Grundzüge der Wirtschaftsinformatik

Bearbeitet von
Peter Mertens, Freimut Bodendorf, Wolfgang König, Matthias Schumann, Thomas Hess, Peter Buxmann

12. Auflage 2017. Buch. X, 218 S. Softcover
ISBN 978 3 662 53361 1
Format (B x L): 16,8 x 24 cm

Rechner und deren Vernetzung

P. Mertens, F. Bodendorf, W. König, M. Schumann, T. Hess, P. Buxmann, *Grundzüge der Wirtschaftsinformatik*,
DOI 10.1007/978-3-662-53362-8_2

2.1 Rechner

Ein Rechner besteht i. d. R. aus den Komponenten *Hardware, Betriebssystem* und *Anwendungssoftware* und tritt für den Nutzer in verschiedenen Formen und Varianten in Erscheinung, wie bspw. als PC, mobiles Endgerät oder für den Anwender nicht unmittelbar erkennbar (s. ► Abschn. 2.2.1). Das *Drei-Schichten-Modell* von Hardware, Betriebssystem und Anwendungssoftware charakterisiert grundlegend den Aufbau und die Zusammenarbeit dieser Komponenten eines Rechners vor dem Hintergrund des betrieblichen Einsatzes (vgl. ◘ Abb. 2.1).

Hardware beschreibt alle physischen Geräte und Komponenten, die Rechenprozesse und Datentransfer ermöglichen (s. ► Abschn. 2.1.1).

Software bildet die Voraussetzung für den Betrieb eines Rechners und bezeichnet allgemein in einer Programmiersprache geschriebene Programme, die nach Übersetzung auf einem Rechner ausführbar sind. Man unterscheidet nach dem Kriterium der Nähe zur Hardware bzw. der Nähe zur Anwendung zwischen Betriebssystem einerseits und *Anwendungssoftware* andererseits.

Eine zentrale Anforderung des *Betriebssystems* eines Rechners besteht darin, die physischen Leistungen der Hardware einfacher nutzbar zu machen und für die konkrete Ausführung der Softwareanwendungen zur Verfügung zu stellen. Beispielsweise wäre es unwirtschaftlich, in jedem Anwendungsprogramm eine eigene Druckersteuerung vorzusehen, die Vorkehrungen für den Fall trifft, dass kein Papier mehr verfügbar ist. Darüber hinaus sind vielfältige weitere Verwaltungs- und Überwachungsleistungen zu erbringen, die im Rahmen einer Betriebssystemsoftware zusammengefasst werden.

Die für die spezifische Tätigkeit ausgelegte *Anwendungssoftware* wird in den meisten Fällen auf Basis eines Betriebssystems genutzt und gliedert sich in zwei Klassen: Als *Standardsoftware* bezeichnet man Programme, die nicht für einen einzelnen Anwender, sondern für eine Vielzahl von Kunden mit gleichen oder ähnlichen Aufgaben produziert werden. Demgegenüber wird *Individualsoftware* (z. B. zur Steuerung einer Gepäckbeförderungsanlage) speziell auf den Bedarf eines Benutzers hin entwickelt und kann häufig ohne Anpassungen nicht von anderen Anwendern (andere Abteilungen oder Unternehmen) eingesetzt werden.

2.1.1 Hardware

Unter Hardware versteht man vereinfacht ausgedrückt alle physischen Komponenten und Geräte, aus denen sich ein Computer oder Rechnernetzwerk zusammensetzt, also Instrumente mit z. B. den Attributen Länge und Gewicht.

Ein typischer Arbeitsplatzrechner (PC) besteht aus folgenden Hardwarebestandteilen:

- Prozessor
- Arbeitsspeicher
- interne Festplatte
- Geräte zur Dateneingabe (z. B. Tastatur, Maus, Scanner) und Datenausgabe (Bildschirm, Drucker)

Darüber hinaus verfügt ein solcher Arbeitsplatz zumeist über eine kabelgebundene oder kabellose Netzwerkschnittstelle (z. B. Netzwerkkarte oder WLAN-Modem), wodurch der Computer in ein Kommunikationsnetz eingebunden werden kann (s. ► Abschn. 2.2). Externe Speichermedien wie außerhalb des Gehäuses betriebene Festplatten oder USB-Speichersticks können an einen Rechner angeschlossen werden. Neben stationären Rechner-Arbeitsplätzen haben in den letzten Jahren portable Geräte wie Notebooks, Tablets und Smartphones zunehmend an Bedeutung gewonnen.

