Klaus Hegemann, Udo Schaefer

Basiswissen IT-Berufe

Einfache IT-Systeme

9. Auflage

Bestellnummer 01620

Bildungsverlag EINS
westermann

Die in diesem Werk aufgeführten Internetadressen sind auf dem Stand zum Zeitpunkt der Drucklegung. Die ständige Aktualität der Adressen kann vonseiten des Verlages nicht gewährleistet werden. Darüber hinaus übernimmt der Verlag keine Verantwortung für die Inhalte dieser Seiten.

service@bv-1.de
www.bildungsverlag1.de

Bildungsverlag EINS GmbH
Ettore-Bugatti-Straße 6-14, 51149 Köln

ISBN 978-3-427-**01620**-5

westermann GRUPPE

Vorwort

Das vorliegende Buch ist Teil einer Fachbuchreihe, die insbesondere für die informations- und telekommunikationstechnischen Berufe (IT-Berufe) konzipiert wurde. Allen IT-Berufen liegt eine Lernfeldkonzeption zugrunde, die aus insgesamt 11 Lernfeldern besteht.

Die Inhalte dieses Fachbuches decken die im aktuellen Rahmenlehrplan ausgewiesenen Unterrichtsinhalte des Lernfeldes 4 (Einfache IT-Systeme) für alle fünf klassischen IT-Berufe ab (IT-Systemelektroniker/-in, Fachinformatiker/-in Fachrichtung Anwendungsentwicklung, Fachinformatiker Fachrichtung Systemintegration, IT-Systemkaufmann/-frau, Informatikkaufmann/-frau). Darüber hinaus sind in dieser Auflage in einem Kapitel bereits die grundlegenden Begriffe des für die Neuordnung der IT-Berufe vorgesehenen, neuen, inhaltlichen Schwerpunkts „IT-Sicherheit“ einbezogen. Außerdem sind Teile aus Lernfeld 7 enthalten (speziell für den Beruf IT-Systemelektroniker/-in).

Die inhaltlichen Schwerpunkte dieses Lernfeldes sind kapitelweise aufbereitet. Jedes Kapitel schließt mit Fragen zur (Selbst-)Überprüfung erworbener Fachkompetenz, teilweise auch mit einfachen lernfeldbezogenen Handlungsaufgaben.

Handhabung
Das vorliegende Fachbuch ist sowohl Informationsbasis als auch unterrichtsbegleitendes Nachschlagewerk bei der Lösung komplexer Handlungsaufgaben. Die chronologische Bearbeitung der Kapitel ist nicht zwingend erforderlich, vielmehr kann sie sich an den Erfordernissen der jeweils in den Unterricht eingebrachten lernfeldübergreifenden Handlungsaufgaben orientieren.

Neben den grundlegenden Kapiteln über die Hard- und Software eines PCs sowie die IT-Sicherheit (Kap. 1–3) kann bei Bedarf auch auf die Kapitel über die Vorgänge bei der Informationsverarbeitung (Kap. 4) oder die elektrotechnischen Grundlagen (Kap. 5) zurückgegriffen werden. Kapitel 5 beinhaltet auch die speziell für IT-Systemelektroniker/-innen erforderlichen Grundkenntnisse zur Elektroinstallation (z. B. Leitungsdimensionierung und Schutzmaßnahmen nach VDE). Der unterrichtende Fachlehrer hat zudem die Möglichkeit, die vom jeweiligen IT-Beruf abhängige Bearbeitungstiefe einzelner Kapitel zu variieren. Aufgrund der sachlogischen Struktur ist das Buch auch zum individuellen Selbststudium und zur Prüfungsvorbereitung geeignet. Der zugehörige Aufbauband, auf den in einigen Kapiteln verwiesen wird, trägt den Titel „Vernetzte IT-Systeme“ und ist ebenfalls im Bildungsverlag EINS erhältlich.

Für Berufsbezeichnungen o. Ä. wird aus Gründen der besseren Lesbarkeit meist die männliche Form verwendet. Selbstverständlich sind jeweils Männer und Frauen gemeint.

Die Autoren

Inhaltsverzeichnis

serielle Busleitung (z. B.: Kupferdoppelader oder Lichtwellenleiter) sieht somit prinzipiell folgendermaßen aus:

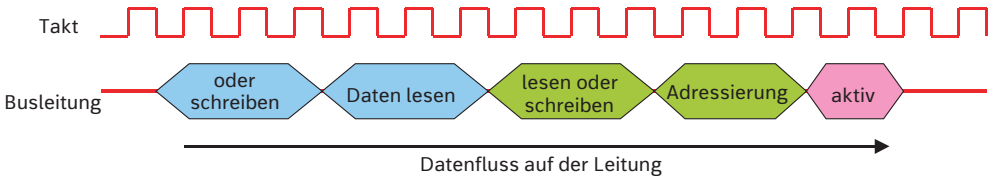


Bild 1.67: Signalaktivität auf einem seriellen Bus (Hinweis: Die Aktivitäten müssen von rechts nach links gelesen werden.)

Bei einem seriellen Bus wird die **Datenübertragungsrate** in **kbit/s**, **Mbit/s** oder **Gbit/s** angegeben (Dezimalpräfixe). Zunehmend erfolgt auch die Angabe in **Kibit/s**, **Mibit/s** oder **Gibit/s** (Binärpräfixe; Kap. 4.3.2).

Zur Erhöhung der Übertragungsrate lassen sich bei Bedarf je nach Spezifikation des seriellen Busses auch mehrere Links zusammenschalten, über die dann *gleichzeitig*, aber *taktunabhängig* voneinander Daten übertragen werden können. Hierbei entstehen keine Probleme wegen unterschiedlicher Signallaufzeiten auf den verschiedenen Leitungen, wie sie bei hohen Taktfrequenzen auf einem parallelen Bus auftreten können. Aktuelle Vertreter serieller Bussysteme sind USB (Kap. 1.6.3) und Firewire (Kap. 1.6.4).

1.6.3 USB

Die Abkürzung **USB** steht für **U**niversal **S**erial **B**us (universeller serieller Bus) und bezeichnet einen von einem Firmenkonsortium (Compaq, Hewlett-Packard, IBM, Microsoft, NEC u. a.) entwickelten Standard für den Anschluss externer Geräte an einen *seriellen* digitalen Bus.

Bei USB handelt es sich um einen sogenannten **freien Standard**, d. h., alle Spezifikationen sind frei verfügbar und somit für die Herstellung und Vermarktung von USB-Produkten ohne Lizenzgebühren anwendbar. USB wurde seit seiner ersten Veröffentlichung ständig weiterentwickelt und ist inzwischen in verschiedenen Versionen verfügbar, die sich insbesondere in der jeweils unterstützten Datenrate unterscheiden. Auch die verwendeten Stecker und Buchsen wurden versionsabhängig weiterentwickelt, sodass untereinander trotz bestehender technischer Abwärtskompatibilität inzwischen in vielen Fällen entsprechende Verbindungsadapter erforderlich sind.

Version (Veröffentlichung)	Modus	Max. Übertragungsrate ($Ü_{max}$)	Typ. Nutzdatenrate**
USB 1.0/1.1 (1994/1998)	Low Speed Full Speed	1,5 Mibit/s 12 Mibit/s	950 Kibit/s 7,6 Mibit/s
USB 2.0 (2000)	High-Speed	480 Mibit/s	300 Mibit/s

Version (Veröffentlichung)	Modus	Max. Übertragungsrate ($Ü_{max}$)	Typ. Nutzdatenrate**
USB 3.1 Gen 1 (USB 3.0*) (2008)	SuperSpeed	5 Gibit/s	2,2 Gibit/s
USB 3.1 Gen 2 (USB 3.1*) (2013)	SuperSpeed+	10 Gibit/s	6,7 Gibit/s

*Bild 1.68: USB-Versionen, *: ursprüngliche Bezeichnung; **: Werte gerundet; (Gen: „Generation"; Angabe der Datenraten auch mit Dezimalpräfixen möglich; Kap. 4.3.2)*

Zwischen der Veröffentlichung einer weiterentwickelten Version und der flächendeckenden Marktpräsenz entsprechender Geräte vergeht meist ein gewisser Zeitraum. Die für 2018 erwartete USB-Version 3.2 wird gegebenenfalls erneut eine Verdopplung der Übertragungsrate bringen ($Ü_{max}$: 20 Gibit/s; Nutzdatenrate ca. 13 Gibit/s).

USB sieht versionsübergreifend unterschiedlich schnelle Betriebsmodi vor, um jedem angeschlossenen Gerät eine adäquate Übertragungsgeschwindigkeit zur Verfügung stellen zu können. Der gleichzeitige Betrieb von Geräten mit verschiedenen Datenübertragungsraten ist problemlos möglich. Hierbei werden die Daten seriell in Paketen mit unterschiedlicher Größe und in unterschiedlichen Zeitabständen übertragen (bei hohen Datenraten also mehr Pakete pro Zeiteinheit; z. B. blaue Pakete in Bild 1.69). Jedes Paket beginnt mit einem Header.

Als **Header** bezeichnet man den Datenbereich am Anfang eines Paketes (Informationskopf), der Informationen über die Ursprungs- und die Zieladresse, Paket-ID-Nummer sowie ggf. zur Steuerung und zur Fehlerkorrektur enthält (in Bild 1.69 gelb markiert).

