laufzeit des Abos verwendet werden.

Quelle: http://www.chip.de/artikel/Sky-startet-erste-UHD-Sender-im-Oktober-Jetzt-gibt-s-4K-TV_100667812.html, Abruf: 30.09.2016

IFA: Neue Sharp-Fernseher inklusive 8k-TV & Harman Kardon-Soundsystem

Auf der IFA in Berlin präsentiert SHARP ein komplett neues TV-Line-up und wirft zugleich einen Blick in die Zukunft. So zeigt SHARP als einer der ersten Hersteller auch gleich mehrere Prototypen von für den japanischen Markt konzipierten 8k-Fernsehern mit IGZO-Display-Technologie im 85 und 98 Zoll-Format und sogar einen 27 Zoll-Monitor mit 8k-Auflösung. Die neuen Spitzenmodelle für den deutschen Markt bieten Ultra-HD/4k-Auflösung, High Dynamic Range (HDR) und bis zu 75 Zoll Bilddiagonale.

SHARP führt im neuen Sortiment sechs Serien von UHD-TVs mit Bildschirmen zwischen 43 und 75 Zoll Diagonale. Für eine gute Bildqualität sollen die Bildverbesserungsalgorithmen ACE PRO Ultra und Advanced Color Engine PRO sorgen. SHARPs Active-Motion-Technologie stellt darüber hinaus sicher, dass auch die Bewegungsschärfe stets optimal ist. Die Flaggschiffe der CUF8672-Serie gehen noch einen Schritt weiter und unterstützen Ultra-HD-Bilder mit hohem Dynamikumfang (HDR). Ein Ultra-HD-fähiger Triple-Tuner mit Empfangsmöglichkeiten für Funk-, Kabel- und Satellitenfernsehen, sowie mindestens je drei bis vier HDMI- und USB-Anschlüsse (davon einmal USB 3.0), die Vielfalt für externe Quellen bieten. 4K-Videos aus Drohnen, Camcordern oder Actioncams sowie hochauflösende Fotos von der Digitalkamera lassen sich dank HEVC/H.265-Unterstützung direkt aus dem Internet auf das Fernsehgerät streamen. Alternativ stehen zahlreiche drahtlose Verbindungsmöglichkeiten zur Verfügung. Mit Bluetooth, DLNA, MHL und Miracast lassen sich Inhalte von Smartphones, Tablets oder Notebook-PCs übertragen. Abgerundet wird SHARPs „smarter“ Ansatz von der Aquos Net+ Smart-TV-Plattform.

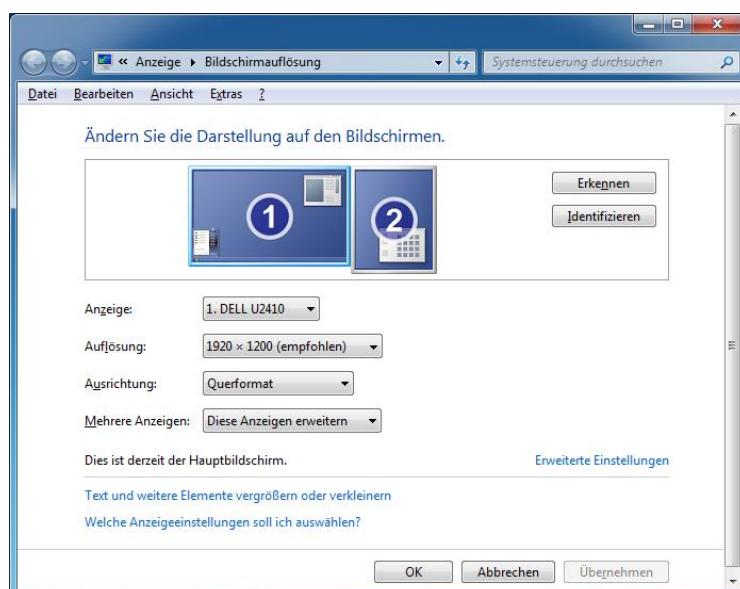
Quelle: <http://www.areadvd.de/news/ifa-neue-sharp-fernseher-inklusive-8k-tv/>, gekürzt; Abruf: 01.10.2016

3.8.6 Monitor

Monitor und Grafikkarte müssen logischerweise miteinander kommunizieren und somit gemeinsame Standards teilen, wie den Typ des Anschlusses (HDMI, Display-Port, VGA etc), die unterstützte Farbtiefe und Auflösung. Kaufentscheidende Faktoren für Monitore sind:

- Diagonale (angegeben in Zoll/Inch)
- Helligkeit (angegeben in cd=Candela; je höher desto besser)
- Kontrast (zB: 1000:1; je höher desto besser)
- Blickwinkel (zB: 176°; je höher desto besser)
- Punktdichte (zB: 85dpi; je höher desto besser)

An die meisten (auch onboard) Grafikkarten können oft mehrere Monitore angeschlossen werden, da in der Regel sowohl ein analoger als auch ein digitaler Anschluss verbaut sind oder die Grafikkarte für den Multi-Monitorbetrieb ausgelegt ist. Windows sollte sämtliche Monitore über Plug&Play erkennen und diese in der Systemsteuerung unter Anzeige einbinden. Dort kann eingestellt werden, ob der Desktop über mehrere Monitore erweitert werden oder einfach dupliziert werden soll. Außerdem können an dieser Stelle die Ausrichtung (Querformat oder Hochformat) und die Auflösung für jeden angeschlossenen Monitor eingestellt werden.



Auf mobilen Geräten müssen Sie einen Monitor meist erst mit der Tastenkombination FN+F4 oder FN+F5 aktivieren. Oft funktioniert das auch mit der Taste WINDOWS+P. Damit ein Monitor unter Windows automatisch erkannt wird muss er natürlich eingeschaltet sein ☺

Weitere Informationen hierzu online unter <http://windows.microsoft.com/de-at/windows/move-windows-between-multiple-monitors#1TC=windows-7>

3.9 Gehäuse und Netzteil

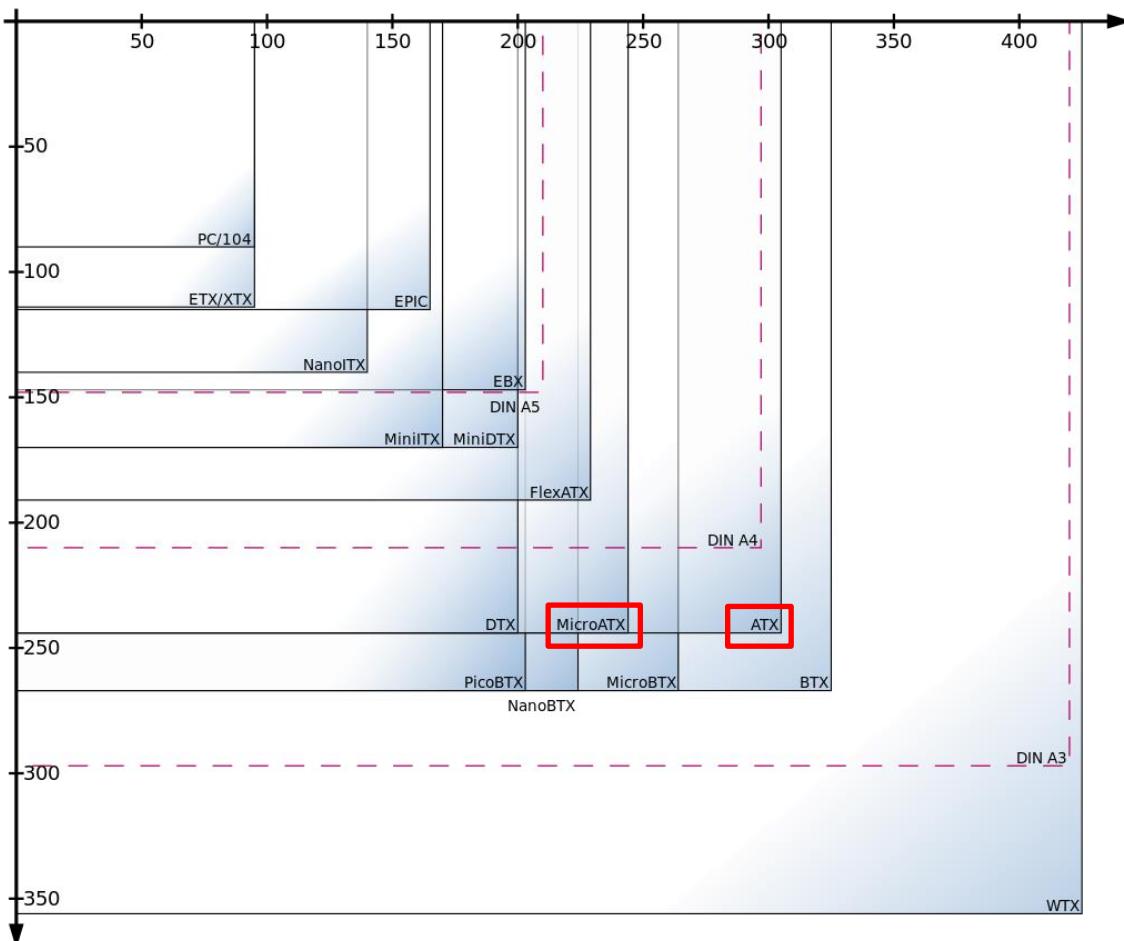
Das Computergehäuse hat die Funktion, alle Komponenten des Computersystems korrekt zu platzieren und vor äußereren Einflüssen zu schützen. Das könnten Erschütterungen, Hitze, Staub und Ungeziefer etc. sein. Da die elektronischen Komponenten auch unter Spannung stehen sollen natürlich auch die Anwender/innen geschützt werden. Gehäuse stehen in allen möglichen **Typen** zur Verfügung. Big-Towers, Desktops, Mini-Towers, Cubes etc.



Die Auswahl des Gehäusetyps bleibt weitgehend dem Einsatzzweck überlassen. Während ein Tower wohl eher dann eingesetzt wird, wenn mehrere Laufwerke eingebaut werden sollen, eignen sich Desktops eher für den klassischen Arbeitsplatz.

Nicht dem Zufall sollte man allerdings den **Formfaktor für das Mainboard** des Gehäuses überlassen. Da das Mainboard eine bestimmte Größe hat und im Gehäuse natürlich nicht locker sitzen darf muss es befestigt werden. Dies geschieht mit Schrauben, die durch bestehende Löcher im Mainboard mit dem Gehäuse verschraubt werden.

Werden klassische Desktop-Rechner angeschafft, dann sind die Bauformen **ATX** und **Micro-ATX** (μ ATX) nach wie vor die vorherrschenden Formate. Diese beiden Formate haben ungefähr die Fläche eines A4-Papiers, weichen jedoch in Länge und Breite voneinander ab.



Beispiel

Antec Sonata III, 400W ATX - Abmessungen (BxHxT): 206x425x463mm •
extern: 3x 5.25", 2x 3.5" • intern: 4x 3.5" (quer, Laufwerksschienen) •
Lüfter (vorne): 1x 120mm (optional) • Lüfter (hinten): 1x 120mm • Front
I/O: 2x USB 2.0, 1x eSATA, 1x Kopfhörer, 1x Mikrofon • Farbe: schwarz •
Fronttür

1. Wie viele interne 3,5"-Laufwerke können eingebaut werden?



2. Welche Anschlüsse befinden sich vorne?

Eine weitere Recherche zeigt, dass folgendes Netzteil mitgeliefert wird:

Antec EarthWatts 400, 400W ATX 2.2 - Lüfter: 80mm • PFC: aktiv • Anschlüsse: 4x SATA, 2x 6-Pin PCIe • +3.3V: 20A • +5V: 20A • +12V1: 17A • +12V2: 17A • -12V: 0.8A • +5V SB: 2.5A • durchschnittliche Effizienz: 83%, 80 PLUS zertifiziert • Formfaktor: ATX PS/2 • Abmessungen (BxHxT): 150x86x140mm • Herstellergarantie: drei Jahre

3. Wie viele Festplatten im SATA-Format können angeschlossen werden?
4. Es soll eine Grafikkarte eingebaut werden, die in Hochlast bis zu 250W verbrauchen soll. Ist das Netzteil dafür geeignet?

A large, empty grid area for writing notes, consisting of approximately 20 columns and 20 rows of small squares.

3.10 Betriebssysteme

Das Betriebssystem (OS, Operating System) ist das grundlegende Computerprogramm. Es steuert die Hardware, koordiniert die Ressourcenzugriffe der Anwendungsprogramme und stellt dem Benutzer Steuerungsmöglichkeiten zur Verfügung. Folgende Aufgaben werden von Betriebssystemen übernommen:

3.10.1 Funktionen eines Betriebssystems

Prozessmanagement

Während des Betriebs laufen mehrere Anwendungen und Systemaufgaben. Da es dabei nicht möglich sein soll, dass eine Anwendung oder Aufgabe zum Beispiel die gesamte Rechenkraft in Anspruch nimmt, organisiert das Betriebssystem die Aufgaben in mehrere Prozesse und weist diesen (meist dynamisch) Ressourcen zu.

Speichermanagement & Dateiverwaltung

Betriebssysteme übernehmen die Verwaltung des Arbeitsspeichers sowie die Datenspeicherung auf Massenspeicher über spezielle Dateisysteme. Somit müssen sich Programmierer/innen nicht mehr darum kümmern, wo bestimmte Inhalte im Arbeitsspeicher abgelegt werden. Durch einheitliche Dateisystem-Standards wird es auch möglich, dass Dateien auf unterschiedlichen Betriebssystemen geöffnet, gelesen, bearbeitet und gespeichert werden können.

Steuerung und API

Da Computer mit unterschiedlicher Hardware von unterschiedlichen Herstellern arbeiten übernimmt das Betriebssystem über Treiber die Kommunikation mit diesen Geräten und stellt den Softwareentwickler/innen spezielle Schnittstellen zur Verfügung, damit ihre Software mit unterschiedlicher Hardware trotzdem gleich funktioniert. Dadurch wird sichergestellt, dass sich die Programmierer/innen nicht in hunderte technische Anleitungen einzelner Geräte einarbeiten müssen. Vielmehr werden sogar wunderbare Entwicklungsumgebungen zur Verfügung gestellt, die das Entwickeln von Software erleichtern.

Ein- und Ausgabesteuerung

Betriebssysteme übernehmen über die Erfassung von Ereignissen die Kommunikation mit den Anwendern über bestimmte Peripheriegeräte (Tastatur, Tablet, Mikrofon, Touchscreen) und übernehmen gleichzeitig auch die Steuerung diverser Ausgabegeräte wie Bildschirm, Datenträger oder Netzwerke.

Benutzeroberfläche

Betriebssysteme bieten zwei Arten von Benutzeroberflächen: Einerseits die Konsole, in der die Benutzer per Tastatureingabe Befehle eingeben können, was vor allem in der Serververwaltung etc. weit verbreitet ist. Andererseits die grafische Benutzeroberfläche (GUI=Graphics User Interface) die es erlaubt, dass dem Benutzer einheitliche Schaltflächen, Menüs, Symbole, Töne sowie Aktionen wie Mausklicks, Tastatureingaben oder Gesten zur Verfügung stehen. Damit wird die Usability bzw. das „Nutzungserlebnis“ enorm gesteigert.

3.10.2 Aufbau eines Betriebssystems

Der **Kernel** (Kern) ist das Grundlegende Programm eines jeden Betriebssystems. Es läuft bis zum Herunterfahren des Rechners permanent auf dem System und steuert alle wesentlichen Komponenten des Betriebssystems. So lädt der Kernel beispielsweise Treiber von Komponenten oder startet und beendet Prozesse, die dann weitere Aufgaben übernehmen. Da das Grundsystem des Betriebssystems direkt in der CPU für die Organisation aller Komponenten sorgt muss der Kernel ganz eng für die CPU und ihre Architektur kompiliert (Übersetzung in Maschinensprache) werden.

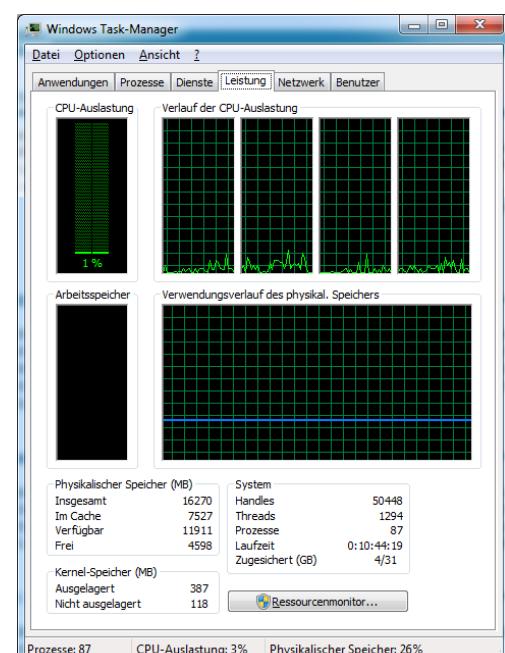
Systemprogramme nehmen Steuerungen und Analysen für das Betriebssystem vor. So gibt es Systemprogramme, die für das Umbenennen, Löschen oder Kopieren von Dateien und Ordnern zuständig sind. Andere Systemprogramme überwachen und regeln den Netzwerkverkehr und wieder andere kümmern sich um die grafische Benutzeroberfläche.

Die **Programmierschnittstelle** oder auch API (application programming interface) stellt Anwendungsprogrammen (zB: Firefox, Outlook, Word und Excel etc.) bestimmte standardisierte Schnittstellen und Bibliotheken zur Verfügung. Diese ermöglicht, dass die entwickelte Anwendung zum Beispiel auf eine Webcam zugreifen kann, unabhängig davon, von welchem Hersteller sie gebaut wurde.

Die **grafische Benutzeroberfläche** ist bei Mac OS und Windows fest im System verankert. Sie startet automatisch mit dem Rechner, weswegen die Benutzer auf diesen Systemen in der Regel niemals aufgefordert werden irgendwelche Systembefehle einzugeben. Die GUI hat meist spezielle Namen. So wird eine Oberfläche auf Mac OS X AQUA genannt. Die Windows-8-Oberfläche hieß ursprünglich METRO, bevor sie aus namensrechtlichen Gründen auf New-Design-UI umbenannt werden musste.

In **Prozessen** werden sämtliche ausgeführten Programme, Anwendungen und Dienste angezeigt, die im Hintergrund oder in der GUI ausgeführt werden. Es gibt Systemdienste die permanent laufen. So stellt beispielsweise der Prozess winlogon.exe sicher, dass sich Benutzer am Rechner An- und Abmelden können. Würde er nicht beim Systemstart mitgeladen werden könnte man sich mit seinem Account gar nicht anmelden. Viele Hersteller lassen im Hintergrund Prozesse starten und laufen um ihre Software aktuell zu halten oder das Nutzerverhalten zu protokollieren. Dementsprechend lohnt es sich, diese Prozesse regelmäßig zu überwachen. Eine schöne Übersicht der häufigsten Windows-Prozesse finden Sie unter <http://www.neuber.com/taskmanager/deutsch/prozess/index.html>.

Mit der Tastenkombination **STRG+ALT+ENTF** können Sie unter Windows den Taskmanager starten. Dieser zeigt Ihnen nicht nur an welche Anwendungen, Prozesse und Dienste gerade laufen sondern auch, wie hoch die Auslastung Ihrer CPU und Ihres Arbeitsspeichers bzw. auch Ihrer Netzwerkverbindungen ist.



3.10.3 Marktanteile von Betriebssystemen

Betriebssysteme sind prinzipiell stark für unterschiedliche Bereiche ausgelegt. Neben dem – immer mehr an Bedeutung verlierenden – Markt für Desktop-PCs sind auch Smartphones, Tablets, Server und Kleinstrechner, wie sie mittlerweile in fast jedem Haushalt oder in Autos vorkommen, wichtige Einsatzbereiche.

3.10.3.1 Desktop PC und Tablets

Auf klassischen Desktop-PCs ist nach wie vor Windows mit – je nach Statistik – 80 % bis 90 % in den unterschiedlichsten Versionen klarer Marktführer. Mit Respektabstand folgen danach Betriebssysteme von Apple und diverse Linux-Derivate. In den letzten Jahren hat sich der Marktanteil von Windows-Systemen jedoch in Summe etwas abgeschwächt, was aber vor allem auf die stärkere Verbreitung von Tablet-PCs zurückgeführt werden kann.

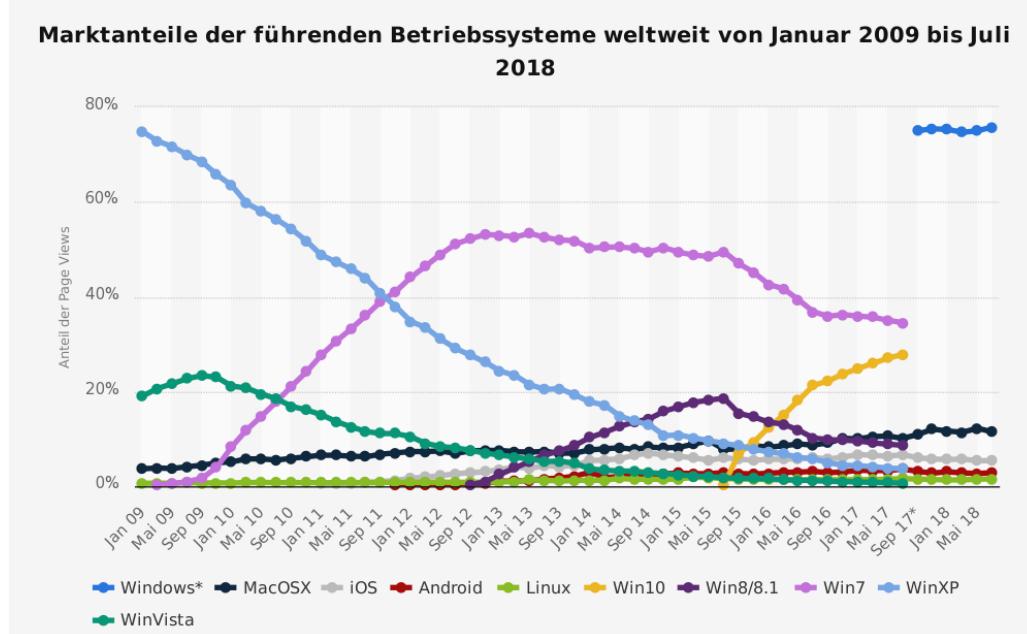
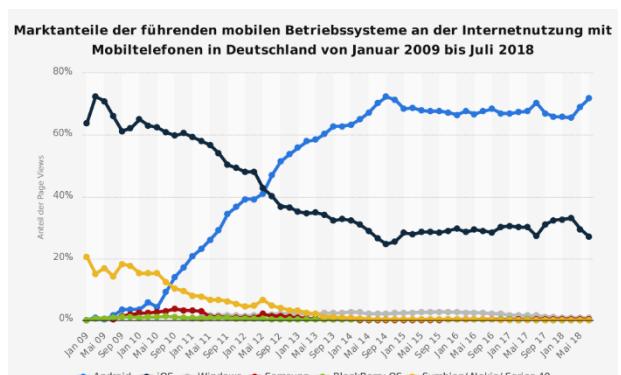


Abbildung 3-1: Marktanteile (gemessen über PageViews) von Betriebssystemen

3.10.3.2 Smartphones

Wie auf dem Markt für Desktop-PCs gibt es auch beim Markt für mobile Devices klare Marktbeherrschende Stellungen. Hier ist Android von Google das mit Abstand am weitest verbreitetste System am Markt.



3.10.3.3 Server

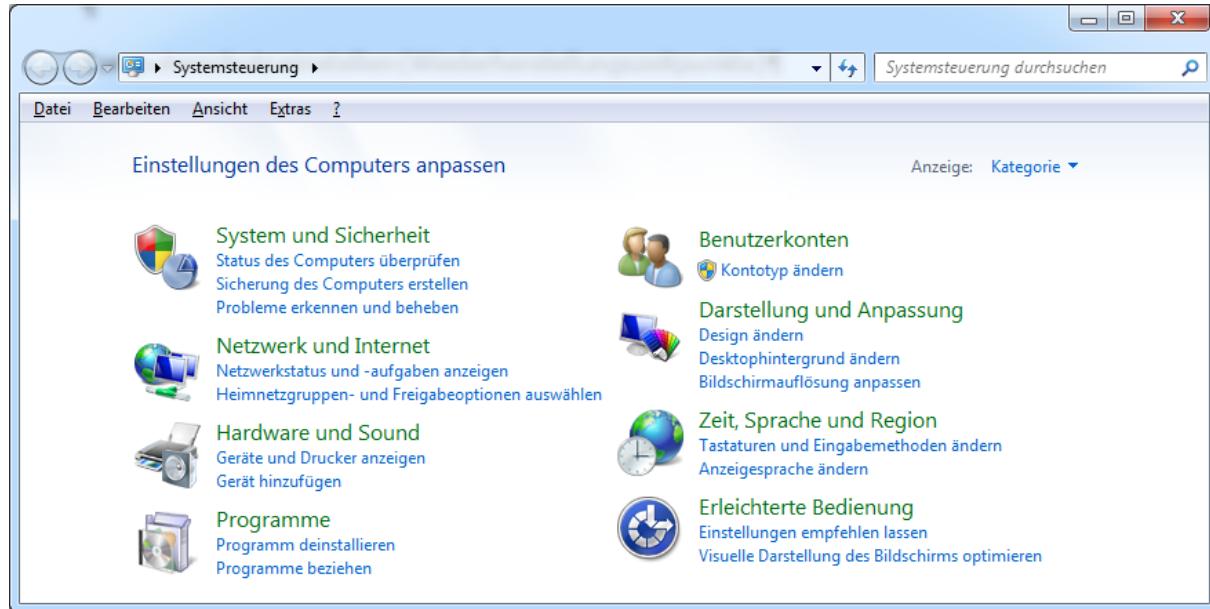
Auf klassischen kleineren Server-Systemen kommen mit ca. 60 % Linux und mit 30 % Windows-Betriebssysteme zum Einsatz. Je größer das Server-System, desto stärker verlagert sich dieser Wert zu Linux/Unix. Fast alle Hochleistungsserver setzen auf ein Derivat eines Unix-Betriebssystems.

3.10.3.4 Sonstige Devices

Auf vielen anderen Geräten wie auf Fernsehgeräten, Soundanlagen, in Autos, ja sogar in Waschmaschinen und Kühlschränken werden Linux/Unix-Systeme eingesetzt.

3.10.4 Wichtige Standardfunktionen unter Windows

Die Schaltzentrale eines typischen Windows-Rechners ist die Systemsteuerung. Dort finden Sie alle Hilfsprogramme, die zum Installieren und Deinstallieren von Programmen, von Hardware oder Netzwerkkomponenten notwendig sind. Außerdem können Sie System- und Sicherheitseinstellungen vornehmen und die lokalen Benutzerkonten verwalten.



Sämtliche Funktionen können an dieser Stelle natürlich nicht erklärt werden. Dennoch sollten Sie sich mit den zentralen Funktionen und deren Einstellungsmöglichkeiten von Windows in einer ruhigen Minute vertraut machen. Einige wichtige Einstellungen werden im Folgenden vorgestellt:

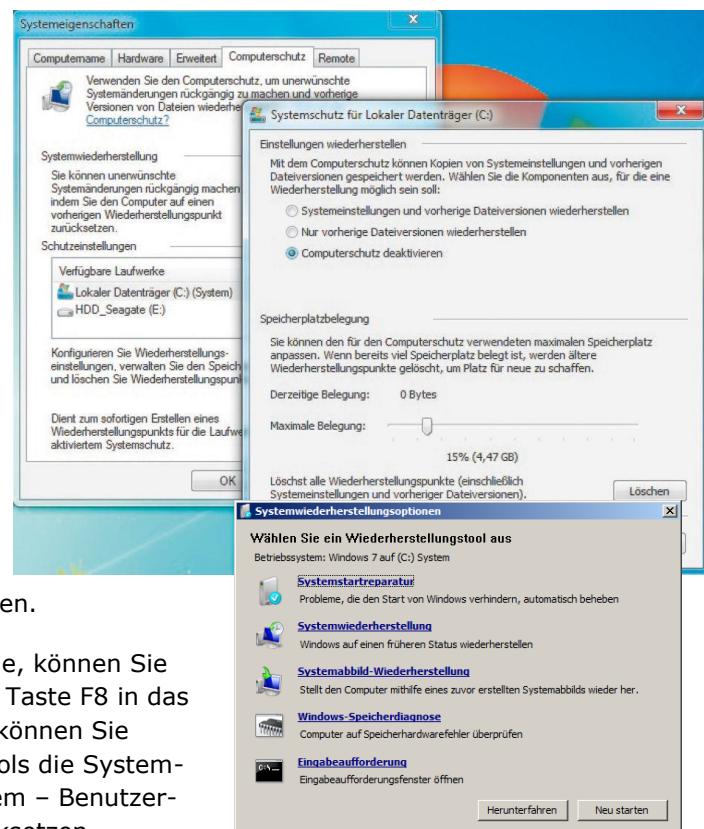
3.10.4.1 Systemeinstellungen wiederherstellen (Wiederherstellungszeitpunkte)

Nach der Installation von Windows sollten Sie auf Ihrem Rechner zwingend den Computerschutz aktivieren. Der Computerschutz dient dazu, unerwünschte Änderungen am System rückgängig zu machen und einen Wiederherstellungszeitpunkt aus der Vergangenheit auszuwählen.

Das ist dann sinnvoll, wenn eine Software- oder Treiberinstallation zu einem fehleranfälligen System führen. Damit werden automatisch Sicherungen von Ihrem System erstellt und von Windows mit Versionen versehen.

Es werden so viele Versionen gespeichert wie Sie dem Tool Systemschutz an maximaler Speicherplatzbelegung einräumen.

Gibt es beim Starten des Systems Probleme, können Sie noch vor dem booten des Systems mit der Taste F8 in das Bootmenü von Windows 8 gelangen. Dort können Sie aus den verfügbaren Wiederherstellungstools die Systemwiederherstellung auswählen und ihr System – Benutzerdateien sind davon ausgenommen – zurücksetzen.



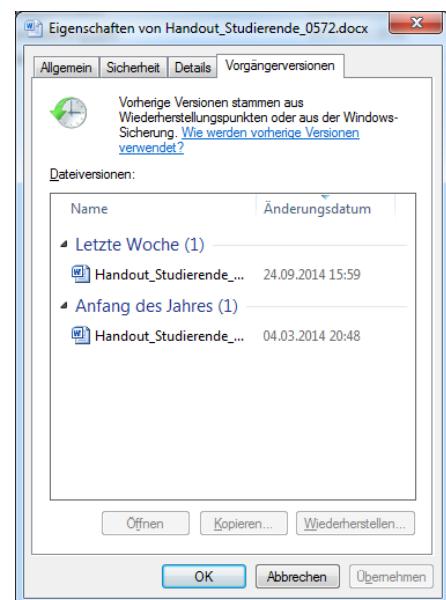
3.10.4.2 Dateiversionen wiederherstellen

Ebenfalls in den Systemeinstellungen können Sie neben der Wiederherstellung der Systemeinstellungen auch die Wiederherstellung von Dateiversionen aktivieren.

Diese Funktion ist besonders für Netzlaufwerke sehr zu empfehlen, da es bei kurzen Netzwerkunterbrechungen in sehr seltenen Fällen zu Datenverlust kommen kann oder, dazu, dass ein anderer Benutzer eine Datei überschreibt.

Ist das der Fall, kann eine vorige Version der Datei ganz einfach mit einem Rechtsklick auf die Datei mit der Auswahl „Vorgängerversion wiederherstellen“ angezeigt werden. Die bestehende Dateiversion kann entweder gesondert geöffnet, kopiert oder gänzlich wiederhergestellt werden.

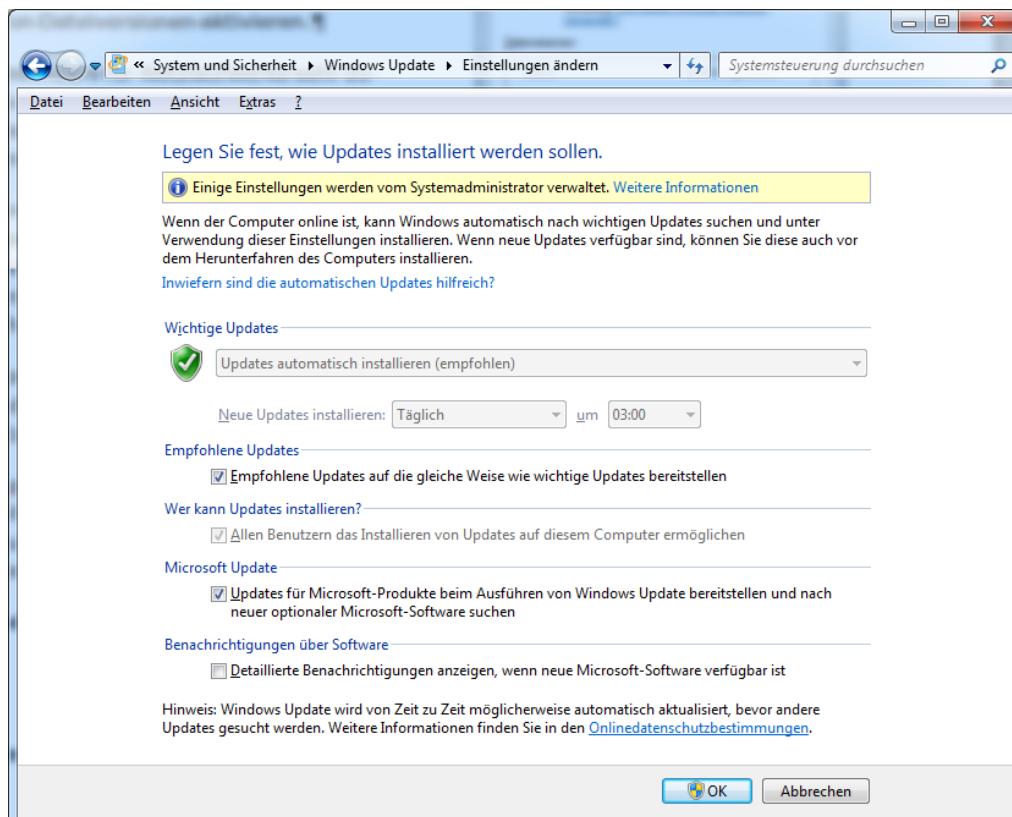
Wie viele Dateiversionen als Sicherung gehalten werden hängt davon ab, wie hoch die Maximale Speicherplatzbelegung in der Option Systemschutz für das entsprechende Laufwerk gesetzt wurde.



Die Dateiversionierung ist keinesfalls mit einem Backup etc. gleichzusetzen. Ist das Laufwerk zum Beispiel von einem Virus befallen, ist mit hoher Wahrscheinlichkeit auch die Dateiversion betroffen. Fällt das Laufwerk aufgrund eines Hardwaredefekts aus, sind natürlich auch die unterschiedlichen Dateiversionen verloren.

3.10.4.3 Automatisches Update einrichten

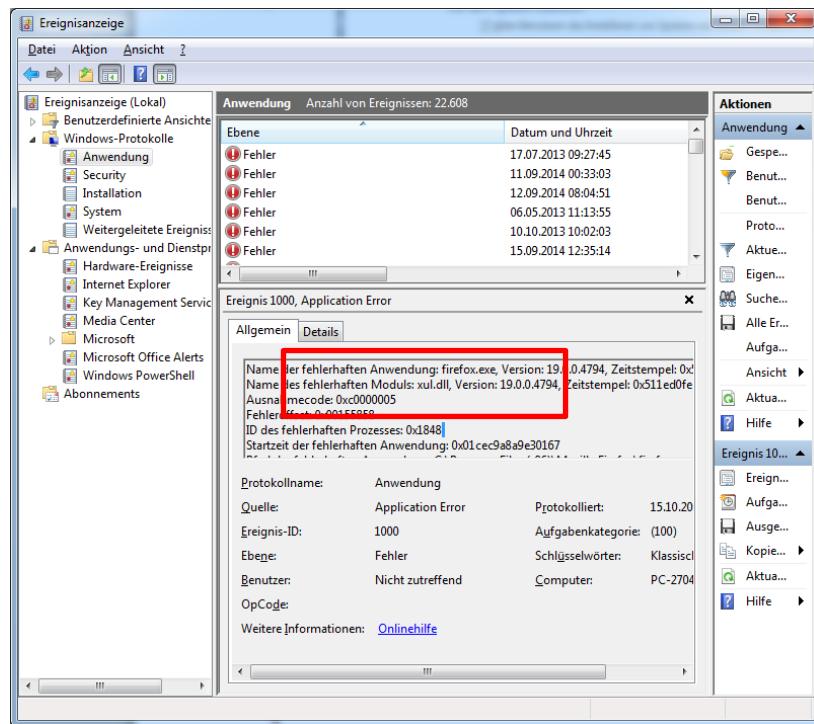
Vor allem wenn Sie mehrere Computer in einem Netzwerk betreuen ist es fundamental notwendig, die Einstellungen für das Windows Update richtig zu setzen. Hier sollte die Option „Updates automatisch installieren“ aktiviert und die Benachrichtigungen für die Verfügbarkeit deaktiviert. Somit werden Updates automatisch beim Starten und Herunterfahren des Computers installiert und konfiguriert.



3.10.4.4 Ereignisanzeige

Die Ereignisanzeige unter Windows ist sozusagen die zentrale Protokollablage. Treten Fehler auf kann hier nachgeforscht werden, durch welches Ereignis dieser Fehler aufgetreten ist. Die Ereignisanzeige erreicht man über den Bereich Wartung der Systemsteuerung.

Im nachfolgenden Beispiel ist im Protokoll für die Anwendungen am 15.10.2013 ein Fehler aufgetreten, der zu einem Absturz von Firefox.exe geführt hat. Schuld war das Modul xul.dll. Diese Information kann nun dazu verwendet werden eigenständig im Netz nachzuforschen, was die Datei xul.dll bewirkt oder diese Information an den Support weiterzuleiten.



3.10.4.5 Benutzer einrichten

Das Verwalten von Benutzern ist unter Windows auf lokaler Ebene denkbar einfach. In der Systemsteuerung können Sie im Bereich Benutzer neue Benutzerkonten hinzufügen, bearbeiten oder löschen. Jeder Benutzer erhält automatisch seinen eigenen Bereich für persönliche Dateien, auf die andere Benutzer, mit Ausnahme jener mit der Rolle Administrator, nicht zugreifen können.

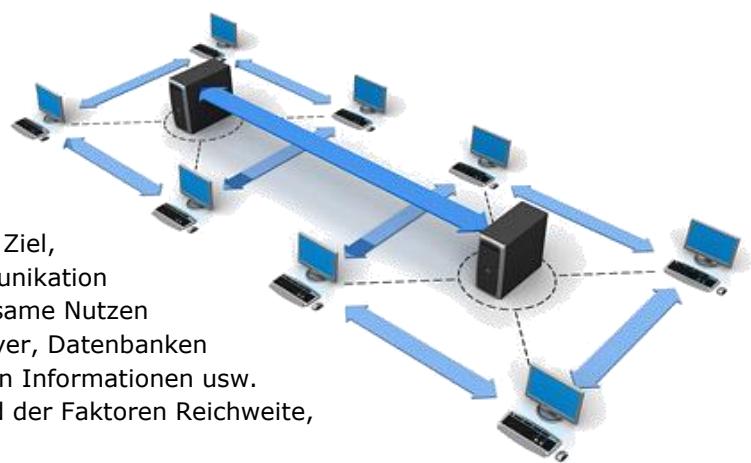


Problematisch ist das Arbeiten mit einem Administratorenkonto im produktiven Betrieb. Ruft nämlich zum Beispiel ein Administrator unbeabsichtigt eine kompromittierte Website mit Schadsoftware auf, kann diese unbeachtet im Hintergrund Schadsoftware installieren. Bei normalen Benutzern würde das aufgrund fehlender Zugriffsrechte zu einer Fehlermeldung führen.

Um diese Problematik zu entschärfen wurde mit Windows Vista die „User Account Control (UAC)“ (Benutzerkontensteuerung) eingeführt die auch den Administrator bei der Installation von Software jedes Mal zur expliziten Bestätigung auffordert.

4 Netzwerke

In der Informatik versteht man unter einem Netzwerk in der Regel einen Verbund technischer Systeme, in der Regel einzelner Computer. Ein Netzwerk kann jedoch auch aus Sensoren oder Anschlüssen etc. bestehen. Das Ziel, Netzwerke aufzubauen ist einerseits die Kommunikation zwischen den einzelnen Rechnern, das gemeinsame Nutzen unterschiedlicher Ressourcen wie Drucker, Server, Datenbanken usw. oder auch das gemeinsame Berechnen von Informationen usw. Gemeinhin können Computernetzwerke anhand der Faktoren Reichweite, Technologie und Topologie klassifiziert werden.



4.1 Klassifizierung von Netzwerken

4.1.1 Reichweite von Netzwerken

4.1.1.1 Lokale Netzwerke

Als lokale Netzwerke gelten **Personal Area Networks** (PAN) werden Netzwerke bezeichnet, das aus Kleingeräten wie Mobiltelefonen, PDAs, Uhren etc. aufgebaut werden kann. In der Regel erfolgt die Kommunikation innerhalb eines PANs drahtlos, zum Beispiel über Bluetooth oder IrDA (Infrarot).

Ein **Local Area Network** (LAN) ist ein lokales Netzwerk, das an ein einzelnes zusammenhängendes Areal gebunden ist, wie einen Raum oder ein Gelände. Nahezu jedes Unternehmen, jede Schule, jede Universität oder jede andere größere Organisation vernetzt ihre Computer über ein LAN. Während unter LAN meist eine physische Verkabelung mit Kupfer- oder Glasfaserkabeln (Lichtwellenleiter) verstanden wird, bezeichnet man unter WLAN (Wireless LAN) jene Netzwerke, die über Funk miteinander verbunden werden. Oft besteht ein lokales Netzwerk in einer Organisation jedoch aus einer Kombination aus einem oder mehreren LANs und WLANs.

4.1.1.2 Nichtlokale Netzwerke

Metropolitan Area Networks (MAN) bezeichnen Netzwerke, die auf ein Stadtgebiet beschränkt sind und somit eine Stadt, Gemeinde oder andere abgrenzbare Region umfassen. Ein Beispiel dafür wären innerstädtische universitäre Netzwerke, innerstädtische Netzwerke von ISP (Internet Service Provider) usw.

Wide Area Networks (WAN) sind Netzwerke, die meist mehrere Städte, eine größere Region oder sogar ein ganzes Land abdecken. In Österreich wäre das zum Beispiel das universitäre AcoNet oder die Internet Provider A1, UPC, Silverserver usw.



Global Area Networks (GAN) sind weltweite Netzwerke, die mehrere Länder, ganze Kontinente oder sogar die ganze Welt miteinander verbinden. Das größte GAN bezeichnet man heutzutage als „Internet“. Es gibt aber auch andere GANs, die für wissenschaftliche, militärische oder geheimdienstliche Zwecke verwendet werden.

4.1.2 Technologien von Netzwerken

Sowohl bei LAN und WANs werden unterschiedliche Technologien verwendet. Üblich ist bei WANs der Einsatz von **Glasfaserverbindungen**, da diese sehr hohe Datenübertragungsraten leisten können. Im Gegensatz zu Kupferkabel ermöglichen diese auch das Überbrücken deutlich höherer Distanzen. Fast alle LANs sind über Glasfaser miteinander verbunden.

Anders jedoch meist die Verkabelung auf der „letzten Meile“ (vom MAN des ISP) zu den Endanwendern, also der Punkt zwischen Teilnehmeranschluss und Wählamt/Vermittlungsstelle. Für diese Verbindung wurde das bestehende Telekommunikationsnetz verwendet, das auf **Kupferkabeln** basiert. Auch in größeren Gebäuden wurde bis vor wenigen Jahren noch Kupferkabeln für die Verbindung von Stockwerken und anderen größeren Distanzen verwendet. Heutzutage werden bei Neubauten fast überall statt Kupferkabeln Glasfaserkabeln verlegt, da diese als zukunftssicher gelten. Zur Signalübertragung jedoch später mehr.

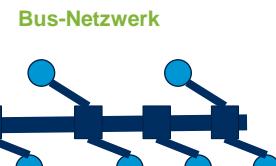
4.1.3 Topologien von Netzwerken

Wesentlich für die Beschreibung von Netzwerken ist die physikalische oder logische Grundform, in der die einzelnen Geräte organisiert sind. Diesen Aufbau bezeichnet man als Topologie. Bestimmte Netzwerkhardware und bestimmte Standards setzen unterschiedliche Topologien voraus, mit denen jeweils wieder unterschiedliche Ziele verfolgt werden können.

4.1.3.1 Broadcast-Netzwerke

Unter Broadcasting-Netzwerken bezeichnet man solche Strukturen, in denen Informationen an alle im Netzwerk angeschlossenen Rechner gesendet werden.

So bezeichnet man als **Bus-Topologie** ein Netzwerk, in dem die einzelnen Knoten hintereinander an einem einzigen Kabelstrang angeschlossen sind. Die beiden Enden eines Bus-Netzwerks sind jedoch nicht miteinander verbunden. Jeder Knoten kann daher auf alle Informationen zugreifen, die in das Übertragungsmedium eingespeist werden. Der Vorteil einer solchen Struktur ist, dass das Routing entfällt, also die Steuerung des Datenverkehrs mit Sender und Empfänger.

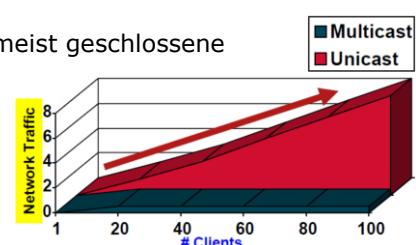


Ähnlich ist auch der Aufbau einer **Ring-Topologie**. Hier hängen ebenfalls alle Knoten an derselben logischen Leitung. Somit erhält auch hier jeder Rechner die gleiche Information. Die bekannteste Ring-Topologie ist Token Ring. In einem Token Ring-Netzwerk wird durch einen Token versucht Kollisionen von Datenpaketen dadurch zu verhindern, dass nur ein Rechner im Netzwerk für eine bestimmte Zeit Daten senden darf. Danach kommt der nachfolgende Rechner im Ring an die Reihe usw.



Da jeder Rechner in Broadcasting-Netzwerken prinzipiell von jedem anderen Knoten sehr leicht zu erreichen ist, würden solche Topologien in offenen Netzwerken zu einem hohen Sicherheitsrisiko führen. Deswegen filtern die meisten Router in öffentlichen Netzen Multicast-Pakete (also jene Datenpakete, die prinzipiell an alle angeschlossenen Knoten adressiert sind) heraus.

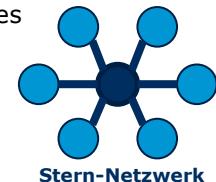
Wenn Broadcast-Netzwerke verwendet werden, dann sind diese meist geschlossene Systeme. Wie zum Beispiel bei IPTV, also Fernsehangebote von Internet Service Providern und auch andere Dienste, die das gleiche Signal an viele Rechner adressieren. Diese verwenden Multicast-Broadcasting um den Datenverkehr im Netzwerk im Gegensatz zu Unicast-Netzwerken (Point-to-Point) drastisch zu verringern.



4.1.3.2 Point-to-Point-Netzwerke

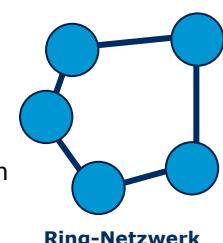
Bei Point-to-Point-Netzwerken (P2P) sind jeweils zwei Rechner direkt miteinander oder über einen Knoten (node) verbunden. Es gibt daher beim Senden von Nachrichten meist keine direkte Verbindung zwischen dem Sender und dem Empfänger. Die Datenpakete müssen daher über Intermediäre geleitet werden. Damit diese Weiterleitung funktioniert, müssen alle beteiligten Rechner ein bestimmtes Routing-Protokoll unterstützen, damit die Nachricht auch wirklich beim Empfänger ankommt.