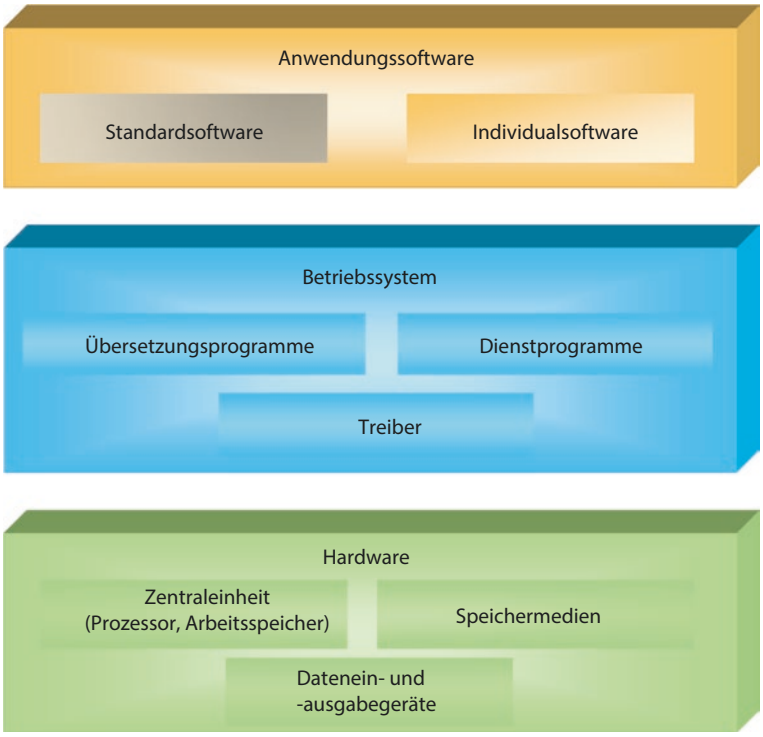

Abb. 2.1 Drei-Schichten-Modell von Rechnersystemen

Der grundlegende Arbeitsablauf eines Rechners beginnt mit der Dateneingabe, z. B. über die Tastatur, optische Lesegeräte oder über das Netz. Diese werden in der Zentraleinheit nach einer Vorschrift, genannt Programm, verarbeitet und anschließend etwa auf einem Bildschirm, Drucker, einem Speichermedium oder über das Netz ausgegeben. Diesen Ablauf bezeichnet man als *Eingabe-Verarbeitung-Ausgabe-Prinzip* (EVA-Prinzip).

2.1.1.1 Zentraleinheit: Prozessor und interner Speicher

Die *Zentraleinheit* eines Rechners besteht aus einem Prozessor (Central Processing Unit, CPU), dem Arbeitsspeicher und einer Schnittstelle für Geräte zur Dateneingabe und -ausgabe. Die Daten und Befehle, die der Prozessor unmittelbar zur Ausführung und Berechnung neuer Daten benötigt, werden temporär im Arbeitsspeicher abgelegt. Hersteller von Mikroprozessoren drücken deren Leistungsfähigkeit i.d.R durch die Maßzahl Gigahertz (GHz) aus, welche die Taktfrequenz des Prozessors angibt. Sie determiniert, wie viele Milliarden Befehle pro Sekunde ausgeführt werden können, erlaubt jedoch keinen direkten Rückschluss auf die Verarbeitungsgeschwindigkeit, denn die interne Verarbeitungsgeschwindigkeit eines Prozessors ist z. B. auch davon abhängig, wie schnell der Arbeitsspeicher operiert und wie schnell zwischen Prozessor und Hauptspeicher kommuniziert werden kann. Diese Komponenten sind mit sog. *Bussen*, die man sich als mehradrige Kabel vorstellen mag, verbunden. Busse dienen in einem System der Verbindung und dem Daten- und Befehlsfluss der Komponenten untereinander. In den letzten Jahren werden PCs zumeist mit *Mehrkernprozessoren* ausgestattet. Hierbei befinden sich auf einem Chip mehrere parallel arbeitende Prozessorkerne.