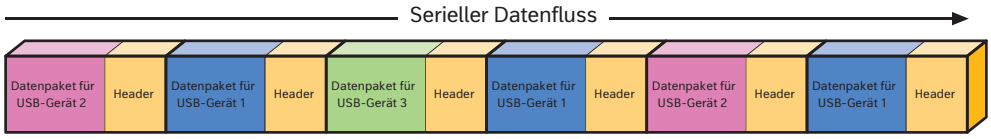


Bild 1.69: Serieller Datenfluss bei USB (Grundprinzip)

Zur seriellen Übertragung wird bis USB 2.0 ein spezieller **NRZ**-Leitungscode verwendet (**N**on **R**eturn to **Z**ero, im Prinzip binäre 0- und 1-Signale; Kap. 4.1.2), dem zur Synchronisation ein Taktsignal hinzugefügt ist. Zur Vergrößerung der Effizienz bei der Datenübertragung erfolgt bei USB 3.1 Gen 1 der Datentransport mit dem sogenannten 8B/10B-Leitungscode (Kap. 1.7.1). Bei USB 3.1 Gen 2 wird dann der 128B/132B-Leitungscode verwendet (Leitungscodes: „Vernetzte IT-Systeme", Kap. 4.1.9).

Aufgrund der Header sowie der Übertragung zusätzlicher Prüfdaten zur Fehlererkennung, Füllbits (**Bit-Stuffing**: Einfügen von Zusatzbits zur Synchonisation) und/oder Leitungscodierungen ist die erzielbare *Nutzdatenrate* bei allen USB-Versionen stets wesentlich kleiner als die spezifizierte maximale Übertragungsrate (≤ 70 % $Ü_{max,}$ Bild 1.68).

Zur Steuerung aller Busaktivitäten ist jeweils ein zentraler Controller erforderlich, der sämtliche angeschlossenen Geräte überwacht.

Allgemein wird ein PC (oder ein anderes Gerät) mit steuernden Funktionen für angeschlossene (USB-)Geräte als **Host** bezeichnet.
Ein Gerät, das Kommunikationsleitungen zu angeschlossenen peripheren Geräten an einer zentralen Stelle bündelt und eine elektrische Verbindung herstellt, bezeichnet man als **Hub**.
Die Anschlüsse an einem Hub werden **Ports** genannt. An jedem Port kann nur ein einziges peripheres Gerät angeschlossen werden.
Ein PC, der als USB-Host fungiert und über mehrere USB-Ports für den direkten Anschluss externer USB-Geräte verfügt, wird auch als **Root Hub** bezeichnet.

Heutige PCs unterstützen meist verschiedene USB-Standards und verfügen daher über mehrere entsprechende USB-Controller, die entweder im Chipsatz integriert oder als separate ICs auf dem Motherboard platziert sind (Kap. 1.4). Diese entsprechen einem der folgenden vier Controller-Standards.

Bezeichnung	Erläuterung
UHCI	– **U**niversal **H**ost **C**ontroller **I**nterface – Unterstützt USB-1.0- und -1.1-Funktionen (Datenraten bis 1,5 Mibit/s oder 12 Mibit/s im Low- oder Full-Speed-Modus) – Entwickler: Intel und VI Technologies
OHCI	– **O**pen **H**ost **C**ontroller **I**nterface – Gleiche Funktionen wie UHCI, arbeitet jedoch geringfügig schneller – Meist eingesetzt in Kombination mit Chipsätzen, die nicht von Intel oder VIA stammen – Entwickler: Compaq, Microsoft und National Semiconductor
EHCI	– **E**nhanced **H**ost **C**ontroller **I**nterface – Unterstützt USB-2.0-Funktionen (Datenrate bis 480 Mibit/s im High-Speed-Modus) – Bei Anschluss von USB-1.0/1.1-Geräten reicht der EHCI-Controller den Datenverkehr an einen nachgeschalteten UHCI- oder OHCI-Controller weiter, der auf dem gleichen Chip implementiert ist. – Fehlt ein EHCI-Controller, können auch USB-2.0-Geräte nur im Low- oder Full-Speed-Modus arbeiten.
xHCI 1.0 **xHCI 1.1**	– Extensible **H**ost **C**ontroller **I**nterface – Unterstützte zunächst nur USB 3.1 Gen 1 (xHCI 1.0: Datenrate bis ca. 5 Gibit/s im SuperSpeed-Modus), inzwischen auch Gen 2 (xHCI 1.1: Datenrate bis ca. 10 Gibit/s im Modus SuperSpeed+). – USB 3.1 Gen 1 und Gen 2 sind technisch abwärtskompatibel zu vorherigen USB-Standards durch Kombination mit einem EHCI, ein gleichzeitiger Betrieb im High-Speed- und im Super-Speed(+)-Modus ist aber nicht möglich; zudem werden unterschiedliche Kabel- und Steckertypen verwendet (Kap. 1.6.3.1).

Bild 1.70: Standards der USB-Controller

USB-taugliche Hubs und Endgeräte werden mit einem speziellen Symbol gekennzeichnet und müssen ein standardisiertes Interface zur Verfügung stellen, welches u. a. die folgenden Merkmale besitzt:

- Unterstützung des jeweiligen USB-Protokolls
- Reaktion auf standardisierte USB-Operationen (z. B. Konfiguration oder Reset)
- Bereitstellung von Informationen über die jeweils implementierten Funktionen

Bild 1.71: USB-2.0-Logo (siehe auch Bild 1.83)

Da USB eine 7-Bit-Adressierung verwendet, lassen sich insgesamt bis zu 127 Geräte (Devices) anschließen, z. B. externe DVD/BD-Laufwerke, Drucker, Scanner, digitale Kameras, Spiele-Adapter sowie Maus und Tastatur. Die Topologie von USB entspricht in etwa einem baumförmigen System, welches in einzelne Ebenen aufgeteilt ist.

Der Begriff **Topologie** (engl. *topology*) bezeichnet die Art der Leitungsführung, in der die Geräte miteinander verbunden werden.

An der Spitze steht hierbei der PC als USB-Host, der in der Regel bereits über mehrere USB-Anschlüsse verfügt, somit also auch die Funktion eines Hubs erfüllt (1. Ebene in Bild 1.72).

Jeder USB-Controller im PC stellt eine bestimmte Anzahl interner und externer USB-Ports zur Verfügung. An einen PC mit insgesamt acht USB-Ports lassen sich demnach bis zu acht USB-Devices – Endgeräte oder Hubs – anschließen, die dann die nächste Ebene bilden (2. Ebene in Bild 1.72). Reine Endgeräte werden auch als **Knoten** (Nodes) bezeichnet. Es gibt aber auch spezielle **Multifunktionsgeräte** (Compound Devices), an die sich dann wiederum weitere Endgeräte anschließen lassen. Diese Multifunktionsgeräte erscheinen dem Host wie ein Hub mit mehreren permanent angeschlossenen Knoten.

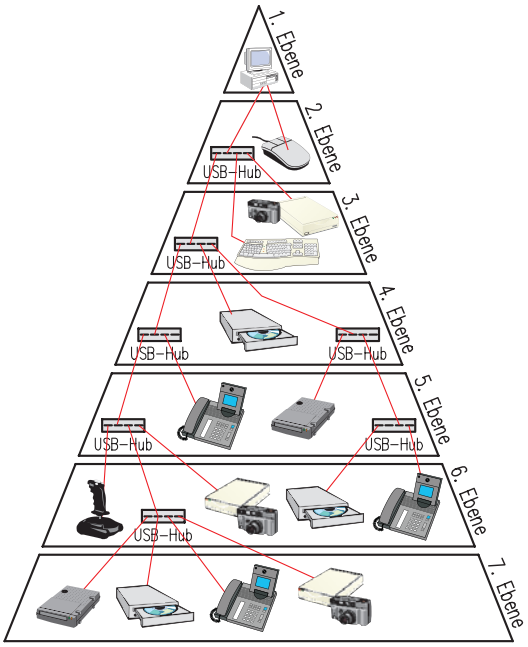


Bild 1.72: Topologie des USBs

An die Hubs der 2. Ebene in Bild 1.72 können weitere Endgeräte oder Hubs angeschlossen werden, die dann die nächste Ebene bilden. Auf diese Weise sind bis zu sieben Ebenen möglich. Betrachtet man allein die Ebenen, in denen Hubs hintereinandergeschaltet werden, so gibt es bei USB insgesamt fünf Hub-Ebenen (in Bild 1.72 Ebene 2 bis 6). Eine größere Anzahl von Hub-Ebenen verursacht Übertragungsprobleme – u. a. bedingt durch Laufzeiteffekte – und ist daher nicht erlaubt. Der Universal Serial Bus weist somit eine baumförmige Struktur auf, bei der die Hubs jeweils die Verbindungen zu einer weiteren Ebene schalten. Während des laufenden Betriebs können Geräte hinzugefügt oder abgetrennt werden („**Hot Plugging**"), die dann automatisch erkannt und initialisiert werden („**Plug and Play**"). Zu beachten ist, dass bei angeschlossenen Speichermedien (z. B. externe USB-Festplatte) die Daten oftmals erst PC-intern zwischengespeichert werden. Um beim Trennen einen möglichen Datenverlust zu vermeiden, sollte hier der Anschlussstecker erst *nach* einer ordnungsgemäßen Abmeldung entsprechend den Vorgaben des jeweiligen Betriebssystems abgezogen werden.

Alle USB-Geräte besitzen eine fest verdrahtete Hardware-Erkennung – bestehend aus Herstellerangaben, Seriennummer und Produkterkennung – um den Bus nach einem Reset oder dem Neustart korrekt initialisieren zu können. Dazu gehören auch Informationen bezüglich der Geräteklasse, Art der Stromversorgung und möglicher Übertragungsband-

breiten. Während der Initialisierung spricht der Host ebenenweise alle Knoten an und weist jedem Gerät eine eindeutige ID (User **ID**entification) zu.