Bei der **Stern-Topologie** sind alle Knoten mit jeweils einem Kabel über ein zentrales Gerät (Verteiler) miteinander verbunden. Das ist bei P2P-Netzwerken typischerweise ein Switch, manchmal auch ein Hub. Fällt ein Knoten aus, hat das keine Auswirkung auf den Rest des Netzwerks. Fällt hingegen der Verteiler aus, ist keine Kommunikation zwischen den Knoten mehr möglich. Das Netzwerk kann jedoch durch neue Knoten sehr einfach erweitert werden. Als Nachteil gilt der hohe Verkabelungsaufwand.



Stern-Netzwerk

Bei der **Ring-Topologie** ist jeder Knoten mit jeweils zwei anderen verbunden. Dadurch ergibt sich ein ringförmiges Netzwerk. Der Datentransfer erfolgt hier in eine Richtung bis zum Bestimmungsort. Dadurch, dass jeder einzelne Knoten als Verstärker auftreten kann, sind sehr weite Übertragungsdistanzen möglich. Fällt ein Knoten aus, dann bricht jedoch das Netzwerk zusammen, so die Daten nicht einfach in die andere Richtung übertragen werden können (Reverse Mode).



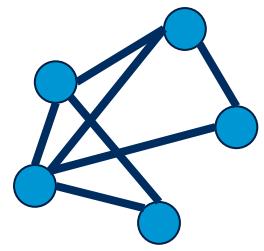
Ring-Netzwerk

Bei der **Baum-Topologie** werden Nachrichten hierarchisch an den jeweils nächst höheren Knoten übertragen. Ausgehend von einem zentralen Kabelstrang gehen die „Verästelungen“ in beliebige Richtungen ab, an denen entweder einzelne Knoten oder ganze Netzwerke (Baum-, Ring- oder Stern) hängen können. In Baum-Netzwerken können neue Nodes sehr einfach hinzugefügt oder entfernt werden ohne die Funktionsweise des Netzwerks zu beeinflussen. Fehlfunktionen von übergeordneten Nodes können jedoch zu Netzausfällen führen. Außerdem müssen tw. sehr viele Nodes überbrückt werden um Datenpakete zuzustellen.



Baum-Netzwerk

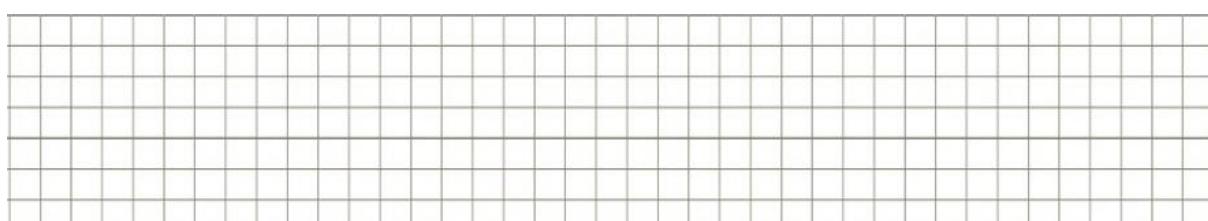
In **vermaschten Netzwerken** (meshed networks) muss jeder Knoten mit zumindest zwei anderen Knoten direkt verbunden sein. Dadurch ist eine gewisse Sicherheit gegenüber von Ausfällen gegeben, da die Datenpakete jeweils über einen alternativen Weg gesendet werden können. Sind alle Knoten miteinander direkt verbunden spricht man von einem vollständig vermaschten Netzwerk, der ausfallsichersten Form eines Netzwerks. Die Nachteile liegen bei solchen Netzwerken jedoch in den Ressourcen (Kabel etc) sowie im hohen Routing-Aufwand von Datenpaketen.



Vermaschtes Netzwerk

4.1.3.3 Physikalische und logische Topologien

Wichtig ist, dass es einen Unterschied zwischen der physikalischen und der logischen Topologie geben kann. Die physikalische Topologie kann zum Beispiel aus praktischen Gründen heraus gewählt worden sein, obwohl von der Funktion des Netzwerkes her eine komplett andere Anwendung herrscht. Wird für die Verbindung von 5 PCs zum Beispiel ein HUB eingesetzt, dann liegt eigentlich ein busförmiges Netzwerk vor, da die Datenpakete an alle angeschlossenen PCs gesendet werden. Wird hingegen ein Switch verwendet, sind nur die jeweiligen Partner in den Datenaustausch eingebunden und es liegt somit ein sternförmiges Netzwerk vor.

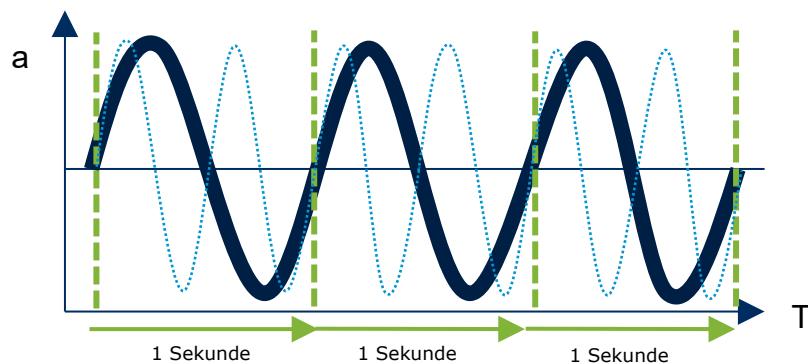


4.2 Grundlagen der Signal- und Datenübertragung

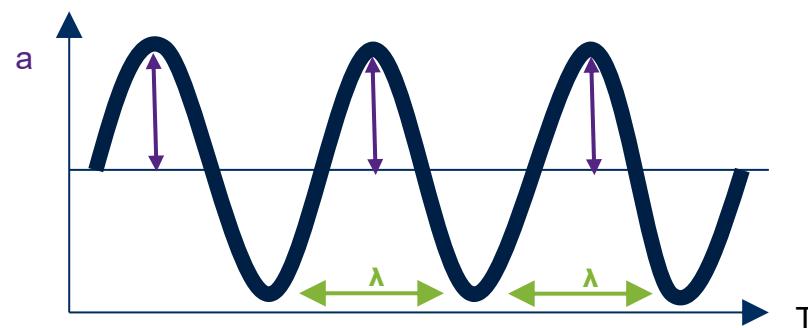
Unter dem Begriff der Datenübertragung versteht man verschiedene Verfahren zur Übertragung von Informationen. Diese Informationen können Sprache, optische Signale oder Daten (Bits) sein. Neben einem Sender und einem Empfänger benötigt man zur Datenübertragung noch eine physikalische Größe (wie zum Beispiel elektrische Spannung oder die Frequenz von elektromagnetischen Wellen).

Elektromagnetische Wellen sind durch Frequenz, Wellenlänge und Amplitude charakterisiert. Beispiele sind Radiowellen, Mikrowellen, Licht, Gammastrahlung etc. Radiowellen sind zum Beispiel solche elektromagnetischen Wellen, deren Wellenlänge zwischen 10 cm und 100 km in einem Frequenzbereich von mehreren Kilohertz bis ca. 3 GHz liegen kann.

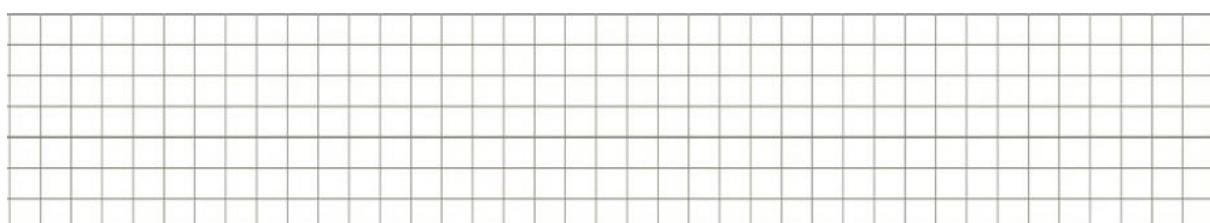
Durch Modulation können bestimmte Frequenzen der Wellen gezielt genutzt werden. Somit wird es zum Beispiel möglich, dass in einem Land mehr als ein TV-Sender übertragen werden kann, über eine Telefonleitung mehr als ein Gespräch übertragen und über ein Kupferkabel sowohl Sprache als auch Daten übertragen werden können. Das gleichzeitige Übertragen von verschiedenen Daten über eine Leitung oder Frequenz bezeichnet man als Multiplexing.



Bei der Signalübertragung wird die **Frequenz f in Hertz (Hz)** angegeben. Sie gibt die Anzahl der Schwingungen in einer **Periode T** wieder. In der oberen Abbildung repräsentiert die dicke dunkle Welle genau 1 Hz in der Periode Sekunde. Die gepunktete hellere Linie repräsentiert hingegen 2 Hz pro Sekunde.

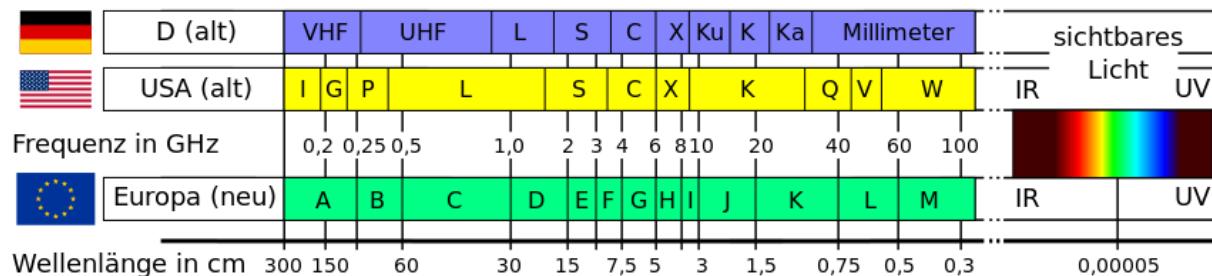


Die **Amplitude a** ist der maximale Ausschlag einer Sinuswelle ausgehend von ihrem Gleichgewicht. Die **Wellenlänge λ** ist die Distanz zwischen zwei durchgehenden Schwingungen.



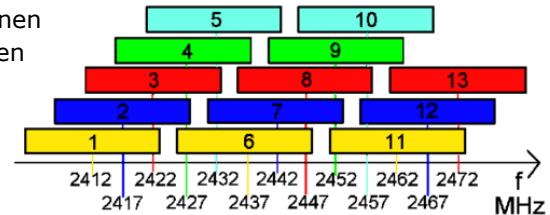
Unterschiedliche Frequenzen sind in sogenannten Frequenzbändern genormt, damit es zu keinen Überschneidungen kommen kann. Diese Frequenzbänder sind meist gesetzlich festgelegt und werden öffentlich vergeben und sind demnach reguliert (zB: GSM, UMTS, LTE etc.). Hierbei ist die Wellenlänge das maßgebliche Kriterium für die Festlegung eines Frequenzbandes.

Die Frequenz des Standards WLAN 802.11.n liegt in der Bandbreite 2,4 GHz bis 2,4835 GHz. Somit beträgt die Wellenlänge 12,5 cm. Dieser Wert ergibt sich aus der Lichtgeschwindigkeit (299.792.458 m/s) geteilt durch die Frequenz in Hertz ($2.400.000.000$) = 0,125 Meter.

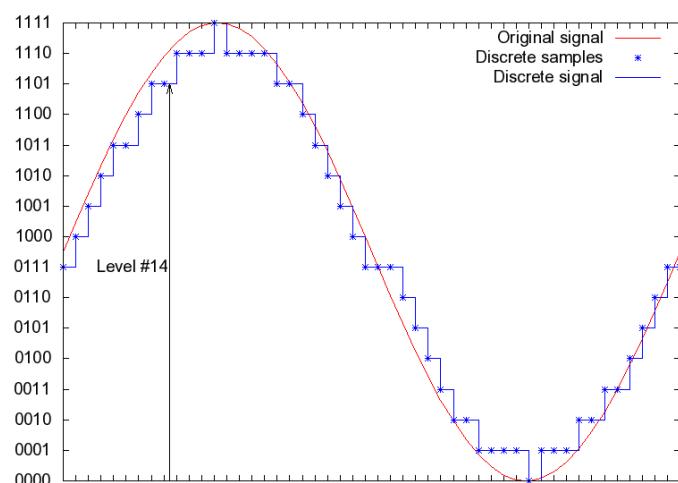


Durch A/D-Wandler (Analog zu Digital) die analogen Wellen in eine digitale Form übersetzt. Dabei sind die folgenden Faktoren für die Datentransferrate notwendig, die angibt, wie viele Daten in einem bestimmten Zeitraum übertragen werden können:

1. Je höher die Bandbreite, desto mehr Kanäle können gleichzeitig benutzt werden und desto mehr Daten können gleichzeitig übertragen werden. WLAN-Standards können zum Beispiel 13 Kanäle verwenden, die – je nach Standard – im Bereich zwischen 2,4 GHz und 2,48 GHz liegen.



2. Je höher die Frequenz pro Periode (zB: Sekunde), desto mehr Symbole (Bits) können in diesem Zeitraum übertragen werden. Wie viele Bits pro Periode übertragen werden können, hängt davon ab, mit welcher Auflösung die analoge Welle digital abgetastet werden kann. Wird ein Eingangssignal zum Beispiel mit 8 Bit ($2^8=256$) abgetastet, bedeutet das, dass das analoge Signal in 256 Stufen übersetzt werden kann und pro Welle somit ein Byte übertragen werden kann.



Ganz Wesentlich ist in der Datenübertragung der Aspekt der **Richtungsabhängigkeit**:

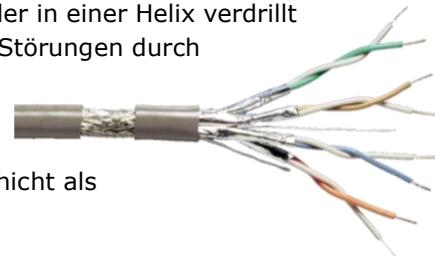
- **Simplex** bedeutet, dass die Daten immer nur in eine Richtung übertragen werden können. Es gibt nur einen Sender und einen oder mehrere Empfänger (zB: Fernsehen, Radio etc.)
- **Halve duplex** bedeutet, dass die Daten immer nur alternierend gesendet oder empfangen werden können (zB: Taxi-Funk)
- Bei **Full Duplex** können die Daten hingegen gleichzeitig gesendet und empfangen werden (zB: Telefon, DSL usw.).

4.3 Träger der Datenübertragung

Über einen Träger werden die Datensignale in einer bestimmten Frequenz gesendet. Dabei werden solche Träger verwendet, die eine möglichst Störungsfreie Kommunikation ermöglichen. Bei kabelgebundenen Netzwerken bestehen die Träger meist aus Kupfer. Lichtwellenleiter (Glasfaser) bestehen aus Kunststoff- oder Quarzglasfasern.

4.3.1 Übertragung per Kabel

Die wichtigsten Kabel für den Aufbau von Netzwerken sind **Twisted-Pair-Kabel**. Diese bestehen aus meistens acht Kupferlitzen, von denen jeweils zwei miteinander in einer Helix verdrillt sind. Dadurch wird verhindert, dass sich die Signalqualität durch Störungen durch elektromagnetische Felder beeinträchtigt wird, wie das der Fall bei parallel laufenden Kabeln wäre. Um Störungen von außen zu vermindern sind diese Kabel meistens noch durch Kupfer oder Aluminium abgeschirmt und natürlich mit einer Kunststoffschicht als Isolierung ummantelt.



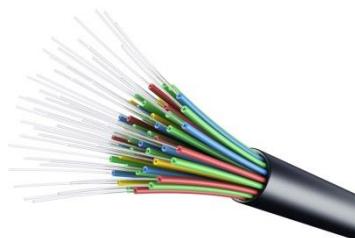
Je nachdem wie gut das Kabel geschirmt ist, können höhere oder eben niedrigere Frequenzen erreicht werden. Je höher die Qualität des Kabels desto höher ist auch die Bandbreite, die erreicht werden kann und desto mehr Daten können übertragen werden. Bei Twisted-Pair-Kabeln kann man die folgenden Kabeltypen (die typischerweise noch in Gebrauch sind) unterscheiden:

Bezeichnung	Länge	Frequenz	Geschwindigkeit			
			10 Mb/s	100 Mb/s	1 Gb/s	10 Gb/s
CAT-5	100m	100 MHz	x	x		
CAT-5e	100m	100 MHz	x	x	x	
CAT-6	100m	250 MHz	x	x	x	x
CAT-6a	100m	500 MHz	x	x	x	x

Häufig werden diese Twisted-Pair-Kabel auch **Patchkabel** genannt. Diese Bezeichnung kommt daher, dass Kabel in bestimmten Längen zB: 1 Meter vorkonfektioniert werden und bereits über RJ45-Anschlüsse an beiden Enden verfügen. Diese Patchkabel werden vorwiegend für den Anschluss der Endgeräte zB an der Netzwerkdoose eingesetzt.



Insbesondere für die infrastrukturelle Verkabelung werden heutzutage jedoch Lichtwellenleiter (LWL) verwendet. Diese Glasfaserkabel erreichen heutzutage eine Kapazität von ca. 1 Terabit pro Sekunde, welche wahrscheinlich auf bis zu 150 Terabit pro Sekunde je Faser gesteigert werden kann⁴. Der große Vorteil von Lichtwellenleitern gegenüber Kupferkabeln ist, dass sehr hohe Reichweiten und höhere Transferraten möglich sind. Da die LWL ohne Strom funktionieren (Unterseekabel ausgenommen) gibt es auch keine elektromagnetischen Störeinflüsse. Der Kerndurchmesser einer Glasfaser liegt zwischen 50 und 1.500 millionstel Metern (µm).



Die Funktionsweise ist, dass zu Beginn der Übertragungsstrecke elektrische Signale über Leucht- oder Laserdiode in Lichtimpulse umgewandelt werden. Am Ende der Leitung wandeln Fotodioden die optischen Signale wieder in elektromagnetische Impulse um.

⁴ <http://www.welt.de/print-welt/article459954/Eine-Glasfaser-erlaubt-maximal-zwei-Milliarden-Telefongespraeche.html>, Abruf am 02.10.2014

4.3.2 Übertragung per Funk

Im privaten Einsatz werden Netzwerke inzwischen weitaus häufiger über **WLAN** (Wireless Local Area Network) aufgebaut als über kabelbasierte Lösungen. Die meisten Internet-Service-Provider liefern bereits Router mit WLAN-Option standardmäßig aus. Der häufigste Standard für die Drahtlose Übertragung von Daten ist der Standard IEEE 802.11 (Arbeitsgruppe des Institute of Electrical and Electronical Engineers), der drahtlose Netzwerke beschreibt.



Ähnlich wie bei den Netzwerkabeln unterscheidet man auch bei WLAN (Wireless LAN, früher auch WiFi genannt) unterschiedliche Standards, die sich hinsichtlich ihrer Reichweite, Übertragungsrate und Funktechnik unterscheiden.

Standard	Frequenz	Brutto-Datenrate
802.11	2,4 GHz	2 Mbit/s
802.11b	2,4 GHz	5,5/11/22 Mbit/s
802.11g	2,4 GHz	54 Mbit/s
802.11a	2,4 GHz	54 Mbit/s
802.11n	2,4 GHz / 5 GHz	450 Mbit/s
802.11ac	5 GHz	1,3 Gbit/s

In letzter Zeit versuchte man die Frequenzen von WLAN vor allem durch das gleichzeitige Nutzen mehrere Kanäle und komplexer Multiplexing-Verfahren weiter zu erhöhen. Gemein ist den Standards allerdings, dass sie fast alle auf der Trägerfrequenz von 2,4 GHz funken, also jene Frequenz, die auch Mikrowellenherde verwenden um Wassermoleküle zu erhitzen. Sie ist lizenziert frei.

Die meisten Endgeräte wie Laptops, Tablets oder Mini-PCs sowie natürlich auch Smartphones sind heutzutage mit WLAN-Adaptoren ausgestattet, die nicht nur einen sondern mehrere Standards unterstützen. Diese Angabe sieht dann in der Gerätebeschreibung wie folgt aus: Unterstützt WLAN IEEE 802.11 a/b/g/n.

Weitere Standards für die Drahtlose Übertragung von Daten sind **UMTS** (3G) oder **LTE** (4G), welche Datenübertragungsraten von bis zu 42 Mbit/s bis zu 150 Mbit/s ermöglichen. Diese Standards nutzen die 800/900/1800-MHz-Frequenzbänder oder auch 2,6 GHz, also jene Frequenzen, die früher für Telefonie verwendet wurden (GSM), welche von der RTR vergeben bzw. für einen bestimmten Zeitraum versteigert werden.

Bei allen Funkstandards muss man jedoch beachten, dass es sich bei den Übertragungsraten sehr stark um ideale Werte handelt. Die realen Datentransferraten sind in der Regel niedriger, da diese von vielen anderen Faktoren mit beeinflusst werden. Das wäre zum Beispiel die Distanz zwischen Router und Empfänger, die Blockaden, die zwischen Router und Empfänger vorhanden sind, weitere Geräte, die auf derselben Frequenz und im selben Kanal funkeln und sonstige Störungen. So hat eine Erhebung der Zeitschrift Konsument im Jahr 2013 gezeigt, dass die maximale Datendurchsatzrate bei den Mobilfunkanbietern im UMTS-Bereich statt bei 42 Mbit/s nur bei 16 Mbit/s lag, also nur knapp 40 % des theoretisch möglichen Werts.



4.3.3 Wichtige Netzwerkgeräte

Es gibt mehrere Netzwerkgeräte, die für die Funktionsweise von klassischen Ethernet-Netzwerken unerlässlich sind. Im Folgenden werden die Geräte HUB, SWITCH und ROUTER kurz vorgestellt.

Hub (Knotenpunkt)

Hubs sind physische Netzwerknoten, die die sternförmige Verbindung von Rechnern erlauben. Hubs sind ähnlich wie Verteilersteckdosen im Stromnetz. Sie leiten die Daten einfach an alle Anschlüsse weiter, unabhängig davon, ob die Datenpakete für das Gerät, das am jeweiligen Anschluss hängt auch tatsächlich bestimmt sind. Hubs werden in der Regel dafür verwendet, schnell zB. ein weiteres Endgerät in ein Netzwerk zu integrieren, wie zum Beispiel einen Drucker etc. IM OSI-Referenzmodell würde ein HUB auf der ersten Schicht arbeiten.



Switch (Umschalter)

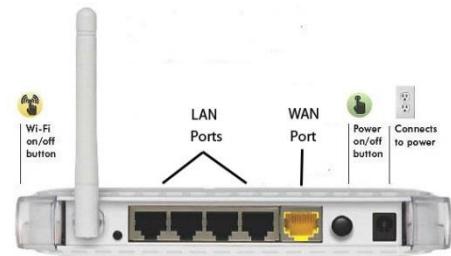
Ein Switch arbeitet ähnlich wie ein Hub. Er ist jedoch etwas „intelligenter“. Da er nämlich im OSI-Referenzmodell schon auf der zweiten Schicht und leiten daher Datenpakete nicht mehr an alle angeschlossenen Geräte weiter. Vielmehr merkt sich der Switch die MAC-Adresse der angeschlossenen Netzwerkkarte und kann dann daher eingehende Pakete gezielt an das Endger



Demgegenüber verfügen Layer-3-Switches über die Möglichkeit, sogar prioritär zu behandeln. Höherwertigere Geräte verfügen über spezielle Zusatzfunktionen wie zum Beispiel die Möglichkeit, virtuelle LANs einzurichten. Das ist zum Beispiel dann sinnvoll, wenn ein Schulnetzwerk und ein Verwaltungsnetzwerk parallel bestehen sollen, es jedoch physisch nur sinnvoll ist, eine Leitung zu nutzen.

Router

Router sind dann sinnvoll, wenn Sie zwei Netzwerke miteinander verbinden möchten. Angenommen, Sie betreiben ein Netzwerk mit 20 Rechnern und möchten, dass Sie alle an das Internet anschließen. Statt 20 gesonderte Anschlüsse bei einem ISP zu erwerben und zu verlegen wird es sinnvoll sein, dass sich diese 20 Rechner einen Anschluss teilen. Dies funktioniert über einen Router, der an ein WAN (also gemeinhin an das Internet) angeschlossen wird und gleichzeitig das Management innerhalb des lokalen Netzwerks übernimmt. Somit hat ein Router auch zwei IP-Adressen. Eine externe Adresse und eine interne Adresse. Über das NAT-Protokoll (Network Address Translation Protocol) weiß der Router genau, welches lokale Gerät welche Anfrage gesendet hat und leitet diese eingehenden und ausgehenden Datenpakete gezielt weiter. In den meisten Fällen sind an SOHO-Routern (Small Office/Home Office) noch zusätzliche LAN-Ports und WLAN verbaut. Somit sind solche Router meistens auch ein Switch.



Netzwerkkarte

Die Netzwerkkarte ist das Bindeglied zwischen dem Desktop-Computer mit dem lokalen Netzwerk. Bei vielen Mainboards sind Netzwerkkarten bereits in den Chipsatz integriert, weswegen auf nahezu allen moderneren Mainboards eine 10/100/1000 Mbit-Netzwerkkarte integriert ist. Oft ist auch eine zweite Netzwerkkarte integriert, nämlich eine W-LAN-Netzwerkkarte. Netzwerkkarten bauen auf der OSI-Schicht 1 eine physische Verbindung zum Netzwerk her und verwenden auf der TCP/IP-Schicht meist Ethernet für den Netzzugang.



4.4 Netzwerkkommunikation verstehen

4.4.1 ISO/OSI Layer Referenz Modell

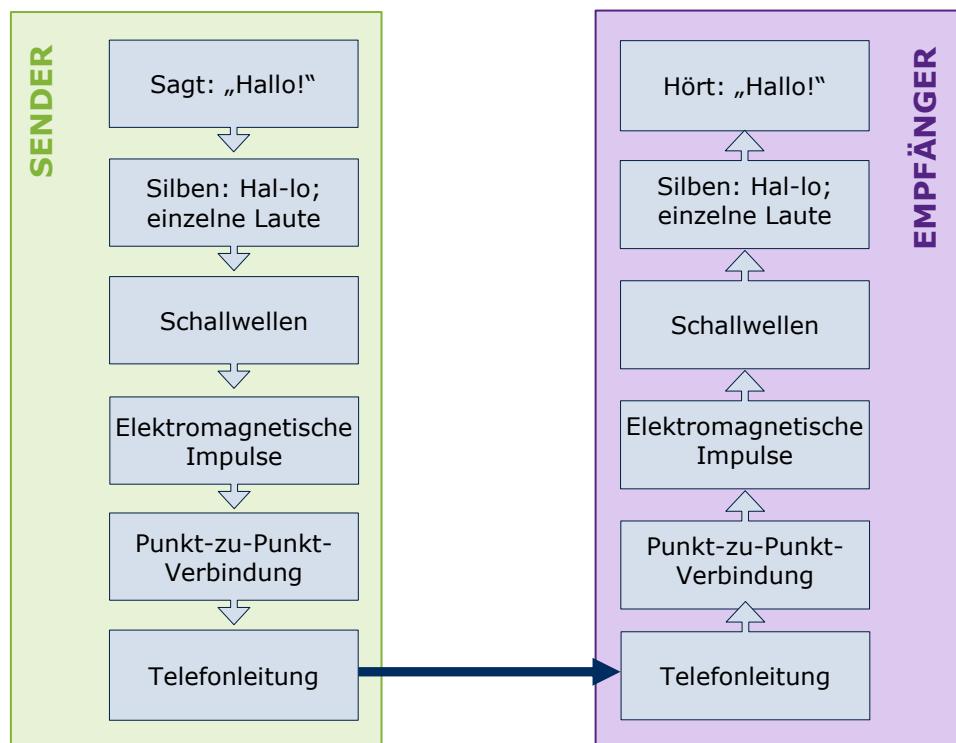
Für einen Laien ist es relativ schwer verständlich, wie genau eine Information von einem Rechner zu einem anderen transportiert wird. Zu viele Faktoren gilt es gleichzeitig zu berücksichtigen wie Anwendung, Ports, Datenübertragungsmodus oder -standard usw. Somit verliert man sich leicht im Dschungel von WLAN über Server, Anwendung, logische und physische Netzwerktopologie usgl.

Um all diese Ebenen, die ein Netzwerk ausmachen, identifizieren zu können bzw. auseinanderhalten zu können, verwendet man Schichtenmodelle. Das verbreitetste ist das OSI-Referenzmodell (OSI=Open Systems Interconnect), das versucht, Netzwerkkommunikation über sieben übereinander angeordnete Schichten zu beschreiben.

Ein Telefongespräch als Beispiel

- Sie rufen über das Festnetz eine Freundin an. Beide Telefone sind physikalisch über eine Telefonleitung miteinander verbunden.
- Beiden Telefonanschlüssen ist eine eindeutige Nummer zugeordnet die gewährleistet, dass Sie Ihre Freundin erreichen und nicht irgendjemand anderen, wie zB den Lehrveranstaltungsleiter!
- Über die Telefonleitung wird jedes Wort, das Sie gesprochen haben über elektromagnetische Impulse übertragen.
- Die Telefone dienen als Bindeglied zwischen den gesprochenen Wörtern und den elektromagnetischen Impulsen, indem sie die akustischen Signale, die in die Hörmuschel gesprochen werden, in elektromagnetische Impulse umwandeln. Am anderen Ende der Leitung angekommen werden diese elektromagnetischen Impulse wieder in akustische Signale übersetzt.

Diese Systematik kann wie folgt skizziert werden:



Wichtig ist bei dieser Darstellung, dass beide Kommunikationspartner nur auf einer Ebene wirklich direkt miteinander verbunden sind, nämlich über die Telefonleitung. Dennoch müssen sich beide Telefone an dieselben Spielregeln halten, damit die Kommunikation reibungslos funktioniert.

Das **OSI-Modell** wird als Referenzmodell für Netzwerkprotokolle verwendet und wurde 1984 als Standard veröffentlicht. Der Zweck des Modells ist, die Kommunikation über unterschiedliche technische Systeme hinweg zu ermöglichen, damit klare Schnittstellen definiert werden können. Das Modell kennt **sieben Schichten**:

Schicht 7 – Anwendung

Auf dieser Schicht werden Informationen aufbereitet und dargestellt. Hier finden die Dateneingabe und die Datenausgabe statt. Somit ermöglicht die Anwendungsschicht die unmittelbare Kommunikation. Ein E-Mail Programm erlaubt zum Beispiel die Eingabe von Text, die es später in ein standardisiertes E-Mail-Format bringt.

Schicht 6 – Darstellung

Auf der Darstellungsschicht werden die Daten für ein bestimmtes System zusammengestellt. Hier passiert die Konvertierung und Übertragung von Datenformaten, Zeichensätzen, grafischen Anweisungen usw. Auch die Verschlüsselung und Dekodierung von Informationen oder die Datenkompression erfolgt an dieser Stelle. Wichtig ist, dass die Informationen bei dieser Schicht am Endgerät schon angekommen sind und dementsprechend bereits verarbeitet werden.

Schicht 5 – Sitzung

Auf dieser Schicht wird die Prozesskommunikation zwischen zwei Systemen gesteuert. Wenn bei einem Telefongespräch beide Gesprächspartner gleichzeitig reden, dann ist die Kommunikation gestört. Somit braucht es klare (implizite) Normen, das zB zuerst der eine Partner ausreden darf bevor der andere sprechen darf. Auf der Sitzungsschicht werden Dienste angeboten, die für einen organisierten und synchronisierten Datenaustausch zur Verfügung stehen

Schicht 4 – Transport

Auf der Transportschicht arbeiten Protokolle wie zum Beispiel TCP oder UDP. UDP wird zum Beispiel beim Übertragen von Videos (Streaming) verwendet, wo es nicht wichtig ist, ob alle Pakete auch tatsächlich ankommen. Fehlen einige Pakete wird das Bild kurze Zeit pixelig. Wird hingegen eine Datei übertragen, dann ist es wichtig, dass alle Informationen in einer genau definierten Reihenfolge ankommen und wieder zusammengesetzt werden können. Dies wäre eine Aufgabe für das TCP-Protokoll. Hier geht es also darum, nach welchem Verfahren die Daten transportiert werden.

Schicht 3 – Vermittlung

In dieser Schicht geht es darum, wie die Datenpakete genau versendet werden sollen. Zum Beispiel wahllos an alle Rechner in einem Netzwerk oder nur an einen bestimmten Rechner. Hier kommt das Routing ins Spiel, also das Weiterleiten von Daten in andere Netzwerke. Das bekannteste Protokoll, das auf dieser Schicht arbeitet ist das IP (Internet Protokoll). Auf dieser Schicht arbeiten zum Beispiel die Hardware Router oder Layer-3-Switches.

Schicht 2 – Sicherung

Hier werden alle Vorkehrungen beschrieben, die dafür sorgen, dass aus den einzelnen Bits, die übertragen – zum Beispiel über elektromagnetische Impulse – ein verlässlicher Datenfluss wird. Eine große Rolle spielt hier zum Beispiel MAC (Media Access Control) oder LLC (Logical Link Control) die dafür sorgen, dass eine Verbindung zwischen zwei Geräten hergestellt, aufrechterhalten und getrennt werden kann. Auf dieser Schicht arbeitet zum Beispiel das Ethernet-Protokoll, WLAN 802.11 usw.

Schicht 1 – Bitübertragung

Auf dieser Schicht steht aus physikalischer Sicht rein die Übertragung der Daten im Vordergrund. Hier wird geregelt, in welcher Struktur die Signale vorliegen sollen. Man beschreibt hier den zulässigen Amplitudenbereich, Start- und Stoppsignale, Übertragungseigenschaften der Medien (Kabel, LWL, Funk usw) usw.

4.4.2 TCP/IP-Referenzmodell

Bereits das ISO/OSI-Referenzmodell zeigt, dass der Datenverkehr in Netzwerken auf mehreren Ebenen abläuft, wobei zwischen diesen Ebenen nur logische Verbindungen bestehen. Die Datenvermittlung selbst erfolgt immer nur auf der ersten Schicht, nämlich der Bitübertragungsschicht. Genauso können jene Protokolle zusammengefasst werden, die man als Internetprotokollfamilie bezeichnet.

OSI-Schicht	TCP/IP-Schicht	Beispiel
Anwendungen (7)	Anwendungen	HTTP, SSH, FTP, SMTP, POP, Telnet, HTTPS, IMAP
Darstellung (6)		
Sitzung (5)		
Transport (4)	Transport	TCP, UDP, SCTP
Vermittlung (3)	Internet	IP (IPv4, IPv6), ICMP, (ARP)
Sicherung (2)	Netzzugang	Ethernet, Token Bus, Token Ring, FDDI, (ARP)
Bitübertragung (1)		

TCP/IP-Protokollsichten können in jeder Netzwerkschicht übertragen werden. Sowohl in einem Ethernet als auch in einem Token-Ring-Netz oder FDDI-Netzwerk. In der **Netzzugang-Schicht** wird beschrieben, welche Netzwerkverkabelung, welche Topologie und welche Zugriffsverfahren genutzt werden. Hier ist das ARP-Protokoll relevant. Das **ARP** (Address Resolution Protocol) ist ein Netzwerkprotokoll, das zu einer bestimmten Netzwerkadresse der Internetschicht die zugehörige physikalische Adresse der Netzzugangsschicht ermittelt (MAC-Adresse). Dieses Protokoll wird fast ausschließlich bei der IPv4-Adressierung in Ethernet-Netzwerken verwendet. Eine MAC-Adresse ist eine eindeutige Nummer für ein Netzwerkgerät die aus 48 Bit besteht und im Hexadezimalformat angeschrieben wird. Ein Beispiel dafür ist: 90:B1:1C:71:06:72. Es können daher insgesamt 2^{48} (also mehr als 35 Billionen) eindeutige MAC-Adressen vergeben werden.

Bei der **Internet-Schicht** geht es um die Vermittlung der einzelnen Datenpakete vom Sender an den Empfänger über ein Netzwerk (mit mehreren Knoten). Auf dieser Schicht arbeiten die Protokolle **IP** (Internet Protocol), **ICMP** (Internet Control Message Protocol) und eben auch ARP. Das Internet-Protocol regelt die Adressierung der IP (IP-Adresse und Subnetzmaske) während das ICMP (Internet Control Message Protocol) für die Kommunikation zwischen den Vermittlungsgeräten zuständig ist. Treten Probleme bei der Paketzustellung auf, wird über das ICMP mitgeteilt, welches Problem aufgetreten ist. Bekannte Anwendungen von ICMP sind zum Beispiel PING oder TRACERT.

Auf der **Transport-Schicht** wird nun – nach der Adressierung – genau geregelt, nach welchem Vorgehen die Daten transportiert werden sollen. Beim **Transmission Control Protocol (TCP)** müssen alle Daten in einer bestimmten Reihenfolge versendet werden. Geht ein Paket verloren, muss es erneut gesendet werden. Wenn zum Beispiel ein Word-Dokument versendet wird, wir typischerweise das TCP-Protokoll verwendet, weil es wichtig ist, dass jeder Buchstabe im Word-Dokument in der richtigen Reihenfolge steht. Das TCP kann also als Transportprotokoll mit Zustellungsversicherung bezeichnet werden. Demgegenüber spielt diese Transportversicherung beim **User Datagram Protocol (UDP)** keine Rolle. Da es hier vielmehr entscheidend ist, in welcher Geschwindigkeit die Datenpakete übertragen werden nimmt man in Kauf, dass es zu kleineren Fehldarstellungen kommen kann, wenn mal ein Paket verloren geht. Beispiele Videostreaming oder VO-IP und andere Multimedia-Anwendungen.

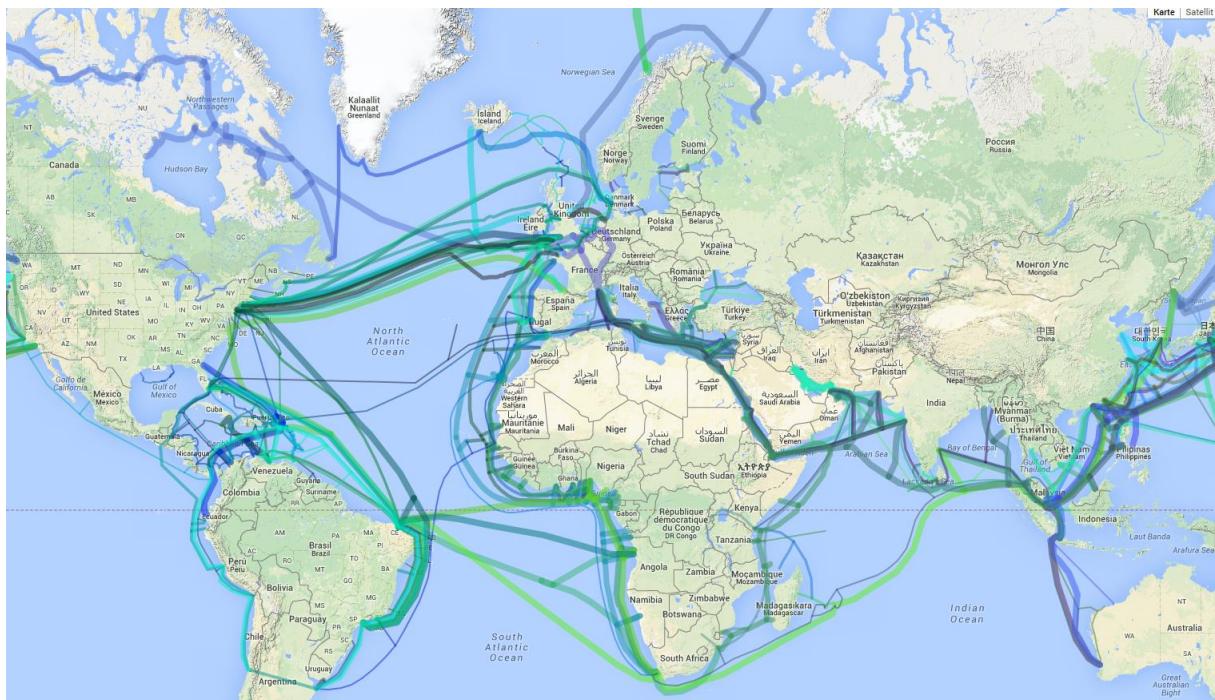
Auf der **Anwendungen-Schicht** geht es dann wirklich um die Daten, die versendet werden sollen. So kann über das HTTP (Hypertext Transfer Protocol) eine Website übertragen werden. Über das File Transfer Protocol (FTP) können Dateien ausgetauscht werden und über das Simple Mail Transfer Protocol (SMTP) können E-Mails versendet werden. Diese Anwendungs-Protokolle nutzen einen bestimmten Port des TCP oder UDP. Dadurch wird sichergestellt, dass ein Paket, das zu einer E-Mail gehört nicht an den Browser geleitet wird usw.

4.5 Der „Aufbau des Internets“

Das Internet ist nichts anderes als ein Verbund von vielen einzelnen Netzwerken. Diese können unterschiedliche Topologie haben, gemeinsam ist jedoch, dass sie eine Adressierung über das IP-Protokoll ermöglichen.

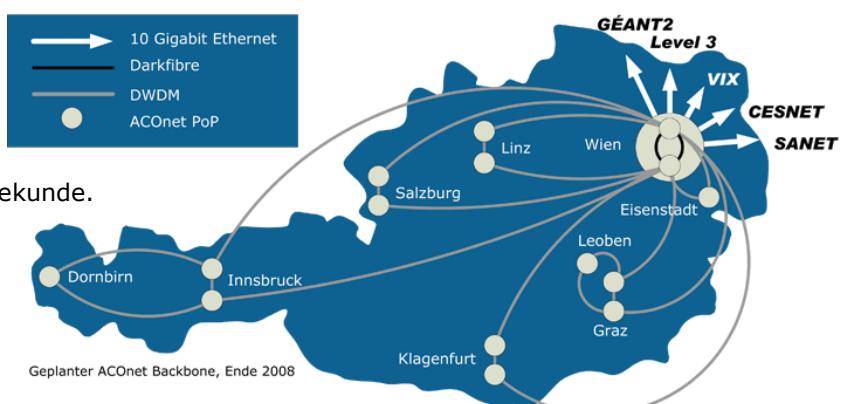
4.5.1 Der physische Aufbau

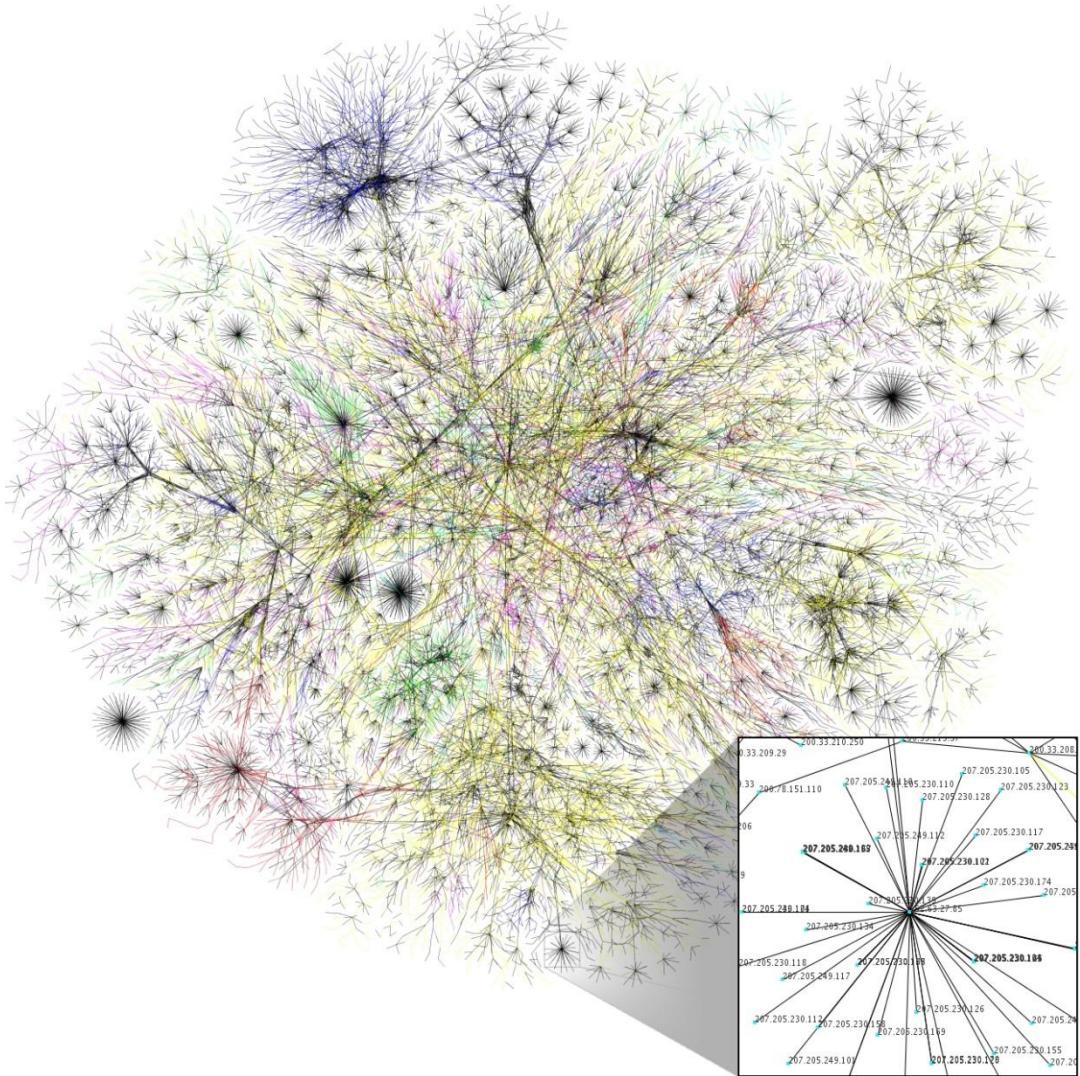
Das Internet besteht aus vielen dezentralen Netzwerken, die miteinander meistens durch Kabelstränge miteinander verbunden sind. Diese Kabel laufen entweder zu Land oder auch unter Wasser, um ganze Kontinente miteinander zu verbinden. Heutzutage werden Kabel mit einer Datendurchsatzrate von bis zu 40 Tbit/s verlegt. Eine gute Übersicht von bekannten Kabeln findet man unter www.cablemap.info.



Natürlich sind die einzelnen Netzwerke auch über Land miteinander verbunden. Dafür werden meist Glasfaserkabel verwendet die hohe Datendurchsatzraten ermöglichen. Meistens führen diese Glasfaserkabel zu Internet Exchange Points (Internet-Knoten/IXP). Die Idee solcher Knoten ist es, den einzelnen Internet Service Providern (ISP) die Möglichkeit zu bieten an einem zentralen Punkt miteinander in Kontakt zu treten. Eine schöne grafische Übersicht aller Internetknoten findet man unter <http://www.internetexchangemap.com>.

In Wien gibt es zum Beispiel zwei Internet-Knoten. VIX1 und VIX2. VIX1 wird vom ZID der Universität Wien in 1010 betrieben und VIX2 vom Unternehmen Interxion in 1210 Wien. Beide Standorte sind miteinander redundant verbunden. Fällt einer aus, kann der andere Knoten einspringen. Über VIX werden pro Sekunde ca. 200.000.000.000 Bit übertragen, also ca. 25 Gigabyte pro Sekunde. Einzelne Netzwerke von Internet-Service-Providern sind ihrerseits direkt mit anderen Netzwerken oder mit einem Internetknoten verbunden.





4.5.3 Das TCP-Protokoll

Das TCP-Protokoll (Transmission Control Protocol) wird zum zuverlässigen bidirektionalen Transport von Daten verwendet. Das bedeutet, dass kein Datenpaket eines Ganzen (zum Beispiel ein Textverarbeitungsdokument) einfach verloren gehen darf und somit einfach Buchstaben oder ganze Sätze fehlen. TCP tauscht an sich keine Daten aus sondern ist lediglich dafür zuständig, in welcher Art und Weise die Datenpakete zwischen zwei Teilnehmern ausgetauscht werden.