Der *Arbeitsspeicher* (Random Access Memory, RAM) setzt sich aus direkt adressierbaren Speicherzellen zusammen, die als Speicherworte bezeichnet werden. Bei einem PC besteht ein Wort i. d. R. aus 4 Byte (1 Byte entspricht 8 Bit und stellt eine Ziffer oder einen Buchstaben dar). Hauptspeicherkapazitäten werden in Megabyte (1 MB = 2^{20} Byte) oder Gigabyte (1 GB = 2^{30} Byte) angegeben. Handelsübliche Rechner besitzen heute eine Arbeitsspeicherkapazität von 4 bis 8 GB.

Alle Programme müssen zum Zeitpunkt ihrer Ausführung vollständig oder partiell (mit dem aktuell auszuführenden Teil) im Arbeitsspeicher zur Verfügung stehen. Im zweiten Fall bietet das Betriebssystem die *virtuelle Speichertechnik* an. Dabei lagert es automatisch Programmteile, die nicht mehr in den Arbeitsspeicher geladen werden können (da z. B. andere Programme ebenfalls zur schnellen Abarbeitung im Hauptspeicher abgelegt sein müssen), auf der Festplatte aus und bringt sie nur bei Bedarf in den Arbeitsspeicher, wodurch sich dieser logisch, jedoch nicht physisch vergrößert. Im Gegensatz zu Festplatten, die Daten auch nach Abschalten des Rechners halten, verliert der Arbeitsspeicher bei einer Unterbrechung der Stromzufuhr alle Informationen, die sich gerade in ihm befinden. Daher wird die Speicherform des RAM als „flüchtiger" Speicher bezeichnet.

Beim sog. *In-Memory-Computing* wird primär der Arbeitsspeicher (s. ► Abschn. 3.1.3) als Datenspeicher verwendet und auf diese Weise das stetige und jeweils sehr zeitraubende „Hin- und Herschaufeln" von Daten zwischen Arbeitsspeicher und interner Festplatte vermieden. Dies führt zu höheren Zugriffsgeschwindigkeiten, wodurch z. B. AS, die eine Echtzeit-Datenverarbeitung bedingen, begünstigt werden. Daten werden dann nur bei Bedarf auf die interne Festplatte geschrieben.

In einem Rechner findet sich zusätzlich ein *Festwertspeicher* (Read Only Memory, ROM), der nur gelesen, nicht jedoch verändert werden kann. Festwertspeicher werden i. d. R. vom Hersteller beschrieben und dienen u. a. der Aufbewahrung grundlegender Teile des Betriebssystems, auf die beim Einschalten des Rechners automatisch zugegriffen wird (z. B. hardwarenahe Programme zur Ansteuerung des Bildschirms oder zur Kommunikation mit der Tastatur).

2.1.1.2 Speichermedien

Aufgabe von *Speichermedien* ist, größere Datenmengen langfristig aufzubewahren und ggf. transportabel zu machen. Speichermedien können intern in einem Endgerät verbaut oder als externe, transportable Speichermedien an Schnittstellen am Gerätegehäuse angeschlossen werden. Als nicht-flüchtiger Speicher behalten sie die Daten auch bei Unterbrechung der Stromzufuhr. Die wichtigsten nicht-flüchtigen Speichermedien sind Festplatten, Speicherkarten und optische Speicher.

Eine herkömmliche *Festplatte* (auch als Magnetplatte bezeichnet) weist i. d. R. mehrere übereinander gestapelte Kunststoff- oder Aluminiumscheiben auf, die mit einer magnetisierbaren Schicht überzogen sind. Daten werden in Form von Bitketten in konzentrischen Spuren durch Magnetisierung dargestellt. Der vielfach als interne Festplatte fest im PC-Gehäuse installierte Plattenstapel dreht sich mit konstanter Geschwindigkeit. Auf die Daten greifen Schreib-Lese-Köpfe zu. Magnetplatten für PC besitzen heute i. Allg. eine Speicherkapazität von mehreren Terabyte. In Großrechnersystemen werden Kapazitäten von mehreren Petabyte (1 PB = 2^{50} Byte) erreicht.