Die Einteilung in **Geräteklassen** dient zur Unterscheidung angeschlossener Geräte mit unterschiedlichen Eigenschaften. Für jede Geräteklasse sind in den USB-Spezifikationen bereits grundlegende Treiber (sogenannte **generische Treiber**) implementiert. Hierdurch sind die meisten USB-Geräte direkt nach Anschluss verwendbar, ohne dass jedes Mal spezielle, gerätespezifische Treiber installiert werden müssen (z. B. Maus, Tastatur, externe Festplatte). Bei Bedarf lassen sich diese allerdings jederzeit nachladen.

Aufgrund der universellen Einsatzmöglichkeiten und der höheren Übertragungsgeschwindigkeit hat USB die ehemals vorhandenen Standardschnittstellen (z. B. serielle und parallele Schnittstellen) weitestgehend ersetzt.

1.6.3.1 USB-Anschluss- und Verbindungstechnik

Mit jedem neuen USB-Standard wurde die mögliche Daten-Übertragungsrate maßgeblich gesteigert, sodass jeweils auch neue Verbindungskabel und Steckverbindungen erforderlich waren.

Bis einschließlich **USB 2.0** werden zur Verbindung der Geräte vieradrige Kabel verwendet, wobei zwei Adern für den bidirektionalen Datenverkehr und zwei Adern für eine begrenzte Energieversorgung angeschlossener Geräte durch den Host vorgesehen sind. Die Datenübertragung erfolgt mit differenziellen Signalen (Kap. 4.1.3).

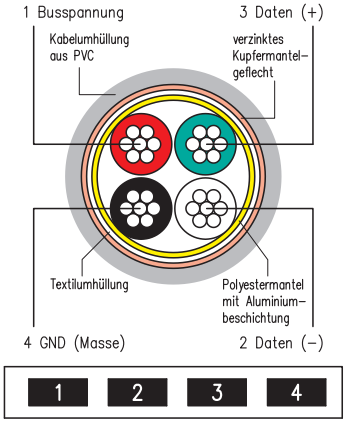
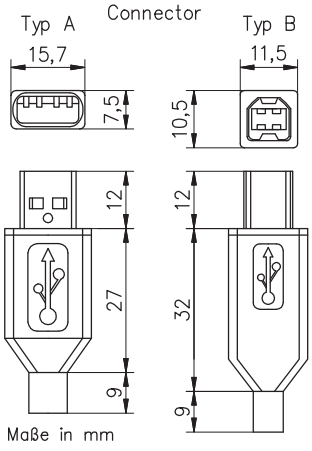
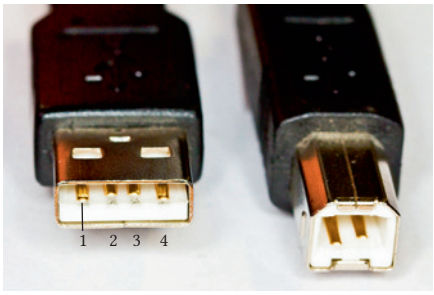


Bild 1.73: Prinzipieller Aufbau eines USB-2.0-Kabels und Kontaktzuordnung

Bei den USB-2.0-Steckverbindungen unterscheidet man grundsätzlich zwischen den Varianten Typ A und Typ B. Beide sind mechanisch inkompatibel, sodass eine Verwechslung beim Anschluss nicht möglich ist. Der breite **Typ-A-Stecker** wird immer in Richtung zum Host, der quadratische **Typ-B-Stecker** wird immer in Richtung Peripheriegerät verwendet (Bild 1.74).





USB 2.0 Typ A-Stecker

USB 2.0 Typ B-Stecker

Bild 1.74: USB-2.0-Steckervarianten

Bei Geräten mit kleinen Abmessungen werden auch spezielle verkleinerte Stecker und Buchsen eingesetzt (Mini- und Micro-USB; Mini-USB ist nicht mehr Bestandteil aktueller Spezifikationen). Diese verfügen meistens über einen zusätzlichen fünften Anschlusskontakt, der zur Geräte-Identifikation dient. Der Micro-USB-2.0-Anschluss dient bei Smartphones (Kap. 1.1.5) derzeit vielfach als Standardverbindung zur leitergebundenen Datenübertragung *und* zum Aufladen des Akkus. Durch die geringfügig unterschiedliche Bauform des aus Edelstahl bestehenden Steckermantels unterscheiden sich auch hier die Typ-A- und Typ-B-Stecker, wobei die Typ-A-Stecker wenig verbreitet sind.

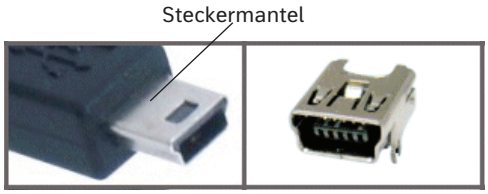


Bild 1.75: Typ B, Mini-USB 2.0

Bild 1.76: Typ B, Micro-USB 2.0

Darüber hinaus existieren verschiedene herstellerspezifische Steckervarianten, die nicht der USB-Norm entsprechen und untereinander auch nicht kompatibel sind. Bei allen Steckerausführungen sind die beiden Kontaktzungen für die Spannungsversorgung länger als die Kontakte für die Signalleitungen (Bild 1.74, Pin 1 und 4). Hierdurch wird sichergestellt, dass beim Einstecken während des laufenden Betriebes die Versorgungsspannung für das Gerät geringfügig eher anliegt als die zu verarbeitenden Daten. Innerhalb dieser kurzen Zeitspanne kann die Geräteelektronik dann jeweils die erforderlichen Betriebswerte annehmen, bevor anliegende Daten verarbeitet werden.

Der Standard **USB 3.1 Gen 1** (alte Bezeichnung **USB 3.0**) bietet eine Erhöhung der Datenrate auf bis zu 5 Gibit/s (SuperSpeed-Modus). Die Datenübertragung im SuperSpeed-Modus erfolgt hierbei richtungsgetrennt über zwei zusätzliche, getrennte Aderpaare (Bild 1.77: Pin 5, 6 und 8, 9) im Vollduplex mit differenziellen Signalen (Kap. 4.1.3). Mit dem Aderpaar für den USB-2.0-Betrieb (Pin 2, 3), sowie zwei Adern für die Spannungsversorgung (Pin 1, 4) besteht ein als USB 3.1 Gen 1 spezifiziertes Kabel somit insgesamt aus acht Leitungen (vier Aderpaare, Bild 1.77).

Aus Gründen der Abwärtskompatibilität zu USB 2.0 hat man den alten Typ-A-Stecker beibehalten und lediglich die Kontaktzahl um fünf zusätzliche Anschlüsse erweitert, die hinter den vorhandenen vier Kontakten angeordnet sind (TX+, TX–, RX+, RX– und Masse; Pin 5 bis 9 in Bild 1.77). Somit passen alte und neue Typ-A-Stecker mechanisch zusammen.

Die Kontaktzunge (oder das Gehäuse) bei den USB 3.1 Gen 1-Steckern/Buchsen ist zur Unterscheidung von reinen USB-2.0-Anschlüssen jeweils blau gefärbt (Bild 1.78). Bei dem alten Typ-B-Stecker hingegen fehlt der Platz für zusätzliche Kontakte, dieser bekommt daher einen Anbau, der so gestaltet ist, dass der alte Typ-B-Stecker in die neue Buchse passt, aber nicht der neue Typ-B-Stecker in die alte Buchse (Bild 1.78 Mitte). Auch die alten, in Kleingeräten (Kamera, Smartphone usw.) verwendeten *Micro*-Versionen des Typ-B-Steckers bieten keinen Platz für neue Pins und erhalten einen Anbau (Bild 1.78 links). Eine *Mini*-Version von USB 3.1 Gen 1-Steckverbindern existiert nicht.

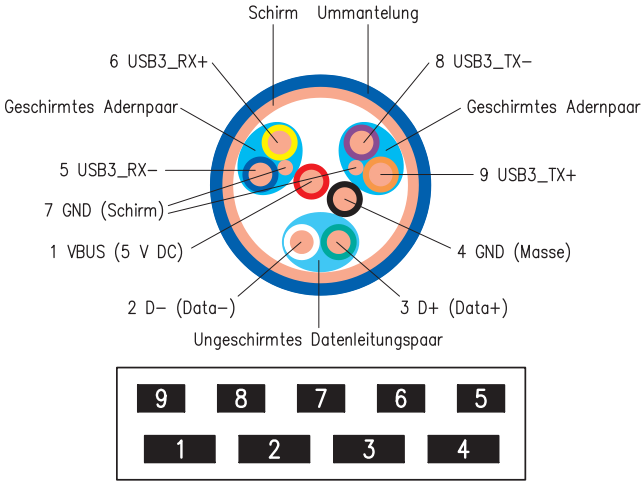
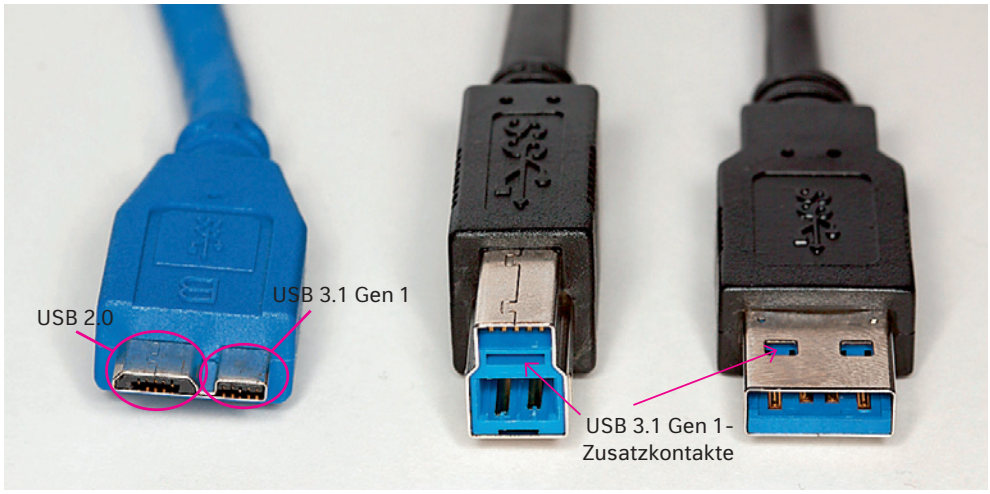