Das TCP geht davon aus, dass alle Datenpakete zugestellt werden müssen und nimmt in Kauf, dass es gelegentlich zu Staus in der Datenverbindung kommen kann. Deswegen wird zunächst beim ersten Verbindungsauflauf – verkürzt gesprochen – versucht, ein Datenpaket zu senden. Ist dieses Datenpaket angekommen, wird im nächsten Schritt versucht doppelt so viele Datenpakete zu senden. Ist dieser Schritt wieder erfolgreich, wird diese Anzahl im nächsten Schritt wieder erhöht usw. usf. Dieses Konzept wird „Sliding Window“ genannt. Bricht die Verbindung während der Datenübertragung zusammen, wird wieder versucht, ein einzelnes der verloren gegangenen Pakete zu senden. Gelingt das, wird die Zahl im nächsten Schritt wieder erhöht usw. bis alle Datenpakete beim Empfänger angekommen sind.

4.5.4 Das IP-Protokoll

Eine IP-Adresse besteht aus 32 bit. Eine typische IP-Adresse wäre daher:

1000100111010000000001100011110 wenn man sie binär notiert. Man teilt IP-Adressen jedoch in 8-Bit-Gruppen ein, womit sich vier Oktette ergeben (4 x 8-Bit-Gruppen): 10001001 11010000 00000011 00011110. Im Dezimalsystem dargestellt entspricht das dann 137.208.3.30

Der momentan noch vorherrschende Standard IPv4 besteht demnach aus 32 Bit und kann daher genau 4.294.967.296 eindeutige IP-Adressen vergeben. Da jedoch immer mehr Endgeräte im Internet anzutreffen sind, werden diese IP-Adressen langsam eng. Somit wurde das IPv6-Protokoll mit 128 Bit entwickelt, das dann 340.282.366.920.938.000.000.000.000.000.000.000 verschiedene IP-Adressen darstellen kann (Das sind ungefähr 340 Sextillionen).

IP-Adressen bestehen eigentlich aus zwei Teilen. Der Adresse und der Subnetz-Maske. Mit dieser Systematik können die IP-Adressen besser vergeben werden. Soll beispielsweise ein Netzwerk mit nur einem Teilnetz eingerichtet werden, dann bekommt man eine IP-Adresse zugeteilt (zum Beispiel 137.0.0.0) und setzt die Teilnetzmaske auf 255.0.0.0. Das bedeutet, dass die Adressen 137.0.0.1 bis 137.255.255.254 alle zu diesem Netz gehören. Das sind dann insgesamt 16.777.214 Teilnehmer, weil eben 24 Bit frei gewählt werden können. Da jeweils zwei Adressen reserviert sind, lautet die Berechnung für die möglichen Hosts $2^{24}-2$.

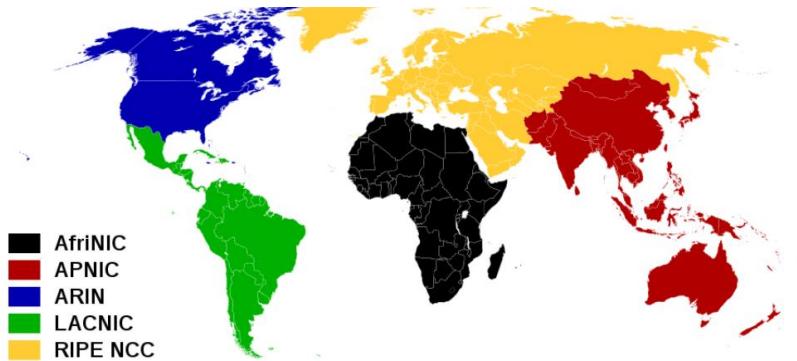
Ein Netzwerk mit einer Subnet-Maske von 255.255.255.0 erlaubt 254 Hosts. In der CIDR-Notation würde man die IP-Adresse wie folgt darstellen: 137.208.3.30/24. Das bedeutet, dass die letzten 8 Bits zum Teilnetz gehören und die ersten 24 Bits zum Adresse.

CIDR-Adresse	Netzmaske	Anzahl der Hosts im Netzwerk
137.0.0.0/8	255.0.0.0	max. 16.777.214
137.208.0.0/12	255.240.0.0	max. 1.048.574
137.208.0.0/16	255.255.0.0	max. 65.534
137.208.48.0/20	255.255.240.0	max. 4094
137.208.48.0/21	255.255.248.0	max. 2046
137.208.48.0/22	255.255.252.0	max. 1022
137.208.48.0/23	255.255.254.0	max. 510
137.208.48.0/24	255.255.255.0	max. 254
137.208.48.128/25	255.255.255.128	max. 126
137.208.48.192/26	255.255.255.192	max. 62
137.208.48.192/27	255.255.255.224	max. 30
137.208.48.192/28	255.255.255.240	max. 14
137.208.48.200/29	255.255.255.248	max. 6
137.208.48.200/30	255.255.255.252	max. 2
137.208.48.200/31	255.255.255.254	Keine
137.208.48.200/32	255.255.255.255	Keine

Beispiel: Wird als CIDR-Adresse die Adresse 203.191.49.48/29 zugewiesen bedeutet das, folgendes:

	Dezimal	Binär
IP-Adresse	203.191.49.48	11001011 10111111 00110001 00110 000
Subnet-Maske	255.255.255.248	11111111 11111111 11111111 11111 000
Gateway	203.191.49.48	11001011 10111111 00110001 00110 000
Host 1	203.191.49.49	11001011 10111111 00110001 00110 001
Host 2	203.191.49.50	11001011 10111111 00110001 00110 010
Host 3	203.191.49.51	11001011 10111111 00110001 00110 011
Host 4	203.191.49.52	11001011 10111111 00110001 00110 100
Host 5	203.191.49.53	11001011 10111111 00110001 00110 101
Host 6	203.191.49.54	11001011 10111111 00110001 00110 110
Broadcast	203.191.49.55	11001011 10111111 00110001 00110 111

Die Zuteilung der IP-Adressen erfolgt zentral durch die ICANN (Internet Corporation for Assigned Names and Numbers). Diese wiederum weist ihren fünf Partnern (Regional Internet Registry) AfriNIC, APNIC, ARIN, LACNIC und RIPE NCC bestimmte Adressbereiche zu. So bekam RIPE NCC von der ICANN 39 /8-Netze zugeteilt, was $39 * 2^{24}$ insgesamt 654.311.424 IPv4-Adressen entspricht. RIPE NCC weist diese wiederum an Internet Service Provider zu, die diese an die Endkunden weiterleiten. Die WU Wien bekam zum Beispiel den Bereich 137.208.0.0/16 zugeteilt. Also alle IP-Adressen zwischen 137.208.0.0 bis 137.208.255.255.



Wichtige reservierte IP-Bereiche

Nicht alle der über 4.000.000.000 IP-Adressen werden öffentlich vergeben. Es gibt einige Ausnahmen, entweder nie vergeben werden oder immer nur private Netzwerke kennzeichnen.

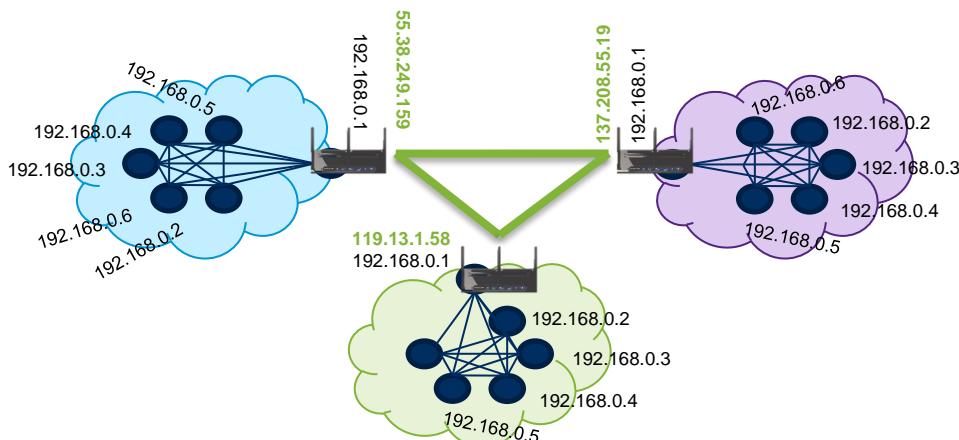
Die IP-Adresse **127.0.0.1** kennzeichnet immer den eigenen Rechner. Er ist auch unter dem Namen localhost erreichbar. Ein Ping auf 127.0.0.1 testet im Wesentlichen, ob die Netzwerkkarte des Rechners funktionsfähig ist oder nicht. Mit **10.0.0.138** erreichen Sie in der Regel Ihren Router.

CIDR	Bereich	Netze	Adressen pro Netz
10.0.0.0/8	10.0.0.0 bis 10.255.255.255	1	16.777.216
172.16.0.0/12	172.16.0.0 bis 172.31.255.255	16	65.536
192.168.0.0/16	192.168.0.0 bis 192.168.255.255	256	256

Außerdem sind die IP-Adressen 224.0.0.0 bis 239.255.255.255 ebenfalls für Netzdienste reserviert. In diesem Fall ist das ein Multicast-Testnetzbereich.

4.5.4.1 Routing im IP-Protokoll

Vorab ist es bei Routing wichtig zu wissen, dass dieses niemals in privaten Netzwerken, also innerhalb eines Netzwerks vorkommt, da hier de facto eine Punkt-zu-Punkt-Verbindung besteht. Über das ARP sind ja innerhalb eines Netzwerks die MAC-Adressen bekannt und somit muss nicht erst eine Route zum Empfänger gesucht werden. Ganz anders sieht es jedoch aus, wenn ein Paket an eine IP-Adresse gesendet werden soll, die sich nicht innerhalb des Netzwerks befindet. Dann nimmt der Router Kontakt mit der „Außenwelt“ auf

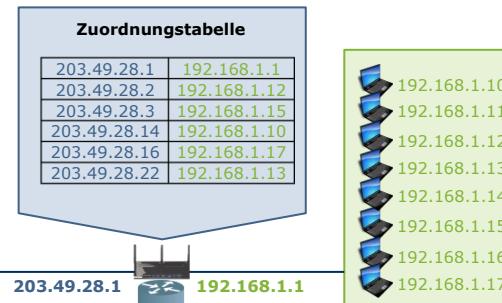


Beim Routing sucht der Router zuerst über das ARP-Protokoll nach, ob sich ein passendes Ziel in seiner Umgebung befindet und leitet das Datenpaket an den nächsten Router weiter, der auf dem Weg zum Ziel liegt. Dadurch, dass ein Router zunächst nie „den“ richtigen Weg zum Ziel kennt, ist der Weg – also, welche Router werden verwendet – zunächst vollkommen offen.

4.5.4.2 NAT: Network Address Translation

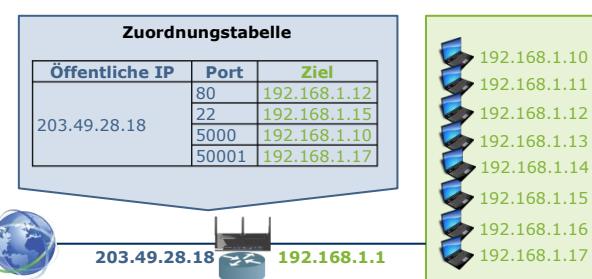
Über NAT werden die Adressen eines privaten Netzwerks über Tabellen öffentlich registrierten IP-Adressen zugeordnet. Angenommen man hat ein Netzwerk mit 200 Rechnern. Davon sollen sechs Rechner mit einer eigenen statischen IP-Adresse von außen erreichbar sein. Weist man nun genau den sechs Rechnern eine eigene IP Adresse zu, dann können die verbleibenden 194 Rechner diese Rechner nicht mehr ohne Routing direkt erreichen und umgekehrt. Um das zu verhindern behilft man sich am Router mit einer Hilfstabelle.

Man trägt einfach eine Weiterleitung in Form einer 1:1-Zuordnung in einem Register ein. Der Router leitet dann die Anfragen direkt an die private IP-Adresse weiter. Wie die interne Struktur des Netzwerks aussieht ist von außen her nicht ersichtlich.



4.5.4.3 IP Masquerading / PAT: Port Address Translation

Eine wichtige Funktion ist das IP-Masquerading, auch Port and Address Translation (PAT) genannt. Wenn man beispielsweise in einem privaten Netzwerk, das über einen Router an das Internet angeschlossen ist, mehrere Rechner betreibt und auf einem zum Beispiel ein Webserver (http, Port 80), auf einem anderen ein FTP-Server (ftp, Port 21) und wieder auf einem anderen ein SMTP-E-Mail-Server (smtp, Port 25) läuft, dann würde jeder einzelne Rechner eine eigene externe IP-Adresse benötigen. Das hieße aber auch, dass die anderen Rechner im Netzwerk ohne Routing nicht mehr direkt mit diesen Rechnern kommunizieren könnten.



Wenn man also nur eine externe – meist dynamische – IP-Adresse für einen Rechner hat, dann kann bei einer existierenden Verbindung zusätzlich auch die Portnummer ausgetauscht werden. Somit würde eine Anfrage der externen IP-Adresse von Port 50001 an den Rechner 192.168.1.17 weitergeleitet werden usw.

4.5.4.4 Zuteilung von IP-Adressen

Welche IP-Adresse einem Client zugeordnet wird, muss im Netzwerk prinzipiell selbst vom Administrator festgelegt werden. Einer Netzwerkkarte sind daher die IP-Adresse und die Subnetz-Maske zuzuordnen. Jede IP-Adresse darf innerhalb eines Netzwerks nur einmal vergeben werden, da es sonst zu massiven Störungen kommen kann.

Da dies in der Praxis jedoch nur bedingt tauglich ist, weil Rechner ein- und ausgeschaltet werden, wurden sogenannte **DHCP-Server** entwickelt (Dynamic Host Configuration Protocol). Dieser Server übernimmt die Zuteilung der IP-Adressen innerhalb des eigenen Netzwerks nach bestimmten festgelegten Kriterien. Somit muss der Administrator des Netzwerks nicht allen neuen Geräten manuell eine IP-Adresse zuweisen.

Auch ISP (Internet Service Provider) teilen den Kunden in der Regel nur dynamische IP-Adressen zu, da die Anzahl der Adressen rar ist. Dadurch ist jedoch ein Server-Betrieb schwer möglich, weswegen. Es gibt jedoch Dienste, mit denen es möglich ist, diesen dynamischen IP-Adressen einen Namen zuzuweisen (zB: dyndns.com).

4.5.5 Anbindungen an das Internet

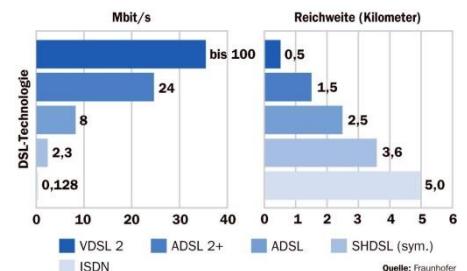
In Privathaushalten erfolgt die Anbindung an das Internet in der Regel über den bestehenden Telefon- oder Kabel-TV-Anschluss. In Neubauten sind in Ballungszentren meistens auch direkt Glasfaserkabel verlegt, weswegen hier höhere Übertragungsraten als mit zB: Kupferkabeln erreicht werden können.

Bei **DSL** (Digital Subscriber Line) werden Daten über ein fache Kupferleitungen gesendet und empfangen, meistens asynchron. Dafür wird in den Kupferkabeln des Telefonnetzes ein Frequenzband genutzt, das oberhalb dessen von analoger Sprachtelefonie liegt. Problematisch an DSL ist jedoch, dass die Datentransferrate mit steigender Reichweite vom Wählamt/Verteiler zunehmend abnimmt. Aus diesem Grund ist es in ruralen Gebieten nicht immer Verfügbar.

Kabelnetzbetreiber stellen in Ballungszentren oft ein Glasfaser-Netzwerk für die Übertragung von Fernsehsignal und Internet zur Verfügung, wobei auch hier unterschiedlich Frequenzen benutzt werden.

Der Zugang zum WAN des Internet Service Providers erfolgt oft über PPP over Ethernet (**PPPoE**) oder Point To Point Tunneling Protocol (**PTP**). Das ist ein Netzwerkprotokoll, das im TCP/IP-Modell auf der Netzzugangsebene arbeitet. Es ermöglicht die Authentifizierung und die Netzwerkkonfiguration und erleichtert den Providern somit die Verwaltung ihrer Netze.

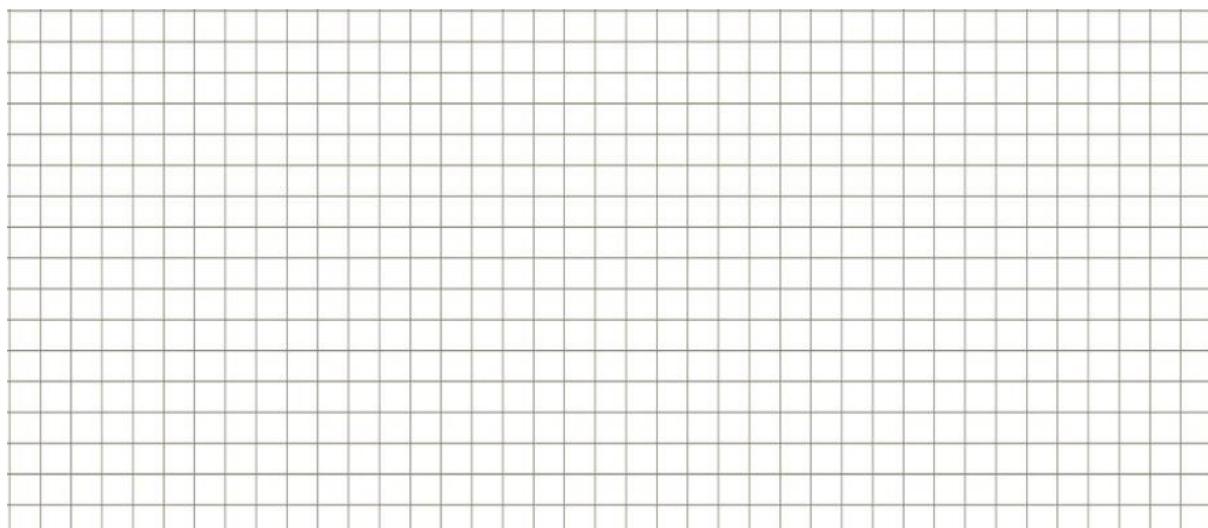
Größere Organisationen in der Regel über **Standleitungen** an das Netz angebunden.



A1 Empfehlung	A1 Festnetz-Internet Plus (8 Mbit/s)	A1 Festnetz-Internet Plus mit Glasfaser Power 16	A1 Festnetz-Internet Plus mit Glasfaser Power 30
Grundnetzgebühr pro Monat:	€ 17,90	€ 23,80	€ 27,80
Gratis Herstellung:	✓	✓	✓
Inkludiertes Datenvolumen:	Unlimitiert	Unlimitiert	Unlimitiert
Stabile und ungeteilte Geschwindigkeit bis zu:	8 Mbit/s Download 768 kbit/s Upload 	16 Mbit/s Download 3 Mbit/s Upload 	30 Mbit/s Download 6 Mbit/s Upload
Inklusive A1 WLAN Box:	✓	✓	✓
A1 Mobil-Internet Basic (optional) **	✓	✓	✓
Ideal für:	<ul style="list-style-type: none"> • Internet surfen • E-Mail • Facebook • YouTube • Musik Streaming • Internet Radio 	<ul style="list-style-type: none"> • YouTube HD • Musik Download • Video Chat • Online Games • Foto-Downloads 	<ul style="list-style-type: none"> • HD Film Download • Online Daten Sicherung (Cloud) • Online Backup • Foto/Video Upload • System Updates

Fiber Power Ultra	
Internet mit Lichtgeschwindigkeit megaschnell für Profis	
Speed	75 Mbit/s 7,5 Mbit/s
WLAN	✓ Gratis WLAN Modem inkl.
Datenvolumen	Unlimitiert
E-Mail	5 Postfächer, 25 Aliasen
Webspace	250 MB
Jetzt nur inkl. 19,90* für die ersten 3 Monate, danach 25,90	
mit 49,90	

Versuchen Sie mit der Adresse www.speedtest.net herauszufinden, wie hoch die Download- und Upload-Rate Ihrer Internetverbindung im Moment ist.



Wenn Maschinen zocken

Wieder haben Hochfrequenzhändler beim jüngsten Börsencrash kräftig mitverdient. Welchen Schaden richtet der automatisierte Computerhandel tatsächlich an?

Von Nadine Oberhuber, 31. August 2015, 22:27, www.zeit.de



Im Schatten des Supercomputers. Ein Börsianer an der New York Stock Exchange © Justin Lane /dpa

Win-win-Situationen sind etwas sehr Schönes. Doppelsieg-Strategien, bei denen alle Parteien am Ende einen Nutzen erzielen.

Aber wenn wir ehrlich sind: Sie sind verdammt selten. Anfangs hielten viele Börsen den vollcomputerisierten Hochfrequenzhandel für so eine Win-Win-Strategie. Computerprogramme wickeln dabei innerhalb von Millisekunden Börsengeschäfte ab. Damit wollten die großen Handelsplätze für mehr Wettbewerb sorgen und somit auch für bessere Kurse. Das Trading sollte für alle Anleger fairer werden, indem man den automatisierten Superhändlern den Zugang gewährte. Das war die Hoffnung.

Doch nach dem Crash an den Weltbörsen vergangene Woche werden wieder Zweifel laut: Sind die Hochfrequenzhändler wirklich gut für den Markt? Oder sind sie nicht eher eine Gefahr?

Zumindest eines sind sie ganz sicher: eine wahre Größe im Börsengeschäft. Mehr als 50 Prozent des gesamten US-Aktien-Handelsvolumens geht auf ihr Konto, ähnlich viel ist es bei deutschen Aktien. Sie sind "die dominante Komponente im Markt und können ihn in fast allen Bereichen in seiner Performance beeinflussen", stellte eine Untersuchung der amerikanischen Börsenaufsicht SEC jüngst fest.

Seitdem die New York Stock Exchange und Nasdaq den Hochfrequenzhändlern mit der Neuregulierung im Jahr 2005 den Weg geebnet haben, ist die Branche immer wieder in die Kritik geraten. Vor allem nach dem Börseneinbruch im Mai 2010 stand sie im Fokus: Eine bedenkliche Order löste damals so viel automatisierte Verkaufsordern aus, dass der amerikanische Börsenindex binnen Minuten um 1.000 Punkte einbrach – um neun Prozent. Der Crash vernichtete Börsenwerte in Milliardenhöhe. Gewinner waren letztlich die Hochfrequenzhändler, die sowohl beim Absturz, als auch beim anschließenden Wiederaufschwung kräftig mitverdienten.

Fünf Jahre später hat sich an dem lukrativen Geschäftsmodell wenig geändert. Vergangene Woche bejubelte Brian Donnelly, Gründer und Chef von Volant Trading, öffentlich die historischen Profite nach dem Einbruch der weltweiten Börsen: "Das war wohl unser bester Tag seit dem Flashcrash 2010."

Die Flashboys nutzen das System aus

Der amerikanische Autor Michael Lewis nennt Trader wie Donnelly "Flash Boys". In seinem gleichnamigen Buch vom vergangenen Frühjahr erhebt er den Vorwurf: Sie nutzen das System aus, indem sie Gewinne abschöpfen, die es ohne sie überhaupt nicht gäbe. Die Computerhändler fingen mit ihren superschnellen Datenverbindungen die Kauforder von Großanlegern ab. Sie kaufen dieselben Aktien einen kurzen Moment vor ihnen, treiben damit die Preise und geben die Papiere zu überhöhtem Kurs weiter. Oder sie legten mit einer Vielzahl von fingierten Aufträgen die Rechner von Großinvestoren für Millisekunden lahm und nutzen die Zwischenzeit, um die Preise der betreffenden Aktien zu treiben oder zu drücken und den Gewinn abzuschöpfen. Mit Algorithmen und schnellen Datenleitungen übervorteilten sie die übrigen Marktteilnehmer. Heute noch schicken sie per Glasfaserkabel oder Infrarotlaser die Daten. Eines Tages könnten sie diese mit Hohlkernkabeln oder Neutrinos um die Welt schicken.

Die Hochfrequenzhändler beruhigen. Andere Marktteilnehmer, die noch klassisch handelten, würden von ihren schnellen Geschäften profitieren: Die größeren Volumina und die vielen Käufe und Verkäufe würden für mehr Liquidität im Markt und damit auch bessere Preise sorgen. Ohne Hochfrequenzhandel müssten manche Käufer länger auf die Ausführung einer Order warten und eventuell höhere Preise zahlen – so ihre Theorie.

"Gefährlich für die Stabilität des Marktes"

Mittlerweile zweifeln aber viele Ökonomen daran, dass das stimmt. Nobelpreisträger Joseph Stiglitz spricht den Hochfrequenzhändlern jede Form des gesellschaftlichen Nutzens ab und meint sogar, dass sie das Funktionieren der Märkte verhindern. Der Soziologe Dirk Helbing von der ETH Zürich hält sie sogar für "gefährlich für die Stabilität unserer Wirtschaft und Gesellschaft". Es sei sogar justizibel, was die Händler da trieben, meint der Jurist Peter Kasiske von der Universität München: Wenn Algorithmen mit Unmengen von Aufträgen andere Handelssysteme verlangsamen und damit eine nicht vorhandene Nachfrage vortäuschen, dann sei das strafbar. Es seien "räuberische Handelsstrategien, bei denen Märkte gezielt gestört werden". Deutschland hat deswegen per Gesetz den Hochfrequenzhandel eingeschränkt. Was aber wenig daran ändert, dass die Verwerfungen in anderen Ländern den hiesigen Markt ebenfalls stark treffen.

Werden die Hochfrequenzhändler wenigstens ihrem eigenen Anspruch gerecht, zusätzliche Liquidität für die Märkte zu schaffen? Wirtschaftswissenschaftler sind sich noch uneins. Flash-Boys-Autor Lewis glaubt, dass die Profi-Händler zwar für mehr Aktivität und Volatilität sorgten, die Kurse also stärker schwankten. Aber die Handelbarkeit der Papiere verbesserte sich nicht dadurch.

Extremere Marktschwankungen

Die US-Börsenaufsicht SEC wollte es genauer wissen und hat alle verfügbaren wissenschaftlichen Studien weltweit ausgewertet. Ihr Fazit: Zum mindesten sind Hochfrequenzhändler bei Weitem nicht nur so harmlose "Market Maker" im Dienste der Liquidität. Die Hälfte ihrer Verkäufe und Käufe erfolgt mit dem Ziel, "aggressiv die Marktliquidität abzuschöpfen". Unterm Strich sorge der Frequenzhandel für extremere Schwankungen im Markt. Das führt zu höheren Kosten bei anderen Marktteilnehmern, also auch bei Privatanlegern und Fondsgesellschaften, die für Kleinanleger Aktien kaufen.

Für den großen Flashcrash von 2010 steht inzwischen fest: Die schnellen Computerhändler haben ihn zwar nicht ausgelöst. Aber erst ihre Reaktion hat zu dem enormen Kursausschlag binnen Minuten geführt. Die Hälfte des Handelsvolumens beim Absturz ging auf ihre Rechnung. Am darauffolgenden Aufschwung beteiligten sie sich dagegen nur zu 36 Prozent. Das heißt: Die schnellen Trader prügeln die Kurse weitaus stärker herunter, als nötig – und halfen ihnen danach weniger hinauf. Von den Riesengewinnen damals schwärmen die Börsianer heute noch. Win-win-Situationen aber sehen anders aus.

4.5.6 Das Domain Name System (DNS)

Das Domain Name System (DNS) ist nach dem IP-Protokoll einer der wichtigsten Dienste in der Internetprotokollfamilie. Es handelt sich hierbei um einen Dienst zur Namensauflösung. Umgangssprachlich kann das DNS auch als riesiges Telefonbuch bezeichnet werden.

Damit man sich nicht sämtliche IP-Adressen merken muss (zB: 137.208.3.182 für die Website der WU Wien) kann man einzelnen IP-Adressen einen Domainnamen zuordnen. Diese Domainnamen werden dann von einem DNS-Server in ihre IP-Adresse übersetzt und die Anfrage des Benutzers wird an den Browser weitergeleitet.

4.5.6.1 Domain Namen

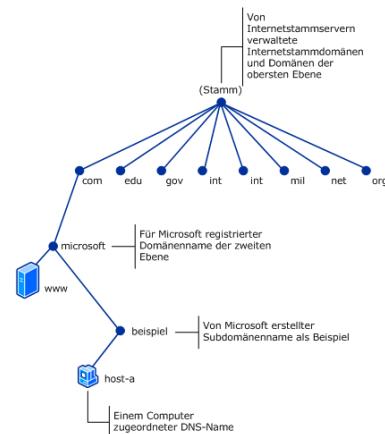
Domainnamen sind nach einer bestimmten Topologie aufgebaut. Zunächst gibt es Top-Level-Domains (TLD) wie zum Beispiel com, edu, net, gov, org usw.

Diese werden von einer Vergabestelle (NIC = Network Information Center) verwaltet. Für die TLD at wäre das die nic.at

Bei diesen Stellen können Domainnamen (Second-Level-Domains) registriert werden, wie zum Beispiel wirtschaftsinformatik oder microsoft oder yahoo usw. Registriert man zum Beispiel bei nic.at die Domain wirtschaftsinformatik.at kann man diese Domain auf seinen eigenen HTTP-Server verweisen lassen und man kann eine Homepage einrichten.

Betreibt man komplexere oder mehrere Seiten kann man auch Subdomains einrichten. Subdomains sind Third-Level-Domains, die vom Inhaber der Second-Level-Domain selbst angelegt werden können. Man könnte zum Beispiel Subdomains für unterschiedliche Sprachen anlegen (de.wirtschaftsinformatik.at der en.wirtschaftsinformatik.at) oder für unterschiedliche Inhalte (zB: experte.wirtschaftsinformatik.at oder anfaenger.wirtschaftsinformatik.at).

Vollständige Domainnamen bezeichnet man als Fully Qualified Domain Name (FQDN). Diese würde man wie folgt anschreiben:



Third-Level-Domain	Second-Level-Domain	First-Level-Domain	Root-Label
de	wirtschaftsinformatik	at	.
www	wirtschaftsinformatik	at	.
www	google	Com	.

Second-Level-Domains müssen nicht direkt beim Registrar selbst gekauft werden. Fast jeder Internet Service Provider (ISP) tritt hier als Zwischenhändler auf und bietet seinen Kund/innen den Erwerb von Domainnamen an.

Will man eine Domain registrieren, dann muss zuerst überprüft werden, ob diese nicht bereits vergeben ist. Ist dies der Fall, dann kann mit dem Inhaber Kontakt aufgenommen werden und über eine Ablöse (auf privater Basis) verhandelt werden. Ist die Domain noch frei, kann sie ganz einfach – meist über ein Webshop-System – registriert werden.

Domain Suche/Auswahl
Fügen Sie die gewünschte(n) Domain(s) dem Warenkorb hinzu, und/oder suchen Sie nach zusätzlichen Domains. Falls die Domain schon delegiert ist, können Sie die Whois-Daten abfragen.

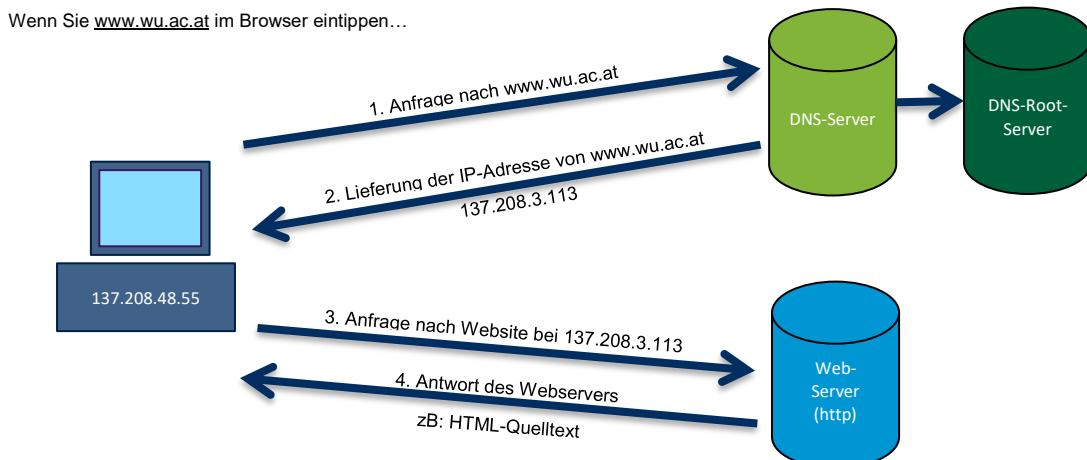
WEITER →

Ergebnis der Domainsuche

skrapid.at ist bereits delegiert. skrapid.co.at ist bereits delegiert. skrapid.or.at ist noch frei.	WHOIS ABFRAGE WHOIS ABFRAGE → IN DEN WARENKORB
--	---

4.5.6.2 Namensauflösung

Wenn Sie in Ihrem Browser zur Adresse www.wu.ac.at navigieren möchten, dann wird an den DNS-Server eine Anfrage gesendet, welche IP-Adresse der Domain wu.ac.at zugeordnet ist. Ist dieser Eintrag am DNS-Server nicht verfügbar, wird bei einem DNS-Root-Server nachgefragt, ob dieser die Adresse kennt. Weltweit gibt es 14 solcher Root-Server.



Gibt es einen Eintrag für wu.ac.at, dann leitet der DNS-Server die zugehörige IP-Adresse an den anfragenden Rechner weiter. Dieser weiß nun, an welche IP er die Anfrage senden muss, um die Homepage der WU Wien zu erreichen, nämlich 137.208.3.113. Er kontaktiert den Webserver über das http-Protokoll und bekommt als Antwort den Quelltext der Homepage geliefert.

Internet-Nutzer tricksen Netzsperren mit alternativen DNS aus

5. Oktober 2014, 11:36

Kurzer Konfigurationsaufwand, große Wirkung - Angebot von Google bis zum CCC

Nach wochenlangem juristischen Gerangel war es am Donnerstagabend dann doch so weit: Seitdem sind in Österreich die ersten Netzsperren aktiv. Aufgrund einer einstweiligen Verfügung wurden die Seiten kinox.to und movie4k bei den meisten Providern blockiert. Wer diese auf ihren ursprünglichen Adressen ansurfen will, bekommt statt dem erwarteten Inhalt nur mehr eine simple Fehlermeldung.

Schwache Sperre

Dies liegt daran, dass die Sperre lediglich über eine Veränderung der Domain-Name-System-(DNS)-Datenbank bei den Providern implementiert ist. Diese ist dazu, die die IP-Adresse eines Servers (beispielsweise: 194.116.243.20) - also jene Zahlenkombination über die er anderen Rechnern bekannt ist - einer für Menschen einfach merkbar Adresse wie derStandard.at zuzuweisen. Nun haben also die österreichischen Provider schlicht die Einträge für die von den Rechteverwertern beanstandeten Domainnamen verändert.

DNS-Alternativen

Und genau dieser Umstand macht es den Nutzern nun so einfach die aktuellen Netzsperren auszutricksen. Es ist nämlich keineswegs notwendig, die DNS-Einträge des eigenen Anbieters zu verwenden. Wer schon bislang alternative DNS-Server verwendete, merkte von der Aktivierung der Netzsperren in Österreich exakt: Nichts. Und solche öffentlich verfügbare DNS gibt es zuhauf, so hat etwa Google [seit einigen Jahren eigene DNS im Angebot](#). Und neben speziellen Services wie [DNS.Watch](#) oder [OpenDNS](#) hat sogar der deutsche Chaos Computer Club [ein entsprechendes Angebot](#). In all diesen sind die alten Zuweisungen für kinox.to und movie4k weiterhin aktiv. (apo, derStandard.at, 5.10.2014, gekürzt)

Prüfen Sie beim Anbieter www.easynome.eu oder einem anderen beliebigen Anbieter, welche Domains mit Ihrem Nachnamen noch zu registrieren sind.

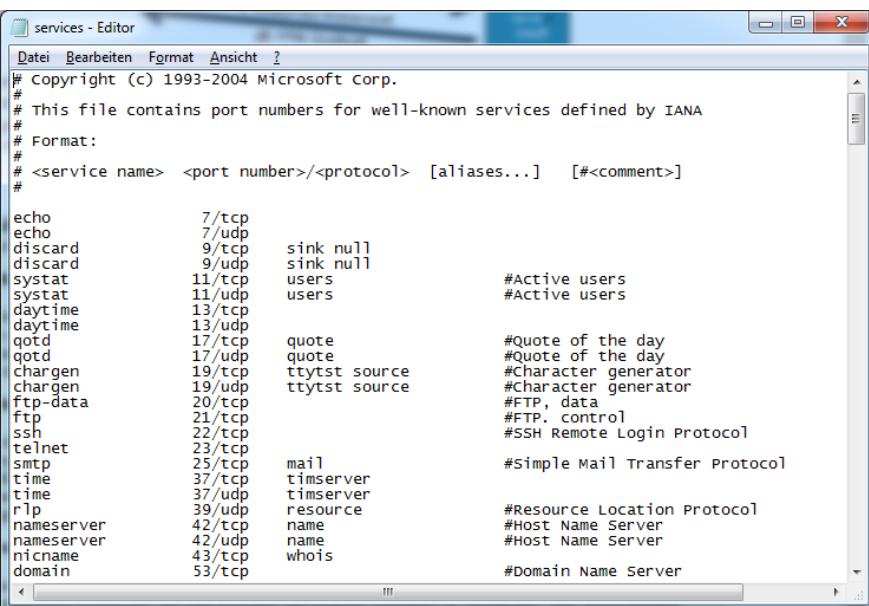
4.5.7 Ports

Ein Port stellt sicher, dass ein Datenpaket, das von einem Rechner gesendet wird, vom dortigen Betriebssystem auch eindeutig der Anwendung zugeordnet wird, für die es bestimmt wird. Ports könnte man mit einer Briefkastenanlage eines Wohnhauses vergleichen. Alle Anschriften haben zwar dieselbe Adresse, es gibt jedoch unterschiedliche Briefkästen, weil die Briefe ja an bestimmte Menschen zugestellt werden sollen, die Zugriff auf die Briefkästen haben.

Ports sind Teil der Transportschicht und werden sowohl TCP- als auch UDP-Verbindungen und – Datenpaketen zugeordnet. Die Notation 137.208.3.113:80 würde bezeichnen, dass ein Datenpaket an den Port 80 des Rechners mit der IP-Adresse 137.208.3.113 gesendet werden soll. Das Betriebssystem weiß dann, dass der Port sozusagen der Briefkasten der Anwendung HTTP ist (also des Webservers) und leitet das Datenpaket an diesen weiter.

TCP/IP-Schicht		Beispiel
Anwendungen		HTTP Port 80/TCP SSH Port 22/TCP FTP Port 20/21/TCP SMTP Port 25/TCP HTTPS Port 443/TCP IMAP Port 143/TCP
Transport		TCP, UDP, SCTP
Internet		IP (IPv4, IPv6), ICMP, (ARP)
Netzzugang		Ethernet, Token Bus, Token Ring, FDDI, (ARP)

Insgesamt gibt es 65535 mögliche Ports, wovon die ersten 1024 standardisiert sind. Sie sind sozusagen fix für bestimmte Anwendungstypen reserviert (zum Beispiel für Webserver, E-Mail-Server usw.). Unter Windows finden Sie eine Auflistung aller standardisierten und registrierten Ports unter %WINDIR%\system32\drivers\etc\services.



```

services - Editor
Datei Bearbeiten Format Ansicht ?
# Copyright (c) 1993-2004 Microsoft corp.
#
# This file contains port numbers for well-known services defined by IANA
#
# Format:
#
# <service name> <port number>/<protocol> [aliases...] [#<comment>]
#
echo      7/tcp
echo      7/udp
discard   9/tcp    sink null
discard   9/udp    sink null
sysstat   11/tcp   users           #Active users
sysstat   11/udp   users           #Active users
daytime   13/tcp
daytime   13/udp
qotd     17/tcp   quote           #Quote of the day
qotd     17/udp   quote           #Quote of the day
chargen  19/tcp   ttyst source   #Character generator
chargen  19/udp   ttyst source   #Character generator
ftp-data 20/tcp
ftp       21/tcp
ssh       22/tcp
telnet   23/tcp
smtp     25/tcp   mail            #Simple Mail Transfer Protocol
time     37/tcp   timserver
time     37/udp   timserver
rlp      39/udp   resource
nameserver 42/tcp   name           #Host Name Server
nameserver 42/udp   name           #Host Name Server
nicname  43/tcp   whois
domain   53/tcp

```

Eine schöne Übersicht aller verfügbaren Ports finden Sie auf WIKIPEDIA unter http://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports

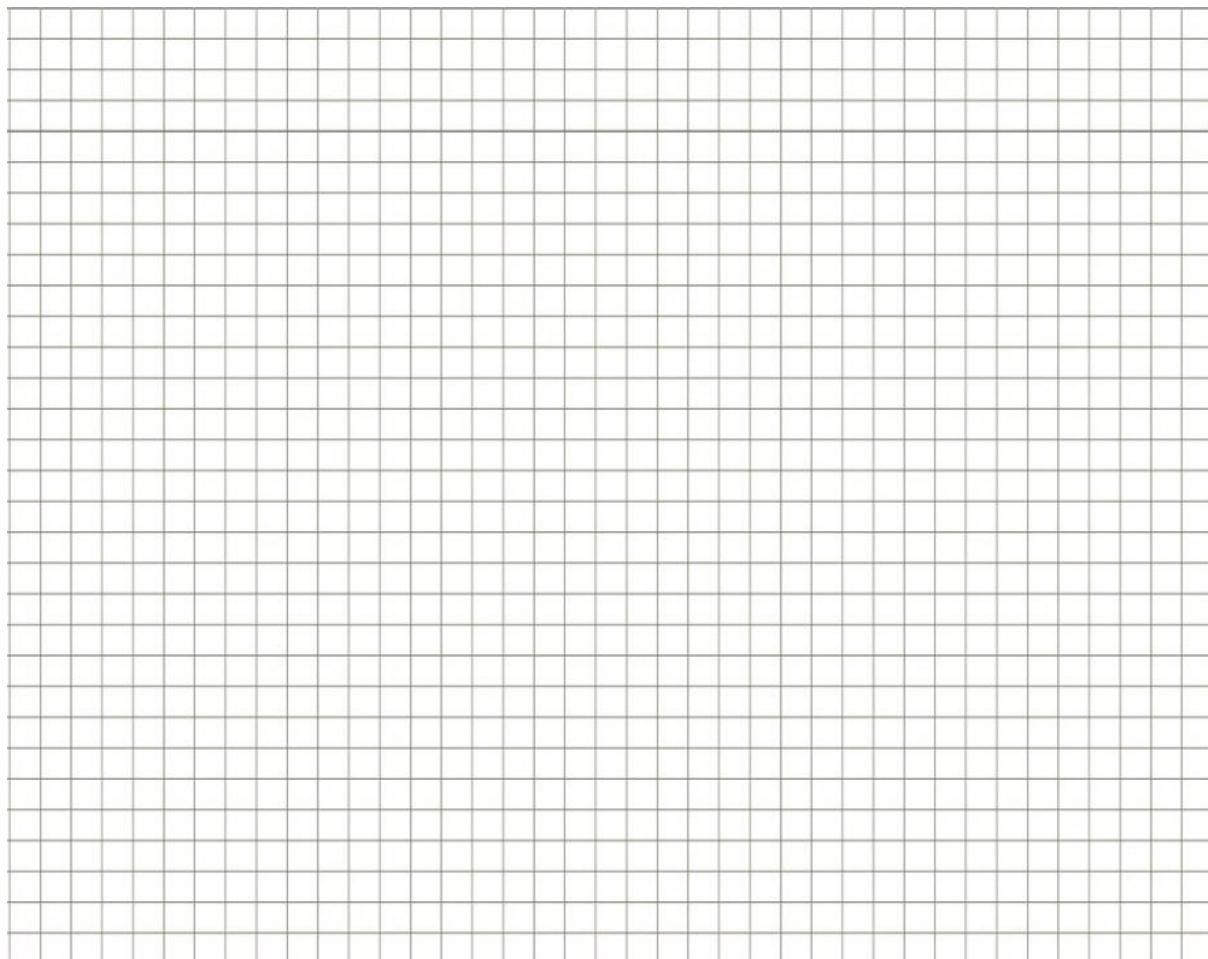
Ports sind ein wesentlicher Bestandteil für das ermöglichen von Kommunikation zwischen Rechnern. Sie werden jedoch auch oft für das Filtern oder Drosseln von Datenverkehr eingesetzt.

So können Internet-Service-Provider unerwünschten Datenverkehr von zB: FileSharing-Diensten reduzieren oder sogar gezielt verbieten. Man kann Ports auch komplett über eine Firewall gezielt sperren. Ports werden von Angreifern auch sehr oft zum Eindringen in Systeme verwendet. Dementsprechend sollten alle Ports, die nicht zwingend verwendet werden sollten, gesperrt werden.

Das Tool TCPView für Windows zeigt wunderbar, welche Prozesse gerade über welches Protokoll auf welchem Port mit welchem Rechner eine Verbindung geöffnet haben. Dieses Programm kann unter <http://technet.microsoft.com/de-at/sysinternals/bb897437.aspx> kostenlos heruntergeladen werden.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
firefox.exe	7324	TCP	127.0.0.1	55216	127.0.0.1	55217	ESTABLISHED
firefox.exe	7324	TCP	127.0.0.1	55217	127.0.0.1	55216	ESTABLISHED
explorer.exe	3824	UDP	127.0.0.1	60752	*	*	
Dropbox.exe	4604	TCP	137.208.48.217	54227	108.160.167.179	80	ESTABLISHED
communicator...	4912	TCP	137.208.48.217	54211	137.208.29.68	443	ESTABLISHED
communicator...	4912	TCPV6	[2001:628:404:30:b055:d503:6740:c0fd]	56324	[2001:628:404:b:0:...]	443	ESTABLISHED
CmRcService...	3384	TCP	0.0.0.0	2701	0.0.0.0	0	LISTENING
CmRcService...	3384	TCPV6	[0:0:0:0:0:0:0:0]	2701	[0:0:0:0:0:0:0:0]	0	LISTENING
ComExec.exe	3844	UDP	127.0.0.1	54428	*	*	LISTENING

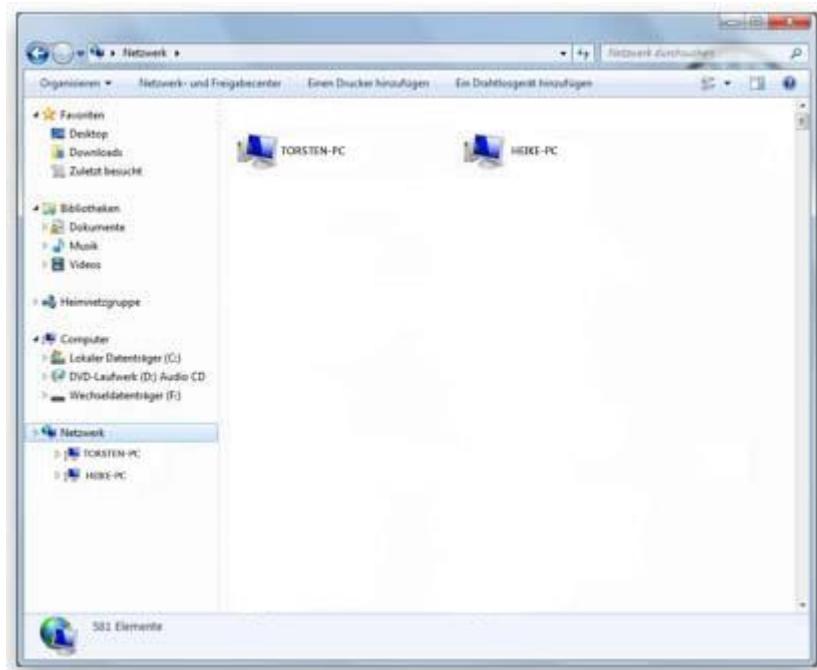
Endpoints: 130 Established: 25 Listening: 46 Time Wait: 0 Close Wait: 0 [2001:628:404:b:0:0:0:75]



4.6 Im Netzwerk zurechtfinden

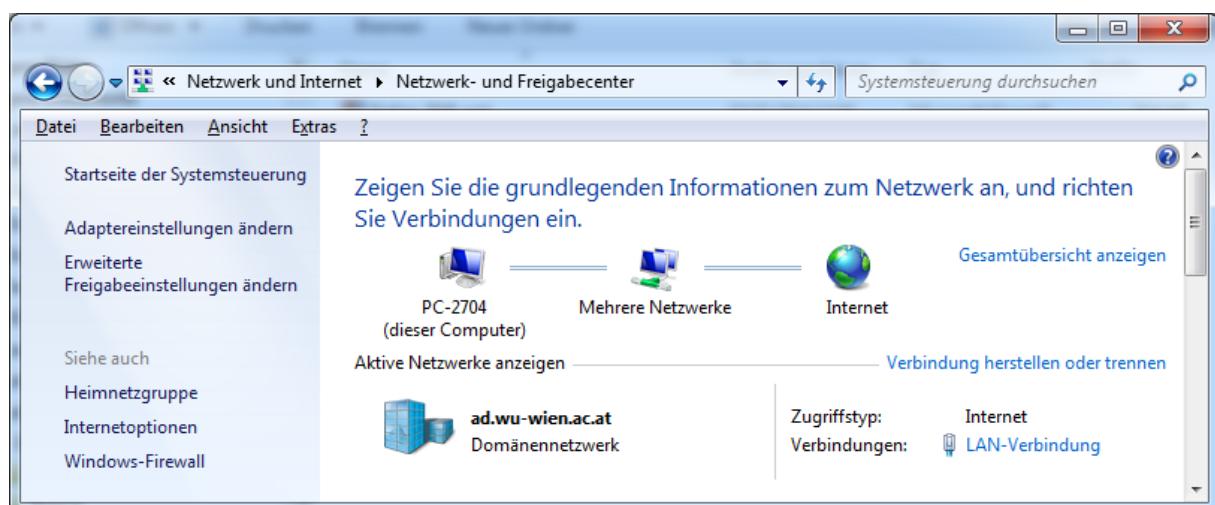
Sobald die physische Verkabelung hergestellt ist und die Rechner richtig konfiguriert sind, ist die Administration eines einfachen Netzwerkes kein großes Problem. Wenn Sie ein Netzwerk über einen Switch aufgebaut haben und keinen DHCP-Server betreiben, müssen Sie die Zuordnung der IP-Adressen inkl. Subnetzmaske per Hand vornehmen.