Die *Flash-Speichertechnik* verwendet Halbleiter-Speicherbausteine zur Datenspeicherung, in denen, anders als bei konventionellen Festplatten zur Datenabfrage, Speicherbestandteile nicht bewegt werden müssen. Sie ist zudem stromsparender und ermöglicht schnelleren Datenzugriff. Daher finden Flash-Speicher häufigen Einbau in mobilen Endgeräten (s. ► Abschn. 2.2.1). *Solid State Disks* sind Flash-Speicher, die die Funktion einer Festplatte erfüllen und besonders schnelle Zugriffszeiten und Übertragungsraten jenseits derer von Festplatten erreichen können.

Mit dem vergleichsweise höheren Preis pro Speichereinheit werden sie als interne Festplatte in hochwertigen Notebooks verbaut.

Sollen Datenbestände z. B. zwischen nicht vernetzten Rechnern ausgetauscht werden oder Sicherungskopien ausgelagert werden, so greift man auf transportable externe Speichermedien zurück, z. B. USB-Sticks.

Speicherkarten (auch als Flash Card oder Memory Card bezeichnet) sind transportable Speichermedien im Miniaturformat, welche auf der Flash-Speichertechnik basieren und ohne permanente Stromversorgung Daten speichern können. Verbreitete Speicherkartenvarianten sind bspw. die Micro Secure Digital Memory Card (microSD), welche z. B. in Mobiltelefonen zum Einsatz kommt, und die Compact Flash Card (CF), die teilweise in professionellen Digitalkameras verwendet wird. *USB-Massenspeicher* nutzen zumeist ebenfalls die Flash-Speichertechnik, kommunizieren aber über den Universal Serial Bus (USB). Die am häufigsten verwendete Form ist der USB-Stick. USB ist ein Busstandard, der speziell für den Anschluss von Geräten an die externen Schnittstellen eines Rechners entwickelt wurde.

Externe Festplatten sind Magnetplatten oder auf der Flash-Technologie basierende Datenträger in tragbaren Gehäusen, die über USB-Schnittstellen mit einem Rechner oder digitalen Endgerät verbunden werden. Als externe Speichermedien werden sie zur Datensicherung oder kurzfristigen Speicherplatzerweiterung verwendet.

Optische Speicher verlieren im betrieblichen Arbeiten an Bedeutung und finden zunehmend Verwendung als spezieller Datenträger für Multimediainhalte. Daten werden mit einem Laserstrahl auf der unterhalb einer transparenten Schutzschicht liegenden Speicherschicht aufgezeichnet, wobei deren Oberfläche verändert wird. Diese Strukturen sind wiederum mittels Laserstrahl abtastbar. Es werden verschiedene Techniken unterschieden: CD-ROMs (Compact Discs Read Only Memory) haben eine Kapazität von bis zu 700 MB (dieser Wert entspricht ca. 80 Audiominuten als Audio-CD mit Musikdaten in nicht komprimierter Auflösung). Die für komplexe audiovisuelle Anwendungen konzipierte Blu-ray Disc hat die DVD (Digital Versatile Disc, häufig auch digitale Video Disc) größtenteils substituiert. Ihre Speicherkapazität beträgt rund 25 GB. Den Nachfolger der Blu-ray Disc stellt die Ultra-HD Blu-ray Disc dar, welche eine Speicherkapazität von bis zu 100 GB aufweist.

2.1.1.3 Endgeräte zur Datenein- und -ausgabe

Endgeräte als physisch eigenständige Einheiten treten entweder auf Veranlassung des Computers mit dem Nutzer in Aktion oder können als funktionsintegriertes Endgerät Aufgaben unabhängig vom Rechner erfüllen, wie z. B. ein *Drucker* mit Kopier-Funktion.

Um die verschiedenen Komponenten eines Rechners miteinander zu verknüpfen, sind diese mit Schnittstellen ausgestattet. So können der Zentraleinheit Befehle erteilt und Daten ein- und ausgelesen werden. Eine Schnittstelle i. Allg. ermöglicht die Verbindung von Komponenten mit unterschiedlichen Eigenschaften innerhalb eines Systems. Um miteinander kommunizieren und Daten austauschen zu können, werden gemeinsame Standards festgelegt, wie im Falle von Hardwareschnittstellen zum Beispiel ein Protokoll (s. ► Abschn. 2.3.1), das etwa den Ablauf eines sog. Handshakes als Kommunikation zweier Geräte oder Komponenten festlegt, wie beispielsweise das gegenseitige Erkennen als berechtigte Kommunikationspartner. Interne Hardwareschnittstellen verbinden Prozessor, Arbeitsspeicher und interne Festplatte. Endgeräte zur Datenein- und -ausgabe können an internen Schnittstellen als ein Bestandteil eines funktionsintegrierten Endgeräts fest verbaut sein, wie die Tastatur und der Bildschirm eines mobilen PCs (Notebook). Externe Hardwareschnittstellen, z. B. USB, erlauben den Anschluss von Endgeräten außerhalb des Gerätegehäuses, wie etwa einer Maus, oder von externen Speichermedien (s. ► Abschn. 2.1.1.2).