Bild 1.77: Prinzipieller Aufbau eines USB 3.1 Gen 1-Kabels und Kontaktzuordnung



USB 3.1 Gen 1
Micro-Typ B-Stecker

USB 3.1 Gen 1
Typ B-Stecker

USB 3.1 Gen 1
Typ A-Stecker

Bild 1.78: USB 3.1 Gen 1-Stecker und -Buchsen

Bei **USB 3.1 Gen 2** verdoppelt sich die Übertragungsrate gegenüber der Vorgängerversion auf bis zu 10 Gibit/s. Gleichzeitig wird eine neue Steckerform definiert, die eine symmetrische Bauform aufweist. Dieser „**Typ-C-Stecker**“ hat eine mittig angeordnete Kontaktzunge, die beidseitig mit den gleichen Anschlusspins versehen ist und somit in beiden Orientierungen (d. h. auch um 180° gedreht) in die entsprechende Typ-C-Fassung gesteckt werden kann.

Im Gegensatz zu den bisherigen Verbindungskabeln mit Typ-A- und Typ-B-Steckern befindet sich an *beiden* Enden eines USB 3.1 Gen 2-Kabels der *gleiche* Typ-C-Stecker (Bild 1.79). Er ist kleiner als der bisherige Typ-A-Stecker (Bild 1.74) und damit nicht mehr kompatibel zu den bisher verwendeten Stecksystemen. Um diese weiter nutzen zu können, werden diverse Adapter kabel angeboten. Einige Boards liefern auch (eingeschränkte) USB 3.1 Gen 2-Leistungsmerkmale an einer bereits rückseitig vorhandenen, speziellen Typ A-Buchse (siehe Bild 1.89).

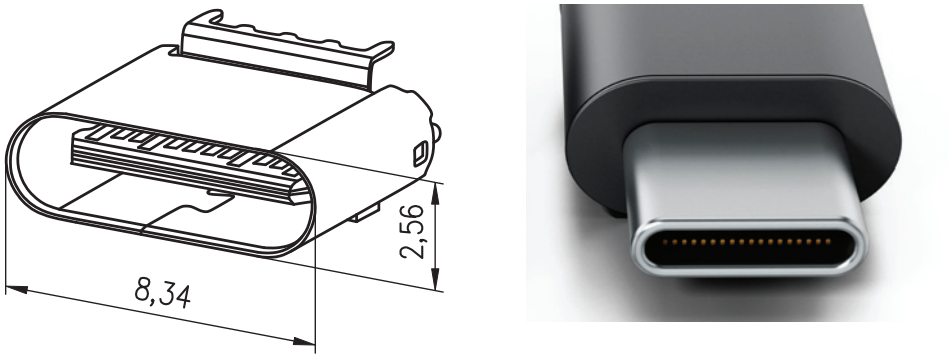
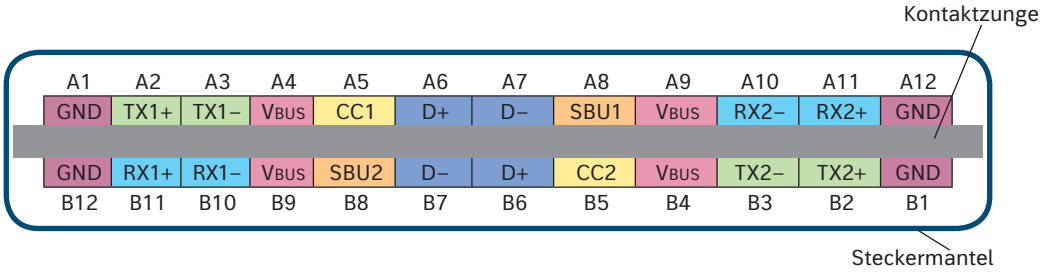


Bild 1.79: USB Typ C-Stecker



Pin-Nr.	Belegung der Kontaktzunge
A1, A12 B1, B12	**GND**: Ground
A2, A3 B2, B3	**TX1+, TX1-**: High Speed Data Path 1 (Transmit USB or Transmit DP Alt-Mode) (Verwendung von zwei Leitungspaaren!)
A4, A9 B4, B9	**VBus**: Bus Power
A5 B5	**CC1, CC2**: Configuration Detection
A6, A7 B6, B7	**D+, D-**: USB 2.0 Bus Interface (Verwendung von einem Leitungspaar!)
A8 B8	**SBU1, SBU2**: Secondary Bus System (Alternate Connection; Headphone Analog Signal)
A10, A11 B10, B11	**RX2+, RX2-**: High Speed Data Path 2 (Receive USB or Transmit DP Alt-Mode) (Verwendung von zwei Leitungspaaren!)

Bild 1.80: Anschlussbelegung USB Typ C-Stecker

Neu ist, dass der Typ C-Stecker in Kombination *mit* USB, aber auch gänzlich *ohne* USB-Datenverbindung mannigfaltig genutzt werden kann. Hierzu werden sogenannte **Alternate-Modes** definiert, bei denen den einzelnen Anschlusspins und Verbindungsleitungen auch andere Funktionen zugeordnet werden können. Alternative Modi sind beispielsweise:

- **Display Port Alternate Mode (DP Alt-Mode)**; mit entsprechenden Geräten können Display-Port-Signale bis zur Version 1.3 (Kap. 1.7.6.5) über eine Typ-C-Steckverbindung transportiert werden, die ein Display in UHD-Auflösung (Kap. 1.9.4) ansteuern; bei entsprechender Aufteilung der Datenpfade des USB 3.1 Gen 2-Kabels ist auch die gleichzeitige Übertragung von USB- *und* Display-Port-Signalen möglich.
- **Audio Adapter Accessory Mode (AAA-Mode)**; bei künftigen Geräten kann die 3,5-mm Audio-Buchse entfallen, der Anschluss von Kopfhörern und Lautsprechern funktioniert dann auch mit entsprechenden Adaptern (z. B. USB-Typ-C-Stecker auf 3,5-mm-Audio-Buchse) über USB-Hubs.

Der Typ C-Stecker ist mit entsprechenden Adapterkabeln auch kompatibel zu anderen Schnittstellen-Signalen, z. B. HDMI und MHL (Kap. 1.7.6). Darüber hinaus verwendet Apple ab Thunderbolt 3 ebenfalls den Typ-C-Stecker für seine Geräte (Kap. 1.7.7).

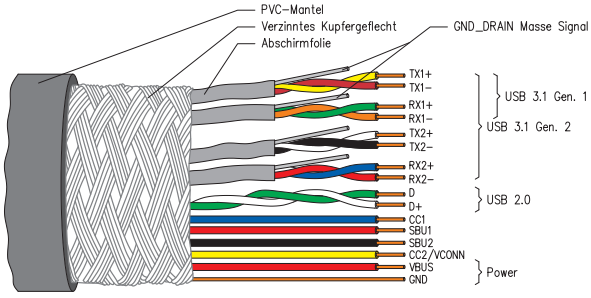


Bild 1.81: Aufbau eines USB 3.1 Gen 2-Full Featured Kabels

Um sämtliche Übertragungsmöglichkeiten nutzen zu können, ist ein mit *allen* Verbindungsleitungen ausgestattetes USB 3.1 Gen 2-Kabel (**FFC**: **F**ull **F**eatured **C**able; Bild 1.81) erforderlich. Über einen im Typ-C-Stecker implementierten elektronischen Chip (Stromversorgung über Pin V_{Conn}; Bild 1.81) können hierbei die jeweiligen Schnittstellensignale detektiert werden. Zu beachten ist, dass in der Praxis nicht jedes Kabel mit USB-Typ-C-Anschlüssen über diese Leitungs-Vollausstattung verfügt. Ob die genannten Funktionalitäten bei Vollausstattung unterstützt werden, hängt aber auch von der seitens der Hersteller *in* den jeweiligen Geräten implementierten Elektronik ab.

1.6.3.2 USB-Energieversorgung

Von Beginn an ermöglichte ein USB-Anschluss prinzipiell auch eine Energieversorgung angeschlossener Geräte ohne eigene Stromversorgung über das für die Datenübertragung verwendete USB-Kabel („**Bus-Powered-Devices**“). Diese war zunächst aber lediglich auf kleinere Geräte mit einer vergleichsweise geringen Energieaufnahme begrenzt. Geräte mit höherer Leistung mussten über eine separate Stromleitung (Kap. 5.3.2.3) mit Energie versorgt werden („**Self-Powered-Devices**“).

Ziel der schrittweisen Entwicklung war jedoch, möglichst alle angeschlossenen Geräte über einen USB-Anschluss mit Energie zu versorgen und bei mobilen Geräten gleichzeitig auch den Akku in kurzer Zeit zu laden. Aus diesem Grund erfolgte – zeitgleich mit, aber unabhängig von der Entwicklung der USB 3.1 Gen 2-Spezifikation für den Datenverkehr – die Entwicklung einer Spezifikation zur gleichzeitigen Verwendung der USB-Typ-C-Steckverbindung zur erweiterten Energieversorgung angeschlossener Geräte.