Alle PCs, die sich in Ihrem Netzwerk befinden werden im Bereich Netzwerk angezeigt, den Sie stets über den Windows-Explorer erreichen können



4.6.1 Netzwerkkarte konfigurieren

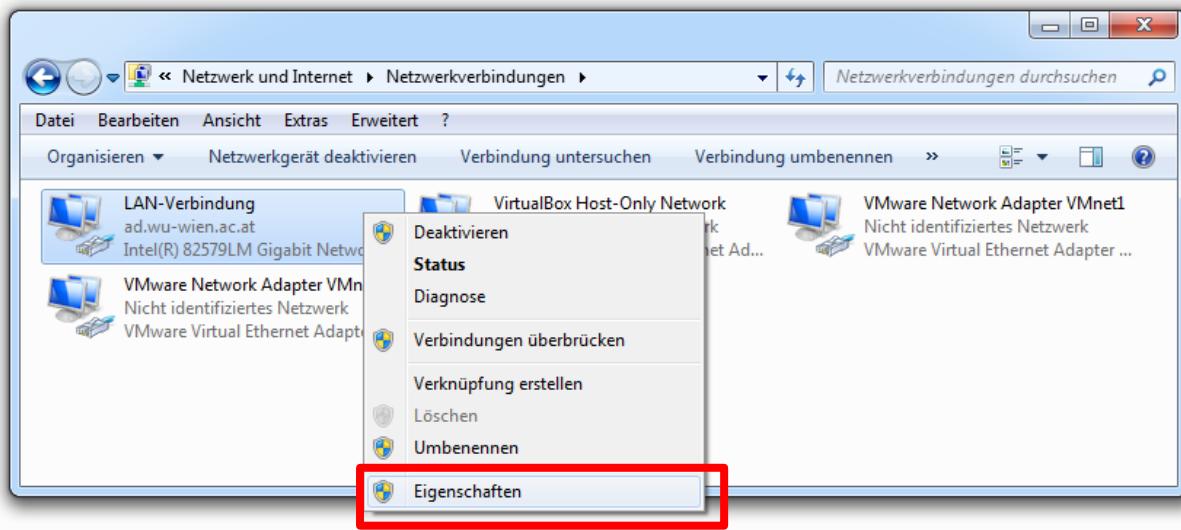
Zur Konfiguration Ihrer Netzwerkadapter gelangen Sie am besten über die Systemsteuerung über den Bereich **Netzwerk und Internet**. Dort gelangen Sie über die Option Netzwerkstatus und – aufgaben anzeigen zu Ihren Netzwerkinformationen.



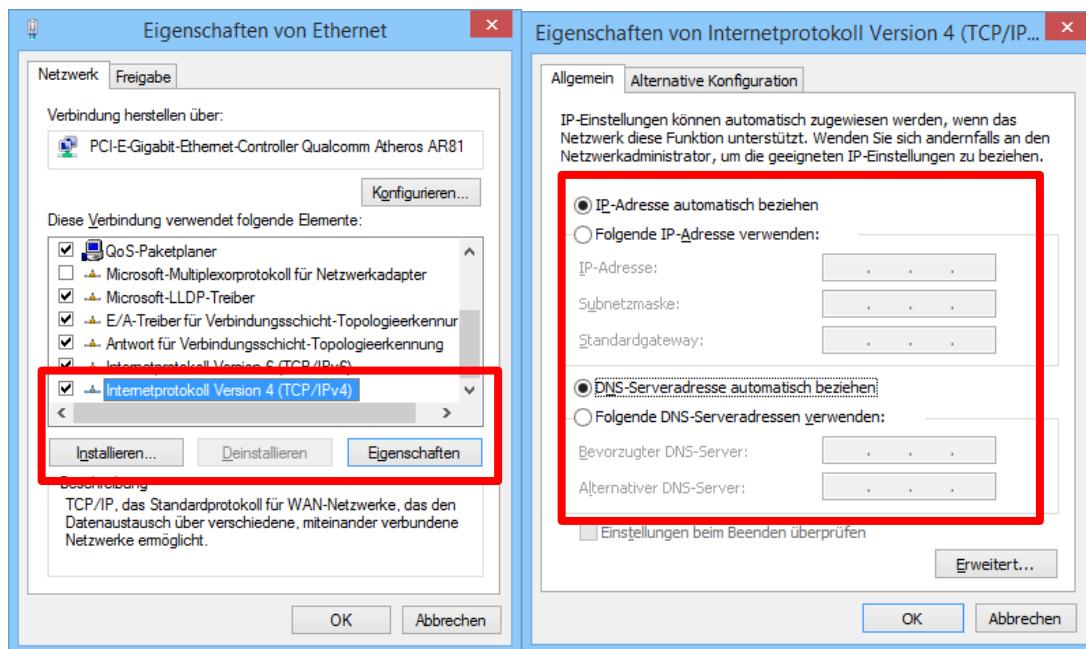
In dieser Ansicht ist dargestellt, mit welchem Netzwerk der Computer gerade verbunden ist. Wenn kein Netzwerk eingerichtet ist, muss zuerst die Netzwerkkarte in den Adapttereinstellungen eingestellt werden.

4.6.1.1 Netzwerk einrichten

In den Adaptereinstellungen finden Sie eine Auflistung aller physischen und virtuellen Netzwerkkarten. Meistens haben Sie hier zwei Karten verfügbar. Die Netzwerkkarte mit RJ45-Anschluss und Ihre WLAN-Netzwerkkarte. Um eine LAN-Verbindung einzurichten klicken Sie mit der rechten Maustaste auf Ihre Netzwerkkarte und wählen Sie den Punkt Eigenschaften.



Dort finden Sie nun eine Auflistung aller Elemente, die für diese Verbindung verfügbar sind. Dabei handelt es sich um diverse Netzwerkprotokolle, von denen das Internetprotokoll Version 4 (TCP/IPv4) von Interesse ist. Zuerst muss der Eintrag markiert werden und anschließend können die Eigenschaften bearbeitet werden.

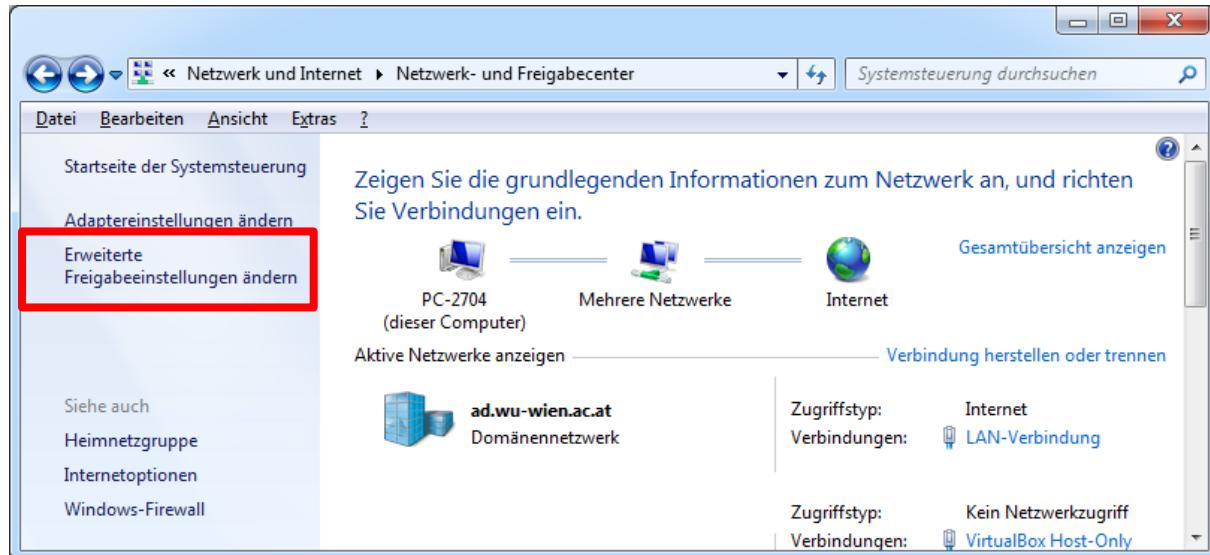


In den Eigenschaften von Internetprotokoll Version 4 kann nun eingestellt werden, dass sowohl die IP-Adresse als auch die DNS-Serveradresse automatisch bezogen werden sollen. Dies ist die Standardeinstellung, wenn ein DHCP-Server im Netzwerk eingesetzt wird.

Ist das nicht der Fall muss die IP-Adresse manuell eingetragen werden und die Subnetzmaske ergänzt werden. Soll zusätzlich die Internet-Verbindung eines bestimmten Computers im LAN benutzt werden, muss dessen IP-Adresse als Standardgateway eingetragen werden. Als DNS-

Serveradresse wird die IP zu einem verfügbaren Server eingetragen. Zum Beispiel 8.8.8.8 (Google) oder einen anderen öffentlich verfügbaren.

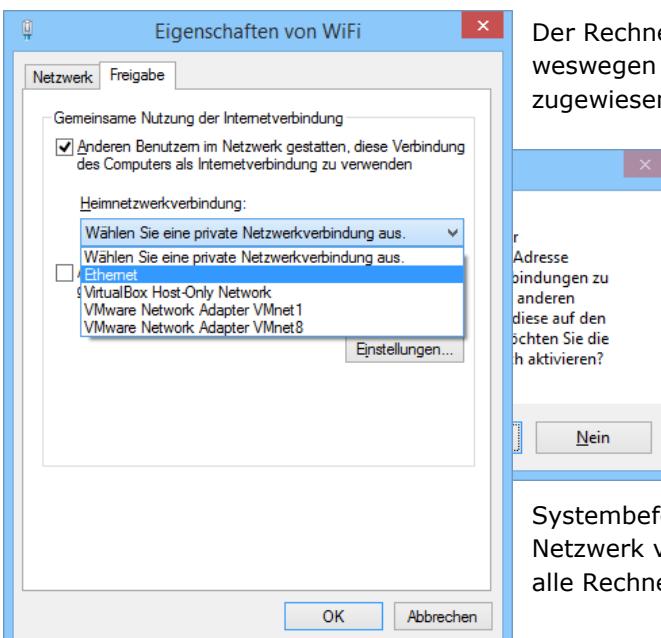
Sobald mehrere Rechner im Netzwerk mit derselben Subnetzmaske eingerichtet wurden scheinen diese in der Netzwerkumgebung auf. Ist das nicht der Fall, müssen die Einstellungen in den Erweiterten Freigabeeinstellungen angepasst werden.



Dort kann nämlich angegeben werden, ob die **Netzwerkerkennung** eingeschaltet ist oder nicht, das heißt, ob der Netzwerkcomputer in einem Windows-Netzwerk für die anderen Geräte sichtbar ist. An dieser Stelle kann auch die **Datei- und Druckerfreigabe** aktiviert werden und der **öffentliche Ordner** freigegeben werden.

4.6.1.2 Internetverbindung freigeben

Wenn es einen Rechner gibt, der direkt an das Internet angeschlossen ist, dann können alle anderen Rechner, die sich im gleichen Windows-Netzwerk befinden, diese Netzwerkverbindung nutzen, solange der Rechner eingeschaltet ist. Dafür wählen Sie aus den Eigenschaften der Verbindung, die Sie freigeben möchten die Registerkarte Freigabe, aktivieren die Option und wählen aus, mit welcher Netzwerkkarte das Netzwerk verbunden ist, das Ihre Verbindung nutzen soll.



Der Rechner fungiert ab sofort als Standardgateway, weswegen ihm die statische IP-Adresse 192.168.137.1 zugewiesen werden muss.

Den anderen Computern muss nun ebenfalls eine IP-Adresse beginnend mit 192.168.137.X zugewiesen werden.

4.6.2 ARP

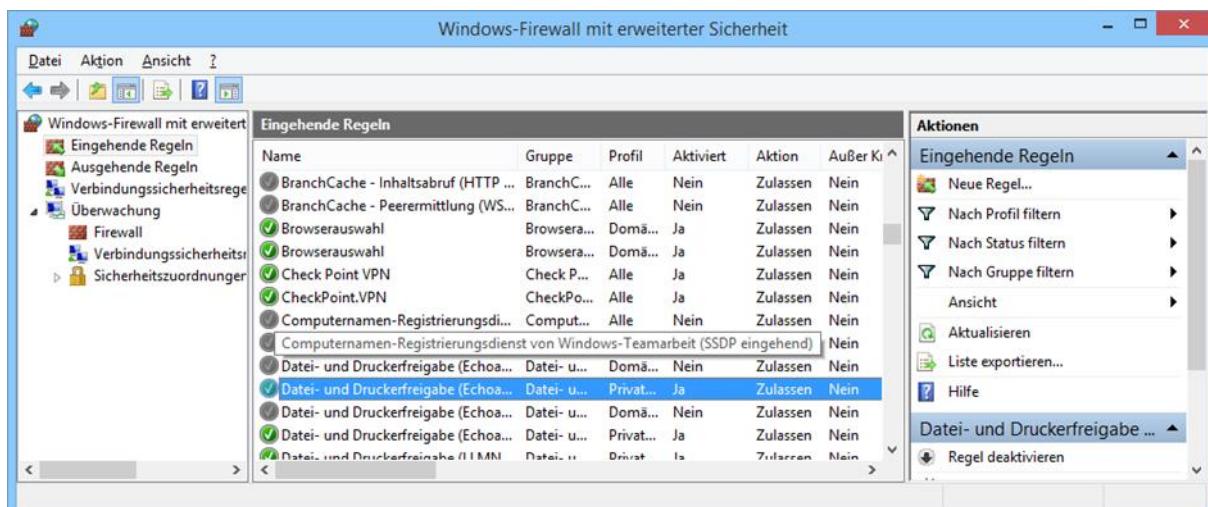
Kann ein Rechner im Netzwerk nicht erreicht werden, so kann das na unterschiedlichen Gründen liegen. Ist der Rechner eingeschaltet und ordnungsgemäß verkabelt, können Sie mit dem Systembefehl **arp-a** feststellen, ob der Rechner im Netzwerk vorhanden ist. Auf den ARP-Befehl müssen alle Rechner reagieren.

Internetadresse	Physische Adresse	Typ
137.208.48.1	50-3d-e5-78-88-5a	dynamisch
137.208.48.36	00-40-8c-e8-c2-53	dynamisch
137.208.48.37	00-40-8c-e8-c2-55	dynamisch
137.208.48.38	00-40-8c-e8-c2-5b	dynamisch
137.208.48.41	00-22-19-1f-42-8d	dynamisch
137.208.48.43	b8-ac-6f-91-8a-1b	dynamisch
137.208.48.45	b8-ca-3a-81-73-aa	dynamisch
137.208.48.48	90-b1-1c-76-50-31	dynamisch
137.208.48.49	00-22-19-1c-78-eb	dynamisch
137.208.48.51	78-fd-94-80-0e-28	dynamisch
137.208.48.53	00-22-19-1e-da-5f	dynamisch
137.208.48.55	b8-ca-3a-a1-73-4a	dynamisch
137.208.48.59	90-b1-1c-76-4f-e5	dynamisch
137.208.48.64	00-24-e8-45-a2-ed	dynamisch

Ist der Rechner im Netzwerk vorhanden und reagiert nicht auf einfache ICMP-Befehle (ping oder tracert), dann wird der Befehl wahrscheinlich von der (Windows)-Firewall blockiert.

4.6.3 Ports und Firewall

Die Firewall sorgt dafür, dass zunächst alle Ports, die typischerweise nicht zwingend gebraucht werden geschlossen sind, um Angreifern eine geringere Angriffsfläche zu bieten. Dementsprechend müssen viele Ports für unterschiedliche Dienste erst freigeschaltet werden. In der Windows-Firewall (Systemsteuerung\System und Sicherheit\Windows-Firewall) können Sie gezielt einzelne Regeln aktivieren, um zum Beispiel die Datei- und Druckerfreigabe zu aktivieren, die notwendig ist, dass Windows-Rechner innerhalb eines Netzwerks angezeigt werden.



Bei der Windows-Firewall handelt es sich um eine Software-Firewall. Das heißt, dass im Hintergrund stets ein Programm läuft, das den eingehenden Datenverkehr überprüft und Datenpakete, die an Ports adressiert sind, die von der Firewall gesperrt sind, verwirft.

Demgegenüber stehen Hardware-Firewalls, die den eingehenden Verkehr nach bestimmten Regeln filtern und ähnlich wie ein Switch im Netzwerk integriert werden.



4.6.4 Netzwerk unter Windows

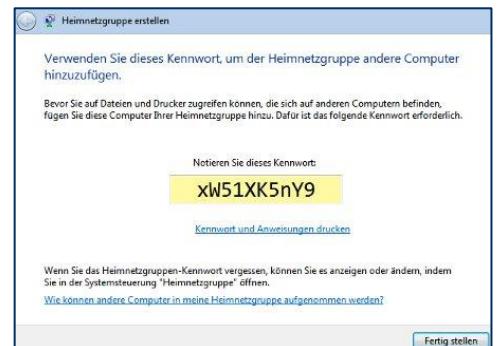
4.6.4.1 Heimnetzwerkgruppe

Windows erlaubt die sehr einfache Einrichtung eines Heimnetzwerks. Das ist ein logisches Netzwerk, dem einzelne Rechner als Mitglieder hinzugefügt werden. Der Vorteil eines solchen Heimnetzwerks ist, dass dabei die Datei- und Druckerfreigabe zwischen den teilnehmenden Computern vereinfacht wird.

Da nicht jeder Computer, der sich zB per WLAN an dem Netzwerk anmeldet auch automatisch

Teilnehmer des Heimnetzwerks sein soll, wird für die Teilnahme einmalig ein Passwort benötigt, um auf Dateien und Drucker zugreifen zu können, die sich auf anderen Computern befinden.

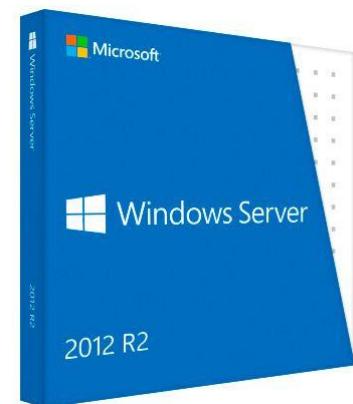
Ein Heimnetzwerk bedingt im Wesentlichen, dass sich alle Computer im gleichen physischen Netzwerk befinden und die Netzwerkkonfiguration so eingestellt ist, dass alle Rechner im gleichen TCP/IP-Netzwerk vorhanden sind. Das kann mit dem Kommandozeilen-Befehl arp -a leicht festgestellt werden.



4.6.4.2 Domäne

Eine Domäne besteht in einem Windows-Netzwerk aus mehreren Computern sind Servern. Ein Netzwerkadministrator verwendet den Domänen-Server um die Sicherheit und Berechtigungen für alle Computer in der Domäne zu kontrollieren. So kann zum Beispiel dezidiert eingestellt werden, dass nur Mitglieder der Benutzergruppe Lehrer Zugriff auf ein bestimmtes Netzlaufwerk haben oder dass die Benutzer der Gruppe Schüler auf dem Netzlaufwerk Schularbeiten nur einmalige Schreibrechte haben usw.

Da sowohl Computer als auch Benutzer in einer Domäne erst spezifisch erfasst werden müssen kann nicht jeder beliebige Computer Teil einer Domäne sein. Der Rechner muss erst vom Administrator freigeschaltet werden. Die Anmeldung an einer Domäne erfolgt direkt bei der Windows-Anmeldung am zentralen Domänen-Server. Dadurch ergibt sich der Vorteil, dass sich die Teilnehmer eines Netzwerks an jedem beliebigen Rechner im Domänen-Netzwerk anmelden können und ihnen dort ihre eigenen Dateien und Einstellungen präsentiert werden.



Weiters kann der Administrator gezielt einstellen, welche Einstellungen am Computer verändert werden dürfen. Das betrifft vor allem die Installation von Software, von Hardware oder das Vornehmen von tieferen Einstellungen im System (Firewall, Registry usw.).

Domänen-Netzwerke sind hochgradig skalierbar. Es können Domänen für nur wenige Nutzer bis hin zu tausenden Teilnehmern eingerichtet werden. Außerdem können Domänen über mehrere lokale (physische) Netzwerke gelegt werden und somit mehrere Standorte miteinander verknüpft werden.

4.7 WLAN-Verwalten

Wenn Sie einen W-LAN-Router betreiben, dann können Sie diesen direkt über seine IP-Adresse ansprechen. Welche IP-Adresse ab Werk eingestellt ist, entnehmen Sie am besten dem Handbuch. Bei Routern, die Sie selbst gekauft haben ist das meist 192.168.0.1 oder 192.168.1.1. Bei Routern Ihres ISP könnte das 10.0.0.138 oder 10.0.0.1 und manchmal funktioniert auch einfach die Adresse <http://www.routerlogin.net>. In einem Windows-Netzwerk wird der Router – sofern Sie sich ordnungsgemäß verbunden haben, in der Netzwerkumgebung im Bereich Gateways angezeigt.

Wichtig ist, dass Sie die Unterseite Ihres Routers genauer betrachten. Dort finden Sie meistens den PIN für den geschützten Zugang, die SSID und die MAC-Adresse des Routers.



Da die Konfigurationsoberfläche von Routern meist über ein Webinterface läuft, das vom Hersteller entwickelt wurde, unterscheidet es sich in seiner Oberfläche und Bedienung sehr oft. Die im Folgenden vorgestellten Funktionen (am Beispiel eines TP-Link-Routers) werden aber von nahezu allen handelsüblichen WLAN-Routern abgedeckt.

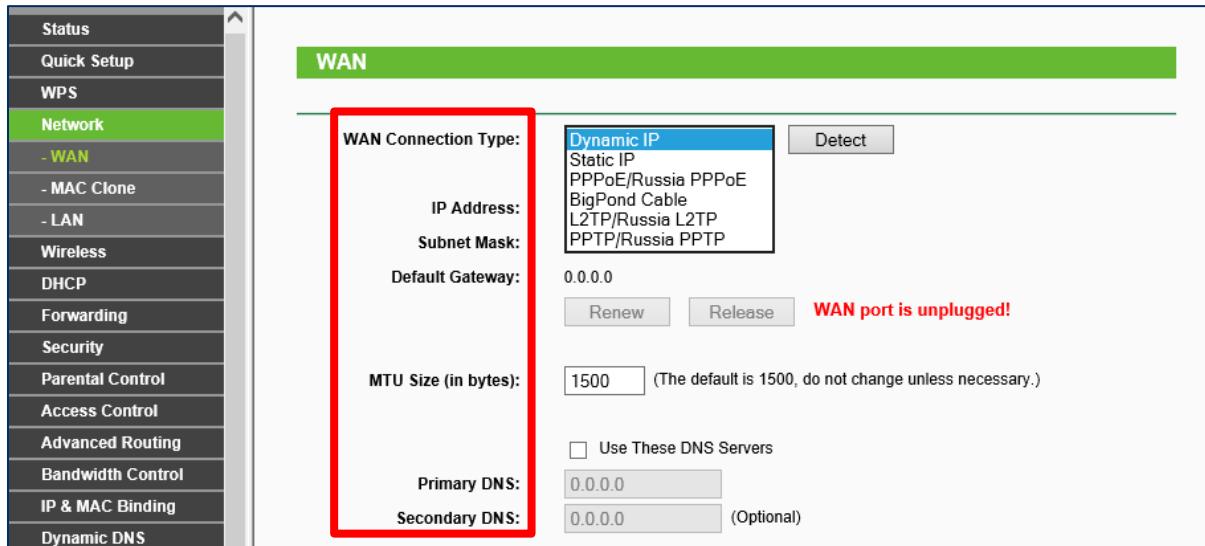
4.7.1 WPS (Wi-Fi Protected Setup)

WPS ist ein Standard, mit dem sehr einfach neue Geräte in einem geschützten Heim-WLAN registriert werden können. Um ein neues Gerät (zum Beispiel eine neue Smartphone) im WLAN zu registrieren muss entweder ein PIN verwendet werden oder am Router eine Taste gedrückt werden. Wird lediglich ein PIN verwendet, muss jedoch in Kauf genommen werden, dass dieser von einem Angreifer in der Regel relativ schnell geknackt werden kann. Meist kann man im Router-Interface über eine Funktion wie „Geräte hinzufügen“ die Registrierung für einen kurzen Zeitraum starten.

4.7.2 WAN-Setup (Wide Area Network)

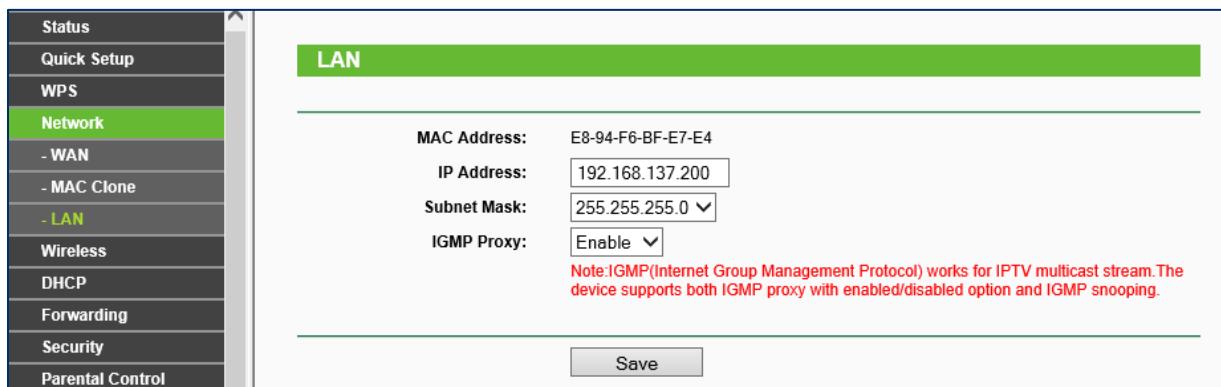
Das Wide-Area-Network ist in der Regel das Netzwerk des Internet Service Providers (ISP). Dieser erlaubt meist über die explizite Freischaltung einer Telefon- oder Kabelleitung die Registrierung eines Routers im Netzwerk. Per DHCP-Server wird die Registrierung des Routers im Netzwerk meist automatisch vorgenommen.

Soll die Verbindung manuell eingerichtet werden, zum Beispiel, um eine statische IP zu verwenden, muss die IP-Adresse, die Subnetz-Maske, der Standard-Gateway und auch der primäre und sekundäre DNS-Server angegeben werden. Diese Informationen werden vom ISP zur Verfügung gestellt.



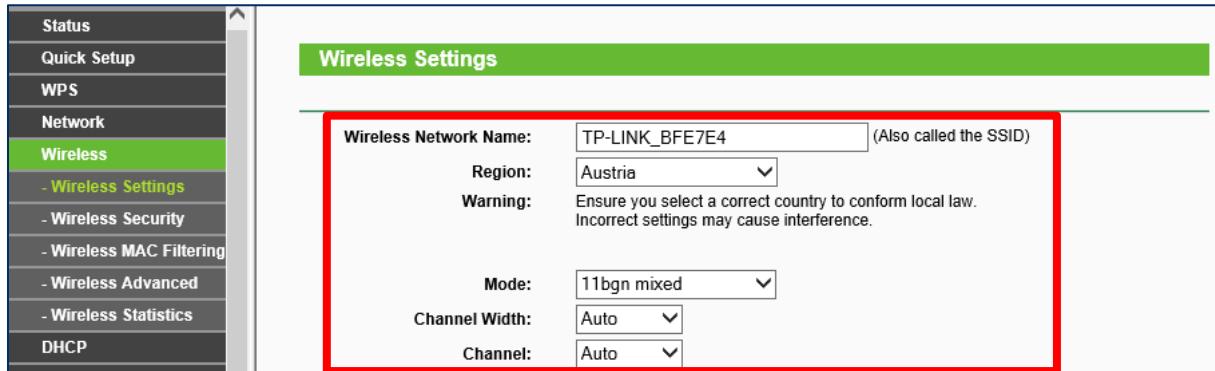
4.7.3 LAN-Setup (Local Area Network)

Da ein Router zwei Netzwerke miteinander verbindet müssen ihm zwei IP-Adressen zugeordnet werden. Über die lokale IP-Adresse wird in der Regel das Router-Interface aufgerufen. Sie beginnt meist mit 192.168.X.X oder mit 10.X.X.X. Die IP-Adresse kann flexibel vergeben werden und hat nur Auswirkung auf jene Geräte, die im lokalen LAN verwendet werden. Wird diesen der Standard-Gateway nicht über DHCP mitgeteilt, muss er auf allen angeschlossenen Rechner geändert werden.



4.7.4 Wireless-Setup

Jenseits von der LAN/WAN-Konfiguration befindet sich meist eine gesonderte Option für die Einstellung der Drahtlosübertragung. Einerseits kann dort meist die SSID (Netzwerkname) sowie der Funkmodus geändert werden. Hier sollte auch die entsprechende Region eingestellt werden, da es nicht in jedem Land erlaubt ist, auf jedem beliebigen Kanal zu funken.



Mit dem Tool inSSIDer (www.inssider.com) kann grafisch dargestellt werden, welche Netzwerke in der Umgebung den gleichen Übertragungskanal nutzen. Hier sollte ein Kanal eingestellt werden der nicht stark frequentiert ist.



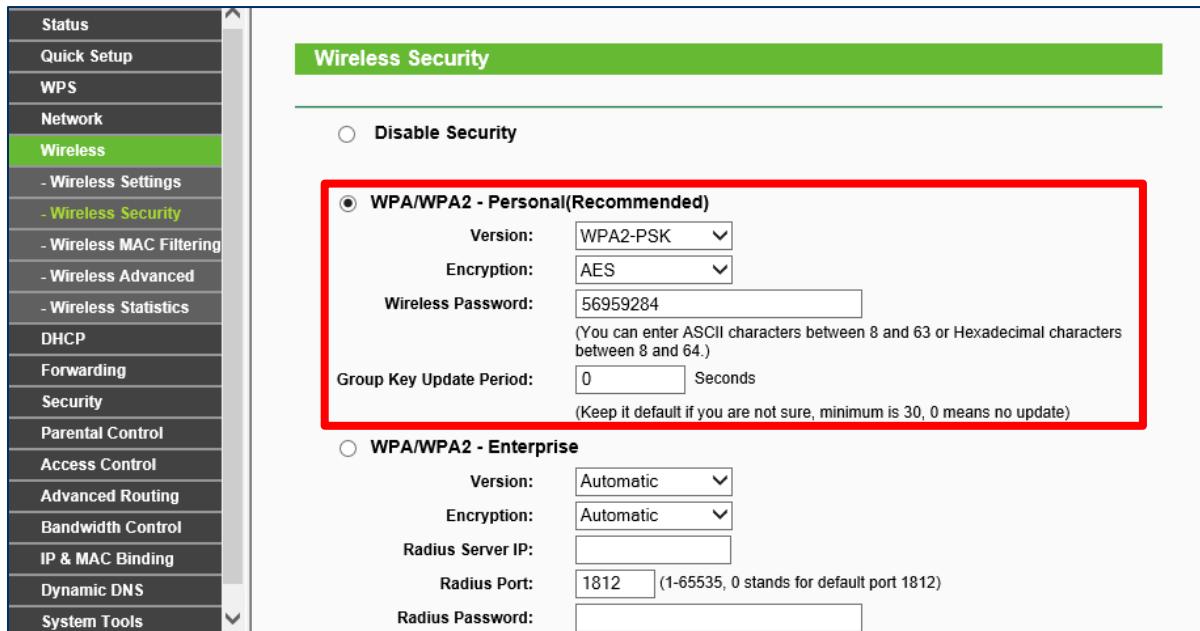
Manche Router können nicht nur auf einem Kanal senden und empfangen sondern auf mehreren Kanälen. Im oberen Beispiel fungt der WLAN-Router TP-LINK_BFE7E4 sowohl auf dem Kanal 4 als auch auf Kanal 8. Alle anderen Router funkten jeweils nur auf einem Kanal.

Der Leistungspegel des Empfangs wird in Dezibel angegeben. Typischerweise ist das bei WLANs Dezibel in Milliwatt (dBm). Alle Werte im Bereich 0 bis -80 dBm sind noch tolerabel. WLANs mit einer geringeren Signalstärke werden von den meisten WLAN-Treibern gar nicht mehr angezeigt, da die Verbindungsstabilität und die Übertragungsrate zu gering wären.

4.7.5 Verschlüsselung (WIFI Security)

Da die Datenpakete bei WLAN über Funk übertragen werden, können diese prinzipiell von jedermann abgefangen und gelesen werden. Deswegen sollten sie mit einer bestimmten Technologie verschlüsselt werden.

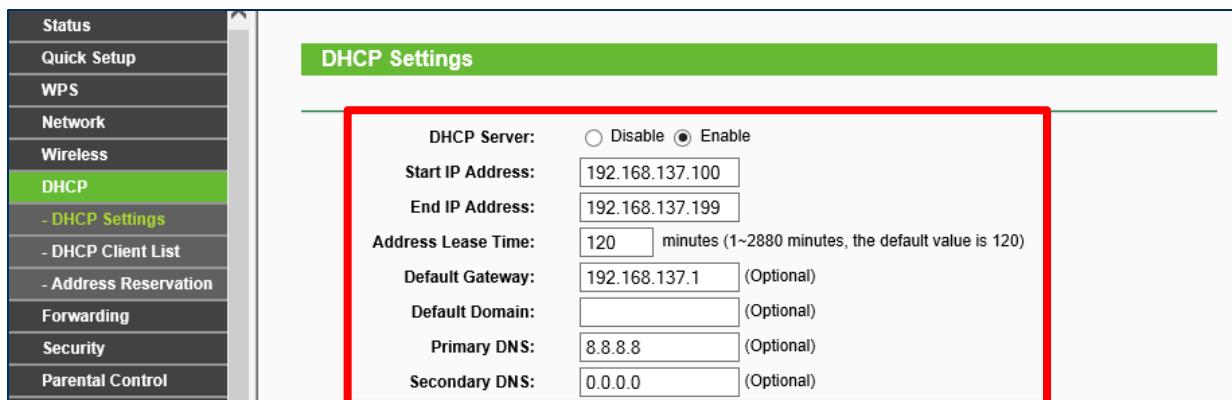
Im Privatbereich sollte hier unbedingt der Standard WPA2 mit einem möglichst komplexen Passwort bestehend aus Buchstaben, Zahlen und Sonderzeichen eingesetzt werden. Der Standard WEP und der Standard WPA sollten aus Sicherheitsgründen nicht mehr verwendet werden.



In großen WLAN-Netzwerken wird in der Regel die Verschlüsselung über WPA2-Enterprise vorgenommen. Dabei wird ein Remote Authentication Dial-In User Service (RADIUS)-Server eingesetzt. Der Radius-Server übernimmt dabei die Überprüfung der Authentifizierung, also das Überprüfen von Benutzernamen und Passwort. Windows Server 2012 kann diese Rolle über die Konfiguration des NPD-Dienstes in der Regel übernehmen (<http://technet.microsoft.com/de-de/library/cc731853.aspx>).

4.7.6 DHCP-Server

Der DHCP-Server übernimmt die automatische Registrierung des Endgeräts im WLAN. Das heißt, die Geräte erhalten eine dynamische IP zugewiesen, die sich bei jeder Verbindung verändern kann. Bei jedem DHCP-Server kann sowohl der Bereich für diese dynamischen IP-Adressen, die IP-Adresse des Standard-Gateways und die DNS-Server eingetragen werden.



4.7.7 Dynamisches DNS - DDNS

Wenn vom Internet Service Provider lediglich dynamische IP-Adressen zugewiesen werden (was in der Regel der Fall ist) kann zwar zB ein Webserver, eine Cloud etc. betrieben werden. Da sich die Adresse jedoch immer ändert, müsste diese vor dem Zugriff immer zuerst ermittelt werden.

Abhilfe dafür schaffen DDNS-Services. Anbieter sind hier DynDNS oder NO-IP. Diese erlauben es, einen bestimmten Namen zu registrieren zB: wirtschaftsinformatik.no-ip.org. Die Zugangsdaten dafür werden dann beim Router im Bereich DDNS eingetragen und der Service muss aktiviert werden. Ist dies der Fall nimmt der Router regelmäßig mit dem DDNS-Service Kontakt auf und teilt diesem seine aktuelle IP-Adresse mit.

The screenshot shows a web-based configuration interface for a router. On the left is a vertical menu bar with the following items: Status, Quick Setup, WPS, Network, Wireless, DHCP, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, and Dynamic DNS. The 'Dynamic DNS' option is highlighted in green. The main content area has a green header bar with the text 'DDNS'. Below it, there are input fields for 'Service Provider' (set to 'No-IP (www.noip.com)'), 'User Name', 'Password', and 'Domain Name'. There is also a checkbox for 'Enable DDNS' which is unchecked. At the bottom, the status message 'DDNS not launching!' is displayed, along with 'Login' and 'Logout' buttons. The overall layout is clean and organized, typical of a network configuration tool.

4.8 Wie sicher ist mein WLAN?

Dieser Artikel aus der c't 9/2014 gibt einen schönen Überblick welche Angriffsmöglichkeiten in Funknetzen möglich sind und welche Konsequenzen ein „erfolgreicher“ Angriff haben könnte.

Der Router verteilt nicht nur Internet über LAN und WLAN, er erfüllt auch eine wichtige Schutzfunktion als Firewall: Alle Angriffe laufen zunächst einmal bei ihm auf. Eine Weiterleitung von Datenpaketen an die Rechner im lokalen Netz findet nur statt, wenn eine solche explizit eingerichtet wurde. Seine zentrale Rolle macht den Router allerdings selbst zu einem verlockenden Angriffsziel: Frei nach dem Motto „Haste einen, haste alle“, hat ein Router-Einbrecher den Datenverkehr des gesamten Netzwerks unter seiner Kontrolle. Dient der Router auch als VoIP-Telefonanlage, kann der Angreifer außerdem kostspielige Telefonate auf fremde Kosten führen. Solange die Verfügbarkeit des Internets nicht beeinträchtigt wird, ist die Wahrscheinlichkeit, dass der Einbruch auffliegt, gering. Es gibt bis dato keine Möglichkeit, Router-Manipulationen automatisch, etwa per Antivirus-Software, zu erkennen.

Dass die Angreifer inzwischen mit großer krimineller Energie daran arbeiten, Router-Schwachstellen zu finden und zu Geld zu machen, ist spätestens seit Anfang des Jahres belegt: Nachdem einigen Fritzbox-Besitzern horrende Telefonrechnungen durch Auslands-Telefonate und Premium-Rufnummern entstanden sind, stellte sich heraus, dass es sich um eine professionell vorbereitete Angriffswelle handelt, in deren Mittelpunkt eine bis dato unbekannte Sicherheitslücke steht. Die Täter fanden eine Schwachstelle, die seit Jahren in der Fritzbox-Firmware schlummerte und laut AVM nicht einmal von vier externen Sicherheitsfirmen aufgespürt worden war. Allein bei einem c't bekannten regionalen Telefonanbieter sind über 200 000 Euro Schaden entstanden. Der Gesamtschaden dürfte in die Millionen gehen.

Obwohl AVM zügig Sicherheitsupdates für alle betroffenen Modelle lieferte, stießen wir Ende März bei einem Kurztest in verschiedenen DSL-Netzen noch auf etliche verwundbare, also nicht aktualisierte Fritzboxen: 100 000 lieferten uns konkrete Versionsinformationen, davon waren rund

30 000 – also fast jede Dritte – verwundbar. AVM selbst erklärt, dass mittlerweile nur noch weniger als 20 Prozent der verkauften Geräte verwundbar seien. Egal, welche Prozentzahl man nimmt: Angesichts der enormen Verbreitung der Fritzbox, man geht von einem Marktanteil von über 50 Prozent aus, bedeuten beide, dass immer noch Millionen von Geräten anfällig sind.

Das zeigt, dass sich noch nicht genug herumgesprochen hat, dass man den Router – genau wie seit jeher den Rechner – regelmäßig warten und mit Updates versorgen muss. Wer immer noch eine verwundbare Fritzbox betreibt, muss mit unangenehmen Konsequenzen rechnen: Seit Anfang März kursieren im Netz alle Informationen, die ein Angreifer benötigt, um die Lücke auszunutzen. Der Angriffs-Code kann potenziell auf jeder Webseite lauern – auch auf jenen, die für gewöhnlich sauber sind. Sogar über HTML-Mails funktioniert die Attacke.

Lückenhaft

Lücken in der Router-Firmware sind jedoch keinesfalls ein exklusives AVM-Problem. Fast jeder Hersteller war schon mindestens ein Mal betroffen. Anfang März hat es unter anderem Geräte von D-Link im großen Stil erwischt: Der Admin einer in Deutschland und Österreich vertretenen Restaurantkette informierte uns darüber, dass innerhalb einer Nacht alle 19 D-Link-Router in den Filialen manipuliert wurden. Die Geräte waren nicht ohne Weiteres zu finden, hatten also nicht etwa aufeinanderfolgende öffentliche IP-Adressen, sondern waren im Adressbereich der Telekom verteilt. Das bedeutet, dass die Angreifer höchstwahrscheinlich auch alle anderen verwundbaren Router in diesem Bereich gekapert haben.

In den Restaurants kam das D-Link-Modell DSL-321B zum Einsatz, das der Hersteller als DSL-Modem vermarktet. Es lässt sich jedoch auch in einen Router-Modus versetzen – einschließlich aller damit verbundenen Risiken. Die Angreifer haben den eingestellten DNS-

Auf ct.de/fritz können Sie überprüfen, ob Ihre Fritzbox verwundbar ist.

Server verändert und konnten so den gesamten Internetverkehr auf sich umleiten, mitlesen und manipulieren. Sie konnten sogar das Zustandekommen von verschlüsselten Verbindungen verhindern, was oft dazu führt, dass die Daten im Klartext übertragen werden. Als wir D-Link befragten, konnte sich das Unternehmen die Angriffe zunächst nicht erklären. Kurz darauf entdeckte die Firma jedoch eine Monate alte Firmware auf ihrem FTP-Server, welche die Geräte zwar absicherte, aber gleichzeitig auch ein neues Sicherheitsloch aufriss. Wenig später lieferte der Hersteller eine Lösung in Form eines weiteren Updates. Es ist bereits auf Ende 2013 datiert, war zuvor jedoch nicht öffentlich erhältlich.

Die Modem-Router wurden anfangs mit einer Firmware ausgeliefert, in der eine fatale Sicherheitslücke klafft. Betroffen ist der Embedded-Webserver Allegro RomPager, der die Admin-Oberfläche ausliefert. Sendet man diesem eine simple HTTP-Anfrage, schickt er einen Export der Router-Konfiguration zurück, der auch das Admin-Passwort enthält. Bei der ersten Firmware ist das Web-Interface auch noch über das Internet zugänglich – selbst dann, wenn der Router-Besitzer dies in den Einstellungen deaktiviert. So konnten die Angreifer die verwundbaren Modem-Router bequem aus der Ferne aufspüren und übernehmen.

D-Link

D-Link DAP-1150, DWL-2100AP, 704P, DIR-615, DSL-500T, DSL-502T, DSL-504T, DSL-562T, DSL-G604T, DWL-7000AP, DWL-7100AP, DNS-320, DNS-325, DSL-2750U, DWL-2100AP, DIR-280, DSL-2740B

01/15/14	[+]	DWL-2100AP - Configuration Disclosure	[SET IP]
15/01/14	[+]	DSL-2750U - Authentication Bypass	[SET IP]
05/08/12	[+]	D-Link DSL-2640U PPoE Data Disclosure (ADSL Router)	[SET IP]
09/08/13	[+]	D-Link DSL-2740B - Enable Remote Management	[SET IP]
09/08/13	[+]	D-Link DSL-2740B - Disable Firewall	[SET IP]
09/08/13	[+]	D-Link DSL-2740B - Disable Wireless MAC Filter	[SET IP]
07/26/13	[+]	DIR 865L PHP file inclusion	[SET IP]
07/26/13	[+]	DIR 865L PHP file inclusion	[SET IP]
04/23/13	[+]	D-Link DIR-615 D3 - Remote Command Execution	[SET IP]
04/23/13	[+]	D-Link DIR-615 D3 - Change Admin Password CSRF	[SET IP]
03/19/12	[+]	DSL-2640B change admin password CSRF	[SET IP]

Wer im Netz nach Router-Modellen sucht, findet oft auch dazu passende Exploits.

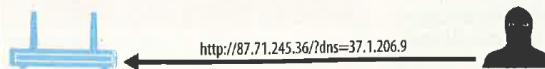


Viele Provider unterstützen die Faulheit ihrer Kunden, indem sie den voreingestellten WLAN-Schlüssel auf den Router schreiben.

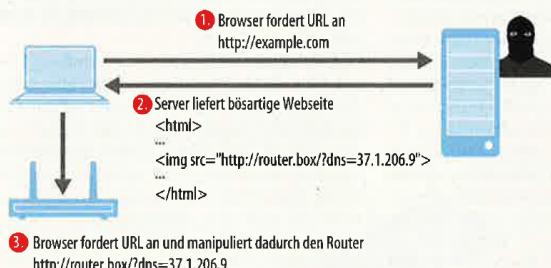
Praxis | Router-Sicherheit: Angriffe und Lücken

So werden Router angegriffen

Router sind insbesondere auf drei Wegen angreifbar: direkt über offene Dienste, indirekt über manipulierte Webseiten und Mails sowie drahtlos über das WLAN.