Zu den wichtigsten Endgeräten zur Dateneingabe neben Tastatur und Maus zählen der *Touchscreen*, optische Belegleser und Lesegeräte zur Erfassung von elektromagnetischen Wellen. Bei einem Touchscreen deutet der Benutzer auf ein Objekt auf dem Bildschirm, und optische oder magnetische Sensoren registrieren die Berührung sowie die Positionierung (z. B. bei Smartphones oder bei Geldautomaten). Die Eingabemethode *Multitouch,* deutsch *Mehrfingergestensteuerung*, ermöglicht schnelle Eingabebefehle ohne Maus und Tastatur.

Ein *optischer Belegleser* erfasst genormte Daten, z. B. Bar-, OCR (Optical Character Recognition)- oder QR (Quick-Response)-Code, indem die einzugebende Vorlage abgetastet wird, um Hell-Dunkel-Unterschiede zu erkennen und auszuwerten. Optische Eingabegeräte benutzt man z. B. an Scannerkassen in Supermärkten oder in Kreditinstituten zum Einlesen von Formularen. Eine Variante optischer Belegleser sind Scanner, welche die Vorlage in Bildpunkte zerlegen und als Graubild oder farbig erfassen (z. B. Fotos und Grafiken). Zu Eingabegeräten zählen ebenfalls sog. *RFID (Radio Frequency Identification)-Lesegeräte*, die der Erfassung von elektromagnetischen Wellen dienen, welche von an Gegenständen oder Lebewesen befindlichen RFID-Transpondern ausgesendet werden (s. ► Abschn. 4.3.3.3). Sind zum Beispiel in Bibliotheken Bücher mit *RFID-Transpondern* ausgestattet, so können ganze Stapel auf einmal aus- oder eingebucht werden, ohne dass die Bücher einzeln aufgeschlagen werden müssen, um einen Barcode zu scannen.

Ein weiterer Weg der Befehlseingabe ist die *Sprachsteuerung*, bei der die Stimme des Benutzers durch akustische Sensoren zur Befehlseingabe verwendet wird. Da die Eingabe ohne Blickkontakt des Nutzers zum Bildschirm und ohne Verwendung einer Tastatur erfolgt, eignet sich Sprachsteuerung besonders für mobile Anwendungen.

Die für die betriebliche Informationsverarbeitung wichtigste Ausgabeeinheit ist der *Bildschirm* (Monitor). Neben der Datenausgabe unterstützt er auch die Eingabe, da auf dem Bildschirm z. B. auch Masken zur Datenerfassung und Symbole (Icons) zur Aktivierung von Programmen dargestellt werden. Speziell bei mobilen Endgeräten, wie Smartphones oder Tablets, kombiniert der Bildschirm als Touchscreen die Funktionen eines Eingabe- und Ausgabegeräts. Eine weitere wichtige Ausgabeeinheit ist der *Drucker*. Verwendung finden sowohl Tintenstrahl- als auch Laserdrucker. Der *Tintenstrahldrucker* setzt Zeichen und Grafiken aus Einzelpunkten zusammen und spritzt sie als schnell trocknende Tinte auf das Papier. Beim *Laserdrucker* wird die Seite als Ganzes im Drucker aufgebaut und mittels Toner auf das Papier übertragen.