USB Power Delivery 2.0 (**UPD** oder **USB-PD**) ist die Bezeichnung einer Spezifikation des **USB-IF** (**USB I**mplementers **F**orum) über eine *bidirektional* mögliche Energieversorgung zweier Geräte, die über ein USB 3.1 Gen 2-Kabel mit Typ-C-Stecker verbunden sind. Hierbei werden – unabhängig von einer aktiven Datenübertragung – über die USB-Power-Anschlusspins mithilfe des UPD-Protokolls und entsprechenden in den Geräten vorhandenen Konfigurationscontrollern die *Richtung* der Energieversorgung sowie die *Größe* von Strom und Spannung ausgehandelt.

Die bis dato vorhandenen Energieversorgungen über USB (Low-Powered, High-Powered, USB-BC; Bild 1.82) können als Vorstufen der aktuellen USB-PD-Spezifikation angesehen und dieser entsprechend zugeordnet werden.

Version	Bezeichnung/ Profil		Energieversorgung (max.)	Bemerkungen/Beispiele
USB 1.0/1.1	Low-Powered		5 V/0,1 A	Tastatur, Maus
USB 2.0	High-Powered		5 V/0,5 A	Scanner, externe 2,5-Zoll Festplatten; begrenzt auch Ladefunktion kleinerer Mobilgeräte möglich (USB-BC bis 2,5 W, siehe unten)
USB 3.1 Gen 1	High-Powered		5 V/0,9 A	Smartphone
	USB Battery Charging (USB-BC)		5 V/1,5 A	Spezifikation für USB-Ladegeräte; Port-Bezeichnung: **DCP** (**D**edicated **C**harging **P**ort)
USB 3.1 Gen 2	**Profile USB Power Delivery 2.0**	1*	5 V/2 A	kleinere, portable Geräte
		2	5 V/2 A 12 V/1,5 A	Tablets, Netbooks, Scanner
		3	5 V/2 A 12 V/3 A	Notebooks
		4	5 V/2 A 12 V/3 A 20 V/3 A	Drucker
		5	5 V/2 A 12 V/5 A 20 V/5 A	Displays, aktive Lautsprecherboxen

Bild 1.82: Energieversorgung über USB (:abwärtskompatibel zu USB 2.0 und USB 3.1 Gen 1)*

Viele Geräte benötigen im Moment der Inbetriebnahme einen wesentlich höheren Einschalt- bzw. Anlaufstrom als im normalen Betriebszustand (z. B. 2,5-Zoll-Festplatten, Anlaufstrom bis ca. 0,8 A, Betriebsstrom bis ca. 0,25 A; siehe auch Kap. 5.1.4.2). Zwar werden hierdurch USB-2.0-Ports kurzzeitig überlastet, verkraften dies jedoch in der Regel schadlos. Um auch Geräte mit etwas höherem Strombedarf über einen USB-Port speisen zu

können (USB-BC, Bild 1.82), unterstützen einige Geräte auch die auf einer EU-Richtlinie basierende **Battery Charging Specification** für USB-Ladegeräte.

Das aktuelle USB-Power Delivery 2.0 definiert fünf Versorgungsprofile mit unterschiedlichen Leistungsanforderungen (Bild 1.82). Die Stromflussrichtung und der Leistungsbedarf – zur Energieversorgung eines angeschlossenen Gerätes und/oder zu Ladezwecken – wird hierbei während der Initialisierung über entsprechende Konfigurationscontroller, die unabhängig von der Datenübertragung arbeiten können, für jede Kabelverbindung individuell zwischen den beiden angeschlossenen Geräten ausgehandelt. In der UPD-Nomenklatur wird hierbei unterschieden zwischen **Provider**-Geräten, deren USB-Anschlüsse als Energiequelle fungieren (**DFP**: **D**ownstream **F**acing **P**ort), und **Consumer**-Geräten, deren USB-Anschlüsse dann Verbraucher darstellen (**UFP**: **U**pstream **F**acing **P**ort). Unter Umständen kann der USB-Anschluss eines Gerätes auch beide Funktionen aufweisen (**DRP**: **D**ual **R**ole **P**ort). Das Gerät mit dem höheren Energiepotenzial kann hierbei jeweils die Stromversorgung übernehmen, bei veränderten Verhältnissen kann das System entsprechend umschalten.

Ein **USB-Anschluss**, der mit USB 3.1 Gen 2 konform ist *und* die USB-PD Spezifikationen erfüllt, stellt eine **Kombination aus einer schnellen Datenschnittstelle und einem bidirektionalen Energieverteilsystem dar.**

So könnte beispielsweise ein PC ein angeschlossenes Display über das USB-Kabel mit Bildsignalen und Strom versorgen, das Energieversorgungskabel des Displays würde in diesem Fall nicht benötigt. Andererseits könnte das gleiche Display bei Verbindung mit dem Energieversorgungsnetz aber auch den Akku eines über USB angeschlossenen Tablets laden.

Für die erhöhte Leistungsübertragung ab Profil 2 sind spezielle USB-Kabel erforderlich. Zu beachten ist, dass nicht alle USB 3.1 Gen 2-Anschlüsse und Kabel die USB-PD-Spezifikationen (bzw. sämtliche Profile) erfüllen. Vom USB-IF zertifizierte Logos an Geräten, Anschlüssen und Kabeln sollen daher Auskunft über die jeweils unterstützten Merkmale geben (Bild 1.83).

Symbol	Bedeutung	Übertragung
	SS – USB 3.1 Gen. 1 „SuperSpeed“	Datenrate bis zu 5 Gibit/s ($Ü_{max}$); keine Unterstützung von USB-PD (jedoch ist geräteabhängig USB-BC möglich)
	SS+ oder SS10 – USB 3.1 Gen. 2 „SuperSpeed+“	Datenrate bis zu 10 Gibit/s ($Ü_{max}$); keine Unterstützung von USB-PD (jedoch ist geräteabhängig USB-BC möglich)
	SS+DP oder SS10 DP – USB 3.1 Gen. 2 „SuperSpeed+“ mit DisplayPort Integration	Gleiche Spezifikationen wie normaler USB 3.1 Gen. 2-Anschluss; zusätzlich Übertragung von Display-Signalen via DisplayPort (Kap. 1.7.6.5) möglich
	Blitz – Thunderbolt 3	Als USB-Type-C-Anschluss ausgeführt; Übertragungsart: USB 3.1 Gen 2 und auch Thunderbolt 3 (Kap. 1.7.7)
	Zusatz „PD“ oder Batterie-Symbol (Power Delivery)	zusätzlich zur jeweiligen Datenübertragungsrate (5 bzw. 10 Gibit/s) wird USB-PD unterstützt; ab USB 3.1 Gen 2 kann – abhängig vom Versorgungsprofil (Bild 1.82) und den verwendeten Leitungen – bis zu 100W übertragen werden

Bild 1.83: USB-IF Symbole (Beispiele)

Die in den Spezifikationen angegebenen maximalen Kabellängen (meist < 1,5 m) sollten nicht überschritten werden, da es ansonsten leicht zu Induktionsstörungen (Kap. 5.5.1.5) kommen kann. Bei längeren Übertragungsstrecken können entsprechende Signalregeneratoren eingesetzt werden, die das Signal aufbereiten.

1.6.3.3 Sonstige USB-Spezifikationen

USB-OTG (**O**n-**T**he-**G**o) stellt eine Erweiterung ab dem USB-2.0-Standard dar und spezifiziert eine USB-Geräteklasse, die untereinander ohne einen zwischengeschalteten PC als Steuergerät (Host) Daten austauschen kann. Durch eine implementierte Protokollergänzung verfügen OTG-Geräte selbst über die Fähigkeit, begrenzt die Rolle eines Hosts zu übernehmen. Ein USB-Gerät mit begrenzter Übernahme von Host-Eigenschaften wird als **Dual-Role-Gerät** bezeichnet. OTG-fähige Geräte können mit Steckverbindern ab dem USB-2.0-Standard verbunden werden. Da die Host-Funktion bei OTG-Geräten beliebig tauschbar ist, muss sich der Benutzer keine Gedanken über das richtige Anstecken von Kabeln machen.

Des Weiteren gibt es **Wireless-USB**-Produkte, die insbesondere bei den sogenannten **HID**-Anwendungen (**H**uman **I**nterfaces **D**evices), also Tastaturen, Mäusen und Gamepads für Spielekonsolen, Anwendung finden. Eine drahtlose USB-Strecke besteht aus einem entsprechenden Sender, der in einen USB-Anschluss eingesteckt wird, und einem USB-Transceiver im angeschlossenen Gerät. Aus Sicht des Rechners verhält sich die Funkstrecke wie ein USB-Kabel. Die Funkübertragung (meist Datenrate bis 1 Mibit/s im ISM-Band 2,4 GHz, Reichweite ca. 10 m, Frequenzsprungverfahren mit 79 Kanälen) ist ähnlich der bei Bluetooth, allerdings mit einem erheblich einfacheren Protokoll.

1.6.4 Firewire

Firewire ist die Kurzbezeichnung für ein serielles Bussystem, das ursprünglich auf einer Entwicklung für eine schnelle serielle Datenübertragung der Firma Apple basiert.

Durch den Zusammenschluss verschiedener namhafter Hersteller der Computer- und der Audio-/Video-Industrie (z. B. Adaptec, AMD, Apple, IBM, Microsoft, Philips, Sony, TI, JVC, Yamaha u. a.) wurde diese Entwicklung modifiziert und führte 1995 zur Veröffentlichung des primären Firewire-Standards, dessen Originalbezeichnung **IEEE 1394–1995** lautet.