Direkter Angriff

Über das Internet erreichbare Router-Dienste sind ein gefundenes Fressen für den Angreifer. Beim **direkten Angriff** scannt er automatisch große IP-Adressbereiche, um zum Beispiel herauszufinden, bei welchem Internet-Nutzern ein Dienst auf dem HTTP-Port 80 antwortet. Oftmals handelt es sich dabei um das Web-Interface eines Routers, das Attacken aus dem Internet nicht viel entgegenzusetzen hat. Besonders leicht hat es der Angreifer, wenn das Admin-Passwort nicht geändert wurde – dann kann er etwa mit der Kombination admin:admin die volle Kontrolle übernehmen. Doch selbst wenn der Betreiber ein langes und kompliziertes Passwort gesetzt hat, schützt ihn das nicht zwangsläufig vor dem Angriff. In vielen Embedded Devices wie Routern klaffen Sicherheitslücken, durch die man die Authentifizierung umgehen kann, indem man etwa das Admin-Passwort ausliest oder Router-Befehle am Webinterface vorbeischleust.

Cross Site Request Forgery

Auch Dienste, die nicht direkt über Internet erreichbar sind, kann ein Angreifer attackieren, nämlich über **Cross-Site-Request-Forgery (CSRF)**. Dabei setzt er eine Webseite auf, die etwa ein Bildelement enthält (img), dessen Quell-URL auf den Router zeigt. Wird die Webseite, die auf einem beliebigen Server liegen kann, aufgerufen, versucht der Browser des Besuchers, das Bild nachzuladen. Das führt zum Beispiel zu einer HTTP-Anfrage an http://router.box/html/admin?function=setdns&dnsip=37.1.206.9. Das kann schon ausreichen, um den vom Router genutzten DNS-Server zu verstellen, wodurch der Angreifer den Internet-Traffic manipulieren kann. Auch das Ausnutzen von Schwachstellen ist auf diese Weise möglich. Der Angriffscode kann auf jeder beliebigen Webseite lauern. Immer wieder werden auch seriöse Sites über ihren Anzeigen-Lieferanten kompromittiert. Sogar über HTML-Mails lassen sich die folgenreichen Router-Befehle einschleusen.

Lokaler Angriff auf das WLAN

Viele WLAN-Router lassen sich nach wie vor drahtlos kompromittieren. Und zwar auch dann, wenn die als ausreichend sicher geltende WPA2-Verschlüsselung im Einsatz ist. Ein Angreifer muss sich beim **lokalen Angriff auf das WLAN** nämlich nicht mal die Mühe machen, aufwendig die Verschlüsselung zu knacken: In vielen Fällen kann er den WPA-Key herausfinden und sich dann ganz normal verbinden. Insbesondere bei diversen Provider-Routern wird der voreingestellte WPA-Schlüssel nach einem öffentlich bekannten Algorithmus generiert. Im einfachsten Fall benötigt dieser als Eingabe nur die MAC-Adresse des Routers – die jeder in Funkreichweite herausfinden kann. Unter Umständen führt auch das Durchprobieren der WPS-PINs zum Erfolg. Know-how ist für eine solche WLAN-Attacke kaum noch nötig, da man im Netz unter anderem Android-Apps findet, die auf Knopfdruck in fremde Netze einbrechen.

Das ganze Ausmaß der Katastrophe zeigte sich, als wir das Netz nach weiteren, für diese Lücke anfälligen Geräten durchsuchten. Den verwundbaren Server nutzen neben D-Link nämlich noch diverse weitere bekannte Hersteller wie LevelOne, TP-Link und Zyxel. Bei sehr vielen dieser Router ist das Web-Interface über das Internet ansprechbar: Weltweit konnten wir etwa 24 Millionen potenziell verwundbare Geräte aufspüren; davon allein 100 000 in Deutschland. Für einige der betroffenen Modelle gab es seit Jahren kein Firmware-Update. TP-Link schickte uns eine Liste mit gleich 30 betroffenen Modellen, für die „sukzessive Sicherheitsupdates zum Download bereitstehen“ sollen.

Stichproben zeigten, dass herstellerübergreifend fast alle Geräte tatsächlich anfällig waren. Innerhalb von Minuten hätten wir eine Router-Armee aus Hunderten Einheiten aufstellen können, die Befehle bereitwillig, aber stillschweigend ausführt. Allerdings sind auf diese Idee offenbar auch schon andere gekommen: Viele der Router waren be-

reits gekapert. Das konnten wir an dem eingesetzten DNS-Server 37.1.206.9 erkennen, der sich auch in den Modem-Routern der Restaurantkette fand.

Hereinspaziert

Allein die Tatsache, dass Dienste des Routers über das Internet erreichbar sind, ist ein Sicherheitsproblem für sich. Auf den Embedded-Systemen laufen nicht selten steinalte Server-Anwendungen, die man als Nutzer in der Regel nicht auf den aktuellen Stand bringen kann. Zudem sind die Skripte, die das Web-Interface generieren, nicht gegen Angriffe aus dem Internet gehärtet. Der Passwortschutz der Web-Oberfläche mag Junior davon abhalten, die Jugendschutzfilter abzuschalten, stoppt aber kaum einen ambitionierten Hacker. Kurzum: Wer Router-Dienste über das Internet erreichbar macht, sollte ganz genau wissen, was er tut. Welche Dienste ein Router anbietet, muss der Kunde leider selbst herausfinden. Dabei hilft der Netz-

werkcheck von heise Security, den Sie unter dem c't-Link am Ende des Artikels finden.

Anfang des Jahres zeigte sich, dass offenbar nicht mal die Hersteller so ganz genau wissen, welche Dienste ihre Router anbieten. Bei etlichen Modellen von Cisco, Netgear und Linksys wurde ein mysteriöser Backdoor-Dienst entdeckt, der bereitwillig Zugangsdaten wie das Admin-Passwort, den WLAN-Schlüssel und VPN-Logins rausrückt. In Tausenden Fällen war der undokumentierte Dienst sogar über das Internet erreichbar. Die Hersteller mussten nach eigener Aussage selbst erst mal ergründen, was es damit auf sich hat. Inzwischen gibt es diverse Firmware-Updates, die den Dienst abschalten. Hinter dem Phänomen steckt vermutlich der OEM-Hersteller Sercomm, der die betroffenen Geräte für die Netzwerkausrüster produziert hat. Ob es sich um eine absichtlich installierte Hintertür oder eine vergessene Warnungsschnittstelle handelt, ist unklar.

Im vergangenen Jahr sind wir sogar auf ein Router-Botnet gestoßen, das ganz darauf

ausgelegt war, den Datenverkehr der Opfer nach Zugangsdaten zu durchforsten. Die manipulierten Router hielten im durchgeschleusten Datenverkehr Ausschau nach unverschlüsselten Login-Informationen, etwa für Web-Anwendungen, FTP-Server und Mail-Accounts. In Kooperation mit dem LKA Niedersachsen gelang es uns, die beteiligten Kontroll-Server abzuschalten.

Feindbild Nachbar

Auch lokale Angriffe sind nach wie vor eine Bedrohung: Zwar sind inzwischen die meisten privaten WLANs WPA2-verschlüsselt, jedoch werden sie oft aus Bequemlichkeit mit dem voreingestellten WPA2-Schlüssel (WLAN-Passwort) betrieben. Dies begünstigen die Router-Anbieter, indem sie den Key auf die Unter- oder Rückseite des Geräts drucken. Bei vielen Modellen lässt sich dieser Schlüssel leicht knacken, nämlich wenn er auf Grundlage von Informationen wie der MAC-Adresse des Routers generiert wird, die auch ein Angreifer in Funkreichweite sieht.

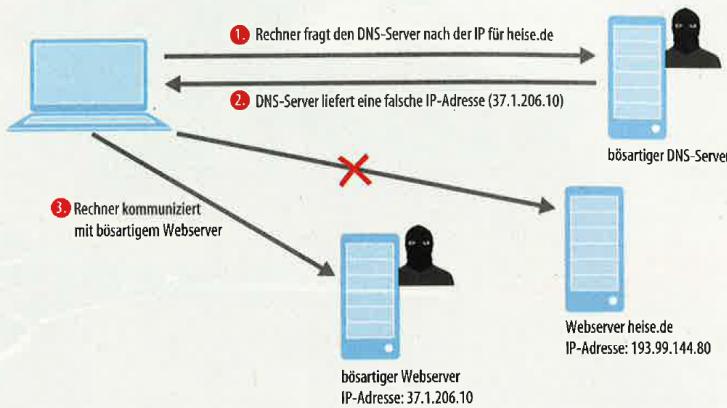
Ein Dauerproblem sind die Geräte des OEM-Herstellers Arcadyan, der sich das unsichere Verfahren sogar patentieren ließ. Arcadyan beliefert unter anderem die Telekom, Vodafone und o2, die allesamt betroffen waren oder sind. Zum Teil gelang der Angriff dort auch über WPS. Die Reaktionszeiten der Hersteller waren höchst verschieden: Vodafone etwa hat zwei Jahre lang wenig unternommen, um die Kunden dazu zu bringen, nach der Router-Installation den WPA2-Schlüssel zu ändern. Erst als mehrere Vodafone-Router im vergangenen Jahr dazu missbraucht wurden, gezielt die Hotline eines Krefelder IT-Dienstleisters lahmzulegen, informierte der Provider seine Kunden und schob ein Firmware-Update auf die betroffenen Router-Modelle. Es änderte zwar nicht den Key, dafür aber die öffentlich einsehbare MAC-Adresse der WLAN-Schnittstelle. Zu diesem Zeitpunkt gab es sogar schon Android-Apps wie das von dem Hannoveraner Schüler David W. entwickelte SpeedKey, das die betroffenen Router auf Knopfdruck knacken konnte.

David W. spielte uns nach der Veröffentlichung der neuen Firmware eine angepasste Angriffsmethode zu, durch die es weiterhin möglich wäre, die Router innerhalb weniger Minuten zu kapern. Als wir Vodafone kürzlich mit den neuen Erkenntnissen konfrontierten, verwies das Unternehmen auf die im Vorjahr durchgeführte Informationskampagne. Aus einer gut unterrichteten Quelle erfuhr c't, dass der Provider zwei Werkstage später damit begann, ein weiteres Firmware-Update an Zehntausende Router zu verteilen. Es zwingt die betroffenen Kunden, den WPA2-Key zu ändern. Leistet man nicht innerhalb von vier Wochen Folge, schaltet der Vodafone-Router seine WLAN-Schnittstelle ab.

Schneller hat o2 gehandelt: Nachdem wir dem Provider im März ein Proof-of-Concept-Tool des Reverse-Engineering-Spezialisten Hanno Heinrichs zugeschickt hatten, das die Anzahl der möglichen Schlüsselkombinatio-

Traffic-Umleitung durch DNS-Manipulation

Kleiner Eingriff, große Wirkung: Wenn der Router-Angreifer die eingestellte DNS-Server-Adresse verändert, kann er den gesamten Internetverkehr auf eigene Server umleiten, mitlesen und manipulieren.



nen erheblich reduziert, hat o2 umgehend damit begonnen, die rund 500 000 potenziell betroffenen Kunden schriftlich zu informieren. Allerdings scheint das Unternehmen den WPA2-Key nach wie vor für keine besonders schützenswerte Information zu halten: Es verschickt seine Router immer noch in unversiegelten Kartons, die jeder unbemerkt auf dem Weg zum Empfänger öffnen kann.

Nie war es für die Angreifer so leicht, mit geringem Aufwand großen Schaden anzurichten. Wer es darauf anlegt, kann sich in einer halben Stunde administrativen Zugang zu ein paar Hundert Routern in deutschen Netzen verschaffen. Statt aufwendig einzelne Rechner zu attackieren, übernehmen die Angreifer gleich den gesamten Internetanschluss. Im Gegensatz zu modernen Desktop-Betriebssystemen leisten Router kaum Gegenwehr; Schutzmechanismen, die einen Angreifer am Ausnutzen einer Schwachstelle hindern würden, sind nicht vorgesehen. Außerdem sind die Eindringlinge den Routern oft um Jahre voraus, wenn Firmware-Updates nicht eingespielt werden und sich die bekannten Sicherheitslücken häufen. Einen unvollständigen, aber trotzdem erschreckenden Überblick liefert die Webseite routerpwn.com. Hier findet man zu Routern fast jeden bekannten Herstellers passende Sicherheitslücken – allein 30 in D-Link-Geräten. Auch die Passwort-Algorithmen einiger Hersteller sind hier dokumentiert.

Sogar die Sicherheitsupdates liefern Hinweise auf Schwachstellen, die in den älteren Firmware-Versionen klaffen: Durch einen Vergleich der Firmware-Images findet man mit überschaubarem Aufwand heraus, welche Dateien der Hersteller verändert hat. Ein Decompiler verrät anschließend, welche Funktionen einer Binärdatei modifiziert wurden.

Angreifer können so auf die Lücken in älteren Versionen schließen und in nicht-aktualisierte Geräte einbrechen. Für den Router-Betreiber bedeutet dies, dass sich die Lage mit jedem ausgelassenen Update zuspitzt. Wer nicht regelmäßig sicherstellt, dass die Firmware seines Routers auf dem aktuellen Stand ist, muss damit rechnen, früher oder später erfolgreich angegriffen zu werden.

Handlungsbedarf

Einige Provider beliefern zumindest die von Ihnen gestellten Router inzwischen über das TR-069-Protokoll selbstständig mit Updates. Wer sich allerdings selbst kümmern muss, wird in der Regel bestenfalls nach dem Einloggen ins Web-Interface auf die Verfügbarkeit einer neuen Firmware-Version hingewiesen. Im schlechtesten Fall findet sich das Update lediglich auf dem FTP-Server des Herstellers, oft vergraben in einer schwer durchschauenden Verzeichnisstruktur. Wie die wichtigsten Hersteller mit dem Update-Problem umgehen, wo man die Updates findet und wie Sie auf dem Laufenden bleiben, haben wir im folgenden Artikel zusammengefasst.

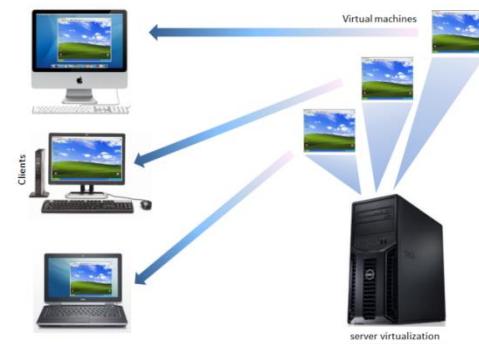
Ab Seite 90 erfahren Sie, wie Sie Ihren Router darüber hinaus möglichst sicher konfigurieren, wodurch viele automatisierte Angriffsversuche ins Leere laufen. Der Artikel „Auswechselspieler“ ab Seite 92 liefert Ihnen eine Notfall-Anleitung für den umgehenden Ersatz eines unsicheren Routers. Ab Seite 96 erfahren Sie schließlich, wie Sie einen ausrangierten PC mit OpenWRT ganz schnell in einen sicheren Übergangs-Router verwandeln. So gewinnen Sie Zeit, bis Sie sich einen Ersatz-Router beschafft haben. (rei)

c't

www.ct.de/1409082

4.9 Virtualisierung

Unter Virtualisierung versteht man die Nachbildung von physischen Ressourcen, also im Wesentlichen das Emulieren von Ressourcen. Beobachtet man die Hardware-Auslastung von Rechnern (Prozessor, Arbeitsspeicher etc.), dann erkennt man, dass die Ressourcen meist nur zu einem kleinen Teil ausgelastet sind. Diesen Umstand macht man sich bei der Virtualisierung zu nutze, indem man – insbesondere auf Serversystemen – die freien Ressourcen dafür einzusetzen, weitere virtuelle Rechner einzusetzen, die die reale Hardware teilen, sich jedoch wie eigenständige unabhängige Computer arbeiten.



4.9.1 Das Konzept der Virtualisierung

Bei der softwareseitigen Virtualisierung wird auf einem Betriebssystem (Wirts- oder Hostbetriebssystem) ein Programm installiert, welches die Erstellung von virtuellen PCs/virtuellen Maschinen (Gastbetriebssystem) ermöglicht. Diese virtuellen Maschinen können virtuelle Prozessoren, virtueller Arbeitsspeicher, virtuelle Netzwerkarten oder auch virtuelle Festplatten zugewiesen werden. Eine Festplatte ist für das Gastbetriebssystem in der Regel nur eine einfache Datei im Dateisystem des Hostbetriebssystems (zB: VHD-Datei = Virtual Hard Disk).

Flexibilität

Die Besonderheit an diesem Konzept ist, dass auf einem Betriebssystem (zB: Windows 8) eine virtuelle Maschine mit dem Betriebssystem Windows XP oder auch eine Linux-Distribution betrieben werden kann. Will man zum Beispiel Software testen oder alte Software einsetzen, dann eignen sich solche virtuellen Maschinen wunderbar, da sie leicht aktiviert und deaktiviert aber auch kopiert und auf einen vorherigen Stand wiederhergestellt werden können.

Virtuelles Netzwerk

Je nachdem wie Leistungsfähig die Ressourcen des Hostbetriebssystems sind können eine oder mehrere virtuelle Maschinen gleichzeitig betrieben werden. Diese virtuellen Maschinen können mit Hilfe eines virtuellen Netzwerkes untereinander und mit dem Hostbetriebssystem kommunizieren.

Auf VMs zugreifen

Auf virtuelle Maschinen kann entweder direkt über das Hostbetriebssystem über ein Anwendungsfenster zugegriffen werden oder man kann sich remote (Fernzugriff) auf eine virtuelle Maschine verbinden und ihre Ressourcen nutzen. Grafische Lösungen wären zum Beispiel die Remotedesktopverbindung von Microsoft, der VLC-Viewer oder das Programm Teamviewer. Lösungen auf Kommandozeilenebene wären SSH oder Telnet.

VM in der „Praxis“

Virtualisierungslösungen sind in der Praxis weit verbreitet. So werden sie bei weitem nicht mehr nur für das Emulieren oder Testen von Software eingesetzt. Aus Ressourcen- und Lizenzgründen werden VM oft als virtueller Arbeitsplatz genutzt aber auch für Cloud-Lösungen oder für Virtualisierungen in Rechenzentren.

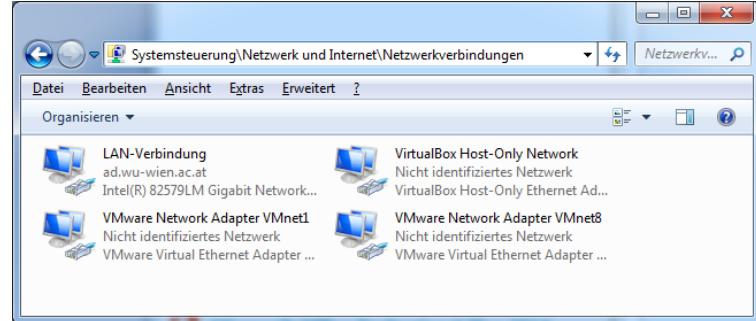
Verbreitete Virtualisierungslösungen

Einer der Big-Player im Virtualisierungsbereich ist VMware. Diese bietet von Desktoplösungen über High-End-Produkte wie vRealize oder vCloud Spezialanwendungen für Rechenzentren an (www.vmware.com/at). Microsoft bietet mit Hyper-V Server 2012 oder Azure eigene Lösung an, die auch in Windows Server 2012 als Serverrolle integriert sind. Eine weitere bekannte Lösung ist Virtual Box von Oracle (www.virtualbox.org).

4.9.2 Virtuelle Maschine installieren (VMware-Player)

Mit Hilfe der Software VMware-Player können ganz einfach virtuelle Maschinen eingerichtet, verwaltet und betrieben werden. Der Einsatz ist für den nicht-kommerziellen Einsatz kostenlos. Die Software kann für Windows oder Linux als 32-bit oder 64-bit unter https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/6_0 heruntergeladen werden.

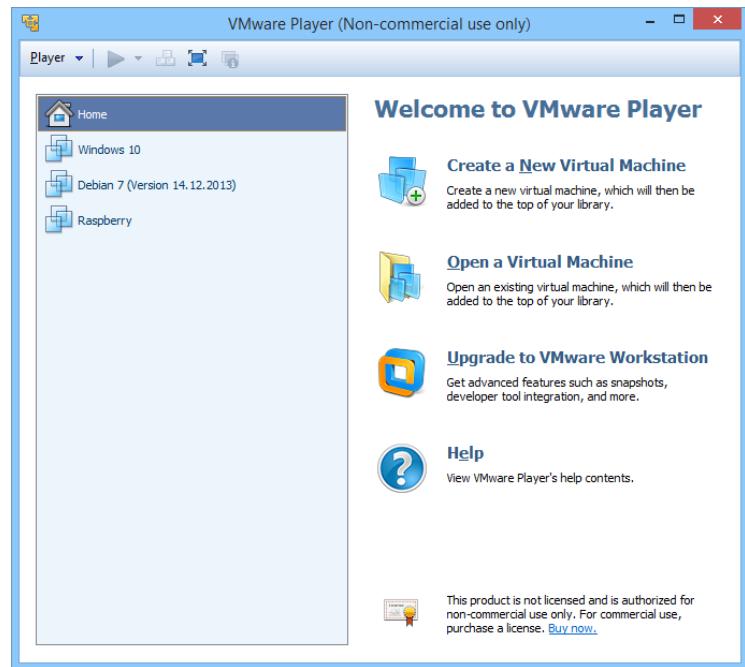
Die Installation der Software verläuft durch lediglich die Auswahl des Speicherorts denkbar einfach. Nach Abfolge der Installationsroutine wird eine Verknüpfung zur Software im Startmenü erstellt. Außerdem werden dem Betriebssystem drei weitere Netzwerkkarten hinzugefügt, die man in der Systemsteuerung finden kann.



Die Oberfläche

Die Übersichtsseite der Software ist denkbar einfach gestaltet. Auf der rechten Seite werden alle virtuellen Maschinen dargestellt, die mit dem Programm erstellt oder verknüpft wurden. Auf der rechten Seite befinden sich die Möglichkeiten, neue virtuelle Maschinen zu erstellen oder bestehende virtuelle Maschinen (zB: von einem USB-Stick, den Sie von jemanden anders bekommen haben) zu öffnen.

Im Menüpfad Player → File → Player Preferences kann eingestellt werden, ob Software-Updates automatisch beim Start der Software gesucht werden sollen und es können die VMware-Tools über die Schaltfläche „Download All Components Now“ heruntergeladen werden.



VMware-Components

Wenn Sie eine virtuelle Maschine installiert oder geöffnet haben dann können die sogenannten „VMware-Tools“ zusätzlich installiert werden. Diese beinhalten für ausgewählte Betriebssysteme aktualisierte Treibersoftware und ermöglichen die tiefere Integration des Gastbetriebssystems in das Hostbetriebssystem. So kann zum Beispiel Drag&Drop zwischen dem Gast- und dem Hostbetriebssystem ermöglicht werden oder es kann der „Unity Modus“ aktiviert werden.

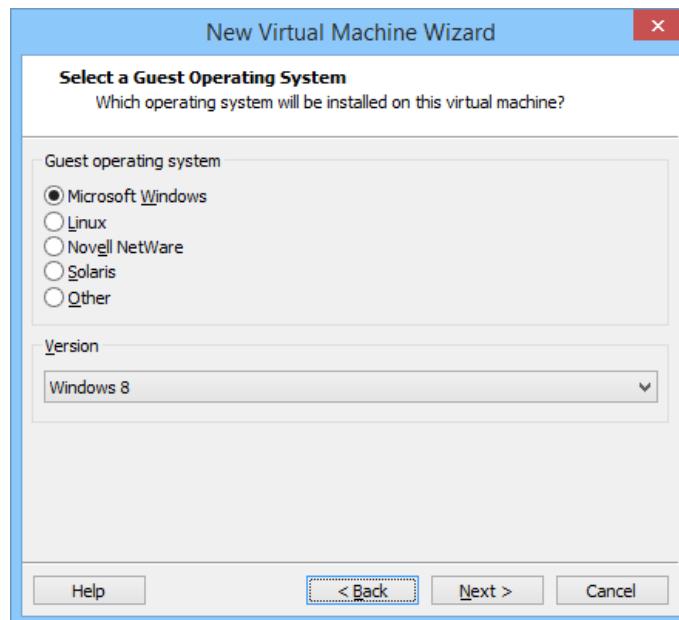
In diesem Modus können einzelne Anwendungen aus dem Gastbetriebssystem wie eine typische Anwendung am Hostbetriebssystem behandelt werden (also als eigenes Fenster).



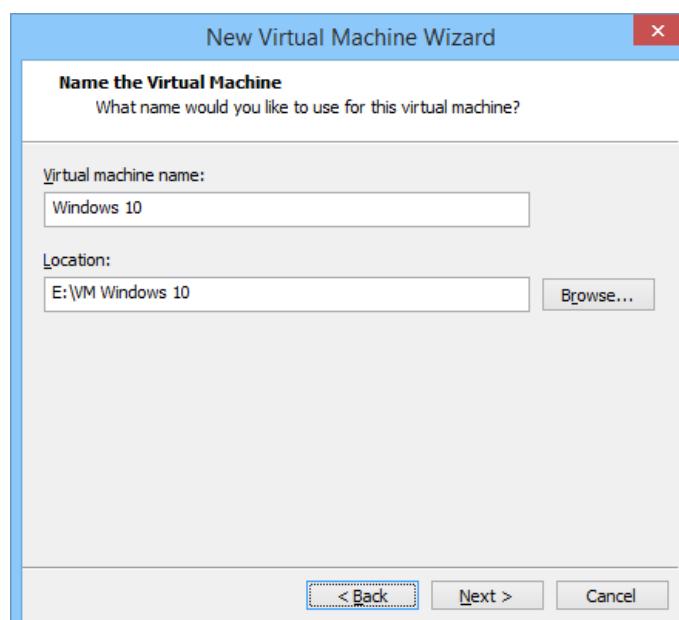
4.9.3 Virtuelle Maschine einrichten

4.9.3.1 Grundsystem festlegen

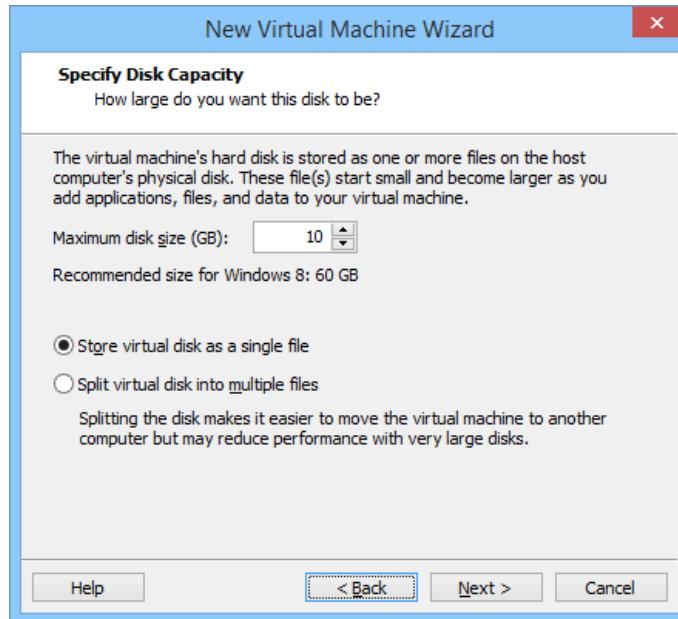
Beim Erstellen einer neuen virtuellen Maschine muss im ersten Schritt ausgewählt werden, welches Gastbetriebssystem darauf installiert werden soll. Das ist deshalb wichtig, da dem Betriebssystem, das installiert werden soll, möglichst optimierte Bedingungen „vorgegaukelt“ werden sollen. Soll also zum Beispiel ein Microsoft Windows Betriebssystem installiert werden, muss die erste Option gewählt werden. Im nachfolgenden Dropdown sollte dann die entsprechende Version ausgewählt werden. Ist die Version nicht vorhanden, muss jene ausgewählt werden, die dem zu installierenden Betriebssystem am ehesten entspricht (zB: Windows 8 bei der Installation von Windows 10).



Im zweiten Schritt muss für die virtuelle Maschine ein Name vergeben werden und der Speicherort bestimmt werden. Dies geschieht am besten über die Schaltfläche „Browse“. Virtuelle Maschinen können auf jedem beliebigen Datenträger installiert werden, also auch auf einem USB-Stick. Für die Installation und den Betrieb empfiehlt es sich aber stark, als Speicherort zunächst die lokale Festplatte auszuwählen.



Bevor die virtuelle Maschine gestartet werden kann muss noch eine virtuelle Festplatte erstellt werden. VMware schlägt automatisch die empfohlene Größe für das gewählte Betriebssystem vor. Es kann zusätzlich gewählt werden, ob diese virtuelle Festplatte in einer einzigen Datei oder in mehreren Dateien gespeichert werden soll. Die zweite Auswahlmöglichkeit erleichtert den Austausch zwischen mehreren PCs, während die erste Auswahlmöglichkeit eine höhere Performance gewährleistet.

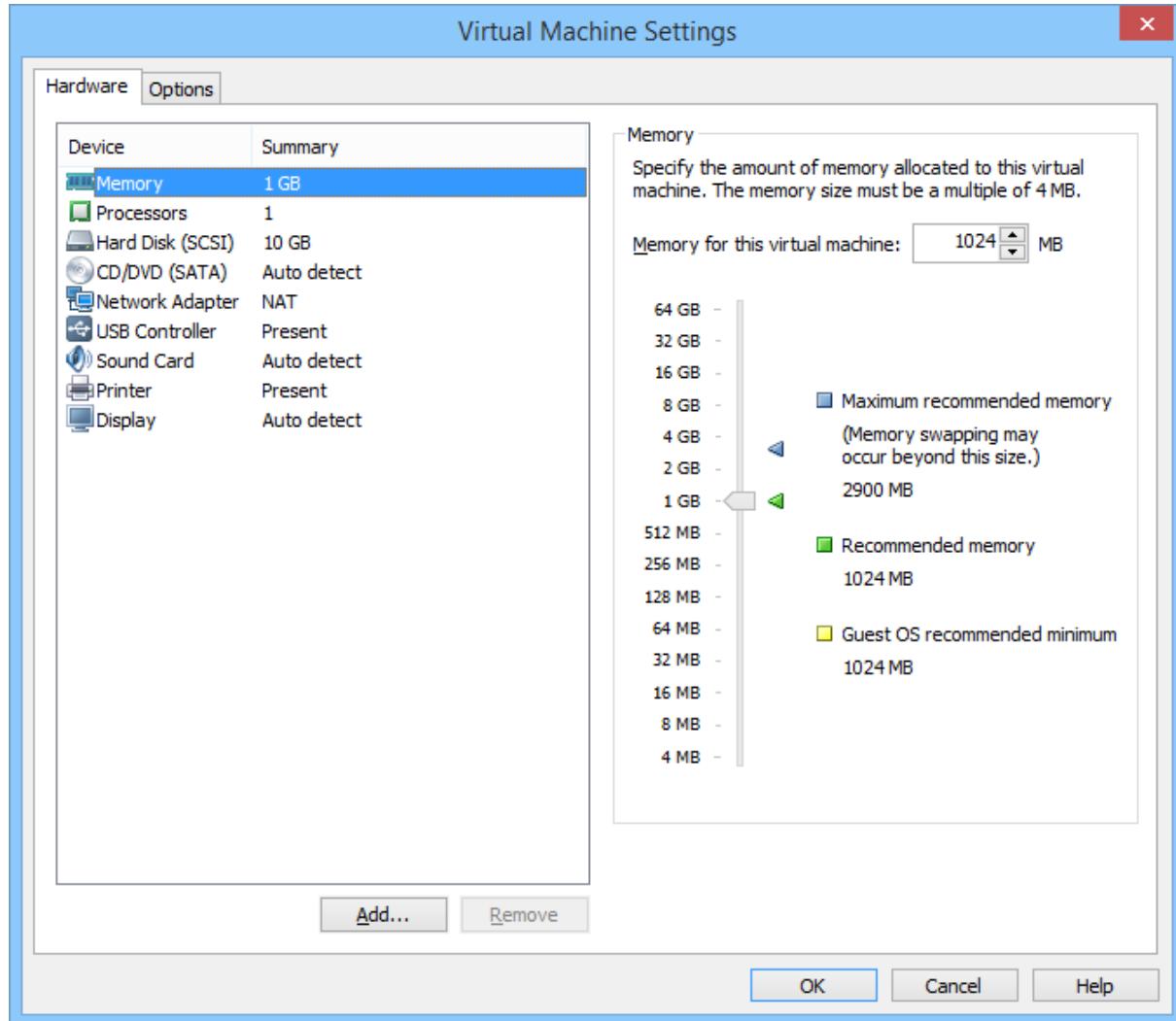


Nach einem Klick auf „Next >“ wird nun die Konfiguration der virtuellen Maschine zusammengefasst. Noch ein weiterer Schritt und die virtuelle Maschine wird im angegebenen Speicherort erstellt. Dabei werden nicht nur eine Datei sondern mehrere Dateien erstellt. Die Bedeutung dieser Dateien ist in der nachfolgenden Tabelle dargestellt:

Dateiendung	Bedeutung
.vmx	Dies ist die Konfigurationsdatei, in der der Name, die angeschlossene (virtuelle) Hardware und der Speicherort der virtuellen Festplatten vermerkt sind. Mit einem Doppelklick auf diese Datei kann die virtuelle Maschine gestartet werden.
.nvram	Diese Datei ist das BIOS der virtuellen Maschine.
vmware.log	In dieser Datei werden alle Statusmeldungen der virtuellen Maschine abgelegt. Liegt zum Beispiel ein Fehler vor, empfiehlt es sich, zuerst mit einem Texteditor einen Blick in diese Datei zu werfen.
.vmdk	Dies ist die virtuelle Festplatte der virtuellen Maschine (für VMware-Produkte). Ein anderer Dateityp für virtuelle Festplatten wäre der Dateityp VHD.
.vmss	Virtuelle Maschinen können entweder heruntergefahren werden (ausgeschaltet) oder auch einfach pausiert werden (Suspend). Diese Funktion ist dem Standby-Modus bei Notebooks sehr ähnlich. Der Vorteil ist, dass recht einfach an der gleichen Stelle in der virtuellen Maschine weitergearbeitet werden kann.
.lck	Beim Starten einer virtuellen Maschine wird eine *.lck-Datei angelegt, die dazu dient, den Zugriffsschutz für die virtuelle Festplatte zu gewährleisten. Somit wird verhindert, dass ein anderer Nutzer die virtuelle Festplatte öffnet und es dadurch zu Datenverlust kommt.

4.9.3.2 Einstellungen ändern

Bevor eine virtuelle Maschine gestartet wird, sollten noch einige Einstellungen getätigt werden. Dafür markiert man am Startbildschirm die gewünschte virtuelle Maschine und klickt auf die Option „Edit virtual machine settings“ in der rechten unteren Ecke.



Memory

Hier kann der Arbeitsspeicher für das Gastbetriebssystem eingestellt werden. Es sollten nicht mehr als die Hälfte des physikalisch vorhandenen Speichers für eine VM zugewiesen werden. Sollte die virtuelle Maschine oder das Hostbetriebssystem spürbar langsam laufen, muss zunächst die Speicherauslastung beider Systeme überprüft werden um dann eine optimale Arbeitsspeicherzuweisung vorzunehmen.

Processors

Hier kann eingestellt werden über wie viele logische Prozessorkerne die virtuelle Maschine verfügen soll. In der Regel reichen für Betriebssysteme ein- oder zwei Kerne. Die Option „virtualization engine“ sollte auf „Automatic“ gesetzt sein, es sei denn, Sie wissen, dass Ihre CPU über einen speziellen Befehlssatz „Intel VT-x/EPT“ oder „AMD-V/RVI“ verfügt, mit denen virtuelle Maschinen optimal unterstützt werden.

Hard Disk (SCSI)

Hier werden die Festplattenkapazität und die Auslastung angezeigt. Ist die Festplatte zu klein bemessen, kann sie – sofern die virtuelle Maschine heruntergefahren ist – über die Schaltfläche Utillites → Expan vergrößert werden. Über die Schaltfläche „Add...“ in der rechten unteren Ecke kann auch eine weitere virtuelle Festplatte zum Gastbetriebssystem hinzugefügt werden.

CD/DVD (SATA)

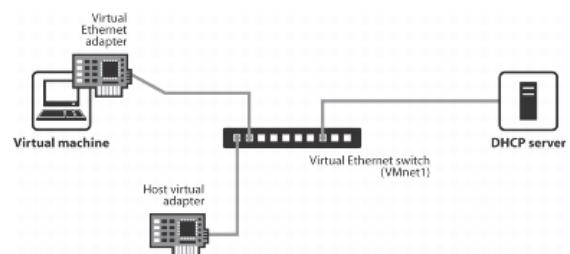
Hier können virtuelle CD oder DVD-Laufwerke hinzugefügt werden. Ein Standardformat für virtuelle CD/DVD-Images ist das Dateiformat ISO. Viele Software-Downloads werden als ISO-Datei (also dem virtuellen Abbild einer CD/DVD) angeboten, auf die Sie über die Option „Use ISO image file“ verweisen können. Alternativ dazu kann auch ein physisches Laufwerk des Hostbetriebssystems eingebunden werden. Wichtig ist, dass die Option „Connect at power on“ aktiviert ist, da sonst die Installation eines Betriebssystems über eine virtuelle CD/DVD nicht möglich ist.

Network Adapter

Dies ist eine der wichtigsten Einstellungen bei der Konfiguration von virtuellen Maschinen. Prinzipiell unterstützt der VMware-Player bis zu 10 verschiedene Netzwerkkonfigurationen. Drei davon sind bereits standardmäßig eingestellt. Das ist auch der Grund, weswegen auf dem Hostbetriebssystem auf einmal drei virtuelle Netzwerkkarten aufscheinen.

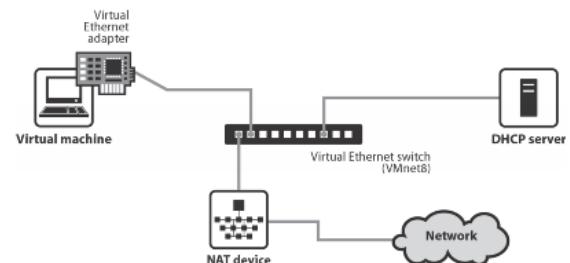
1. Host-only: A private network shared with the host

Bei dieser Einstellung werden die virtuellen Maschinen (mit ihren virtuellen Netzwerkkarten) über einen virtuellen Ethernet-Switch mit dem Hostbetriebssystem (auf dem ebenfalls eine virtuelle Netzwerkkarte mit dem Namen VMnet1 installiert ist) verbunden. Die Zuweisung der IP-Adressen erfolgt über einen DHCP-Server. Die virtuelle Maschine und das Hostbetriebssystem bilden somit ein eigenes virtuelles Netzwerk. Es könnte jetzt ein Heimnetzwerk eingerichtet werden und über ein Netlaufwerk könnten Dateien-, Bilder- und Videos etc. ausgetauscht werden.



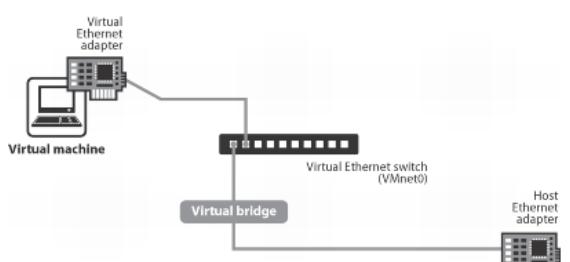
2. Network Address Translation (NAT)

Auch bei dieser Option werden die virtuellen Maschinen über einen virtuellen Switch (hier jedoch VMnet8) mit dem Hostbetriebssystem verbunden. Das Hostbetriebssystem agiert hier als Router (über NAT; vgl. dazu S. 67). Sendet eine virtuelle Maschine eine Anfrage an einen Rechner, der sich nicht im selben virtuellen Netzwerk befindet, wird die Anfrage an den Router weitergegeben, der das Datenpaket dann in ein anderes Netzwerk (zB: das WAN des Internet Service-Providers) weiterleitet. Empfängt das Hostbetriebssystem Datenpakete, wird eben über NAT nachgeschlagen, ob das Datenpaket für eine virtuelle Maschine bestimmt ist. Ist dies der Fall, wird das Datenpaket an diese VM weitergeleitet.

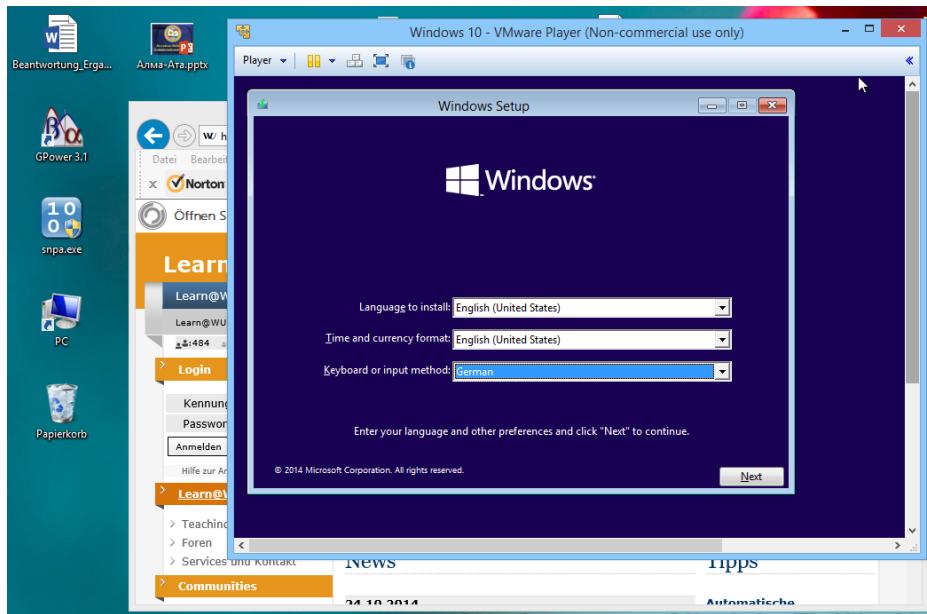


3. Bridget Networking

Bei dieser Option wird kein virtuelles Netzwerk zwischen dem Hostbetriebssystem und der virtuellen Maschine aufgebaut. Vielmehr wird eine virtuelle Brücke verwendet, die es ermöglicht, dass der virtuellen Maschine eine physische Netzwerkkarte des Hostbetriebssystems zugewiesen wird. Verwendet zum Beispiel das Hostbetriebssystem die Ethernet-Netzwerkkarte um sich mit einem WAN zu verbinden, kann der virtuellen Maschine die WLAN-Netzwerkkarte zugewiesen werden, da diese ja vom Hostbetriebssystem nicht verwendet wird.

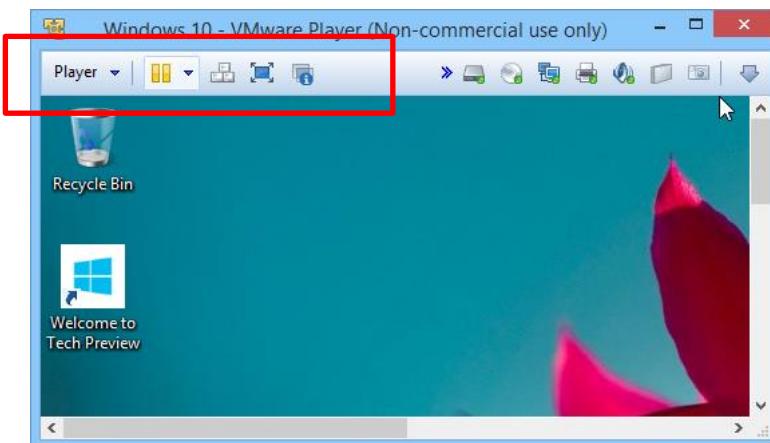


Die virtuelle Maschine verhält sich wie ein „normales Computerprogramm“. Sie wird in einem Fenster ausgeführt, das am Hostbetriebssystem beliebig verschoben, vergrößert, verkleinert und natürlich auch wieder geschlossen werden kann.



Wenn der Mauszeiger in die virtuelle Maschine bewegt wird und ein Klick erfolgt, wird der Mauszeiger von der VM „gescatched“. Das heißt, der Mauszeiger kann nur noch innerhalb der VM bewegen werden. Um den Mauszeiger wieder zu befreien muss die Tastenkombination STRG+ALT gedrückt werden.

In der Menüleiste der virtuellen Maschine kann diese entweder angehalten (pausiert), neu gestartet oder heruntergefahren werden. Außerdem gibt es eine Schaltfläche um die Tastenkombination STRG+ALT+ENTF auf dem Gastbetriebssystem auszuführen. Daneben befindet sich eine weitere Schaltfläche, mit der die VM im Vollbildmodus ausgeführt werden kann.

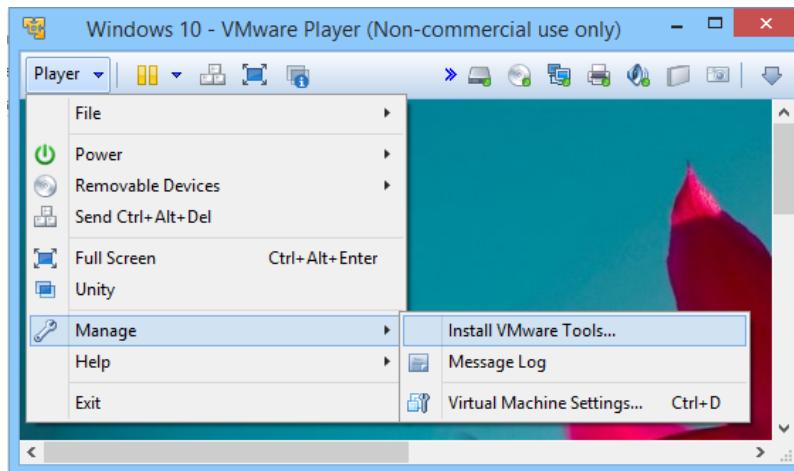


Auf der rechten Seite der Menüleiste werden alle wichtigen virtuellen Geräte des Gastbetriebssystems dargestellt. Die Festplatte, das DVD/CD-Laufwerk, die virtuelle Netzwerkkarte, der Drucker sowie Soundkarte und sonstige Devices wie USB-Sticks oder Webcams. Mit einem Rechtsklick auf eines dieser Symbole kann das ausgewählte Gerät entweder deaktiviert werden oder die Einstellungen geändert werden. So könnte zum Beispiel über die Schaltfläche DVD/CD eine neue virtuelle DVD eingelegt werden.

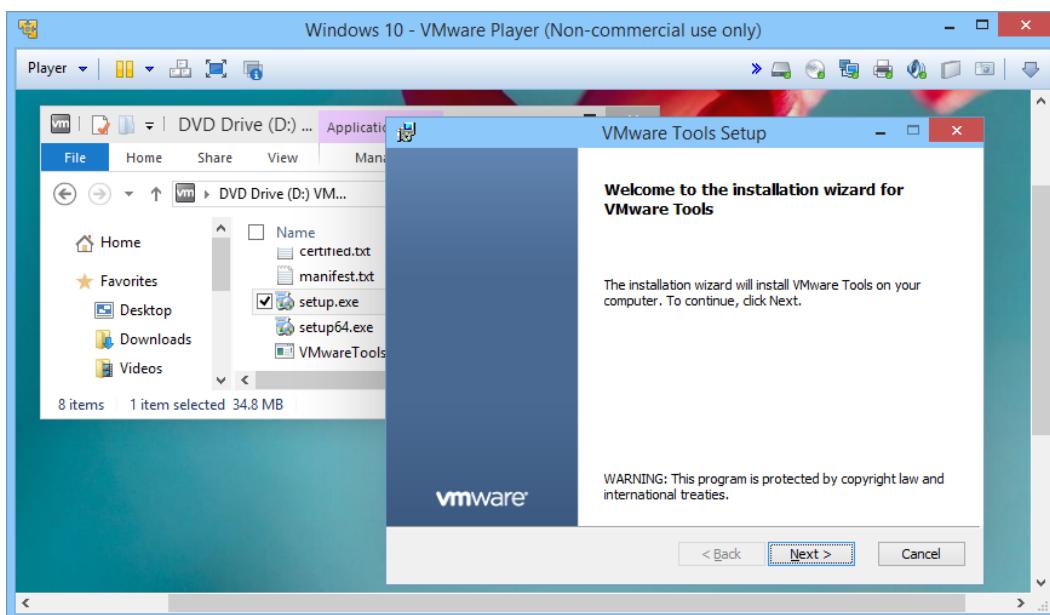
4.9.3.3 Unity-Modus und Treiberinstallation

Es kann sein, dass das Gastbetriebssystem nicht alle virtuellen Komponenten, die die Software VMware-Player zur Verfügung stellt erkennt bzw. nicht über die notwendigen Treiber verfügt. Deshalb kann eine Treiber-CD geladen werden, welche die VMware-Tools installiert. Außerdem sind in diesen VMware-Tools Funktionalitäten enthalten, die die tägliche Arbeit mit einer virtuellen Maschine erheblich erleichtern (zb: Unity-Modus oder Drag&Drop zwischen Gast- und Hostbetriebssystem).