2.1.2 Betriebssystem

Das Betriebssystem (Operating System) hat die Aufgabe, die zunächst unabhängigen Komponenten (z. B. Zentraleinheit, Drucker, Tastatur) miteinander zu verknüpfen. Betriebssysteme bilden die Verbindung zwischen einem Benutzer bzw. Anwendungsprogramm einerseits und der Hardware andererseits (vgl. Tanenbaum 2009). Bei der Bewältigung eines Benutzerauftrags arbeiten die Komponenten koordiniert zusammen. Betriebssysteme haben folgende Anforderungen zu erfüllen:

- Administration der Benutzeraufträge, Zuordnung von Systemressourcen zu Aufträgen und Überwachung der Programmabläufe (Prozess- und Speicherverwaltung)
- Verwaltung der Hardwarebetriebsmittel (Prozessor, Arbeitsspeicher, Peripheriegeräte)
- Verwaltung des Dateisystems (s. ► Kap. 3)
- Vorhalten einer grafischen Benutzungsoberfläche (Graphical User Interface, GUI)

Betriebssysteme unterstützen das sog. *Multitasking* sowie teilweise auch den Multiuser-Betrieb. Durch Multitasking ist der Rechner in der Lage, Programme parallel auszuführen. Beispielsweise

ist es möglich, einen Text zu bearbeiten, während die Maschine dann, solange sie auf die nächste Eingabe wartet, im Hintergrund eine Kalkulation durchführt. Darüber hinaus spricht man von *Multithreading*, wenn es ein Betriebssystem zulässt, dass in einem Programm ein Prozess aus mehreren Teilprozessen (Threads) besteht, die parallel ausgeführt werden können, z. B. bei umfangreichen Grafikberechnungen. *Multiuser-Betrieb* liegt vor, wenn von einem zentralen Rechner mehrere Terminals und damit mehrere Anwender quasi-parallel bedient werden. Beim Singleuser-Betrieb wird hingegen nur ein Nutzer versorgt.

Für Personal Computer werden zurzeit am häufigsten Betriebssysteme der Firma *Microsoft* (MS) verwendet, die sich zu einer Art inoffiziellem Standard entwickelt haben. Windows 10 gestattet die Verwendung für verschiedene Rechnerklassen wie z. B. Desktop-Computer und mobile Endgeräte (s. ► Abschn. 2.2.1), was unter anderem bei der Gestaltung der Elemente der Benutzungsoberfläche berücksichtigt wurde. *Unix-Systeme* erlauben den Multitasking- und den Multiuser-Betrieb. Zudem verfügen einige Varianten über eine integrierte Softwareentwicklungsumgebung. Der Terminus Unix suggeriert eine Einheitlichkeit, die aber so am Markt nicht auffindbar ist. Es existieren verschiedene Versionen und herstellerspezifische Implementierungen (z. B. AIX von IBM oder Mac OS X von Apple). Eine Besonderheit im Umfeld der *Unix-Derivate* sind *Linux-Betriebssysteme*, deren Quellcode im Gegensatz zu kommerziellen Systemen jedermann frei zugänglich ist (s. auch Open-Source-Software, ► Abschn. 5.1.1.2). Dies bietet z. B. Spezialisten die Möglichkeit, eigene Modifikationen vorzunehmen, das Programm auf Sicherheitsbedrohungen hin zu überprüfen und sich an der Weiterentwicklung des Betriebssystems zu beteiligen.

Betriebssysteme werden oftmals bereits mit einer Vielzahl von *Dienstprogrammen* ausgeliefert. Dienstprogramme sind im Gegensatz zu Anwendungsprogrammen (s. ► Abschn. 2.1.3) Teil der Betriebssystemsoftware. Dienstprogramme stellen grundlegende systemnahe Funktionalitäten zur Verfügung, welche die Abwicklung häufig wiederkehrender anwendungsneutraler Aufgaben unterstützen. Dazu zählen etwa Sortier- und Suchroutinen, (benutzungsfreundliches) Kopieren von Dateien sowie Datensicherung und -wiederherstellung.

Auch *Treiber* zum Betrieb gängiger Typen externer Geräte sind im Betriebssystem enthalten oder können durch eine Aktualisierungsfunktion (Update) über eine Internetverbindung von den Servern des Herstellers heruntergeladen und automatisch installiert werden. Unter einem Treiber (Driver) versteht man ein Programm, das als Übersetzer zwischen den Protokollen (s. ► Abschn. 2.3.1) verschiedener Funktionseinheiten oder einer Programm- und einer Funktionseinheit fungiert. Zum Beispiel werden die von einem Rechner an einen Drucker gesendeten Signale durch den Treiber vorher in ein dem Drucker verständliches Format umgewandelt.