IEEE ist die Abkürzung für **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers, eine Vereinigung von amerikanischen Elektro- und Elektronikingenieuren, die für viele Standards in Hardware und Software verantwortlich ist.

Inzwischen existiert eine völlig überarbeitete und fehlerbereinigte Version dieses Standards. Dieser fasst die ursprüngliche Version und die beiden Erweiterungen IEEE 1394**a** und IEEE-1394**b** zusammen (**IEEE 1394-2008**). Darüber hinaus verwendet Sony für diese Technologie aus Marketinggründen die firmeneigene und lizenzgeschützte Bezeichnung **i-Link**.

AUFGABEN

1. Der Begriff „Server“ wird in Kombination mit dem Begriff „Client“ im allgemeinen Sprachgebrauch oftmals mit unterschiedlicher Bedeutung verwendet. Erläutern Sie den Unterschied.
2. Was versteht man unter einem „Rolling Release“?
3. Welche Stufen unterscheidet Windows 10 bei seinen Telemetrieprofilen? Erläutern Sie diese.
4. Was versteht man unter einem „Trusted Platform Modul“ und wozu wird es verwendet?
5. Wozu verwendet man in der PC-Technik „Shortcuts“? Listen Sie tabellarisch einige gängige Windows-10-Shortcuts auf und erläutern Sie deren Funktion.
6. Aus welchem Grund richtet man auf einem PC bzw. in einem Netzwerk sogenannte „Benutzerkonten“ ein?
7. Welche Kategorien von Anwendern unterscheidet Linux? Erläutern Sie die Unterschiede.
8. Was bedeutet im Zusammenhang mit Linux die Abkürzung KDE? Was wird hiermit bezeichnet?
9. Was versteht man bei Linux unter dem Begriff „Mounten“?
10. Aus welchen Basiselementen besteht die Betriebssystemstruktur von macOS?
11. a) Welcher Unterschied besteht zwischen einem Microkernel und einem monolitischen Kernel?

    b) Was ist ein Hybridkernel? Nennen Sie ein Anwendungsbeispiel.
12. Welche Betriebssysteme bieten eine Mehrbenutzerverwaltung?
13. Welchen Zweck hat eine sogenannte Sandbox bei mobilen Betriebssystemen?
14. Wie werden auf den verschiedenen Smartphone-Systemen Apps geupdatet?
15. Wie werden Smartphones mit Betriebssystem-Updates versorgt?

2.6 IT-Sicherheit

Informationen stellen für Unternehmen wichtige Werte dar, die geschützt werden müssen. Gefahren drohen beispielsweise durch Offenlegung, Manipulation oder Zerstörung. Da heutzutage die Erstellung, Sammlung, Speicherung, Verarbeitung und Übermittlung von Informationen zumindest teilweise mithilfe der Informationstechnik erfolgt, ergibt sich für Unternehmen die Notwendigkeit, ihr IT-Umfeld angemessen zu schützen.

Die Sicherheit von Informationen kann auf unterschiedliche Weise bedroht werden: ohne Vorsatz, beispielsweise durch höhere Gewalt (Blitzschlag, Feuer, Überschwemmung), oder mit Vorsatz insbesondere durch Schadsoftware oder Hacker-Angriffe.

Daraus ergeben sich unterschiedliche Aspekte des Begriffs Sicherheit. Im Englischen werden zwei wesentliche Bedeutungen sprachlich differenziert: so besitzt der deutsche Begriff

Sicherheit die beiden Übersetzungen *safety* und *security*. Konventionell versteht man unter *safety* Unfallvermeidung, unter *security* Kriminalprävention. Auf die Informationstechnik bezogen bedeutet *safety* **Funktionssicherheit**. Sie besagt, dass ein IT-System unter normalen Betriebsbedingungen nur die vorgesehenen und keine verbotenen Funktionen ausführt. *Security* wird in der Informationstechnik mit **Informationssicherheit** übersetzt. Informationssicherheit bedeutet, dass ein IT-System keine unautorisierte Informationspreisgabe oder -manipulation zulässt.

Informationstechnisch erfasste, gespeicherte, verarbeitete oder übertragene Informationen bezeichnet man als Daten.

Dabei stützt sich der Begriff **Datensicherheit** vor allem auf den Aspekt des Schutzes (*protection*). Maßnahmen zur Datensicherheit sollen damit einerseits vor unautorisierten Zugriffen schützen (Informationssicherheit). Andererseits gilt es, die Verfügbarkeit der Daten sicherzustellen. Dazu zählt insbesondere die Erstellung von redundanten Datenspeicherungen (Backups), um Datenverluste zu vermeiden.

Der Begriff **Datenschutz** bezieht sich vor allem auf den Schutz personenbezogener Daten. Da diese Daten die Privatsphäre (*privacy*) der betroffenen Personen anbelangen, gelten sie als besonders schutzbedürftig und nehmen dadurch eine Sonderrolle ein. Das **Bundesdatenschutzgesetz** (BDSG) stellt Regeln zum Umgang mit diesen Daten auf. Bürger können ihr Recht auf informationelle Selbstbestimmung wahrnehmen und über Art und Umfang der Nutzung ihrer personenbezogenen Daten bestimmen. In der am 26.5.2018 in Kraft getretenen **Datenschutzgrundverordnung** (DSGVO) werden diese Regeln verschärft und EU-weit vereinheitlicht.[1] (siehe auch „Vernetzte IT-Systeme“, Kap. 1.7).

Funktionssicherheit *(safety)*	Ein System ist funktionssicher, wenn es unter normalen Betriebsbedingungen die festgelegte Funktionalität bietet. Ein funktionssicheres System führt keine unzulässigen Funktionen aus.
Informationssicherheit *(security)*	Ein funktionssicheres System ist informationssicher, wenn es keine unautorisierte Informationspreisgabe oder -veränderung zulässt.
Datensicherheit *(protection)*	Ein funktionssicheres System, das Daten und Systemressourcen vor Verlust und unautorisierten Zugriffen schützt, bietet Datensicherheit. Dazu zählen insbesondere auch Maßnahmen zur redundanten Datenspeicherung (*backup*).
Datenschutz *(privacy)*	Der Begriff Datenschutz bezeichnet den Schutz von Informationen, die eine Person betreffen. Gesetzliche Bestimmungen legen Sicherheitsanforderungen fest und regeln das informationelle Selbstbestimmungsrecht.
Verlässlichkeit *(dependability)*	Ein verlässliches System führt keine unzulässigen Funktionen aus (Funktionssicherheit) und erbringt die festgelegten Funktionen zuverlässig (*reliability*).

Bild 2.38: Aspekte der IT-Sicherheit

IT-Systeme sollen idealerweise **Verlässlichkeit** bieten, also funktionssicher und zuverlässig arbeiten. Um einen funktionssicheren Betrieb zu gewährleisten, setzen Hersteller vor allem auf Maßnahmen, die ein technisches Fehlverhalten des Systems selbst verhindern sollen. Derartige von innen ausgehende Gefahren entstehen dabei insbesondere durch Programmierfehler. Über Strukturierungs- sowie Validierungs- und Verifikationskonzepte kann erreicht werden, dass sich Fehler im Programmcode schneller finden und beheben lassen.

[1] *siehe: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02016R0679-20160504 [05.07.2018]*

Äußere Einflüsse auf IT-Systeme wie Stromausfall, Feuer oder irrtümliche Fehlbedienungen stellen zusätzliche Gefahren für einen verlässlichen Betrieb dar. Dem stehen absichtliche Fehlbedienungen und Hacker-Angriffe gegenüber, die bewusst auf die Auslösung von Fehlverhalten betreffender IT-Systeme abzielen. Mit der fortschreitenden Vernetzung von IT-Systemen bieten die Unternehmen nicht nur autorisierten Nutzern, sondern auch potenziellen Angreifern eine Zugangsmöglichkeit. Insbesondere die Anbindung an das Internet schafft eine deutlich vergrößerte Angriffsfläche, die bei der Absicherung des Systems berücksichtigt werden muss.

2.6.1 Schutzziele

Maßnahmen zum Schutz vor den vielfältigen Bedrohungen zielen insgesamt auf einen Schutz der IT-Sicherheit ab. Dabei ist es hilfreich für die Entwicklung und Beurteilung von Schutzmaßnahmen, dieses allgemeine Ziel in konkrete Schutzziele zu untergliedern.

Abhängig von der konkreten Situation müssen für ein Unternehmen nicht alle im Folgenden aufgeführten Schutzziele relevant sein.

Schutzziel	Beschreibung
Vertraulichkeit	Informationsvertraulichkeit *(confidentiality)* gewährleistet ein System, wenn es keine unautorisierte Informationsgewinnung ermöglicht.
Integrität	Ein System gewährleistet Datenintegrität *(integrity)*, wenn es nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.
Verfügbarkeit	Ein System gewährleistet Verfügbarkeit *(availability)*, wenn authentifizierte und autorisierte Nutzer in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können.
Authentizität	Unter der Authentizität einer Sache *(authenticity)* versteht man deren Echtheit und Glaubwürdigkeit, die anhand ihrer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist.
Verbindlichkeit	Ein System gewährleistet die Verbindlichkeit bzw. Zuordenbarkeit *(non repudiation)* von Aktionen, wenn es dem Durchführenden im Nachhinein nicht möglich ist, die Durchführung einer solchen Aktion abzustreiten.
Anonymisierung und Pseudonymisierung	Unter Anonymisierung versteht man die Veränderung personenbezogener Daten, sodass die Einzelangaben nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person zugeordnet werden können. Die Pseudonymisierung stellt eine schwächere Form der Anonymisierung dar. Dabei wird die Personenzuordnung anhand eines Zuordnungsverfahrens (beispielsweise durch Austausch mit einem Pseudonym) verhindert. Nur bei Kenntnis oder Nutzung des Zuordnungsverfahrens können die Daten einer bestimmten Person zugeordnet werden.