Um die VMware-Tools zu installieren, muss die Installation über die Menüleiste mit „Player → Manage → Install VMware Tools“ aufgerufen werden. Dieser Befehl bewirkt, dass eine virtuelle CD in das CD-Laufwerk des Gastbetriebssystems eingelegt wird.



Sollte die Installation nicht automatisch starten, muss diese direkt über den Arbeitsplatz des Gastbetriebssystems aufgerufen werden (durch Doppelklick auf die Datei „setup.exe“ bzw. „setup64.exe“ bei einem virtuellen 64bit-Gastbetriebssystem).



In der Regel sollte die „typische Installation“ für die VMware-Tools ausreichend sein. Sie kann einige Minuten in Anspruch nehmen, da viele Treiber installiert werden. Ein Neustart des Gastbetriebssystems ist in der Regel notwendig!

Beachten Sie außerdem, dass die VMware-Tools für jede einzelne virtuelle Maschine gesondert installiert werden müssen!

4.9.3.4 Netzwerk einrichten

Natürlich können zwischen dem Gastbetriebssystem(en) und dem Hostbetriebssystem auch Netzwerkverbindungen eingerichtet werden. Wird in den VMware-Einstellungen zum Beispiel die Option NAT gewählt, fungiert das Hostbetriebssystem quasi als Router und teilt mit den Rechnern seine Internetverbindung. Wie in der nebenstehenden Abbildung angezeigt, wird in dieser Einstellung dem Hostbetriebssystem die IP-Adresse 192.168.162.1 zugewiesen. Den Gastbetriebssystemen weist ein DHCP-Server dann eigene Adressen im entsprechenden Bereich zu.

```

Microsoft Windows [Version 6.4.9841]
(c) 2014 Microsoft Corporation. All rights reserved.

C:\Users\Franz-Karl>arp -a
Interface: 192.168.162.1 --- 0x3
Internet Address      Physical Address      Type
192.168.162.1         00-50-56-c0-00-08  dynamic
192.168.162.2         00-50-56-f1-dc-9f  dynamic
192.168.162.255       ff-ff-ff-ff-ff-ff  static
224.0.0.22             01-00-5e-00-00-16  static
224.0.0.252            01-00-5e-00-00-fc  static
224.0.0.253            01-00-5e-00-00-fd  static
239.255.255.250        01-00-5e-7f-ff-fa  static
255.255.255.255       ff-ff-ff-ff-ff-ff  static

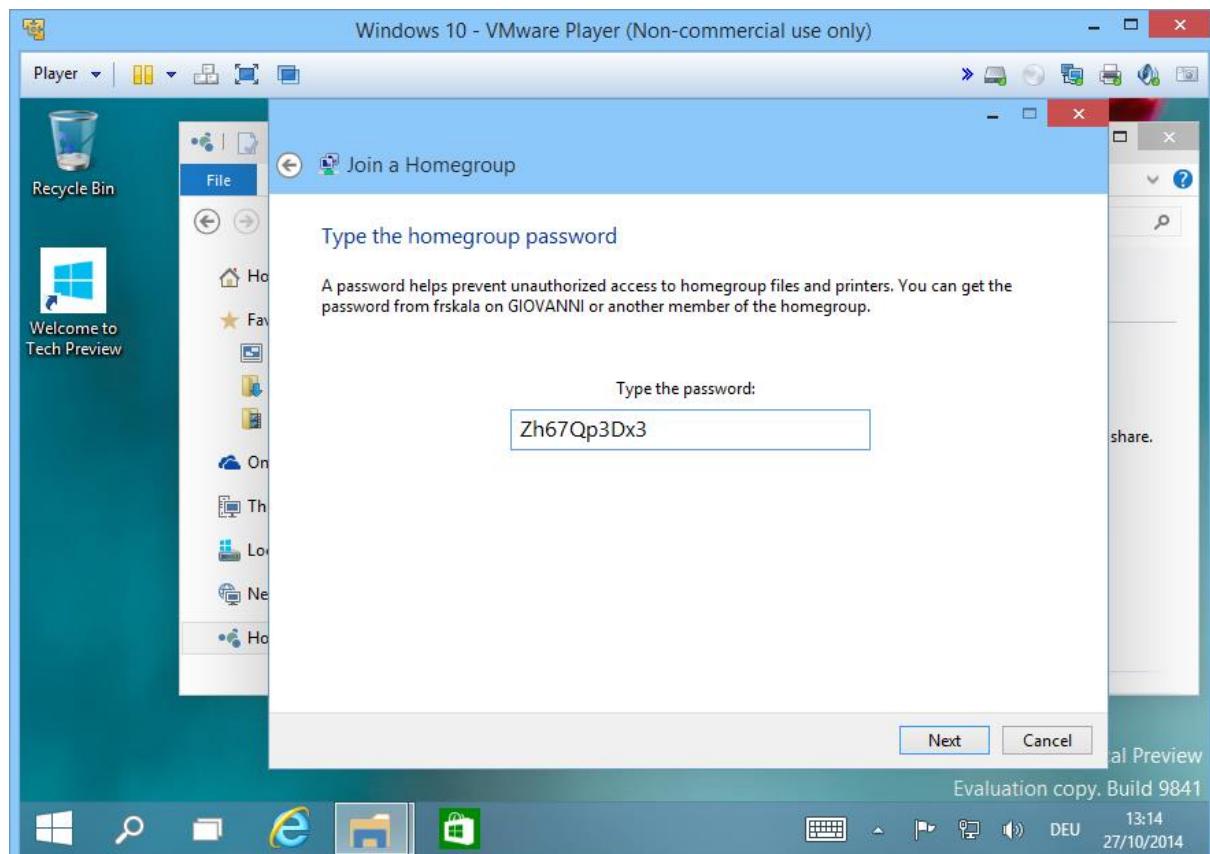
```

Scheinen die Computer in der Kommandozeile mit dem Befehl arp -a auf, dann ist eine Verbindung prinzipiell möglich. Sollten sie nicht im Bereich „Netzwerk“ unter Windows automatisch auftauchen, dann muss die Datei- und Druckerfreigabe in der (Windows-)Firewall erst aktiviert werden.

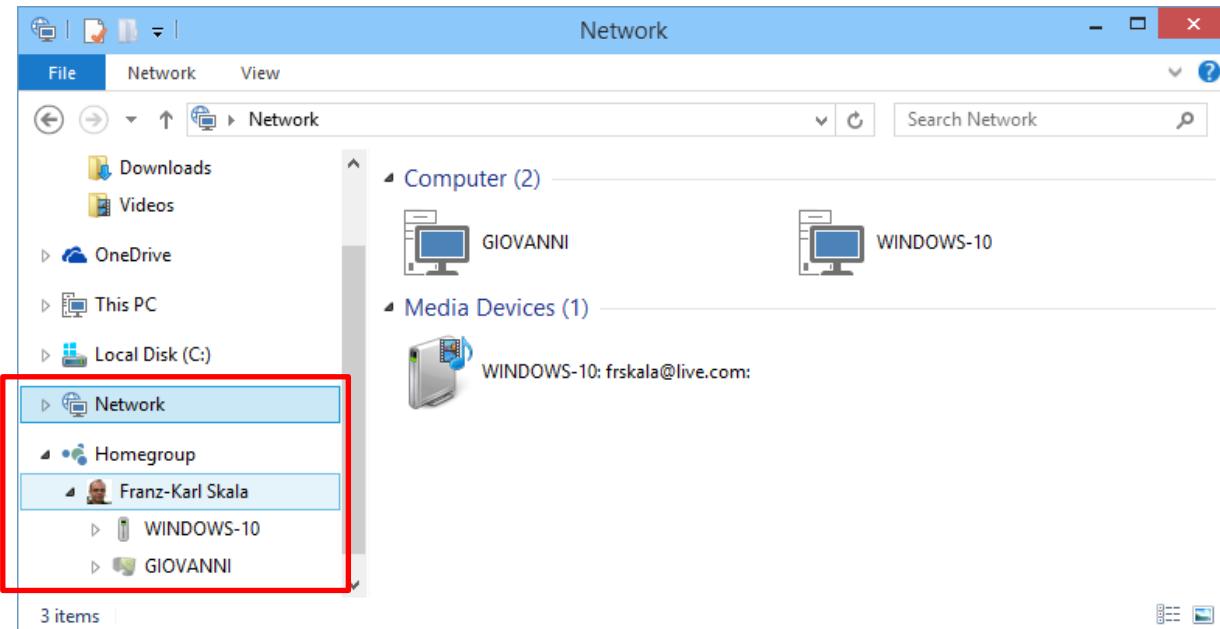
Heimnetzwerkgruppe einrichten

Unter Windows ist es ein leichtes mehrere Computer – im privaten Bereich – miteinander zu verknüpfen. Da hier typischerweise kein zentraler Domänen-Controller eingesetzt wird und es unterschiedliche Benutzernamen und PC-Namen gibt, muss die Funktion „Heimnetzwerkgruppe“ eingerichtet werden. Durch diese wird es möglich, dass Bilder-, Videos- und andere Dateien zwischen berechtigten Computern geteilt werden können.

Dafür muss zunächst auf einem der Computer, die sich im Netzwerk befinden, über „Systemsteuerung → Netzwerk und Internet → Heimnetzwerkgruppe“ eine neue Heimnetzwerkgruppe eingerichtet werden. Dabei wird ein Passwort generiert, das bei den anderen PCs eingegeben werden muss.

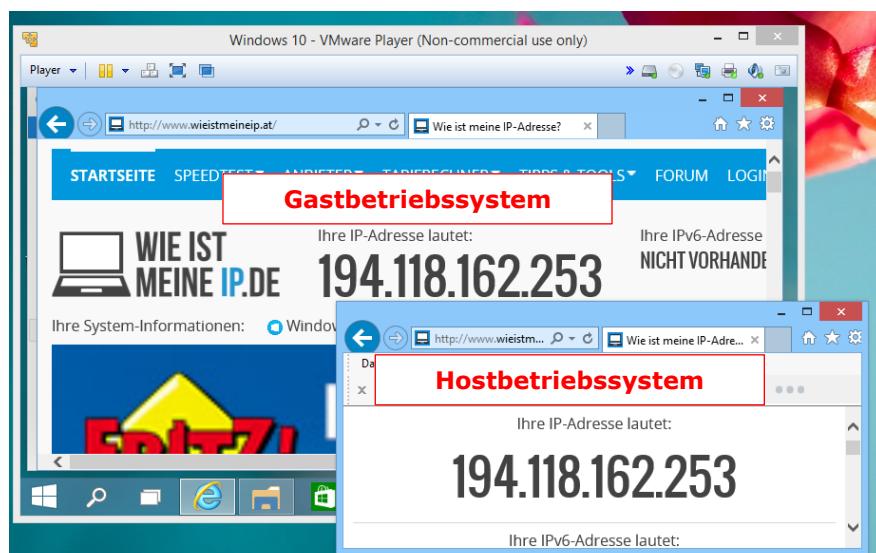
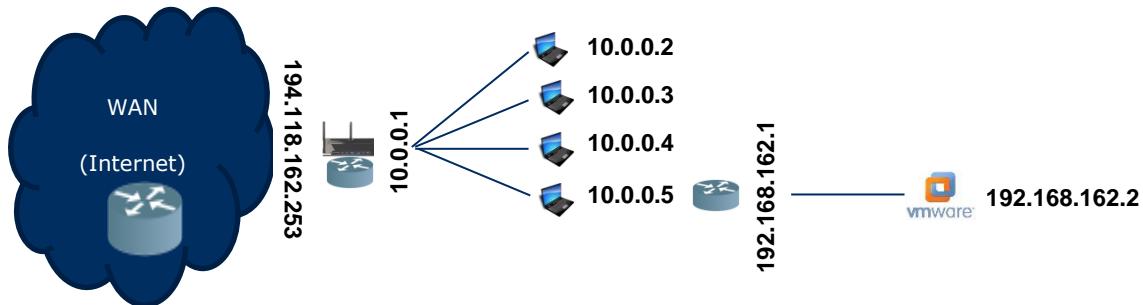


Sind die PCs ordnungsgemäß miteinander verbunden, scheinen diese erstens im Bereich Netzwerk auf und zweitens auch im Bereich Heimnetzwerkgruppe. Dort kann ganz einfach auf die freigegebenen Dateien zugegriffen werden, ohne dass jedes Mal Passwörter und Benutzernamen eingegeben werden müssen.



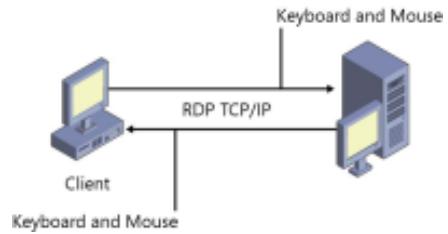
Logischer Aufbau des Netzwerks

Wird eine virtuelle Maschine im NAT-Modus auf einem Hostbetriebssystem betrieben, das seinerseits wieder in einem Netzwerk eingebunden ist, das wiederum an das WAN eines Internet Service-Providers eingegliedert ist, dann haben alle Adressen nach „außen“ hin, also im WAN dieselbe IP-Adresse, da NAT das Routing innerhalb des Netzwerks übernimmt.



4.10 Remote Desktop Verbindung

Das Remote Desktop Protokoll (RDP) ist ein Protokoll von Microsoft, das die Fernsteuerung des Desktops eines entfernten Computers ermöglicht. Das Protokoll ist proprietär und wird von allen Windows Versionen unterstützt. Konkret regelt das Protokoll die Übertragung der Bildschirminhalte sowie Tastatur- und Mauseingaben über das Netzwerk.



TCP/IP-Schicht		Beispiel
Anwendungen	RDP	
Transport	TCP	
Internet	IP (IPv4, IPv6)	
Netzzugang	Ethernet, Token Bus, Token Ring, FDDI	

Das Protokoll läuft in der Regel über den Port 3389. Dieser darf von einer Firewall nicht blockiert werden, da sonst keine Verbindung hergestellt werden kann (Rechner wird nicht gefunden).

4.10.1 Funktionsweise

Über den RDP-Client Remotedesktopverbindung (mstsc.exe) kann eine verschlüsselte Verbindung zwischen zwei Rechnern aufgebaut werden. Dafür sind zwei Voraussetzungen notwendig:

1. Der Remote-Rechner kann direkt über eine IP-Adresse und den Port 3389 erreicht werden!
2. Die Remotedesktopverbindung wurde aktiviert.
3. Administrator-Kennung muss bekannt sein (oder Rechtezuweisungen sind vorhanden).

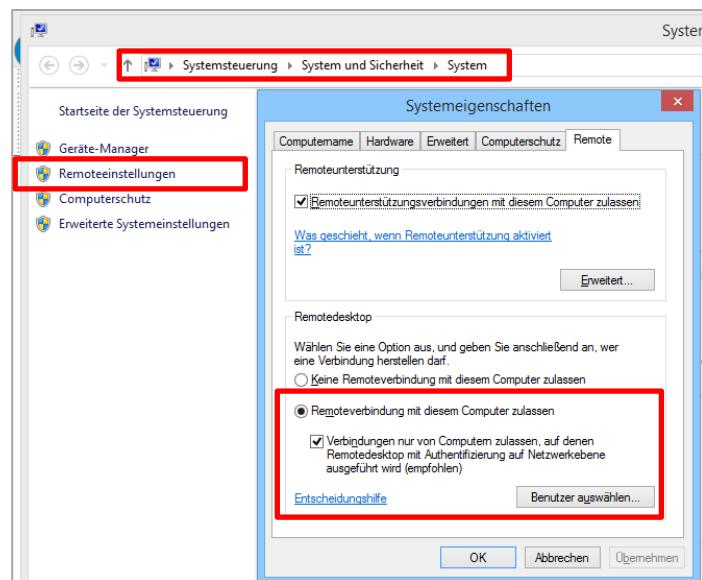
Kann der Remote-Rechner nicht direkt über eine IP-Adresse erreicht werden sondern hängt er in einem Netzwerk, das über eine Gateway-Verbindung an das Internet angebunden ist, ist kein direkter Zugriff möglich, es sei denn, es wird eine VPN-Verbindung zu diesem Netzwerk aufgebaut. Abhilfe schafft dabei der Einsatz eines Remotedesktop-Gatewayservers, der zum Beispiel über Windows Server 2008 oder Windows Server 2012 leicht als Rolle über den Server-Manager hinzugefügt werden kann.

4.10.2 Remotedesktop-Verbindung einrichten

Zunächst öffnet man über die Tastenkombination WINDOWS+PAUSE (oder Systemsteuerung\System und Sicherheit\System) die Systemeigenschaften und wählt dann die Option Remoteeinstellungen.

Dort muss die Option „Remoteverbindung mit diesem Computer zulassen“. Wenn diese Option aktiviert wird, lässt die Windows-Firewall die Verwendung der Remoteunterstützung zu, damit mit dem PC kommuniziert werden kann.

Die Option mit der Authentifizierung auf (Windows)Netzwerkebene sollte aktiviert sein, da dabei die Remotedesktopverbindung erst dann aufgebaut wird, wenn zuvor eine Benutzerauthentifizierung über das Windows-Netzwerk erfolgt ist.



Anschließend können über die Schaltfläche „Benutzer auswählen“ all jene Benutzerkonten hinzugefügt werden, die berechtigt sind, sich über RDP an genau diesem Rechner anzumelden. In einem Windows-Netzwerk mit „Active Directory“ können diese Rechte über Benutzergruppen einfacher verwaltet werden.

4.10.3 Unterstützte Betriebssysteme

Prinzipiell kann eine Remotedesktopverbindung **von** jeden Windows-Rechner hergestellt werden. Auf dem Remote-PC muss jedoch eines der folgenden Windows-Betriebssysteme ausgeführt werden, da sonst leider keine Verbindung möglich ist:

Betriebssystem	Version
Windows 8.1	Pro, Enterprise
Windows 8	Pro, Enterprise
Windows 7	Professional, Enterprise, Ultimate
Windows Vista	Business, Enterprise, Ultimate
Windows XP	Professional

Welche Version des Betriebssystems ausgeführt wird kann leicht mit der Tastenkombination START+PAUSE herausgefunden werden.

4.10.4 Remotedesktop-Verbindung aufbauen

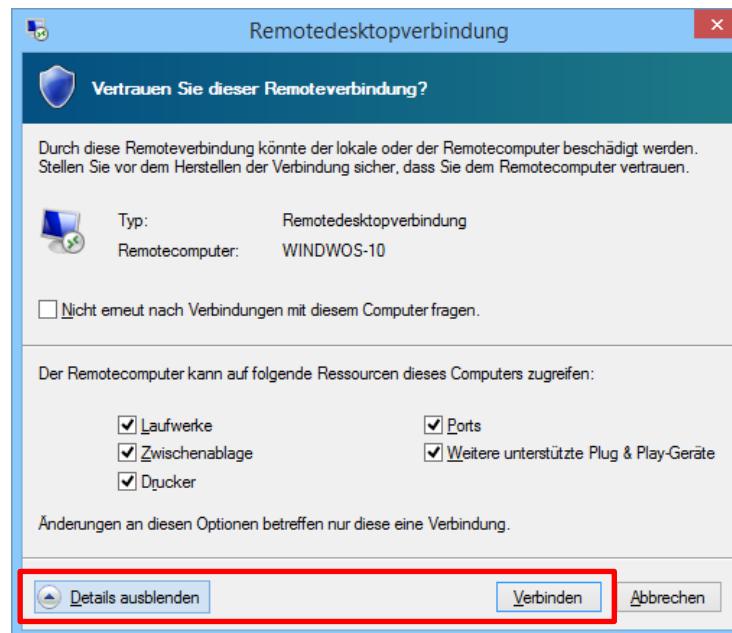
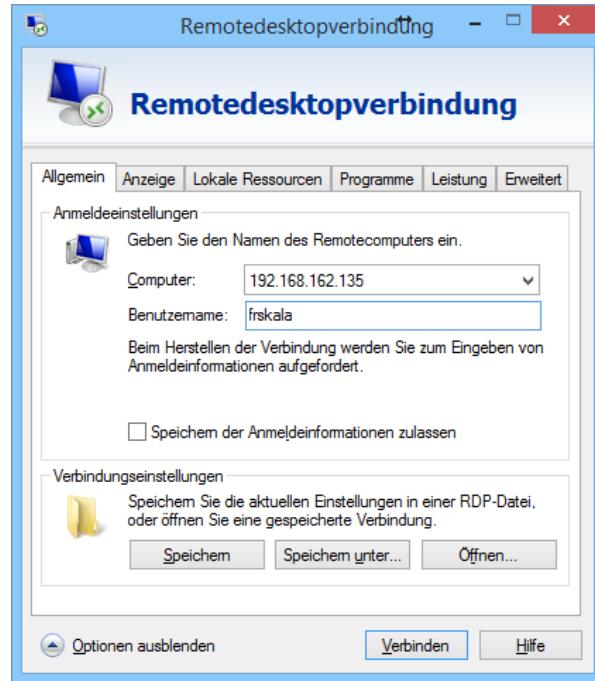
Wenn per RDP auf einen Rechner zugegriffen werden soll, muss auf dem entfernten Rechner RDP aktiviert sein und ein entsprechender Nutzer (Administrator) bekannt sein und natürlich der Name des Rechners bzw. die IP-Adresse.

Sind diese Schritte erfüllt muss ein Client-RDP-Programm gestartet werden. Dieses heißt unter Windows mstsc.exe. Zunächst muss in der Registerkarte „Allgemein“ der Name/die IP des entfernten Rechners eingetragen werden sowie der Benutzer, mit dem die Authentifizierung vorgenommen werden soll.

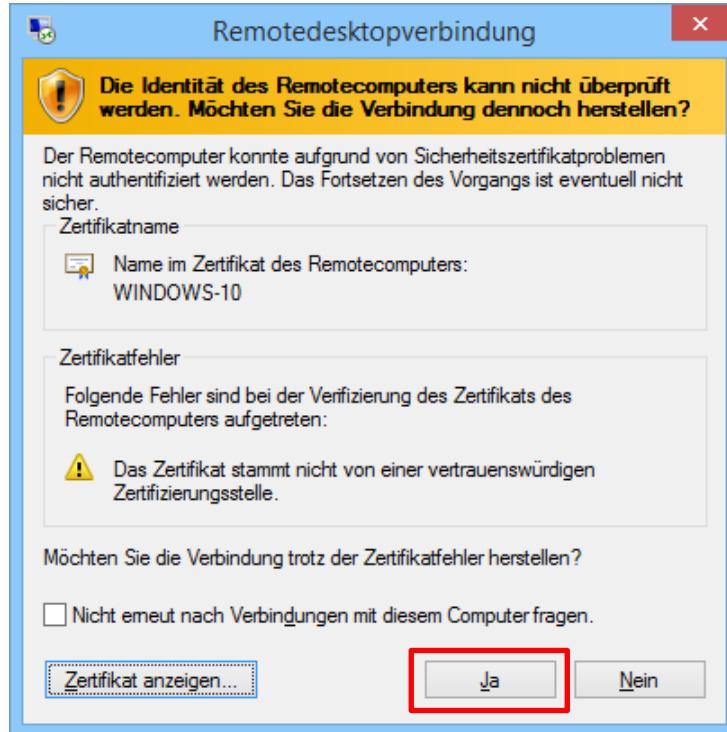
In der Registerkarte „**Anzeige**“ kann die Bildschirmauflösung für das Remote-System für die aktuelle Sitzung eingestellt werden. Unter „**Lokale Ressourcen**“ können die Audio- und Tastatureinstellungen sowie Einstellungen für lokale Geräte vorgenommen werden (Festplatte, DVD-Laufwerk etc) freigegeben werden, die während der Sitzung verwendet auf dem Remote-Rechner verwendet werden können. In der Registerkarte „**Leistung**“ können je nach Verbindungsqualität Übertragungsfeatures wie Desktophintergrund, Schriftartglättung etc. eingeschaltet werden. Ist die Verbindungsqualität eher schlecht, sollte eine Option wie „Modem“ ausprobiert werden; ist die Verbindungsqualität sehr gut, kann auch LAN ausgewählt werden.

In der Registerkarte „**Erweitert**“ kann eine Verbindung über einen Remotedesktopgateway eingerichtet werden. Wenn die entsprechenden Einstellungen am Windows-Server eingestellt wurden, wird der Server intern über die Domäneinstellungen automatisch ermittelt. Alternativ kann die IP-Adresse und die Anmeldemethode auch manuell angegeben werden.

Nachdem auf „Verbinden“ geklickt wurde kann zuerst festgelegt werden, auf welche Ressourcen der Remotecomputer zugreifen darf. Soll zum Beispiel auf dem Remotecomputer eine Software installiert werden, die sich auf einem lokalen Laufwerk befindet, sollte die entsprechende Option aktiviert sein.



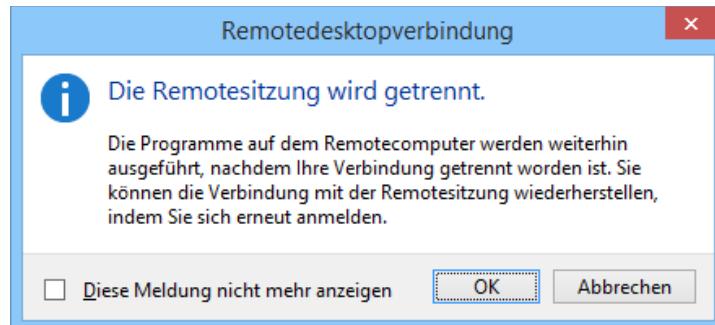
Danach erfolgt die Authentifizierung der beiden Rechner bevor eine direkte Verbindung hergestellt wird. Ist ein Sicherheitszertifikat vorhanden, wird dieses an dieser Stelle angezeigt. Ansonsten erscheint eine kurze Fehlermeldung, die mit „Ja“ bestätigt werden kann.



Die Remote-Desktopverbindung wird in einem eigenen Fenster angezeigt. Dieses kann beliebig vergrößert oder verkleinert werden oder auch in den Vollbildmodus geschaltet werden.



Die Verbindung kann jederzeit beendet werden, indem das Fenster einfach geschlossen wird.



Damit ein Fernzugriff auf den Rechner jederzeit möglich ist, muss auf dem entfernten Rechner die Einstellungen für den Energiesparmodus und für den Ruhezustand auf „Nie“ festgelegt werden, da keine Verbindung mit Rechnern hergestellt werden kann, die sich im Energiesparmodus oder im Ruhezustand befinden oder ausgeschaltet sind.

4.10.5 Häufige Fehler bei Remotedesktop-Verbindungen

Kann keine Verbindung hergestellt werden sollte zunächst systematisch – nach dem TCP/IP-Schichtmodell vorgegangen werden. Zunächst sollte die physische Verbindung auf beiden Geräten überprüft werden (sind alle Kabel angeschlossen, ist eine Netzwerkverbindung vorhanden). Danach sollte sukzessive versucht werden, den entsprechenden Rechner zu erreichen (ARP, Ping, Tracert etc.). Ist zum Beispiel ein PING möglich jedoch keine Remote-Desktopverbindung spricht das dafür, dass eine Firewall den Port 3389 blockiert oder dafür, dass die Remotedesktopverbindung nicht eingerichtet wurde.

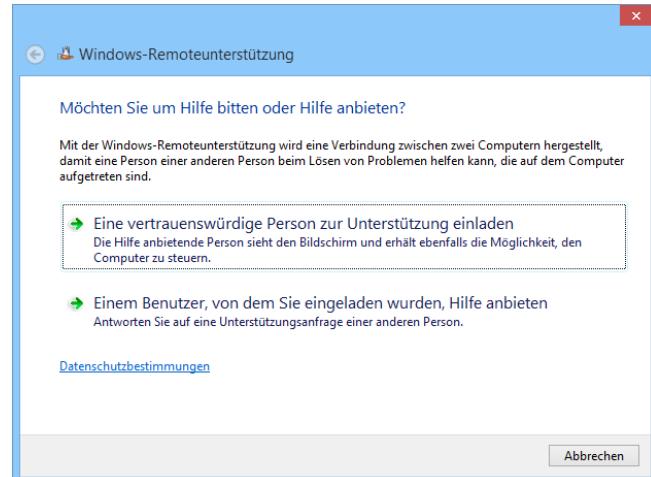
Von microsoft.com ist diese hilfreiche Anleitung entnommen:

1. Öffnen Sie die Windows-Firewall, indem Sie vom rechten Bildschirmrand nach innen streifen und auf **Suchen** tippen (zeigen Sie bei Verwendung einer Maus auf die rechte obere Bildschirmecke, bewegen Sie den Mauszeiger nach unten, und klicken Sie anschließend auf **Suchen**), den Text **Firewall** in das Suchfeld eingeben und dann auf **Windows-Firewall** tippen oder klicken.
 2. Tippen oder klicken Sie auf **Eine App oder ein Feature durch die Windows-Firewall zulassen**.
 3. Tippen oder klicken Sie auf **Einstellungen ändern**.  Sie werden ggf. zur Eingabe eines Administratorkennworts oder zur Bestätigung der Auswahl aufgefordert.
 4. Wählen Sie unter **Zugelassene Apps und Features** die Option **Remotedesktop** aus, und tippen oder klicken Sie dann auf **OK**.
-

4.10.6 Remoteunterstützung unter Windows

Über RDP ist es auch möglich einen Rechner fernzusteuern während ein anderer Benutzer angemeldet ist. Dies funktioniert über das Programm **msra.exe**, sofern auf dem zu entfernten Rechner über WINDOWS+PAUSE in den Remoteeinstellungen die Option „Remoteunterstützungsverbindungen mit diesem Computer zulassen“ aktiviert wurde.

Wird das Programm gestartet kann entweder ausgewählt werden, ob Hilfe benötigt wird und somit eine Verbindung zum aktiven PC aufgebaut werden soll. Alternativ kann einem anderen Benutzer geholfen werden und somit eine Verbindung zu einem Rechner aufgebaut werden.



Aufgabenstellung

Probieren Sie im Hörsaal das Tool mstsc.exe (Remotedesktopverbindung) im praktischen Einsatz aus. Versuchen Sie dabei die folgenden Punkte abzuarbeiten:



Aufgabe	Beschreibung
Netzwerkverbindung	Stellen Sie sicher, dass sich Ihre Computer (Laptops) im gleichen (W)LAN-Netzwerk befinden.
Windows-Version	Stellen Sie fest, ob Ihre Windows-Version die Remotedesktopverbindung unterstützt. (Tipp: WINDWOS+PAUSE zeigt die Version an!)
Wenn Ihre Windows-Version die Remotedesktopverbindung unterstützt suchen Sie sich einen Partner im Hörsaal, dessen Windows-Version die Remotedesktopverbindung unterstützt.	
IP-Adresse	Stellen Sie die IP-Adresse Ihres Laptops fest.
Benutzer anlegen	Legen Sie einen neuen Benutzer mit dem Namen „remote-winf“ an. Geben Sie diesem Benutzer keine Administrationsrechte und ein Passwort, das Sie sich notieren.
Remotedesktopverbindung aktivieren	Aktivieren Sie in den Computereinstellungen die Remotedekstopverbindung und ordnen Sie den neu angelegten Benutzer den berechtigten Benutzern zu.
Verbindung aufbauen	Starten Sie nun das Tool mstsc.exe und bauen Sie eine Verbindung zum Rechner Ihres Partners auf. Dafür benötigen Sie die IP-Adresse sowie den neu angelegten Benutzernamen und das Passwort.
Verbindung aufbauen	Was passiert am Rechner Ihres Partners, wenn Sie versuchen eine Remotedesktopverbindung aufzubauen?
Daten kopieren	Speichern Sie im Ordner „C:\Users\Public\Pictures“ ein schönes Bild Ihrer Wahl und beenden Sie danach die Verbindung. Kann Ihr Partner die Datei danach öffnen?
	Löschen Sie nun den vorhin angelegten Benutzer (ggf. von beiden Rechnern) und deaktivieren Sie die Remotedesktopverbindung in den Computereinstellungen, sofern das gewünscht ist.

--

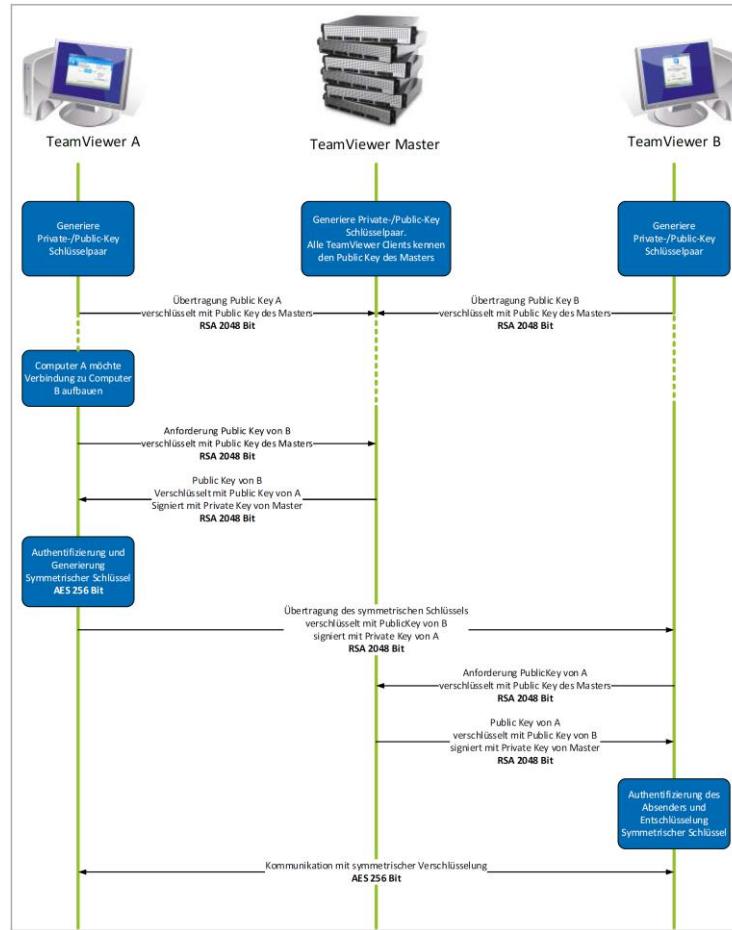
4.11 TeamViewer

TeamViewer ist ein Desktop-Sharing-Programm, das für die Fernwartung, für Webkonferenzen, Webmeetings oder auch für den Dateitransfer zwischen Rechnern. Es handelt sich dabei um ein proprietäres Protokoll, die Software muss daher erworben werden, kann jedoch in einer Freeware-Version gut eingesetzt werden. Es funktioniert in der aktuellen Version mit der IPv4 und öffnet UDP bzw. TCP-Ports.

TCP/IP-Schicht	Beispiel
Anwendungen	TeamViewer
Transport	UDP/TCP
Internet	IPv4
Netzzugang	Ethernet, Token Bus, Token Ring, FDDI

Das Besondere an TeamViewer ist, dass es vereinfacht gesprochen „an der Firewall vorbei“ arbeitet. Es werden können bei TeamViewer keine Direktverbindungen aufgebaut werden. Die Kommunikation wird über einen TeamViewer-Master-Server initialisiert und über TCP oder über http-Tunneling geleitet. TeamViewer nutzt die Ports 80 (HTTP) und 443 (HTTPS) um die Daten zu übertragen, da diese Ports in der Regel nicht von einer Firewall blockiert sind.

TeamViewer arbeitet mit einer Verschlüsselung auf Basis eines RSA Public-/Private Key-Austausches und AES (256 Bit) Sitzungsverschlüsselung. Laut Herstellerangaben ist damit ein Man-in-the-Middle-Angriff ausgeschlossen; somit kann der abgehörte Datenstrom nicht entzifert werden. Die Authentifizierung kann wie folgt dargestellt werden:



Wenn den Herstellerangaben gefolgt werden kann, dann ist TeamViewer durch seine Architektur relativ sicher und auch vor Angriffsszenarien (Brute force, Botnetze etc.) gut geschützt. Problematisch ist jedoch, dass das TeamViewer-Programm ohne Administrationsrechte auf nahezu allen Devices ausgeführt werden kann und dann mit einem Passwort die Steuerung des Computers übernommen werden kann. Das heißt, dass Mitarbeiter auf ihren Rechnern das Programm starten können um zuhause auf die Daten zuzugreifen. Wird mit dem Passwort sorglos umgegangen, dann könnte sogar jemand der nur geringfügig technisch affin ist Zugriff auf sensible Daten erhalten.

Das TeamViewer Hauptfenster besteht aus einer Optionsleiste, in der zwischen Fernsteuerung und Meeting umgeschaltet werden kann. Wird das Tab Fernsteuerung gewählt, findet man hier die Zugangsdaten um die Fernsteuerung des aktuellen Rechners zuzulassen. Dabei gibt es eine spezifische ID unter „Ihre ID“, die als Partner-ID angegeben werden muss, wenn eine Verbindung zum Rechner aufgebaut werden soll. Außerdem kann das Kennwort abgelesen werden, das ebenfalls benötigt wird, um eine Verbindung aufzubauen. Dieses Kennwort kann beliebig oft neu generiert werden.



Unter „Persönliches Kennwort“ kann ein Passwort eingetragen werden, mit dem es möglich wird, jederzeit unter Kenntnis der eigenen ID auf den Rechner zuzugreifen. Dabei wird TeamViewer als Systemdienst automatisch beim Systemstart ausgeführt und das Programm muss nicht jedes Mal neu gestartet werden.

4.11.1 TeamViewer herunterladen

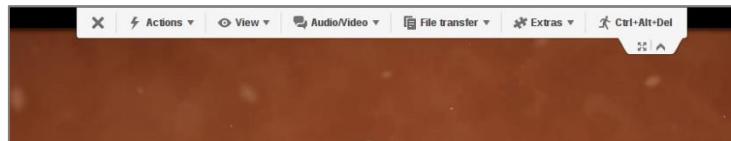
Das Programm kann sowohl für Windows, Mac, Linux oder für Mobile Systeme wie Android, iOS, Windows Phone etc. unter www.teamviewer.com heruntergeladen werden. Dabei sind die folgenden Varianten zu unterscheiden (Windows):

- **Vollversion:** Diese Version enthält alle Funktionen von TeamViewer muss jedoch installiert werden.
- **QuickSupport:** Dieses ist ein einfaches Modul, das heruntergeladen wird und ohne Installation und Administratorrechten Zugriff auf einen Rechner ermöglicht.
- **Host:** Läuft als Systemdienst im Hintergrund und ermöglicht den ständigen Zugriff auf entfernte Systeme.
- **QuickJoin:** Erlaubt ohne Installation die Teilnahme an Online-Präsentationen.

TeamViewer kann für den nicht-kommerziellen Betrieb kostenlos genutzt werden. Soll das Produkt für kommerzielle Zwecke genutzt werden, kostet es je nach Funktionsumfang zwischen € 500,- bis € 2000,- (Stand 12/2014).

4.11.2 Fernsteuerung starten

Um eine Fernsteuerung zu starten müssen sowohl die ID als auch das Passwort für den Remote-Rechner bekannt sein. Danach erfolgt die Verbindung über die Schaltfläche „Mit Partner verbinden“. Nachdem die Verbindung hergestellt wurde erscheint der Desktop des Remote-Systems, der in einem Fenster dargestellt wird. Dabei wird die folgende Menüleiste im Fernsteuerungsfenster angezeigt:



Befehl	Beschreibung	
X	Schließt die aktuelle Verbindung	
Aktionen	Richtungswechsel	Wechselt die Richtung der Fernsteuerungs-Sitzung. Der Partner kann nun Ihren Computer steuern.
	STRG+ALT+ENTF	Führt auf dem entfernten Computer den Befehl aus.
	Computer sperren	Hier kann eingestellt werden, ob der Computer sofort gesperrt wird um zum Beispiel das Benutzerkonto zu wechseln, oder ob der Computer nach dem Sitzungsende automatisch gesperrt werden soll.
	Entfernen Computer neustarten	Hier kann der aktuelle Benutzer am entfernten Rechner abgemeldet oder neu gestartet werden. Sobald der Computer neu gestartet wurde erscheint am steuernden Rechner ein Dialogfenster.
	Tastenkombinationen übertragen	Überträgt Tastenkombinationen (zB: ALT+TAB) direkt an den entfernten Computer.
	Entfernte Eingaben sperren	Sperrt die Maus- und Tastatureingaben die während einer Sitzung am entfernten Rechner ausgeführt werden. Diese können mit STRG +ALT+ENTF (am entfernten Rechner) wieder aktiviert werden.
	Anzeige am entfernten Computer deaktivieren	Schaltet den Bildschirm des entfernten Computers schwarz. Auch dieser schwarze Bildschirm kann über STRG+ALT+ENTF am entfernten Rechner wieder aufgehoben werden.
Shortcuts	Start	Öffnet den Windows 8 Startbildschirm
	App Befehle	Öffnet die Windows 8 App-Leiste
	Charms	Öffnet die Windows 8 Charms-Leiste
	Apps wechseln	Öffnet in die Windows 8 App-Übersicht
	Andocken	Dekkt die Windows Store-App am rechten Bildschirmrand an
Ansicht	Qualität	Hier kann eingestellt werden, wie detailliert die Anzeige übertragen werden soll. Die Einstellung kann hier entweder für optimale Geschwindigkeit oder für optimale Qualität adaptiert werden. In der Regel führt die

		Einstellung „Automatisch“ zu einem sehr brauchbaren Ergebnis.
	Skalieren	<p><i>Original:</i> Überträgt den Bildschirm in der auf dem entfernten Computer eingestellten Auflösung. Ist die Auflösung des entfernten Bildschirms größer als die des lokalen Bildschirms, werden Bildlaufleisten eingeblendet.</p> <p><i>Skaliert:</i> Überträgt den entfernten Bildschirm verkleinert, falls dieser eine höhere Auflösung als der lokale Bildschirm hat.</p> <p><i>Vollbild:</i> Zeigt den entfernten Bildschirm auf dem lokalen Computer in Vollbild an.</p>
	Aktiver Monitor	<p><i>Alle Monitore anzeigen:</i> Sind mehrere Monitore am entfernten Rechner angeschlossen, werden alle Monitore in nur einem Fenster angezeigt.</p> <p><i>Monitor x zeigen:</i> Zeigt einen ausgewählten Monitors des entfernten Rechners an.</p>
	Bildschirmauflösung	Ändert die Bildschirmauflösung am entfernten Computer. Je geringer die Auflösung, desto weniger Daten müssen übertragen werden und desto höher ist dann auch die Leistung/Qualität.
	Einzelnes Fenster auswählen	Hier kann nur ein einzelnes Fenster vom Bildschirm des Partners angezeigt werden.
	Aktualisieren	Erzwingt eine Bildschirmaktualisierung, falls die automatische Aktualisierung fehlschlägt.
	Bildschirmhintergrund entfernen	Blendet den Bildschirmhintergrund des entfernten Computers aus. Dadurch wird eine schnellere Verbindung ermöglicht.
	Entfernten Mauszeiger darstellen	Blendet den Mauszeiger des Partners ein oder aus. Man sieht dann, ob und wie sich der Mauszeiger am entfernten Rechner bewegt.
Audio/Video	Computersounds	Falls aktiviert, wird der Sound des entfernten Computers auf den lokalen Computer übertragen.
	Chat	Es öffnet sich ein Fenster, über das mit dem Partner gechattet werden kann.
	Videos	Öffnet ein Fenster zur Übertragung der Webcam.
	Voice over IP	Öffnet ein Fenster zur Sprachübertragung.
	Telefonkonferenz	Startet eine Telefonkonferenz mit allen Teilnehmern.
Datenübertragung	Dateiübertragung	Öffnet ein Fenster zum Austausch von Dateien zwischen den beteiligten Rechnern.
	Dateibox	Öffnet ein Fenster, mit dem Dateien für den Partner bereitgestellt werden können.
Extras	Weitere Teilnehmer einladen	Es können weitere Teilnehmer zur Fernsteuerung hinzugefügt werden.
	Ferndrucken	Ermöglicht das Drucken vom entfernten Computer aus.
	Screenshot erstellen	Macht ein Foto des Bildschirms des entfernten Computers
	Sitzungsaufzeichnung	Zeichnet die Fernsteuerung als Video auf.
	VPN	Erstellt ein virtuelles Netzwerk zwischen den verbundenen Computern.
	Remote Update	Startet die Überprüfung auf eine aktuellere Version am entfernten Computer
	Systeminformationen	Zeigt die Systeminformationen des entfernten Computers

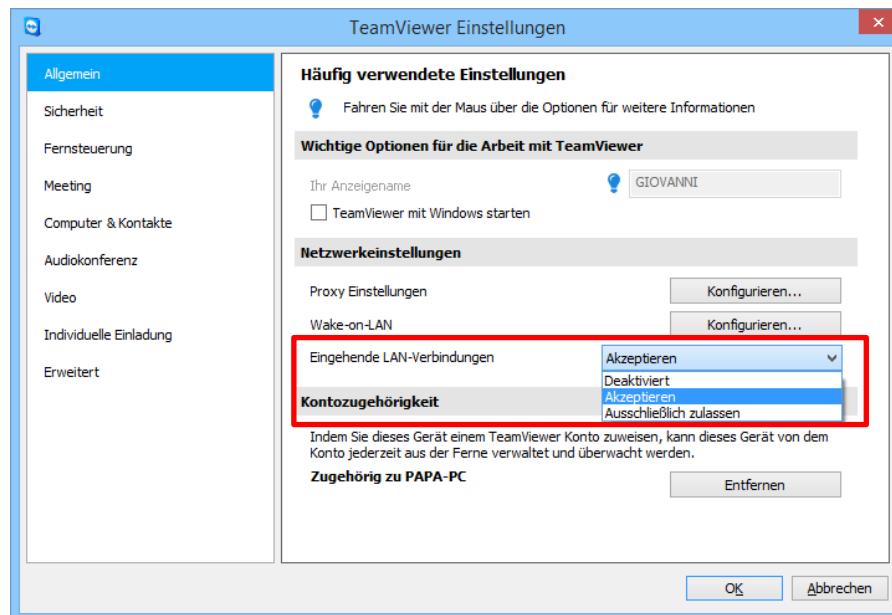
	Verbindungsinformationen	Zeigt Informationen über die aktuelle Verbindung
STRG+ALT+ENTF	Sendet die Tastenkombination STRG+ALT+ENTF an den entfernten Computer. Die Schaltfläche wird automatisch ein- oder ausgeblendet, je nachdem ob sie benötigt wird oder nicht.	

4.11.3 Verbindung über IP-Adresse

Es ist in lokalen Netzwerken auch möglich, direkt über eine IP-Adresse (oder über einen Computernamen) Verbindungen aufzubauen. Dafür muss TeamViewer jedoch so konfiguriert werden, dass eingehende Verbindungen akzeptiert werden.

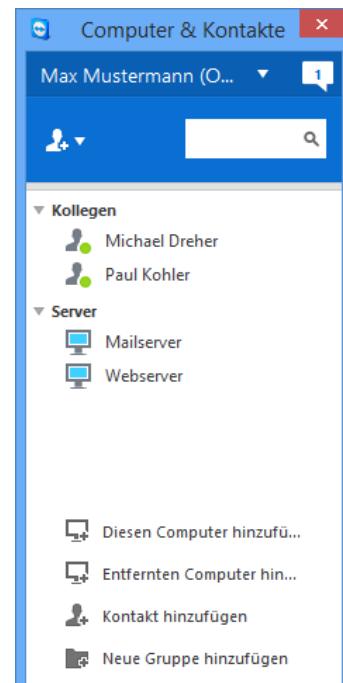
Dafür wird zunächst über das Menü Extras → Optionen in die Registerkarte Allgemein gewechselt. Hier kann nun über die Option „Eingehende LAN-Verbindung“ ausgewählt werden, ob Verbindungen über das LAN deaktiviert, akzeptiert oder überhaupt zwingend sind.