Ein Rechner einschließlich Betriebssystem wird installiert, um den Anwender bei der Lösung seiner Fachaufgabe (z. B. Buchhaltung, Planung) zu unterstützen. Daher muss nun, aufbauend auf der Betriebssystemschnittstelle, ein AS konstruiert werden, das dies leistet. Die Gestaltung derartiger AS (wie auch des Betriebssystems selbst) erfolgt mittels Programmiersprachen. Unter einer Programmiersprache versteht man eine formale, künstliche Sprache, mit der eine auf einer Hardware ablauffähige Software entwickelt werden kann. Mit einer *Programmiersprache* legen Programmierer fest, wie eine Aufgabe durchzuführen bzw. ein Problem zu lösen ist. Die entwickelten Programme bestehen aus einer Menge von Anweisungen (Befehlen) und Ablaufstrukturen, die eine sequenzielle oder parallele Ausführung der Anweisungen festlegen. Verbreitete Programmiersprachen sind z. B. C, C# (gesprochen „C sharp“) und C++ (zur Entwicklung von Anwendungsprogrammen für gängige Desktop-Betriebssysteme), Java (z. B. zur Entwicklung von Android Apps – s. ► Abschn. 2.2.1), Swift und Objective C (zur Entwicklung von Mac OS-Anwendungsprogrammen und Apps für iOS, dem Betriebssystem für mobile Endgeräte von Apple, s. ► Abschn. 2.2.1). Daneben gibt es Abfragesprachen für Datenbanksysteme, wie z. B. SQL

(Structured Query Language). *Softwareschnittstellen* erlauben die Zusammenarbeit zwischen verschiedenen Softwareprogrammen und die Einbindung unterschiedlicher Softwarekomponenten zu einem Produkt, indem sie einen einheitlichen Austausch von Daten und Befehlen ermöglichen.

Die Hardware eines Rechners ist jedoch nicht unmittelbar in der Lage, Anweisungen einer Programmiersprache (*Quellcode*) zu „verstehen". Die Übersetzung eines Quellcodes in eine maschinenlesbare Form (*Maschinencode*) erfolgt durch einen Compiler oder einen Interpreter. *Compiler* übersetzen das gesamte Quellprogramm „in einem Stück" (Batch). Sie prüfen vor der Übertragung das vorliegende Programm auf Syntaxfehler, z. B. ob nach einer „Klammer auf" auch die „Klammer zu" folgt. Im nächsten Schritt wird das Programm übersetzt (kompiliert). *Interpreter* erzeugen dagegen keinen archivierbaren Maschinencode. Vielmehr wird jeder Befehl einzeln abgearbeitet, d. h. schrittweise übersetzt und sofort ausgeführt.

2.1.3 Anwendungssoftware

Ein *Anwendungsprogramm* (engl. „Application Software") – häufig auch AS – verwendet die Ressourcen des Betriebssystems und der zugrunde liegenden Hardware. In der Alltagssprache hat sich außerdem die etwas unglücklich gewählte Bezeichnung „Applikation" eingebürgert. Hiervon ist des Weiteren der Begriff „App" abzugrenzen, welcher eine Kurzform von Application darstellt. Mit Apps sind i. d. R. Anwendungsprogramme für Smartphones und Tablets (s. ► Abschn. 2.2.1) gemeint.

2.1.3.1 Standardsoftware

Standardsoftware umfasst Produkte, die für den Massenmarkt konzipiert wurden. In der Regel werden sie mit Selbstinstallationsroutinen ausgeliefert und ermöglichen oft nur geringe, bei komplexeren Produkten (z. B. funktionsorientierter Software) jedoch auch größere Anpassungen (*Customizing*, s. ► Abschn. 5.2.3.2) an die individuellen Bedürfnisse.