Bild 2.39: Schutzziele

2.6.2 Gefährdungsfaktoren

Um den Schutzbedarf für das IT-System eines Unternehmens bestimmen und beurteilen zu können und entsprechende Maßnahmen damit zu verbinden, muss eine sorgfältige Schwachstellenanalyse durchgeführt werden. Eine Schwachstelle ist dabei eine Schwäche des Systems oder ein Punkt, an dem das System verwundbar ist. Eine Verwundbarkeit ermöglicht die unautorisierte Umgehung oder Manipulation von Sicherungsmaßnahmen.

Die folgende Abbildung listet vorhandene Gefährdungsfaktoren auf und kann als Grundlage zur Verschaffung eines ersten Überblicks dienen.

Bild 2.40: Gefährdungsfaktoren[1]

Maßnahmen zum Schutz dienen dazu, Risiken zu vermindern. Dazu müssen Gefahren, also drohende Schadensereignisse, mit ihrer möglichen Schadenshöhe und ihrer Eintrittswahrscheinlichkeit ermittelt werden.

Das von einer Gefahr ausgehende **Risiko** bezeichnet die **Wahrscheinlichkeit,** mit der das schädigende Ereignis eintritt, und die **Höhe des möglichen Schadens,** der dadurch hervorgerufen werden kann.

Auf dieser Grundlage werden die Maßnahmen so ausgestaltet, dass sie das Risiko auf ein akzeptables Maß reduzieren. Dabei sind vor allem die technische und wirtschaftliche Umsetzbarkeit entscheidende Faktoren.

Eine große Bedeutung kommt dem Schutz vor IT-Angriffen zu. Als Grundlage für zu ergreifende Schutzmaßnahmen erfolgt zuerst eine Risikoanalyse. Aus möglichen Zielen und Fähigkeiten potenzieller Angreifer erstellt man Angreifer-Modelle. Dann wird untersucht, welche tatsächlichen Bedrohungen für die Unternehmens-IT relevant sind und wie hoch der potenzielle Schaden bei einem erfolgreichen Angriff ist. Verknüpft mit der Wahrscheinlichkeit für einen erfolgreichen Angriff, erhält das Unternehmen eine Aussage über die Bedeutung der Bedrohung, das Risiko.

[1] *vgl. IT-Grundschutzhandbuch (2001) des Bundesamts für Sicherheit in der Informationstechnik (BSI)*

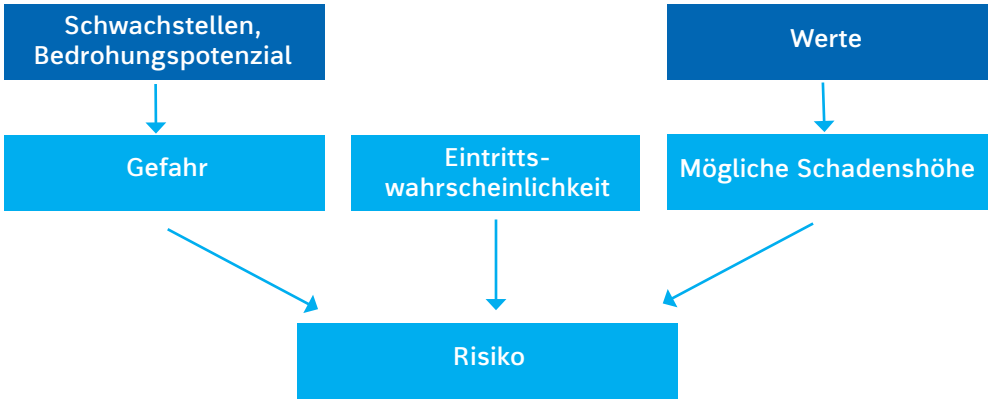


Bild 2.41: Risiko

2.6.3 Verwundbarkeiten

Weist ein System Schwachstellen auf, durch die Sicherungsmaßnahmen unautorisiert umgangen oder manipuliert werden können, ist es verwundbar. Eine erste Einordnung von Verwundbarkeiten geschieht anhand ihrer Wirkungsgrundlage. Kann ein Angreifer physikalische Schwächen des Systems ausnutzen, spricht man von hardwarebasierten Verwundbarkeiten. Ausnutzbare Schwächen in der Informationsverarbeitung durch nachlässige oder fehlerhafte Programmierung werden als softwarebasierte Verwundbarkeiten bezeichnet.

2.6.3.1 Hardwarebasierte Verwundbarkeiten

Hardwarebasierte Verwundbarkeiten entstehen oft durch Fehler im Design. DRAM-Arbeitsspeicher besteht beispielsweise im Wesentlichen aus dicht aneinandergereihten Kondensatoren. Im März 2015 wurde bekannt, dass ein schneller permanenter Zustandswechsel einer Kondensatorzelle den Ladungszustand einer benachbarten Kondensatorzelle in handelsüblichen Arbeitsspeicherbausteinen beeinflussen kann. Diese Verwundbarkeit kann praktisch ausgenutzt werden (*exploit*), um geschützte Speicherbereiche zu beschreiben und auf diese Weise unberechtigt erweiterte Nutzerrechte zu erlangen. Die Verwundbarkeit sowie das Programm zum Machbarkeitsnachweis, ein sogenannter Exploit, wurden unter der Bezeichnung Rowhammer bekannt. Als absoluter **Security-GAU** gelten schwerwiegende Sicherheitslücken im Kernel-Design der meisten Intel- und AMD-Prozessoren, die Anfang 2018 unter den Namen „Meltdown“ und „Spectre“ bekannt wurden. Durch zielgerichtete Angriffsszenarien (sogenannte Side Channel Attacks) kann hierbei sowohl über Betriebssysteme als auch über Treiber und Anwendungssoftware (z. B. Browser) ein Zugriff auf normalerweise geschützte Speicherbereiche erfolgen und Schadcode ausgeführt werden. Trotz Sicherheitsupdates in allen genannten Softwarebereichen (mit teilweise einhergehenden Performance-Verlusten) lässt sich derzeit kein vollständiger Schutz gegen Angriffe auf diese (oder ähnliche, bislang noch nicht festgestellte) Lücken realisieren.

2.6.3.2 Softwarebasierte Verwundbarkeiten

Verwundbarkeiten auf Softwarebasis gehen üblicherweise auf Fehler im Betriebssystem oder in Anwendungsprogrammen zurück. Trotz aller Anstrengungen vieler Softwarehersteller, Fehler in ihren Programmen aufzuspüren und zu beseitigen, werden dennoch

immer wieder neue Verwundbarkeiten bekannt. Betriebssystemhersteller wie Microsoft und Apple stellen monatlich, manchmal sogar im Abstand von wenigen Tagen Updates zur Beseitigung von Verwundbarkeiten bereit.

Software-Verwundbarkeiten lassen sich im Wesentlichen in die folgenden Kategorien einteilen.

- **Puffer-Überlauf (*buffer overflow*)**

  Diese Verwundbarkeit entsteht, wenn die reservierte Länge des Speicherbereichs einer Variablen missachtet wird. Ein solcher Puffer-Überlauf kann beispielsweise dadurch provoziert werden, dass man von einem fünf Elemente umfassenden Feld das zehnte beschreibt. Dadurch werden Speicherbereiche verändert, auf die sonst kein Zugriff besteht. In der Folge kann das zu Systemabstürzen, zur Preisgabe oder Veränderung von geschützten Daten oder zur Veränderung von Nutzerrechten führen.

- **Ungeprüfte Eingaben (*non-validated input*)**

  Programme verarbeiten oft Daten, die vom Nutzer bereitgestellt werden. Die an das Programm übergebenen Daten können bösartiger Natur sein, die das Programm zu einem unbeabsichtigten Verhalten provoziert.

  Betrachtet man ein Bildverarbeitungsprogramm, dann könnte ein Angreifer eine bösartige Bilddatei derart konstruieren, dass sie ungültige Größenangaben enthält. Die bösartig manipulierten Größenangaben könnten das Programm zur Reservierung einer falschen und unerwarteten Speichermenge veranlassen.

- **Kritischer Wettlauf (*race condition*)**

  Ein kritischer Wettlauf entsteht, wenn das Ergebnis einer Operation von der Reihenfolge oder der zeitlichen Abfolge von Einzelereignissen abhängt.

  Kann bei dafür anfälliger Programmierung beispielsweise eine Teiloperation unerwartet verzögert werden, kann dies zu einem unerwarteten Programmablauf, etwa zu einer Endlosschleife (*deadlock*) führen.

- **Schwachstellen der Sicherheitspraktiken**

  Zum Schutz von Systemen und sensiblen Daten können Techniken zur Autorisation, zur Authentifikation und zur Verschlüsselung eingesetzt werden. Software-Entwickler sollten nicht versuchen, eigene Algorithmen zu erstellen, sondern stattdessen auf bestehende Sicherheits-Programmbibliotheken zurückgreifen. Diese wurden bereits umfangreich getestet und überprüft, während die Wahrscheinlichkeit hoch ist, dass durch selbsterstellte Sicherheitsfunktionen neue Sicherheitslöcher entstehen.

- **Zugriffs-Steuerungs-Probleme (*access-control problems*)**

  Die Zugriffs-Steuerung sorgt für die Verwaltung von Rechten für den physikalischen Zugriff auf Ausrüstungsgegenstände sowie die Festlegung von Rechten zur Nutzung von Systemressourcen. Viele Verwundbarkeiten entstehen durch die falsche Vergabe von Zugriffsrechten.