Wichtig ist, dass die Verbindung über IP-Adressen nicht mehr über den TeamViewer-Master-Server erfolgt sondern direkt zwischen den beiden Clients!



4.11.4 Computer und Kontakte

In der Vollversion von TeamViewer besteht die Möglichkeit, Computer in Gruppen zu verwalten. Dabei werden sämtliche Computer entweder nach deren Status angezeigt (Online oder Offline) oder nach eigens definierten Gruppenbezeichnungen.



Aufgabenstellung

Installieren Sie im Hörsaal auf der virtuellen Maschine (Windows) das Programm TeamViewer in der Vollversion. Bearbeiten Sie jetzt die folgenden Aufgabenstellungen:



Aufgabe	Beschreibung
Rahmenbedingungen	<p>Notieren Sie sich Ihre ID und teilen Sie diese Ihrem Nachbarn mit. Generieren Sie danach ein neues Kennwort und teilen Sie dieses ebenfalls Ihren Nachbarn mit.</p>
Fernsteuerung initiieren	<p>Stellen Sie zu Ihrem Sitznachbarn nun eine Verbindung über die TeamViewer Fernsteuerung her. Kann die Verbindung hergestellt werden? Mit welchem Benutzer sind Sie nun angemeldet? Auf welche Dateien können Sie zugreifen?</p>
Fernsteuerung durchführen	<p>Laden Sie nun über die Adresse http://tinyurl.com/winf2014-xampp die exe-Datei herunter und speichern Sie diese auf dem Rechner Ihres Partners.</p>
Pausen müssen sein	<p>Um eine kurze Pause zu machen starten Sie auf dem ferngesteuerten Rechner youtube.com und zeigen Sie Ihrem Partner ein nettes Video. Wie wird das Bild auf Ihrem PC angezeigt? Gibt es zum Beispiel Aussetzer/ruckelt es? Wie erfolgt die Ton-Wiedergabe? Kann der Partner das Video einfach pausieren?</p>
Verbindung umkehren	<p>Trennen Sie nun die Verbindung und versuchen Sie die oben angeführten Punkte nun in getauschten Partnerrollen durchzuführen.</p>

A large, empty grid consisting of 20 columns and 20 rows of small squares, intended for students to write their answers or notes.

5 Web und Server

5.1 Was ist GNU, UNIX, LINUX?

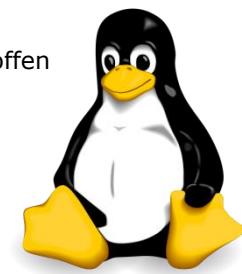
UNIX ist ein Betriebssystem, das ursprünglich von Bell Laboratories (heute AT&T) entwickelt wurde. **UNIX** an sich ist eine geschützte Marke. Der Name darf daher nur von lizenzierten Systemen getragen werden. Auf UNIX-Basis wurden mehrere Betriebssysteme entwickelt (Derivate), wie zum Beispiel Solaris (früher SUN, heute Oracle) oder Mac OS X (Apple).

Der prinzipiell geschlossene Quellcode (nicht öffentlich zugänglich = proprietäre Software) veranlasste zahlreiche Entwickler eigene UNIX-kompatible Betriebssysteme/Projekte zu entwickeln. Das populärste UNIX-Derivat (eigentlich „unixoides System“) ist **Linux**. Es wurde in seinen Grundlagen von Linus Torvalds 1991 entwickelt, mit dem Ziel, auf Intel 386er-PCs lauffähig zu sein. Dieser Betriebssystemkern wird nach wie vor weiterentwickelt und auf www.kernel.org regelmäßig in neuen Versionen veröffentlicht.

Parallel dazu arbeitete Richard Stallman an einem Projekt mit dem Namen **GNU** („GNU's Not Unix“). GNU sollte ein UNIX-kompatibles, aber unabhängiges Betriebssystem darstellen. Dieses GNU-Betriebssystem umfasste bereits zahlreiche Teile eines Betriebssystems mit Ausnahme eines Kernels. Deshalb wurde der Linux-Kernel in das System eingebaut. Der ursprünglich geplante GNU-Kernel ist bis heute nicht fertig (und wird es wohl auch nie werden). Die bekannteste GNU/Linux-Distribution ist **DEBIAN**.

Wesentlich an vielen GNU, Linux oder GNU/Linux-Software ist, dass sie meist Quelloffen ist. Nach dem ursprünglichen Streit nach der Schließung von UNIX, entwickelte Stallman die GNU General Public License. Diese besagt im Wesentlichen, dass:

- das Programm für jeden Zweck kostenfrei nutzbar ist.
- Kopien verteilt werden dürfen.
- die Arbeitsweise des Programms studiert werden kann und
- das Programm den eigenen Bedürfnissen angepasst werden darf.



Heute gibt es zahlreiche Variationen solcher Lizenzen, wie die GPLv2, die Apache Software License, 2.0 (Apache 2.0) unter der zB: auch das Projekt „Android“ vertrieben wird oder die LGPL. Während die GNU GPL besagen würde, dass ein gesamtes Software-Projekt wieder als GNU-GPL (kostenfrei!) veröffentlicht werden muss, wenn auch nur ein Teil eingebaut wurde, der unter der GNU-GPL lizenziert ist, sieht die LGPL (Lesser General Public License) vor, dass nur jener Teil, der unter GNU-GPL in das neu entwickelte Projekt aufgenommen wurde, wieder als GNU-GPL veröffentlicht werden muss. Heute gibt es zahllose Open Source-Lizenzen, die unter anderem von den Mitgliedern der OSI (Open Source Initiative; www.opensource.org) beratend mitentwickelt werden (können).

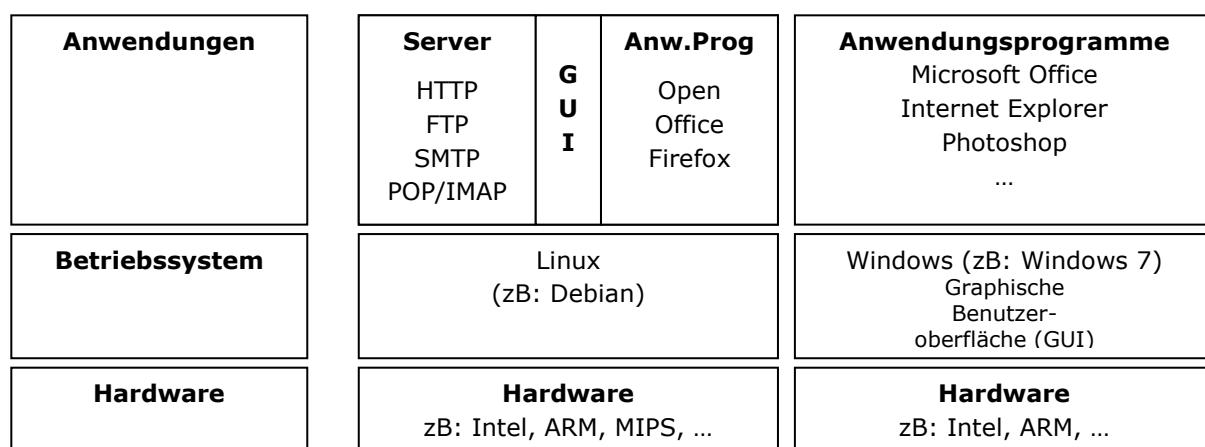
Bekannte Linux-Distributionen

Linux-Distributionen (also Betriebssysteme, die auf dem Linux-Kernel basieren) können meist kostenlos aus dem Netz geladen werden. Sehr populäre Linux-Distributionen sind:

Debian	www.debian.org	<i>Serverbetrieb</i>
Ubuntu	www.ubuntu.com	<i>Heimanwender</i>
	Chromium OS	<i>Von Google speziell für WebBrowsing</i>
	xUbuntu	<i>Speziell für XBOX von Microsoft</i>
Gentoo	www.gentoo.org	<i>Fortgeschrittene Linux-Benutzer</i>
Fedora	www.fedoraproject.org	<i>Nur vollständig frei lizenzierte Software ist installiert</i>
	Red Flag	<i>von asiatischen Staaten entwickelt</i>
SUSE	www.suse.de	<i>Kostenpflichtig</i>
	openSUSE	<i>Kostenfreie Alternative zu SUSE</i>

Architektur von Linux-Systemen

Im Gegensatz zu Windows ist Linux als Multitasking-System konzipiert. D.h. es können mehrere Benutzer gleichzeitig auf einer Maschine arbeiten. Deshalb eignen sich Linux-Systeme auch hervorragend als Server-Systeme. Während Windows-Systeme vorwiegend für Anwender/innen ausgelegt sind und eine grafische Benutzeroberfläche fix im System implementiert haben (GUI = Graphical User Interface) ist dies einer der zentralen Schwachpunkte von Linux. Für den täglichen Betrieb gibt es zwar kostenlose verfügbare Anwendungsprogramme, für viele Einstellungsoptionen muss jedoch auf Ebene der Kommandozeile gearbeitet werden. Das ist der Hauptgrund, warum sich Linux nach wie vor nicht im relevanten Ausmaß im Desktop-Bereich etablieren konnte, obwohl mit Derivaten wie zum Beispiel Ubuntu bereits einige gute Alternativen bestehen. Die Grundarchitektur kann wie folgt dargestellt werden:



Linux kann, im Gegensatz zu Windows, auf zahlreichen Hardware-Architekturen installiert werden. So zum Beispiel auf klassischen Intel x386-Systemen (32/64-bit), ARM-Plattformen, MIPS-Plattformen oder PowerPC (früher Apple, jetzt vor allem Spielkonsole wie Wii, Xbox, Playstation). Somit kann Linux prinzipiell sowohl auf einem Mobiltelefon als auch auf einem Hochleistungsrechner (Supercomputer) installiert werden. Auf Supercomputern (zB: zur Simulation von Kernwaffentests, Seismologie, Erdbebenvorhersage, Meteorologie, Finanzwirtschaft etc.) wird heute vorwiegend Linux als Betriebssystem eingesetzt.

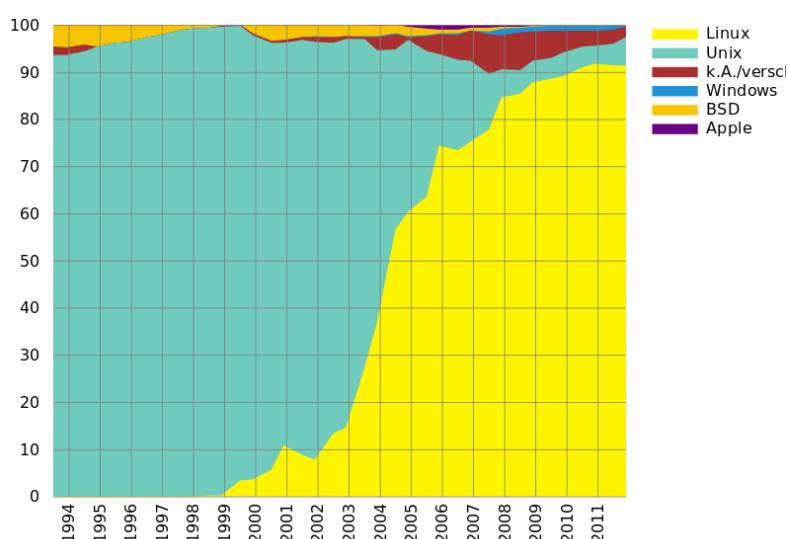


Abbildung 5-1: Betriebssysteme auf den TOP 500-Supercomputern in % (Quelle: wikipedia.org)

Auch auf Smartphones hat Linux zzt. eine marktbeherrschende Stellung. Auf ca. 75 % aller verkauften Smartphones läuft zzt. Android (Linux) bzw. auch iOS (ein UNIX-Derivat von Apple).

Linux installieren

Zunächst muss eine beliebige Installations-CD von einem der Linux-Anbieter heruntergeladen werden. Das sind meistens ISO-Dateien. ISO-Dateien sind virtuelle CD-ROMs, die auf eine physikalische CD/DVD gespielt werden können oder mit einem Programm (zB: VMWare) als virtuelles CD-ROM-Laufwerk eingebunden werden können. Debian kann zum Beispiel von der folgenden Seite kostenfrei bezogen werden: <http://www.debian.org/distrib/netinst>

Hier muss jedoch zuerst ausgewählt werden, auf welchem System das Betriebssystem (OS=Operating System) installiert werden muss. Eine Debian-ISO für i386 (klassische Intel-Desktop-Architektur) kann nicht auf Mobiltelefonen (meist ARMEL) installiert werden usw.

Kleine CDs

Im folgenden werden Image-Dateien mit einer Größe von bis zu 180 MB aufgeführt, die dazu geeignet sind, auf kleine CD-R(W)-Medien mit 80 mm/3.1" Durchmesser geschrieben zu werden. Wählen Sie unten Ihre Hardware-Architektur aus.



[amd64, armel, kfreebsd-i386, kfreebsd-amd64, i386, ia64,](#)

[mips, mipsel, powerpc, sparc,](#)



Kleinere CDs

Im folgenden werden Image-Dateien mit einer Größe von bis zu 40 MB aufgeführt, die dazu geeignet sind, auf CDs im Visitenkarten-Formfaktor zu schreiben (die in verschiedenen Größen verfügbar sind, z.B. mit Durchmesser 58x75 mm/2.3x3"):



[amd64, armel, kfreebsd-i386, kfreebsd-amd64, i386, ia64,](#)

[mips, mipsel, powerpc, sparc,](#)

Speichern Sie diese Datei nun auf der Festplatte, einem USB-Stick usgl. Je nachdem, welche Variante Sie gewählt haben, kann die Größe der ISO-Datei variieren. Es empfiehlt sich, zunächst eine kleine ISO-Datei herunterzuladen, da Debian recht einfach die weiteren Daten direkt aus dem Netz „nachlädt“.

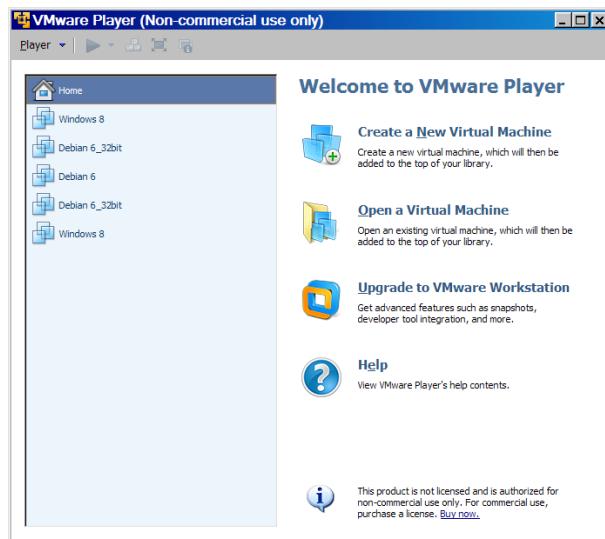


- Wenn Sie die Datei nun auf einem Rechner installieren möchten, müssen Sie die Datei nun auf eine DVD oder CD schreiben. Dafür verwenden Sie am besten ein klassisches Programm, das auf Ihrem PC installiert ist. Möchten Sie hingegen von einem USB-Stick aus installieren, entpacken Sie die Dateien (zB: mit WinZIP oder WinRAR) auf einen USB-Stick. Achtung: Der PC, auf dem das OS installiert werden soll, muss das Booten von USB-Sticks jedoch unterstützen.
- Soll Debian auf einem Virtuellen PC installiert werden, müssen Sie diesen zuerst einrichten und dann das CD-Image als virtuelles CD-Laufwerk einbinden.

Exkurs: Neuen virtuellen PC einrichten

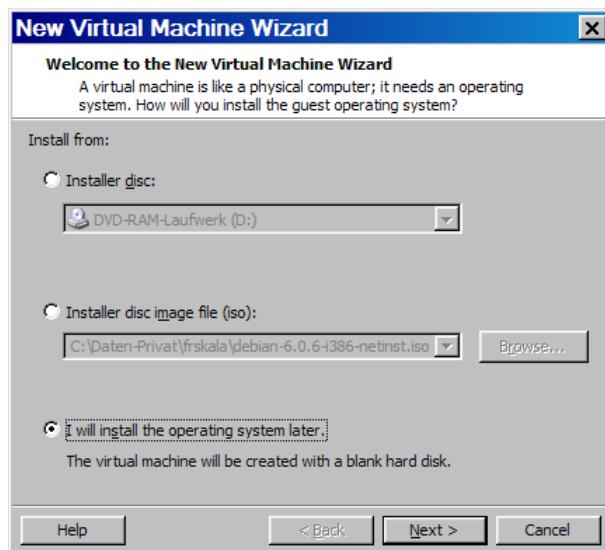
Für die Erstellung virtueller PCs gibt es im Netz eine Vielzahl von Programmen, die tw. kostenpflichtig oder auch kostenlos bezogen werden können. Als sehr verbreitet gelten die Virtualisierungslösungen von VMware. Den VMware-Player können Sie kostenlos aus dem Netz laden: http://www.vmware.com/de/products/desktop_virtualization/player/overview.html

Nachdem Sie den VMware-Player installiert haben, öffnen Sie diesen einfach:

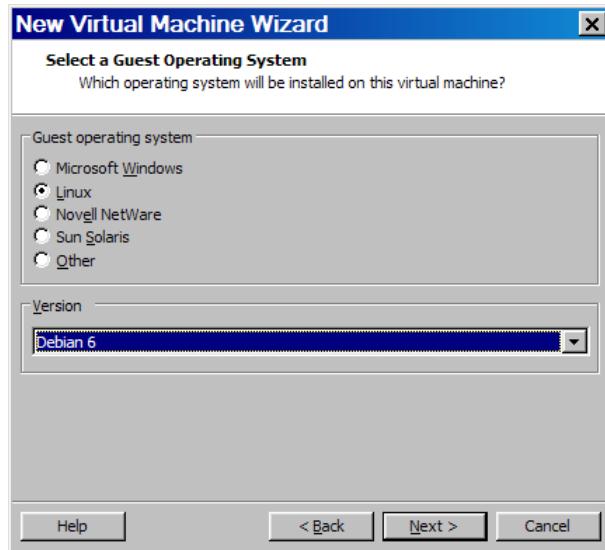


Neue virtuelle Maschine erstellen

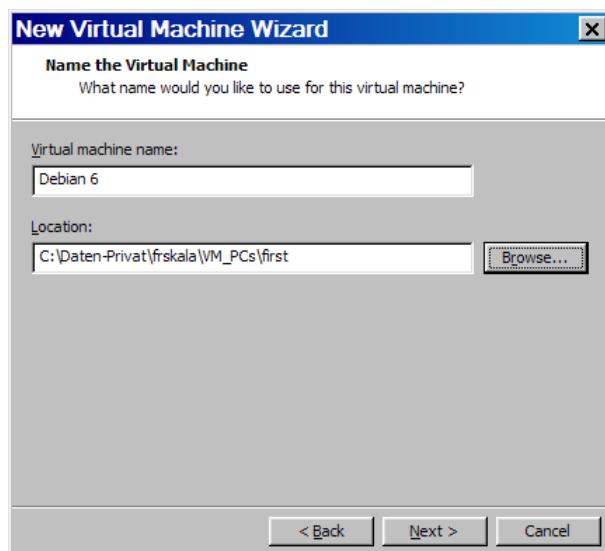
Klicken Sie nun auf die Schaltfläche **Create a New Virtual Machine**. Im anschließenden Dialogfeld wählen Sie die Option **I will install the operating system later** aus und bestätigen mit **Next >**



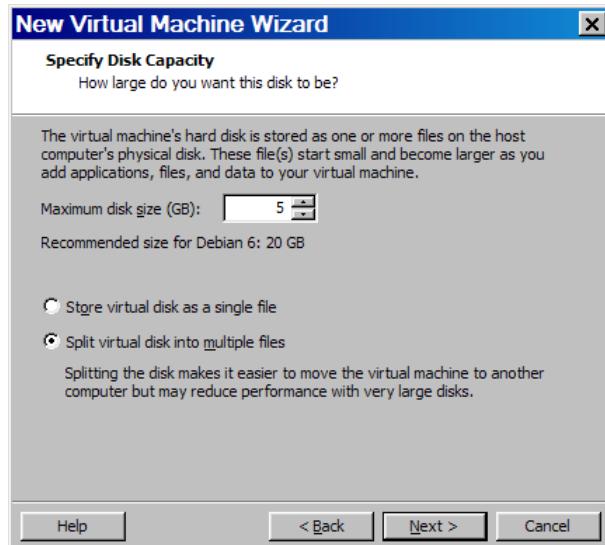
Nun wählen Sie aus, welches Betriebssystem Sie gerne auf der virtuellen Maschine installieren wollen. Diese Funktion sollte richtig ausgewählt werden, damit der VMware-Player richtig mit dem installierten System umgehen kann und es stabiler läuft. Bei einer falschen Auswahl kann es unter Umständen zu Stabilitätsproblemen kommen. Wählen Sie also **Linux** und anschließend als Version **Debian 6** und bestätigen mit **Next >**



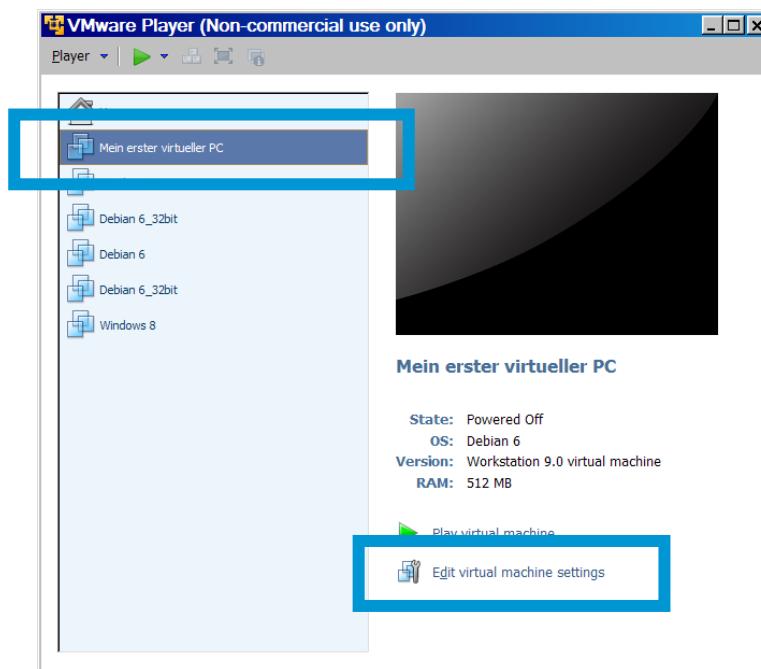
Nun geben Sie einen Namen für Ihre virtuelle Maschine ein (hier **Mein_erster_virtueller_PC**) und unter **Location**, wo die virtuelle Maschine auf der physischen Festplatte gespeichert werden soll. Sie könnten hier auch einen USB-Stick oder ein Netzlaufwerk auswählen. Danach bestätigen Sie wieder mit **Next >**



Jetzt geben Sie an, wie groß die virtuelle Festplatte sein soll, mit der Ihr neuer virtueller PC ausgestattet werden soll. Hier sollten für eine Debian-Testinstallation 5 GB reichen. Wenn Sie genügend Speicherplatz auf Ihrer Festplatte haben (intern oder extern, es ginge auch ein USB-Stick), können Sie hier auch eine größere Festplatte einstellen. Die virtuelle Festplatte können Sie ganz einfach entfernen, wenn Sie die virtuelle Maschine wieder löschen. Um die Dateien später besser verschieben zu können, sollten Sie außerdem die Option **Split virtual disk into multiple files** wählen. Bestätigen Sie anschließend mit **Next >**



Erstellen Sie Ihren virtuellen PC nun mit einem Klick auf die Schaltfläche **Finish**. Er scheint nun im Startbildschirm Ihres VMware-Players auf. Klicken Sie zunächst auf die Schaltfläche **Edit virtual machine settings** um weitere Einstellungen vorzunehmen.



Hier können weitere Einstellungen vorgenommen werden, die die Funktionalitäten Ihrer virtuellen Maschine beeinflussen können. Unter:

- **Memory** können Sie einstellen, wie viel Ihres physischen Arbeitsspeichers für die virtuelle Maschine reserviert sein sollte. Geben Sie hier niemals mehr als die Hälfte (absolutes Maximum) Ihres physischen Arbeitsspeichers frei.
- **Processors** geben Sie an, auf wie viele Kerne Ihres Prozessors die virtuelle Maschine zugreifen darf.
- **Hard Disk** können Sie die Größe Ihrer virtuellen Festplatte verändern.
- **CD/DVD** können Sie der virtuellen Maschine entweder erlauben, direkt das **physical drive** Ihres Rechners zu verwenden oder eine ISO-Datei als Laufwerk zu verwenden. Klicken Sie hier auf **Use ISO image file** und wählen Sie dort die ISO-Datei, die sie von der Seite debian.org heruntergeladen haben.
- **Network Adapter** stellen Sie sicher, dass die Optionen **Connect at power on** und **NAT: Used to share the host's IP address** aktiviert sind.

Bestätigen Sie Ihre Eingaben nun mit einem Klick auf **OK** und starten Sie Ihre Maschine auf der Startseite des VMWare-Players mit einem Klick auf **Play virtual machine!**

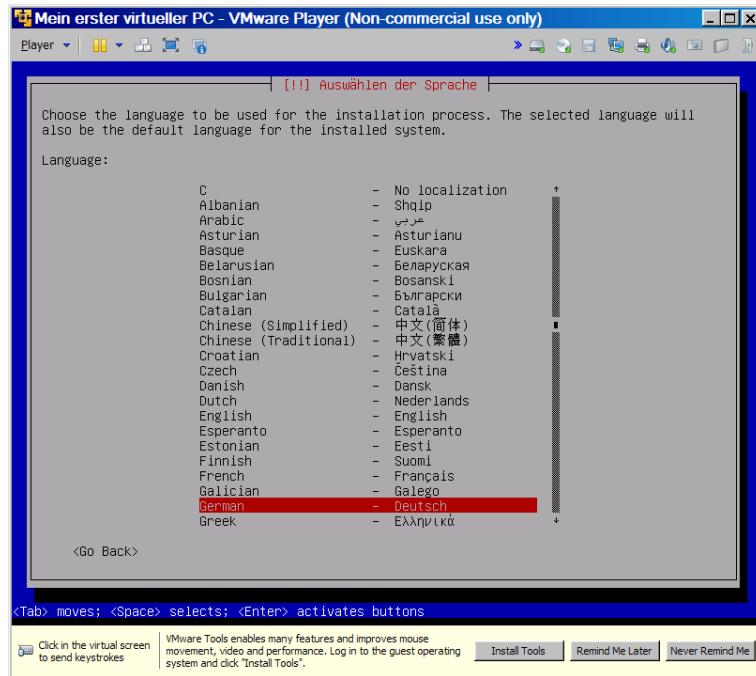
Hinweis: Es kommen jetzt mehrere Hinweismeldungen. Klicken Sie hier, wenn verfügbar, immer die Checkbox **Do not show this hint again** an und bestätigen Sie mit einem Klick auf **OK**. Auch etwaige Meldungen nach Software Updates blenden sie mit einem Klick auf **Remind Me Later** aus. Es wird nun der Installations-Screen von Debian angezeigt!

Wichtiger Hinweis: Der virtuelle PC „benutzt“ sowohl Ihre Tastatur, als auch Ihre Maus. Da Ihre Maus nicht zwei Betriebssysteme gleichzeitig bedienen kann, wird diese vom VMWare-Player „gecatched“. Sie können daher mit der Maus nicht mehr aus dem Fenster des virtuellen PCs hinaus navigieren. Damit die virtuelle Maschine Ihre Maus wieder freigibt, müssen Sie auf der Tastatur die Tasten STRG+ALT gleichzeitig drücken.

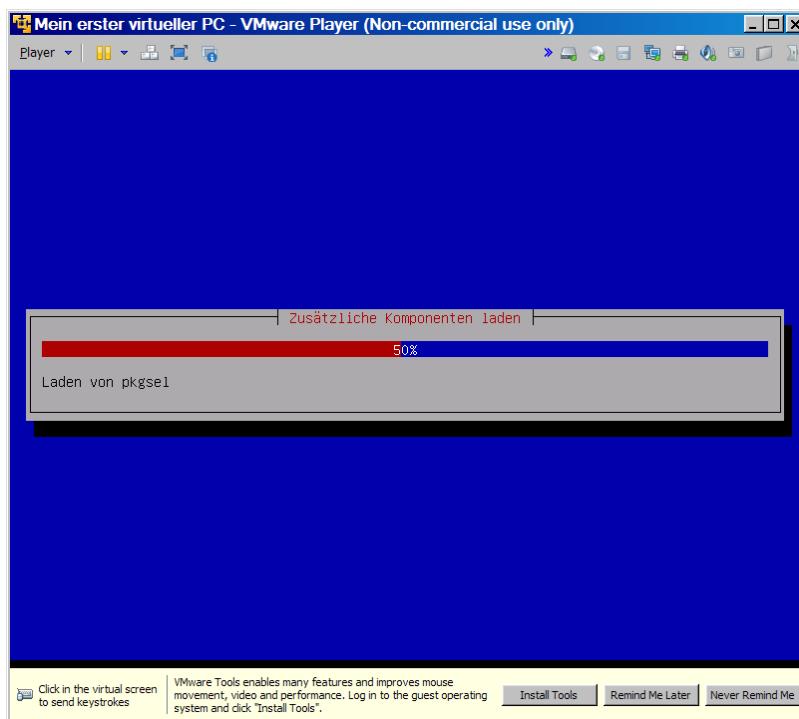
5.2 Debian installieren



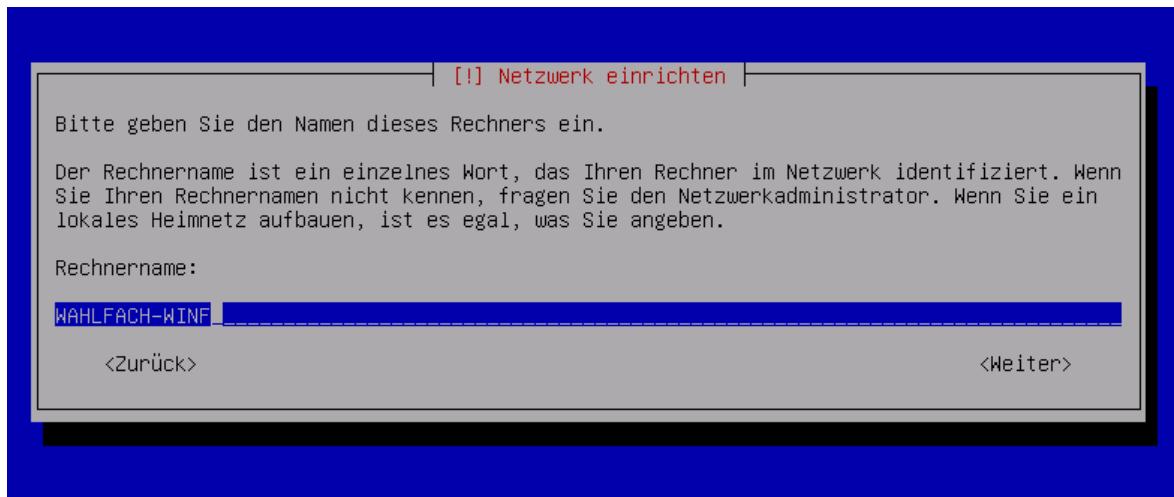
Bestätigen Sie die ausgewählte Option **Install** nun mit ENTER. Sie werden nun aufgefordert, die Installationssprache zu wählen. Navigieren Sie hier mit den Tasten PFEIL-HINAUF oder PFEIL-HINUNTER durch die Auswahl bis zur gewünschten Sprache und bestätigen dann mit ENTER.



Verfahren Sie bei den Angaben **Auswahl des Standorts** und **Tastaturbelegung auswählen** analog zur Sprachauswahl! Haben Sie die notwendigen Angaben eingegeben, lädt die Debian-Installation die notwendigen Dateien.

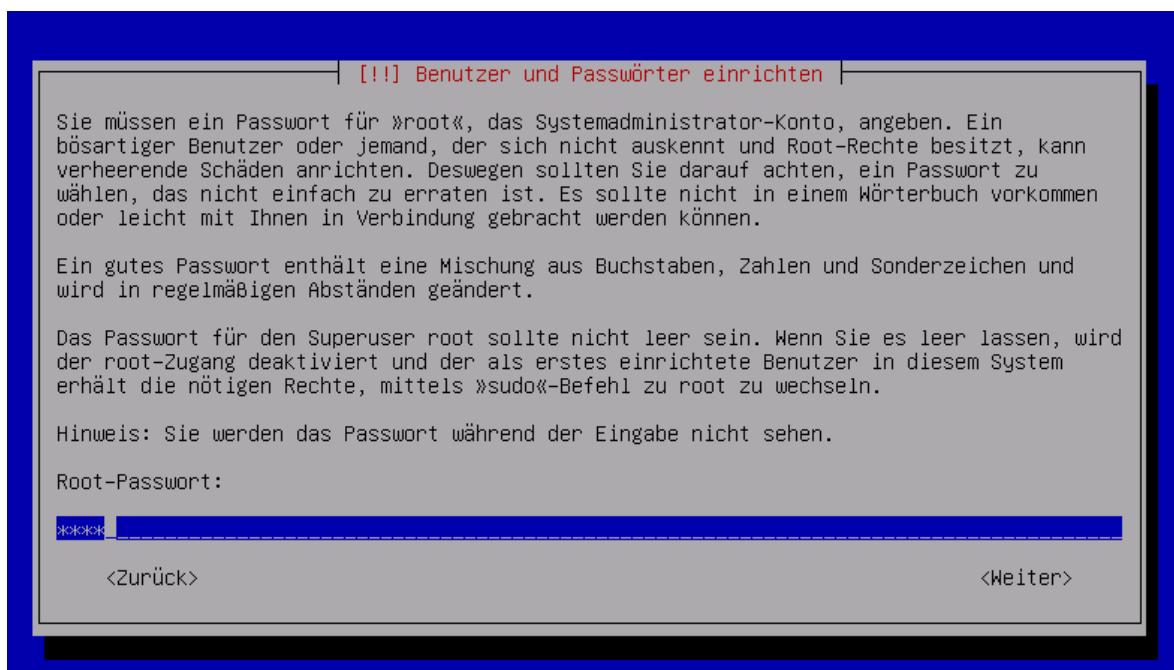


Nach einer kurzen Zeit werden Sie aufgefordert, Ihrem Rechner einen Namen zu geben. Geben Sie hier einen Rechnernamen ein und bestätigen mit ENTER.



Als Domain-Name lassen Sie den Standard-Namen **localdomain** einfach ausgewählt und bestätigen mit ENTER. Nachfolgend müssen Sie ein Administrator-Passwort eingeben. Der Administrator-Benutzername ist auf Linux-Systemen stets **root**. Geben Sie hier ein sicheres Passwort ein und merken Sie es sich. Sichere Passwörter sind eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen und haben mindestens acht Zeichen.

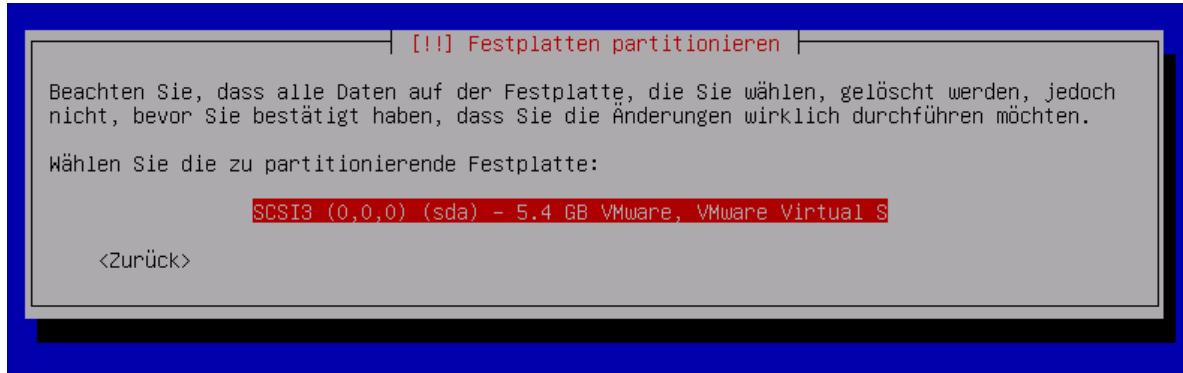
ACHTUNG: Im Gegensatz zu Windows sind UNIX/Linux-Systeme Case-Sensitive. Dh. es wird zwischen Groß- und Kleinschreibung explizit unterschieden!



Nachdem Sie Ihr Passwort zweimal eingegeben haben, geben Sie nun Ihren vollständigen Namen ein und bestätigen wieder mit Enter. Nachfolgend können Sie einen Benutzer für sich erstellen. Geben Sie als Benutzername hier Ihren Nachnamen (beachten Sie die Groß- und Kleinschreibung) und anschließend wieder zweimal Ihr Passwort ein.

Nun müssen Sie Ihre Festplatte partitionieren. Das ist sinnvoll, wenn Sie mehrere Betriebssysteme parallel installieren möchten. Auf diesen Punkt soll an dieser Stelle nicht näher eingegangen werden. Wählen Sie hier den Punkt **Geführt – vollständige Festplatte verwenden** aus und bestätigen Sie mit ENTER.

Auf der virtuellen Maschine ist nur eine Festplatte eingerichtet. Sollen Sie die Installation auf einem Rechner durchführen, der über mehrere Festplatten verfügt, müssen Sie die zu partitionierende Festplatte erst auswählen. Bestätigen Sie wieder mit ENTER.



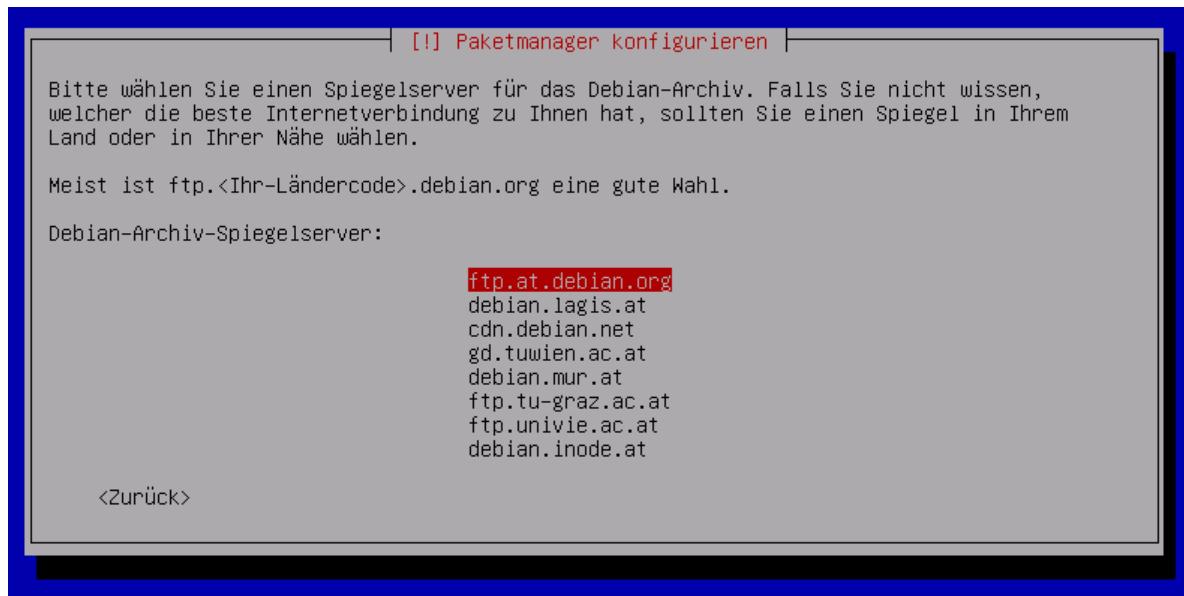
Die Debian-Installation schlägt Ihnen nun mehrere Partitionierungsoptionen vor. Wählen Sie hier am besten zunächst die Option **Alle Dateien auf eine Partition, für Anfänger empfohlen** aus und bestätigen wieder mit ENTER.

Debian zeigt nun an, dass auf Ihrer Festplatte zwei Partitionen eingerichtet werden. Eine primäre Partition, auf der das Betriebssystem eingerichtet wird und Sie später Ihre Dateien speichern werden und eine zweite, wesentlich kleinere SWAP-Partition. Diese ist, umgangssprachlich gesprochen, eine Art Auslagerungsdatei für temporäre Daten. Bestätigen Sie diese Angaben mit der Auswahl von **Partitionierung beenden und Änderungen übernehmen** und ENTER. Da die Partitionierung von Festplatten irreversibel ist, müssen Sie die Sicherheitsabfrage noch einmal bestätigen. Achtung: Hier ist der Punkt **Nein** vorab ausgewählt. Sie müssen daher die Auswahl mit der PFEIL-LINKS-Taste auf **Ja** setzen und dann mit ENTER bestätigen.

Danach wird das Grundsystem installiert...



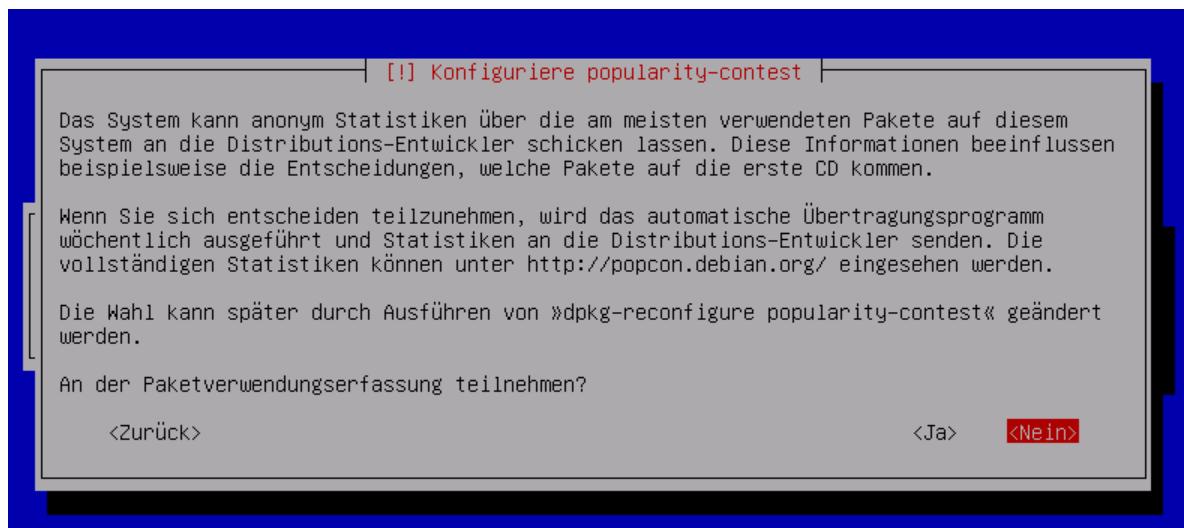
Wie bereits erwähnt gibt es in Debian die Möglichkeit, erst während der Installation weitere Daten direkt aus dem Internet nachzuladen. Dafür müssen Sie zunächst einen Debian-Archiv-Spiegelserver wählen. Es sollte hier ein Server ausgewählt werden, der Ihrem Standort am nächsten ist. Wählen Sie also zunächst zB: **Österreich**.



In Österreich gibt es 8 Debian-Spiegelserver. Einer davon zB: an der TU Wien, ein anderer an der TU Graz und noch einer an der Universität Wien. Wählen Sie hier einen der Server aus (zB: gd.tuwien.ac.at) und bestätigen Sie mit ENTER. Die folgende Eingabemaske (http-Proxy-Daten) können Sie leer mit ENTER bestätigen, es sei denn, sie verwenden einen Proxy-Server (was Sie in der Regel wissen sollten). Es werden nun einige wesentliche Daten vom Spiegelserver (hier ftp.at.debian.org) geladen:

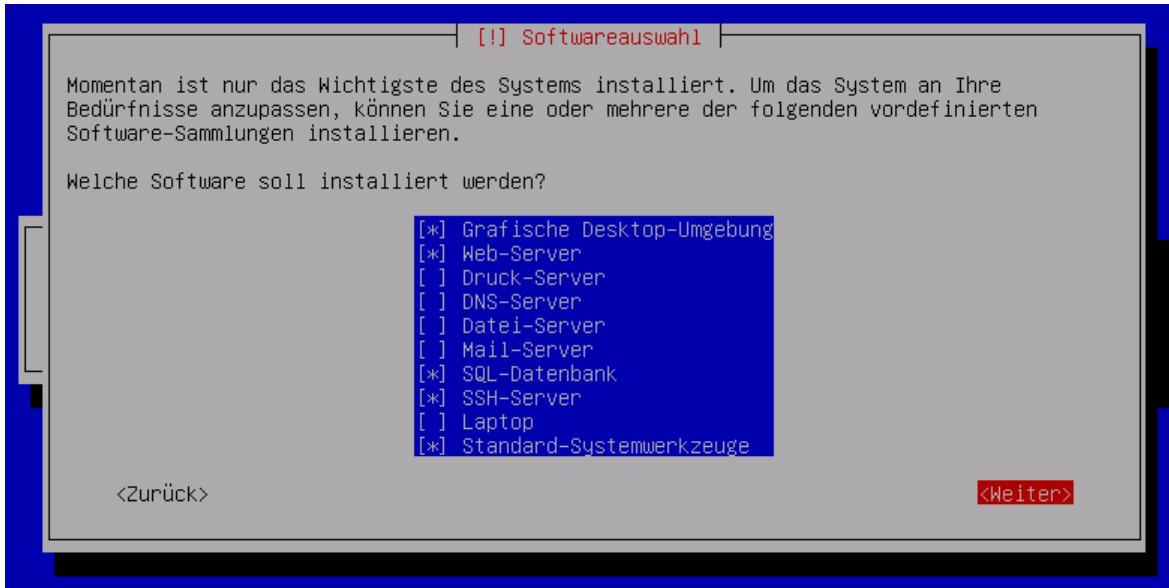


Die Installation des Kernsystems kann schon mal 10-30 Minuten dauern! Nachdem die Installation des Grundsystems abgeschlossen wurde, werden Sie gefragt, ob Sie am Programm der Paketverwendungserfassung (eine Art Feedback-System für die Entwickler) teilnehmen wollen. Diesen Punkt können Sie mit **Nein** und ENTER überspringen.



Nach der Installation des Grundsystems können Sie nun auswählen, welche Standardsoftware installiert werden soll. Keine Angst, Sie können später sehr einfach weitere Software nachträglich installieren, wenn Sie diese benötigen. Sie können die einzelnen Punkte mit den PFEIL-HINAUF und PFEIL-HINUNTER-Tasten durchgehen und mit der Leertaste (SPACE) markieren oder demarkieren.

Stellen Sie jedenfalls sicher, dass Sie den SSH-Server installieren, um remote auf Ihre Installation zugreifen zu können. Weiters können Sie einen Web-Server installieren und eine SQL-Datenbank. Wenn Sie wollen, können Sie auch noch eine GUI (Graphical User Interface) installieren. Das ist jedoch nicht zwingend erforderlich! Auf die Option **Weiter** gelangen Sie, wenn Sie einmal die TABULATOR-Taste drücken. Bestätigen Sie Ihre Eingaben dann mit ENTER.