Bildquellenverzeichnis

Umschlagfoto: fotolia.com, New York: (WavebreakmediaMicreo)

Innenteil:

Fotos

123RF.com, Hong Kong: S. 25 (Stian Olsen), 48.2 (Andrey Armyagov), 71 (alexlmx), 77 (Andrii Hrytsenko), 107.1 (radub85), 143.2 (Vitaly Pozdeyev), 144.1 (stieberszabolcs), 144.3 (Vitaly Pozdeyev), 188.1 (Phana Sitti)

Amazon.de: S. 29

Apple Inc., Cupertino, CA, USA: S. 19.3, 30.3, 95, 96, 127, 277, 278.1, 278.2, 278.3, 278.4, 279.1, 279.2, 279.3, 279.4, 280, 285, 286

ASRock Europe B.V., Nijmegen (NL): S. 34.1, 34.2, 103.1

ASUSTeK COMPUTER INC., Taipeh (Taiwan): S. 33.1

Belkin International, Inc., Playa Vista (Kalifornien/USA): S. 126.1, 126.2

Bildungsverlag EINS GmbH, Köln: S. 131.1, 139, 145, 200, 455.1

Bildungsverlag EINS GmbH, Köln/Klaas Gettner, Langerwehe: S. 52, 89.3, 91, 106, 108, 115.1, 115.2, 121.2, 121.3, 128.1

Bildungsverlag EINS GmbH, Köln/Christel Ivo, Maasholm: S. 229.1, 229.2

Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Dortmund: S. 233.2

CANESPA ESD Protection GmbH, Langenhagen: S. 448.1

Compu-Seite.de/Andreas Worblewski, Gelsenkirchen: S.103.2

Delta Tracing Srs., Marcon, Italy: S. 163.1, 163.2

Deus GmbH, Liederbach: S. 184

DGUV Deutsche Gesetzliche Unfallversicherung Spitzenverband, Berlin: S. 225

DIN CERTCO Gesellschaft für Konformitätsbewertung mbH, Berlin: S. 231.1, 231.2

EEPCA, the European Electrical Products Certification Association, Paris: S. 232.1

Europäische Kommission, Brüssel: S. 232.2, 233.1, 237, 238

Europäische Union, „Communauté Européenne“: S. 230

Fluke Deutschland GmbH, Glottertal: S. 392

fotolia.com, New York: S. 228 (Mrkvica)

GIGA-BYTE Technology Co., Ltd., New Taipei City, Taiwan: S. 309, 310.1, 310.2, 311.1, 311.2, 312.1, 312.2

Google Inc., Mountain View (Kalifornien/USA): S. 30.1

Google Inc./Open Handset Alliance (OHA), Mountain View, CA, USA: S. 282, 283.1, 283.2, 284

Hama GmbH & Co. KG, Monheim: S. 122.1, 175.1

Hauppauge Computer Works GmbH, Mönchengladbach: S. 171

HotHardware.com/Dave Altavilla: S. 162.1, 162.2

Intel Corporation, Santa Clara (USA): S. 51

Intel GmbH Munich, Feldkirchen: S. 95

Intertec Holding Deutschland GmbH, Leinfelden-Echterdingen: S. 233.3

Kingston Technology Corporation, Inc., Fountain Valley (Kalifornien/USA): S. 63.1, 63.2, 63.3, 63.4, 72.1, 72.2, 72.3, 72.4

Lenovo, Morrisville (North Carolina/USA): S. 19.1, 19.2

Linux Kernel Organization, Inc.: S. 272, 275.1, 275.2

Littlefuse Europe GmbH, Bremen: S. 488.4

Meinhart Kabel Deutschland GmbH, Herrsching: S. 497

Memphis Electronic AG, Bad Homburg: S. 61

Microsoft Deutschland GmbH, Unterschleißheim: S. 256, 258, 259, 260, 261.1, 261.2, 262, 265, 266.1, 266.2, 332, 333, 337, 338.1, 338.2, 339, 341, 342, 343

MML UG (haftungsbeschränkt), Gummersbach: S. 471.3

Narda STS GmbH, Pfullingen: S. 460

Netzmafia.de/Prof. Jürgen Plate: S. 90.1, 90.2, 90.3, 90.4

Panasonic Industrial Devices Sales Europe GmbH, Hamburg: S. 79

RAL gGmbH, Bonn: S. 229.3

Rainer Lüssi, Bäretswil (CH): S. 465

RFW Elektronik, Idstein: S. 471.4

Samsung Electronics GmbH, Schwalbach/Ts.: S. 19.4, 21

SanDisk Corporation, Milpitas (Kalifornien/USA): S. 64.2

Schurter AG, Luzern (Schweiz): S. 441.1, 441.2, 441.3, 441.4, 441.6, 487.1, 487.2, 487.3, 488.3

SD-3C, LLC, North Hollywood (Kalifornien/USA): S. 64.1

Shuttle Computer Handels GmbH, Elmshorn: S. 14.1, 14.2

shutterstock.com, New York: S. 18 (Evgeny Karandaev), 138 (vetkit), 144.2 (Keih Homan)

Sony Mobile Communications Inc.: S. 30.2

Stiftung Gemeinsames Rücknahmesystem (GRS) Batterien, Hamburg: S. 227.2

stock.adobe.com, Dublin: S. 15.1 (Kenishirotie), 15.2 (Karramba Production), 17.2 (Romain Quéré), 37 (Oleksandr Delyk), 48.1 (Norman Chan), 92.2 (Destina), 98.2 (Ronald), 107.2 (mat), 124 (Alex), 128.2 (yulia-zl18), 143.1 (littlej78), 179 (Lucky Dragon), 182 (Trezvuy), 407.2 (Birgit Reitz-Hofmann), 471.2 (Jultud)

Tragand Handels- und Beteiligungs GmbH, Berlin: S. 109.1, 144.4, 175.2

Transcend Information Trading GmbH, Hamburg: S. 118

TCO Development, Stockholm, Schweden: S. 234.2

TÜV Rheinland LGA Products GmbH, Köln: S. 232.3, 234.1

Udo Schaefer, Aachen: S. 177.2, 472

USB Implementers Forum, Inc., Beaverton (Oregon/USA): S. 17.1

USB Implementers Forum, Inc., San Francisco (Kalifornien/USA): S. 95

Video Electronics Standards Association (VESA), San José (Kalifornien/USA): S. 95

Western Digital Deutschland GmbH, München: S. 137

Wikipedia gemeinfrei: S. 85 (Simon Budig, Larry Ewing, Anja Gerwinski), 272 (Simon Budig, Larry Ewing, Anja Gerwinski)

Wortmann AG, Hüllhorst: S. 26

Yamaha Music Europe GmbH, Rellingen: S.121.1

Zeichnungen

CANESPA ESD Protection GmbH, Langenhagen: S. 448.2

Bildungsverlag EINS GmbH, Köln/Michele Di Gaspare, Bergheim: S. 27, 33.2, 67, 81, 87, 88, 89.1, 89.2, 92.1, 93, 98.1, 98.3, 101, 109.2, 112, 114, 122.2, 147.1, 147.2, 147.3, 150, 153.1, 153.2, 156, 166, 170, 177.1, 183, 186, 188.2, 189, 191.1, 193, 196, 197.1, 197.2, 197.3, 199, 202, 203, 204.1, 204.2, 206, 207, 209, 212, 214.1, 214.2, 215, 216, 217, 221.2, 297, 298, 299, 316, 320, 345.1, 345.2, 345.3, 346.1, 346.2, 346.3, 347.1, 347.2, 361.2, 362.2, 365, 366, 367, 368, 369, 379, 383, 384, 385.1, 385.2, 386.1, 386.2, 387, 388, 389, 390, 391.1, 391.2, 393.1, 393.2, 394.1, 394.2, 394.3, 395.1, 395.2, 395.3, 395.4, 395.5, 396.1, 396.2, 397, 398, 399, 401, 403, 404, 405.1, 405.2, 407.1, 408.1, 408.2, 409, 410.1, 410.2, 412, 413, 414, 415, 416.1, 416.2, 417.1, 417.2, 418.1, 418.2, 418.3, 418.4, 419.1, 419.2, 419.3, 420.1, 420.2, 420.3, 421, 422, 423, 424.1, 424.2, 424.3, 425, 426.1, 426.2, 426.3, 429, 430, 435, 436, 437.1, 437.2, 438, 440.1, 440.2, 441.5, 442.1, 442.2, 443, 445.1, 445.2, 446.1, 446.2, 447, 449, 450.1, 450.2, 450.3, 450.4, 451.1, 451.2, 452.1, 452.2, 455.2, 455.3, 456.1, 456.2, 456.3, 457, 458, 463.2, 464, 466, 467.1, 467.2, 468, 469, 470.1, 470.2, 471.1, 473.1, 473.2, 474.1, 474.2, 474.3, 475, 476, 477.1, 477.2, 478, 479, 480, 481.1, 481.2, 481.3, 482.1, 482.2, 484.2, 486.1, 482.2, 486.3, 487.4, 487.5, 487.6, 488.1, 488.2, 488.5, 490.1, 490.2, 490.3, 491.1, 491.2, 493, 494.1, 494.2, 495.1, 495.2, 496.1, 496.2, 499, 500, 506, 507.1, 507.2, 508, 509.1, 510.2, 511, 512, 513, 514, 515.1, 515.2, 515.3, 516.1, 516.2, 517, 518

PocketPC GmbH, Augsburg: S. 195

Tomshardware.de/Best of Media Publishing Group, Suresnes (Frankreich): S. 194