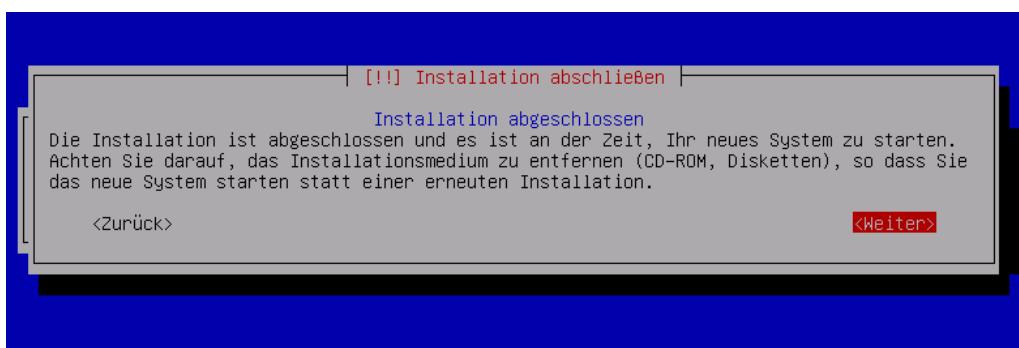


Je nachdem, welche Software Sie zur Installation auswählen, können unterschiedliche Eingabemeldungen erscheinen. Weiters kann die Dauer der Installation unter anderem von Ihrer Software-Auswahl variieren. Sie hängt im Wesentlichen ab von:

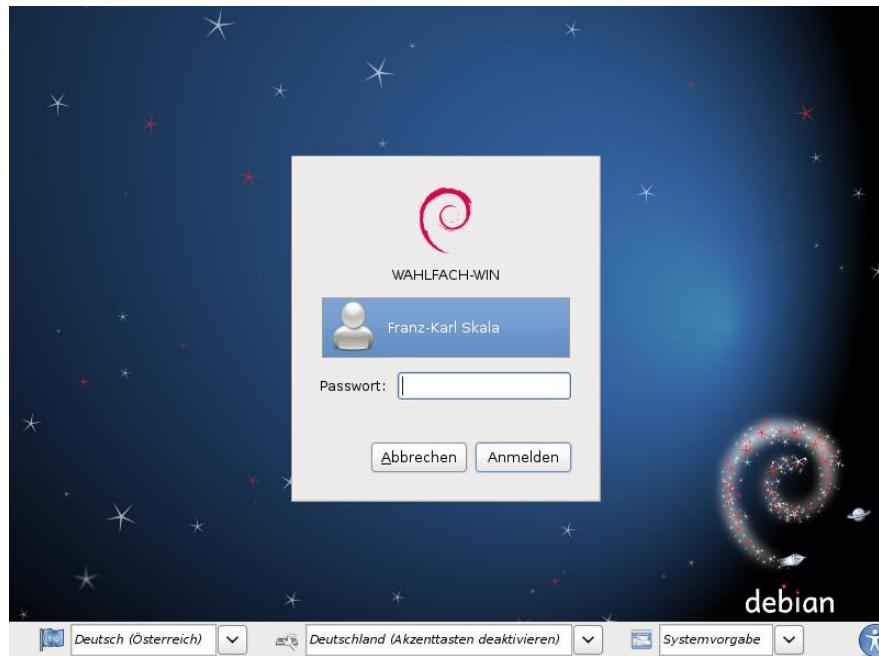
- der Anzahl der ausgewählten Software-Pakete
- der Geschwindigkeit Ihres Internet-Anschlusses
- der Geschwindigkeit des Spiegelservers
- der Leistungsfähigkeit Ihres Rechners

Abschließend werden Sie gefragt, ob Sie den GRUB-Bootloader installieren wollen. Dieser erlaubt es, mehrere Betriebssysteme auf einem System anzusteuern. Wenn nur ein Betriebssystem installiert werden soll, können Sie den Bootloader direkt in den Master Boot Record (MBR) der Festplatte installieren. Bestätigen Sie daher mit **Ja**.

Nun ist die Installation abgeschlossen. Das System muss nun neu gestartet werden. Bestätigen Sie abschließend einfach mit **Weiter** um das System neu zu starten.

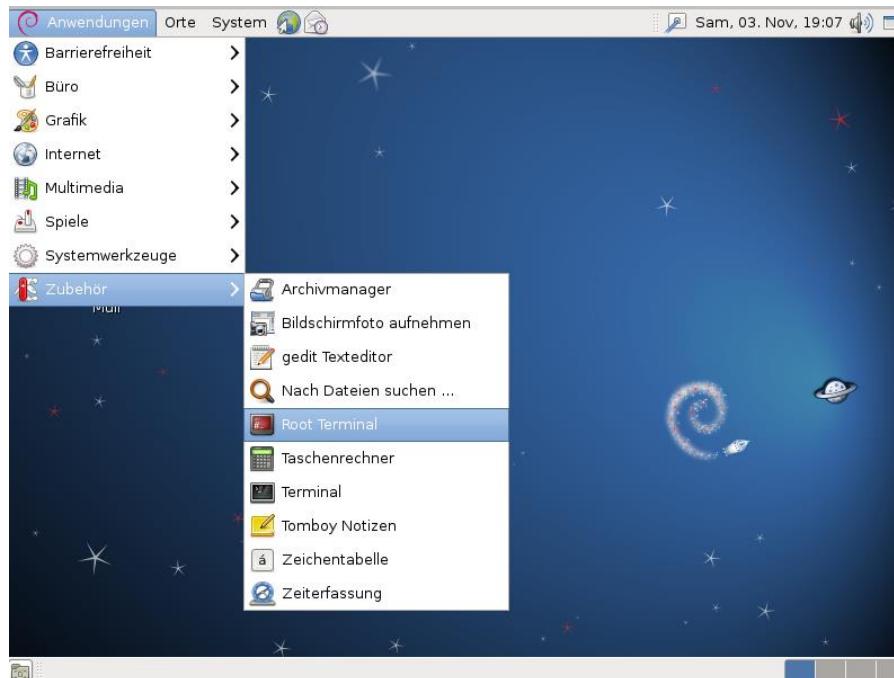


Nachdem das System neu gestartet wurde, können Sie sich über die graphische Oberfläche (GUI; Software=GNOME) mit Ihrem Benutzernamen und Passwort, das Sie während der Installation angegeben haben, am System anmelden, sofern Sie eine GUI-Installation beim Setup ausgewählt haben.

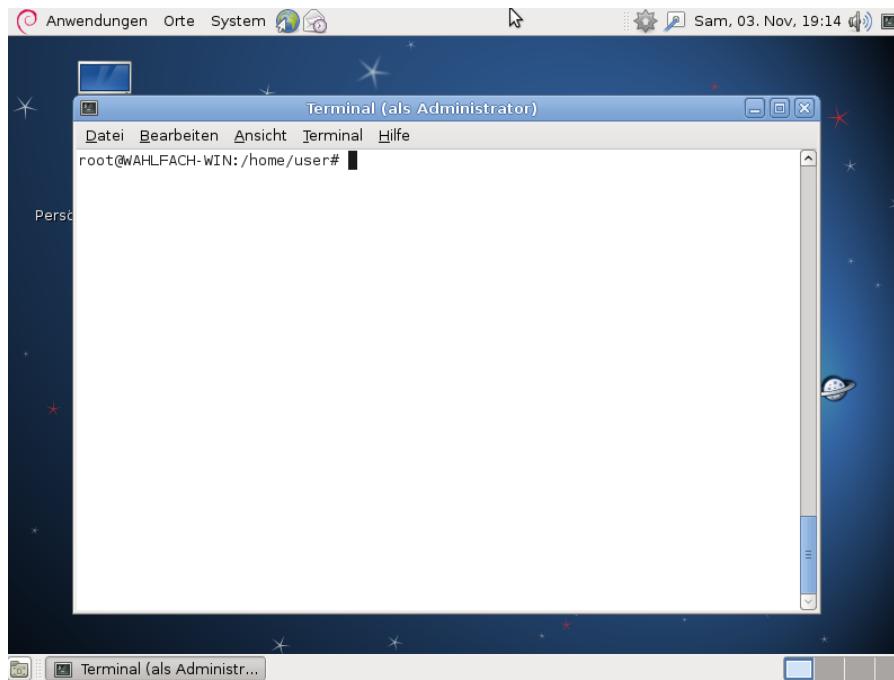


Sie befinden sich nun auf der graphischen Desktop-Umgebung (GUI) Ihrer neuen Debian-Installation. Links oben ist eine Art Startmenü eingeblendet, in dem die wichtigsten Anwendungsprogramme aufgeführt sind. Diese können Sie sich in einer ruhigen Minute durchsehen. Zunächst wird aber erst einmal mit den Shell-Befehlen gearbeitet.

Diese können Sie eingeben, wenn Sie den Root-Terminal (alternativ den normalen Terminal) öffnen. Diesen finden Sie unter **Anwendungen → Zubehör → Root Terminal**



Der Terminal ist der eigentliche Kern des Systems. Die graphische Oberfläche ist ja im Wesentlichen bei Linux-Systemen lediglich eine Anwendung, die das System benutzerfreundlicher macht. Um Linux grundlegend zu verstehen, sollten die wesentlichsten Begriffe auf der Shell-Ebene (Kommandozeile) erlernt werden.



Die Zeile **root@WAHLFACH-WIN:** gibt an, dass der derzeit aktive Benutzer **root** (Administrator) auf dem Rechner mit dem Namen **WAHLFACH-WIN** angemeldet ist. **/home/user** bedeutet, dass gerade dieses Verzeichnis ausgewählt ist. Die Raute (#) markiert immer das Ende dieser grundlegenden Information und bezeichnet damit den Beginn einer neuen Eingabezeile.

5.3 Arbeiten mit Linux

5.3.1 Shell-Befehle

Navigieren durch die Ordnerstruktur

Das Hauptverzeichnis auf Linux-Systemen ist das Root-Verzeichnis. Ähnlich dem **C:**-Laufwerk auf Windows-Systemen. Das Root-Verzeichnis wird jedoch nicht mit **C:** angesprochen sondern mit **/**.

Mit dem Befehl **cd** (change directory) können Sie in ein anderes Verzeichnis wechseln. Um zum Beispiel in das Verzeichnis **/var/www** zu wechseln, geben Sie einfach **cd /var/www** ein.

```
user@rechner:/# cd /var/www
user@rechner:/var/www#
```

Verwalten von Software

Software installieren Sie unter Debian am besten direkt über den Debian-Spiegelserver, den Sie bei der Installation angegeben haben. Hierfür wechseln Sie zunächst in den Shell-Modus und verwalten dann mit dem Schlüsselwort **aptitude** Ihre Software.

Um eine Software zu installieren, tippen Sie einfach den Befehl

```
$ aptitude install name_des_pakets
```

ein.

Um Software wieder zu deinstallieren, geben Sie einfach

```
user@rechner:/# aptitude remove name_des_pakets
```

ein.

Beispiele:

<code>aptitude install openoffice.org</code>	Installiert Open Office
<code>aptitude install apache</code>	Installiert den Apache2-Webserver
<code>aptitude install mysql-server</code>	Installiert den MYSQL-Datenbank-Server
<code>aptitude install php</code>	Installiert die Scriptsprache PHP

Eine Auflistung aller frei verfügbarer Software für Debian finden Sie unter
<http://packages.debian.org/stable/>

System beenden oder neu starten

Das System beenden Sie mit dem Befehl **shutdown**:

```
user@rechner:/# shutdown
```

Wenn Sie das System neu starten möchten, geben Sie den **reboot**-Befehl ein

```
user@rechner:/# reboot
```

Festplatten-Belegung anzeigen

Die aktuelle Belegung der Festplatte lässt sich mit dem Programm **df** anzeigen. Eine schone, übersichtliche Anzeige erhalten Sie mit dem Befehl **df -h**

```
user@rechner:/# df -h
```

```
Filesystem      Size  Used Avail Use% Eingehängt auf
/dev/sda1       4,7G  3,3G  1,2G  74% /
tmpfs          252M    0  252M  0% /lib/init/rw
udev           247M  212K  247M  1% /dev
tmpfs          252M    0  252M  0% /dev/shm
root@WAHLFACH-WIN: #
```

IP anzeigen

Die aktuelle Netzwerkkonfiguration kann mit dem Befehl **ifconfig** angezeigt werden. Die Netzwerkkarte (sofern nur eine installiert) wird als **eth0** bezeichnet.

```

eth0      Link encap:Ethernet  Hardware Adresse 00:0c:29:c9:a4:f4
          inet  Adresse:192.168.216.132  Bcast:192.168.216.255  Maske:255.255.255
          inet6-Adresse: fe80::20c:29ff:fe9:a4f4/64  Gültigkeitsbereich:Verbunden
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metrik:1
          RX packets:4977 errors:0 dropped:0 overruns:0 frame:0
          TX packets:815 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:1000
          RX bytes:1948826 (1.8 MiB)  TX bytes:64334 (62.8 KiB)
          Interrupt:19 Basisadresse:0x2000

```

Dateien erstellen und bearbeiten

Neue Dateien können mit dem Befehl **touch** erstellt werden. Dem **touch**-Befehl folgt der Name der neuen Datei. Danach folgen eine Leerzeile und der Pfad zu dem Ordner, wo die neue Datei erstellt werden soll. Der folgende Befehl erstellt die Datei `winf.info` im Verzeichnis **/home/user/skala**

```
user@rechner:/# touch winf.info /home/user/skala
```

Dateien bearbeiten

Dateien können mit jedem beliebigen Texteditor bearbeitet werden. Ein sehr weit verbreiteter ist NANO, der auf fast jedem Linux-System standardmäßig installiert ist. Wenn zum Beispiel die Datei `/var/www/index.html` bearbeitet werden soll, muss **nano /var/www/index.html** eingegeben werden.

```
user@rechner:/# nano /var/www/index.html
```

In NANO kann aber leider lediglich mit den Pfeiltasten durch den Text navigiert werden. Dennoch lassen sich Textdateien so gut bearbeiten. Nachdem die Änderungen vorgenommen wurden, muss man die Datei mit der Tastenkombination STRG+X beenden. Beim anschließenden Speichern hat man die Option **y** (ja, Änderungen speichern) und **n** (nein, Änderungen verwerfen).



Dateien löschen

Dateien werden mit dem Befehl **unlink** gelöscht. Gefolgt vom Namen der Datei. Das folgende Beispiel löscht die Datei `winf.info` im Ordner `/home/skala`

```
user@rechner:/# unlink /home/skala/winf.info
```

Ordner verwalten

Ordner erstellen

Ordner werden mit dem Befehl **mkdir** erstellt. Gefolgt vom Pfad des Ordners. Das folgende Beispiel erstellt den Ordner /var/www/skala

```
user@rechner:/# mkdir /var/www/skala
```

Ordner löschen

Ordner werden mit dem Befehl **rmdir** gelöscht. Gefolgt vom Pfad des Ordners. Das folgende Beispiel löscht den Ordner /var/www/skala

```
user@rechner:/# rmdir /var/www/skala
```

Dateien/Ordner anzeigen

Eine Übersicht aller Dateien und Ordner kann mit dem Befehl **ls** dargestellt werden. Um zB: alle Dateien und Unterordner des Pfades /var/www anzuzeigen, muss der Befehl **ls /var/www** eingegeben werden.

```
user@rechner:/# ls /var/www
```

Dateien/Ordner suchen und finden

Dateien oder Ordner können mit dem Programm **find** gesucht und hoffentlich gefunden werden. Sucht man nach einem bestimmten Dateinamen, zum Beispiel nach der Datei index.html, muss man einfach den folgenden Befehl eingeben:

```
user@rechner:/# find -name "index.html"
```

Benutzer verwalten

Benutzer werden auf Linux-Systemen einer oder mehreren Gruppen zugeordnet. Es gibt eine Vielzahl von Gruppen unter Linux. Jede Gruppe hat spezifische Berechtigungen. Zum Beispiel, um auf das CD-ROM-Laufwerk zuzugreifen, Dateien auf dem Webserver laden zu können, Bluetooth verwenden zu können usw.

Gruppenmitgliedschaften anzeigen

Der Befehl **id -Gn** gefolgt von dem Benutzernamen listet alle Gruppen auf, denen der Benutzer zugeordnet ist.

```
user@rechner:/# id -Gn benutzername
```

```
root@WAHLFACH-WIN:/# id -G -n user
user cdrom floppy audio dip www-data video plugdev netdev bluetooth scanner
root@WAHLFACH-WIN:/#
```

In diesem Beispiel ist der Benutzer user auf dem Rechner WAHLFACH-WINF den Gruppen user, cdrom, floppy, audio, dip, www-data, video, plugdev, netdev, bluetooth und scanner zugeordnet. Jeder Benutzer hat außerdem ein eigenes Home-Verzeichnis, das unter /home/benutzername zu finden ist.

Benutzer anlegen

Benutzer können ganz einfach mit dem Befehl **adduser** angelegt werden. Diesem Befehl muss der Name des neuen Benutzers folgen. Das folgende Beispiel würde den Benutzer skala anlegen:

```
user@rechner:/# adduser skala
```

Nachdem der Befehl ausgeführt wurde, muss zweimal das Passwort für diesen Benutzer eingetragen werden. Danach können Sie den vollständigen Namen des Benutzers, eine Raumnummer, Telefonnummern und Sonstiges eintragen. Diese Angaben sind jedoch nicht obligatorisch. Zum Abschluss werden Sie gefragt, ob die Informationen korrekt sind. Tippen Sie jetzt **j** gefolgt von ENTER ein, um den neuen Benutzer anzulegen. Wenn ein neuer Benutzer angelegt wird, wird auch automatisch eine gleichnamige Gruppe für diesen Benutzer angelegt!

Benutzer Gruppen zuordnen

Auch das Zuordnen von Benutzern zu Gruppen erfolgt mit dem Befehl **adduser**. Sie tragen einfach zunächst den Befehl, gefolgt vom Benutzernamen und dem Namen der Gruppe ein und bestätigen mit ENTER. Das folgende Beispiel fügt den Benutzer skala der Gruppe www-data hinzu.

```
user@rechner:/# adduser skala www-data
```

```
root@WAHLFACH-WIN:/# adduser skala www-data
Füge Benutzer »skala« der Gruppe »www-data« hinzu ...
Benutzer skala wird zur Gruppe www-data hinzugefügt.
Fertig.
root@WAHLFACH-WIN:/#
```

Zugriffsrechte verwalten

Zugriffsrechte unter Linux für Dateien und Verzeichnisse sind aufgrund der Gruppenstruktur für Laien leider sehr kompliziert zu setzen. Prinzipiell können Zugriffsrechte mit dem chmod-Befehl gesetzt werden. Wichtig ist, dass Lese-, Schreib- und Ausführrechte vergeben werden können. Und zwar sowohl für den Eigentümer, die primäre Gruppe und für alle anderen. Dh, das Leserecht kann drei Mal vergeben werden, ebenso wie das Ausführ- und das Schreibrecht.

Zugriffsrechte anzeigen

Die Zugriffsrechte eines Ordners oder einer Datei kann man sich am besten mit dem Befehl ls –l anzeigen lassen. Wenn Sie sich die Rechte einer Datei ansehen möchten, müssen Sie zuerst mit dem Befehl cd in den entsprechenden Ordner wechseln und dann den Dateinamen eingeben. Der folgende Befehl gibt die Zugriffsrechte für die Datei winf.info im Verzeichnis /home/skala aus:

```
user@rechner:/home/skala# ls -l winf.info
```

```
-rw-r--r-- 1 root root 0 4.Nov 10:57 winf.info
```

Das Ergebnis ist wie folgt zu lesen:

-rw-r--r--	Das sind die gesetzten Zugriffsrechte
1	Die ID des Besitzers der Datei
root	Der Name des Besitzers der Datei
root	Die Gruppe des Besitzers der Datei

Die Datei winf.info gehört also dem Benutzer root, der die ID 1 hat.

Besitz ändern

Um den Besitzer einer Datei zu ändern, benötigen Sie den chown-Befehl. Der folgende Befehl ändert den Besitzer der Datei /home/skala/winf.info auf den Benutzer skala und die Gruppe ebenfalls auf skala. Jetzt dürfen nur noch der Benutzer selbst und alle der Gruppe skala zugeordneten Benutzer auf diese Datei zugreifen:

```
user@rechner:/home/skala# chown skala.skala winf.info
```

Der Befehl ls -l winf.info würde nun die folgenden Rechte ausgeben:

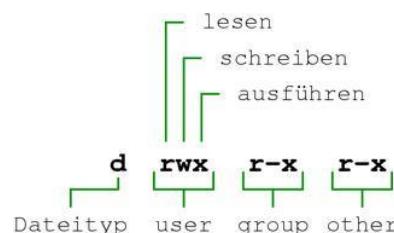
```
-rw-r--r-- 1 skala skala 0 4.Nov 10:57 winf.info
```

Möchten Sie nur den Besitzer-User und nicht die Gruppe ändern, lassen Sie einfach den Punkt gefolgt vom Gruppennamen weg. Das folgende Beispiel ändert nur den Besitzer der Datei winf.info im Verzeichnis /home/skala auf skala und lässt die Gruppenzugehörigkeit unberührt:

```
user@rechner:/home/skala# chown skala winf.info
```

Zugriffsrechte einfach erklärt

Die Zugriffsrechte sind stets zehnstellig und besteht aus einem Bindestrich (-), Leserechte (r), Schreibrechte (w) und Ausführrechte (x). Diese Rechte können sowohl für den Besitzer (u), eine Gruppe (g) oder für Andere (o) gesetzt werden.



- Möchte man, dass nur der Besitzer Zugriff auf eine Datei oder einen Ordner hat, muss man die Rechte auf Folgendes ändern: **-rwx-----**
- Sollen auch der Gruppe Leserechte eingeräumt werden, benötigt man **-rwxr-----**
- Sollen dem Benutzer alle Rechte, der Gruppe Lese- und Ausführrechte und allen anderen nur Leserechte eingeräumt werden, müssen die Zugriffsrechte auf **-rwxr--r--** gesetzt werden.

Im folgenden Beispiel soll nur der Eigentümer (skala) alle Rechte (rwx) und alle anderen (other) nur Leserechte für die Datei /home/skala/winf.info haben. Dafür verwendet man am einfachsten nacheinander die folgenden Befehle:

```
user@rechner:/home/skala# chmod u=rwx winf.info
user@rechner:/home/skala# chmod g=--- winf.info
```

```
user@rechner:/home/skala# chmod o=r-- winf.info
```

```
root@WAHLFACH-WIN:/home/skala# chmod u=rwx winf.info
root@WAHLFACH-WIN:/home/skala# chmod g=--- winf.info
root@WAHLFACH-WIN:/home/skala# chmod o=r-- winf.info
root@WAHLFACH-WIN:/home/skala# ls -l winf.info
-rwx---r-- 1 skala skala 0 4. Nov 10:57 winf.info
```

Chmod rekursiv setzen

Oft ist es sinnvoll, die Zugriffsrechte für einen Ordner inklusive aller Unterordner und Dateien auf einmal zu setzen. Man spricht hier von Rekursivität. Dafür hängen Sie einfach nach der Rechtezuweisung noch ein **-R** vor dem Ordner- oder Dateinamen an. Das nachfolgende Beispiel setzt alle Unterordner und Dateien im Verzeichnis /var/www für den Besitzer auf aktive Lese-, Schreib- und Ausführrechte.

```
user@rechner:/home/skala# chmod u=rwx -R /var/www
```

Benutzer löschen

Benutzer können ganz einfach mit dem Befehl **deluser** gelöscht werden. Der folgende Befehl würde den Benutzer skala löschen. Achtung: das Home-Verzeichnis des Benutzers /home/skala wird dabei nicht gelöscht! Dieses muss der Administrator eigenhändig entfernen!

```
user@rechner:/ # deluser skala
```

Automatisiertes Ausführen von Befehlen

Mit Cronjobs können auf Linux-Systemen Shell-Befehle zu vorgegebenen Uhrzeiten automatisch ausgeführt werden. Es könnte zum Beispiel eingegeben werden, dass der Befehl **reboot** jeden Sonntag um 3:00 in der Früh durchgeführt wird, oder dass ein bestimmtes PHP-Script alle 5 Minuten aufgerufen wird. Verwaltet werden Cronjobs mit dem Programm **crontab**.

Zum Grundverständnis

Es muss dezidiert angegeben werden, zu welchen Minuten, Stunden, Tagen, Monaten oder Wochentagen bestimmte Befehle ausgeführt werden. Ein Asterisk (*) fungiert hier als Wildcard und überspringt eine bestimmte Angabe. Folgende Einstellungen müssen gesetzt werden:

Minute	Stunde	Tag	Monat	Wochentag	Beschreibung
0	0	*	*	*	Es wird täglich um 0:00 etwas ausgeführt
0	3	*	*	0	Es wird jeden Sonntag (0) um 3:00 etwas ausgeführt
*/5	*	*	*	*	Es wird alle fünf Minuten etwas ausgeführt
*	*/1	*	*	*	Es wird jede Stunde etwas ausgeführt
30	12	1-15	*	*	Es wird an den ersten 15 Tagen eines Monats um 12:30 etwas ausgeführt
45	6	*	12	6	Es wird jeden Samstag im Dezember um 6:45 etwas ausgeführt

Cron-Einträge erstellen

Um eine neue Automatisierung hinzuzufügen, muss zunächst das Programm **crontab** im Bearbeitungsmodus aufgerufen werden:

```
user@rechner:/ # crontab -e
```

Es öffnet sich nun ein Editor (NANO) in dem einige Informationen stehen. Diese Informationen sind Kommentare. Das erkennen Sie daran, dass eine Raute (#) zu Beginn einer Zeile steht. Diese Informationen können Sie mit der ENTF-Taste löschen.

```
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
```

Wir könnten nun angeben, dass unser System an jedem Sonntag um 4:00 in der Früh neu gestartet werden soll. Das wäre dann die Zeile: **0 4 * * 0 reboot**

Sie können diese Datei nun einfach mit STRG+X beenden und werden gefragt, ob Sie speichern möchten. Bestätigen Sie hier einfach mit **j** und ENTER.

Cron-Einträge anzeigen

Um die Cron-Einträge anzuzeigen, benötigen Sie einfach den Befehl **crontab -l**. Es werden dann alle aktiven Cron-Einträge aufgelistet.

```
user@rechner:/ # crontab -l
```

Das folgende Beispiel zeigt, dass zwei Cronjobs existieren. Einerseits wird das System jeden Sonntag um 4:00 in der Früh neu gestartet. Andererseits wird alle 5 Minuten ein

Sicherungsprogramm mit dem Namen sicherung.php im Ordner /var/www/automatisierung aufgerufen. Die Bezeichnung >/dev/null gibt hier an, dass jeder sichtbare Output dieser Datei einfach ignoriert bzw. verworfen wird.

```
root@WAHLFACH-WIN:/home/user# crontab -l
0 4 * * 0 reboot
*/5 * * * * /var/www/automatisierung/sicherung.php >/dev/null
```

5.3.2 Übersicht wichtiger Bash-Befehle

Die folgenden Befehle können Sie ganz einfach in der Kommandozeile Ihres Linux-Systems ausführen. Diese Übersicht ist der hilfreichen Liste von palita.net gekürzt entnommen!

Hilfe / Info

Befehl	Beschreibung
man echo	Handbuchseite (manpage) über das Programm "echo" aufrufen Standardmäßig wird das " less " zum Anzeigen benutzt: navigieren mit Pfeiltasten, beenden mit q.
which echo	kompletten Pfad des Programms echo ausgeben
whereis echo	kompletten Pfad zum Programm, zu seinen Konfigurationsdateien und zu seiner Handbuchseite ausgeben
whatis echo	kurze Funktionsbeschreibung zu echo
time whereis echo	whereis echo ausführen und Zeit ausgeben, die das Programm benötigt hat
man --help	Bei den meisten Programmen wird mit dem Parameter --help bzw. -h eine kurze Hilfe mit Syntax ausgegeben

Navigation

Befehl	Beschreibung
cd /home/	zum Pfad /home/ wechseln (change directory)
pwd	aktueller Arbeitsverzeichnis ausgeben (print working directory)
cd	zum Heimatverzeichnis (Standardmäßig /home/benutzername/) wechseln
cd -	zum letzten Verzeichnis wechseln
cd ..	Eine Verzeichniseben hinauf wechseln
ls	Verzeichnisinhalt vom aktuellen Verzeichnis ausgeben ls /home/ gibt den Inhalt von /home/ aus
ls -l	Verzeichnisinhalt vom aktuellen Verzeichnis als Liste mit Dateiinformationen ausgeben. Weitere Optionen für ls -A auch versteckte Dateien anzeigen (mit -a auch . und .. anzeigen) -h Dateigrößen in lesbare Werte umrechnen (kByte, MByte, ...) --color=auto ausgabe Farbig darstellen -S sortieren nach Größe -t sortieren nach Zeit -X sortieren nach Dateiendung -r Sortierung umkehren (reverse) ls -SArh --color=auto einige der hier aufgeführten kombiniert: nach Größe, alle Dateien, Sortierung umkehren, lesbare Größen, Liste
pushd .	aktuellen Pfad zwischenspeichern
popd	zum zwischengespeicherten Pfad wechseln

Dateioperationen

Befehl	Beschreibung
cp datei dateikopie	datei nach dateikopie kopieren Beispiel cp -rv * /ziel/ Alle (*) Dateien, Ordner und Unterordner vom aktuellen Verzeichnis rekursiv (-r) nach /ziel/ kopieren, Status ausgeben (-v)
mv datei /ziel/	verschiebt datei in den Ordner ziel Umbenennen mv datei.txt neuename.txt datei in neuename umbenennen
ln -s original.txt link.txt	erstellt eine Verknüpfung auf den relativen Pfad original.txt mit dem Namen link.txt Wichtig: Wird die Verknüpfung verschoben, wird das Ziel unter dem Relativen Pfad wahrscheinlich nicht mehr gefunden. ln -s /pfad/zu/original.txt link.txt erstellt die Verknüpfung mit absolutem Pfad
mkdir verzeichnis	erstellt den Ordner verzeichnis im aktuellen Pfad mkdir -p /home/benutzer/backup/2013/01 erstellt den Ordner 01 und alle nicht existierenden Ordner darüber
rm datei	datei löschen rm -r ordner/ ordner/ mit gesamtem Inhalt löschen
touch leer.txt	erstellt die Datei leer.txt ohne Inhalt
nano leer.txt	Öffnet die Datei leer.txt im Texteditor nano

Umleitungen (Pipes)

Befehl	Beschreibung
ls -l > liste.txt	Ausgabe von ls nicht ausgeben, sondern in die Datei liste.txt schreiben Wichtig: ist liste.txt nicht vorhanden, wird sie erstellt; ist sie vorhanden, wird der Inhalt überschrieben!
> liste.txt	Inhalt von liste.txt leeren
ls -l less	Ausgabe von ls -l wird an less umgeleitet (= Pipe) Weitere Pipe-Beispiele ls -1A grep jpg Verzeichnisinhalt auflisten, nur Elemente, die jpg enthalten ausgeben ls -1A grep jpg grep -v foto wie voriges, jedoch Elemente, die foto enthalten nicht ausgeben du -s * sort -nr less Größe aller Dateien / Ordner im aktuellen Pfad nach Größe sortiert in less anzeigen

Dateibetrachtung

Befehl	Beschreibung
cat datei.txt	Inhalt von datei.txt ausgeben
more datei.txt	Datei Seitenweise ausgeben, Navigieren mit Pfeiltasten, Leertaste für nächste Seite.
less datei.txt	wie more, jedoch mehr Funktionen (siehe manpage: <code>man less</code>). q zum beenden
nano datei.txt	öffnet datei.txt in nano, ein einfaches Textbearbeitungsprogramm (Strg + X zum Beenden)
vi datei.txt	öffnet datei.txt in vi, ein sehr umfangreiches Textbearbeitungsprogramm (Esc :q! ENTER zum Beenden)

<code>sort datei.txt</code>	gibt datei.txt zeilenweise sortiert aus
-----------------------------	--

Suchen

Befehl	Beschreibung
<code>locate winf</code>	sucht nach Dateien / Ordner mit winf im Dateinamen
<code>find -iname winf</code>	sucht nach Dateien & Ordnern im aktuellen Verzeichnis (und darunter) mit winf im Namen, ignoriere Groß- / Kleinschreibung.
<code>find -type f ! -iname '*.jpg'</code>	sucht nach Dateien, die nicht mit .jpg enden
<code>grep "winf" * --color</code>	sucht zeilenweise nach dem Vorkommen des Wortes winf in jeder Datei im aktuellen Verzeichnis mit farbiger Hervorhebung des Treffers 1.1.1.1 Optionen -i ignoriert Groß- / Kleinschreibung (insensitive) -C 2 gibt jeweils 2 Zeilen vor und nach dem Vorkommen aus -B 2 -A 4 gibt 2 Zeilen davor und 4 Zeilen nach dem Vorkommen aus -n fügt Zeilennummern an -v gibt nur Zeilen aus, die das Ergebnis nicht enthalten
<code>vi datei.txt</code>	öffnet datei.txt in vi, ein sehr umfangreiches Textbearbeitungsprogramm (Esc :q! ENTER zum Beenden)
<code>sort datei.txt</code>	gibt datei.txt sortiert aus

Datenanalyse, Speicher & Prozesse

Befehl	Beschreibung
<code>wc -l datei.txt</code>	Anzahl der Zeilen von datei.txt ausgeben. 1.1.1.2 Zählweisen -l Zeilen zählen -w Wörter zählen -m Buchstaben zählen
<code>lsattr</code>	Dateiattribute anzeigen
<code>diff datei1 datei2</code>	Unterschiede zwischen zwei Dateien anzeigen
<code>df -h</code>	Festplattenspeicher Analysieren (-h = human readable / In größtmögliche Einheit umrechnen)
<code>du -h</code>	Dateigrößen (disk usage) des aktuellen Verzeichnis seinen Dateien anzeigen (-human readable) du -hs zeigt eine Zusammenfassung der Ordner an
<code>free -m</code>	gibt die Speicherauslastung (RAM) in Megabyte aus
<code>file datei.txt</code>	Dateityp von datei.txt ermitteln
<code>md5sum datei.txt</code>	gibt die md5-Prüfsumme von datei.txt aus
<code>lsof</code>	liste aller geöffneter Dateien
<code>top</code>	Prozessviewer, mit q beenden
<code>ps aux</code>	alle Prozess anzeigen
<code>who</code>	eingeloggte Benutzer auflisten

Netzwerk tools

Befehl	Beschreibung
<code>ifconfig</code>	Netzwerkschnittstellen & -Status anzeigen
<code>ifconfig eth0</code>	Infos zur ersten Netzwerkkarte (eth0) anzeigen
<code>netstat</code>	alle Netzwerkverbindungen anzeigen netstat -tup Aktive Internetverbindungen ausschließlich Server anzeigen netstat -tupl Aktive Serververbindungen anzeigen

iptraf	Programm zur Datenverkehrsanalyse Hinweis: ist selten vorinstalliert
host wu.ac.at	Informationen über Hostname / IP von wu.ac.at
traceroute wu.ac.at	Weg zu wu.ac.at verfolgen
ping -c 5 palita.net	wu.ac.at 5 mal einen Ping senden, um zu sehen, ob der Rechner erreichbar ist und wie lange er für eine Antwort benötigt (manche Server geben, trotz Erreichbarkeit, aus Sicherheitsgründen keine Antwort)
hostname	eigenen Hostnamen ausgeben
nslookup wu.ac.at.net	Nameserver-Infos zu wu.ac.at ausgeben
dig wu.ac.at.net	Nameserver zu wu.ac.at abfragen dig @google.de wu.ac.at wie voriges, jedoch google.de befragen dig wu.ac.at AAAA-Record abfragen (ipv6)
ip addr show	Informationen zu Netzwerkkarten und zugehörigen Adressen ausgeben
iftop	zeigt aktuelle Verbindungen und Datenraten an Hinweis: ist selten vorinstalliert

Textmanipulation

Befehl	Beschreibung
sed 's/string1/string2/g' datei.txt	ersetzt string1 durch string2 in datei.txt
sed '/ *#/d; /^ *\$/d' datei.txt	entfernt Kommentare, die mit # beginnen und Leerzeilen aus datei.txt
tr '[:lower:]' '[:upper:]' < datei.txt	Gibt datei.txt in Großbuchstaben aus

Downloads (wget)

Befehl	Beschreibung
wget http://wu.ac.at/download.zip	datei download.zip von wu.ac.at herunterladen und im aktuellen Verzeichnis abspeichern
wget -c http://wu.ac.at/download.zip	Vorher abgebrochenen Download fortsetzen (-continue)

Datum / Zeit

Befehl	Beschreibung
cal -3	Kalender mit 3 Monaten ausgeben (letzter, aktueller und nächster Monat)
date	aktuelles Datum + Uhrzeit ausgeben
uptime	Information über die Laufzeit des Systems

Archivierung / Komprimierung (zip, tar)

Befehl	Beschreibung
tar cf archiv.tar ordner/	ordner/ im aktuellen Verzeichnis in die Datei archiv.tar packen (Linux-Tar Archiv) Weitere Befehle für tar -v verbose (Status ausgeben) -c create (Archiv erstellen) -x extract (Archiv entpacken) -z gzip Komprimierung -j bzip Komprimierung -f Datei Beispiele tar -xf archiv.tar archiv.tar entpacken tar -cfz archiv.tar.gz ordner/ ordner/ packen und mit gzip komprimieren

	tar -vcjf archiv.tar ordner/datei bzip-Archiv aus datei erstellen und details anzeigen
zip archiv.zip *	alle Dateien und Ordner im aktuellen Pfad in archiv.zip packen
unzip archiv.zip	archiv.zip hier entpacken

5.4 Der Apache2-Webserver

5.4.1 Konfigurieren/Warten

Der Apache Webserver ist ein sehr einfach zu konfigurierender und mächtiger Webserver. Er kann in der Shell über **/etc/init.d/apache2** angesprochen werden. Die zwei wichtigsten Konfigurationsdateien befinden sich im Ordner /etc/apache2

In der **apache2.conf** können diverse Einstellungen vorgenommen werden, wie zum Beispiel die Anzahl der gleichzeitig zulässigen Benutzer. In der Datei **ports.conf** kann eingestellt werden, über welche/n Port(s) der http-Server erreichbar ist. Im folgenden Beispiel sind das die Ports 80 und 8010. Sichere Verbindungen (https) sind über den Port 443 möglich.

```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default
# This is also true if you have upgraded from before 2.2.9-3 (i.e. from
# Debian etch). See /usr/share/doc/apache2.2-common/NEWS.Debian.gz and
# README.Debian.gz

NameVirtualHost *:80
Listen 80
Listen 8010

<IfModule mod_ssl.c>
    # If you add NameVirtualHost *:443 here, you will also have to change
    # the VirtualHost statement in /etc/apache2/sites-available/default-ssl
    # to <VirtualHost *:443>
    # Server Name Indication for SSL named virtual hosts is currently not
    # supported by MSIE on Windows XP
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>
```

Apache2 starten

```
user@rechner:/# /etc/init.d/apache2 start
```

Apache2 beenden

```
user@rechner:/# /etc/init.d/apache2 stop
```

Apache2 neu starten

```
user@rechner:/# /etc/init.d/apache2 restart
```

5.4.2 Aufrufen

Alle öffentlich zugänglichen Dateien werden im WWW-Verzeichnis des Webservers gespeichert. Die Standardeinstellung ist **/var/www**. Legen Sie in diesem Verzeichnis die Datei **test.html** an, kann jeder Benutzer die Seite über die Internetadresse <http://ihreip/test.html> aufrufen.

Um die Websites Ihres Servers aufzurufen, starten Sie den Browser und geben entweder

- <http://ihreipadresse>
- <http://localhost>
- <http://127.0.0.1>

ein.



Wichtig ist, dass der Gruppe www-data zumindest Leserechte für Dateien eingeräumt werden, die unter /var/www gespeichert werden. Sonst kann die Datei nicht aufgerufen werden! Hat die Gruppe www-data keinen Zugriff, teilt der Apache-Webserver dies über den Fehlercode 403 (Forbidden) mit! In diesem Fall müssen Sie mit dem Befehl **ls -l** die Zugriffsrechte überprüfen!



5.5 Der MySQL-Datenbank-Server

5.5.1 Was ist der MySQL-Server?

Ein kostenlos verfügbarer Datenbank-Server ist der MySQL-Servers. Dieser kann neben Datenbanken und Tabellen auch Benutzer verwalten und wird in der Regel für viele Open-Source-Anwendungen wie Content-Management-Systeme oder Learning-Management-Systeme verwendet. Informationen zum MySQL-Server finden Sie unter www.mysql.org

5.5.2 Server installieren

Um den MySQL-Server zu installieren, müssen Sie diesen zunächst aus dem Netz laden. Das funktioniert wiederum direkt über den Spiegelserver von Debian, der bei der Installation angegeben wurde. Geben Sie einfach den Befehl **aptitude install** ein, gefolgt vom Namen des Programms, nämlich **mysql-server**

```
user@rechner:/# aptitude install mysql-server
```

Das Paket wird nun am Server gesucht. Wenn es gefunden wurde, wird Ihnen angezeigt, wie viele MB heruntergeladen werden müssen und wie viel Speicherplatz das Programm auf Ihrem Rechner belegen wird. Bestätigen Sie einfach mit **y** und ENTER.

Sie werden nun aufgefordert, ein Passwort für den Administrator (**root**) der Datenbank einzugeben. Achtung: Dies ist nicht der gleiche Benutzer wie der **root**-Benutzer Ihres Linux-Systems! Geben Sie hier das Passwort zweimal ein und bestätigen Sie jeweils mit ENTER. Die Installation läuft nun einfach durch. Der Server sollte automatisch gestartet werden.

5.5.3 Server warten

MySQL stoppen

Den Datenbank-Server können Sie jederzeit mit dem folgenden Befehl stoppen:

```
user@rechner:/# /etc/init.d/mysql stop
```

MySQL starten

Den Datenbank-Server kann mit dem folgenden Befehl gestartet werden, natürlich nur, wenn er nicht bereits läuft:

```
user@rechner:/# /etc/init.d/mysql start
```

MySQL neu starten

Wenn der Datenbank-Server läuft, jedoch neu gestartet werden soll, führen Sie den folgenden Befehl aus:

```
user@rechner:/# /etc/init.d/mysql restart
```

Troubleshooting

In äußerst seltenen Fällen kann der Server nicht mehr reagieren. Meistens, weil zwei Prozesse laufen, oder bei sonstigen Fehlkonfigurationen. Hier müssen Sie dann zunächst alle Prozesse mit dem Namen **mysql** abbrechen (**kill**) und anschließend den Server neu starten.

```
user@rechner:/# pkill mysql
```

5.5.4 PhpMyAdmin

Am einfachsten können Sie Ihren MySQL-Server mit dem Programm phpMyAdmin verwalten. Dieses wird auf dem Webserver eingerichtet und erlaubt Ihnen, Ihre MySQL-Datenbank über einen Webbrower zu verwalten.

Stellen Sie zunächst sicher dass:

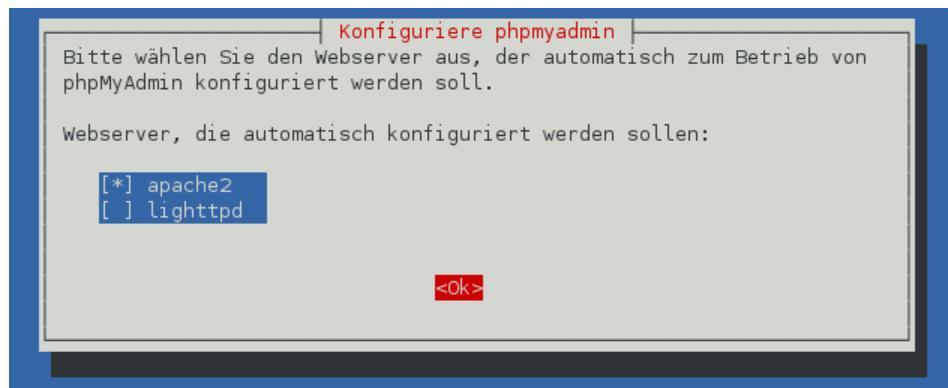
- der Apache2-Server installiert ist und läuft.
- der Mysql-Server installiert ist und läuft.
- PHP installiert ist.

Wenn PHP nicht installiert ist, müssen Sie dieses erst einrichten (vgl. Abschnitt **Fehler!**

Verweisquelle konnte nicht gefunden werden..). Das Programm phpMyAdmin können Sie wie gewohnt direkt über den Spiegelserver installieren:

```
user@rechner:/# aptitude install phpmyadmin
```

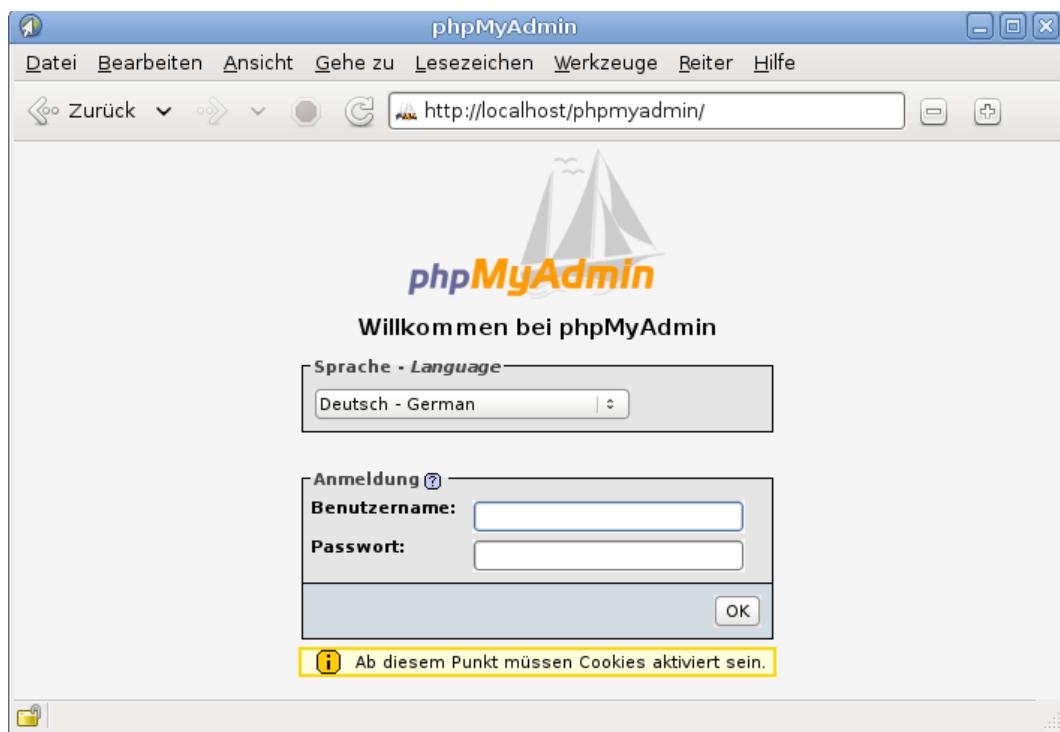
Sie werden nun wieder aufgefordert, die Installation mit **Y** und ENTER zu bestätigen. Kurz danach werden Sie gefragt, ob auch automatisch der Apache2-Webserver für phpMyAdmin konfiguriert werden soll. Stellen Sie sicher, dass diese Option aktiviert ist (verwenden Sie hierfür die Leertaste (SPACE)) und bestätigen Sie dann mit ENTER (zur Option **Ok** wechseln Sie mit der TABULATOR-Taste).



Nun werden Sie aufgefordert, zu bestätigen, dass das Programm phpMyAdmin auf dem MySQL-Server eine neue Datenbank anlegt. Bestätigen Sie hier wieder mit **Ok**. Geben Sie im anschließenden Schritt auch an, dass phpMyAdmin mit **dbconfig-common** konfiguriert werden soll, indem Sie einfach **Ja** mit ENTER bestätigen.

Nun werden Sie aufgefordert, das Passwort für den Administrator (**root**) des MySQL-Servers anzugeben. Dieses haben Sie bei der Installation des MySQL-Servers vergeben. Geben Sie das Passwort ein und bestätigen Sie mit ENTER. Bestätigen Sie die nächste Eingabeaufforderung einfach mit einer leeren Eingabe und ENTER.

Nun ist das Programm phpMyAdmin auf Ihrem Apache2-Webserver installiert. Sie sollten es nun im Browser über <http://localhost/phpmyadmin> aufrufen können.



Mit dem User **root** und dem dazugehörigen Passwort können Sie sich nun über Ihren Webbrower am MySQL-Server anmelden.