Basissoftware

Basissoftware stellt grundlegende systemnahe Funktionalitäten zur Verfügung, die unabhängig von spezifischen Arbeitsgebieten genutzt werden, wie z. B. Firewalls (s. ► Abschn. 2.4), Virenscanner (entdeckt und beseitigt ggf. Schadsoftware), Komprimierungsprogramme (zur Minimierung der Größe einer Datei) und Browser. Als Browser werden allgemein Programme bezeichnet, die eine Suche nach Dateien und deren Platzierung in einer Verzeichnishierarchie ermöglichen (z. B. Windows Explorer). Der Aufbau der Verzeichnisse wird durch Baumstrukturen visualisiert. Wird ein Browser darüber hinaus zur audiovisuellen Darstellung von HTML-Seiten im World Wide Web (WWW) (s. ► Abschn. 2.3.2) verwendet, so spricht man von einem Webbrowser. Der Benutzerzugriff erfolgt durch die Angabe einer URL (Uniform Resource Locator, bspw.: http://www.is-frankfurt.de). Aus Wettbewerbssicht sind zum Vermeiden von Angebotsmonopolen für verschiedene Funktionalitäten der Basissoftware Installationen von Software anderer Anbieter möglich.

Standardbürosoftware

Standardbürosoftware umfasst Programme zur Textverarbeitung (etwa MS Word), zum Erstellen von Präsentationen (z. B. MS PowerPoint), zur Tabellenkalkulation (z. B. MS Excel), zur E-Mail-Kommunikation (inkl. Adress- und Kalenderverwaltung, z. B. MS Outlook) sowie zur Datenbankverwaltung (s. ► Abschn. 3.1). Darüber hinaus sind am Markt integrierte Standardbürosoftwarepakete verfügbar, die Textverarbeitung, Tabellenkalkulation, grafische Bearbeitung

und auch eine Datenbank unter einer einheitlichen Benutzungsoberfläche anbieten (z. B. MS Office oder OpenOffice).

Funktionsorientierte Software

Als funktionsorientierte Standardsoftware werden Lösungen bezeichnet, die aus betriebswirtschaftlicher Sicht eine Funktion unterstützen. Funktionsübergreifend werden mehrere Anwendungsbereiche (z. B. Vertrieb, Materialwirtschaft, Produktion, Finanzwesen und Personalwirtschaft) und deren Prozesse unterstützt. Man spricht dann von funktionsübergreifender integrierter Standardsoftware, welche sich in Module gliedert, die auf eine gemeinsame Datenbasis zugreifen (vgl. Keller 1999). Dieser Aufbau bietet aus Sicht des Anwenders den Vorteil, dass er Software nur für die von ihm benötigten Problemstellungen betreiben muss. Er kann also z. B. Module für die Durchlaufterminierung und den Kapazitätsausgleich im Rahmen der Produktionsplanung und -steuerung erwerben, ohne die Werkstattsteuerung anschaffen zu müssen (s. ► Abschn. 4.4.1.3). Der modulare Aufbau ermöglicht zudem eine schrittweise Einführung neuer Systeme und somit ein langsames Ablösen von Altsystemen. Die Anpassung einer solchen Standardsoftware an spezifische Einsatzbedürfnisse in Unternehmen erfolgt durch das Customizing (s. ► Abschn. 5.2.3.2), ohne dass eine Veränderung des Quellprogramms stattfinden muss. Darüber hinaus werden auch Schnittstellen für individuelle Erweiterungen angeboten.

Eine Ausprägung funktionsorientierter und funktionsübergreifender Software sind sog. *ERP-Systeme* (Enterprise-Resource-Planning-Systeme). Der Begriff ist sehr verbreitet, aber unglücklich gewählt, da diese Systeme gerade beim Umgang mit knappen Ressourcen, z. B. Produktionsengpässen, oft Schwächen aufweisen oder der Funktionsumfang in seiner Komplexität den Nutzer beim Einsatz überfordern kann. Auch die Nutzungsgestaltung kann in ihrer Komplexität den Anwender überfordern. Die beiden weltweit größten Anbieter kommerzieller ERP-Systeme sind SAP und Oracle.

Prozessorientierte Software

Die Grenze zwischen *prozessorientierter* und *funktionsübergreifender Software* ist fließend (vgl. ◘ Abb. 4.2 und 4.18). In erstgenannten Systemen sind Prozesse quer durch unterschiedliche Funktionsbereiche eines Unternehmens zu integrieren. Die Realisierung erfolgt häufig unter Verwendung von zentralen Datenbanken. Sog. *Workflow-Management-Systeme* (WMS, s. ► Abschn. 4.2.2) unterstützen durch verschiedene Funktionalitäten die Beschreibung und Modellierung von Geschäftsprozessen, z. B. Vorgänge zur Erstellung und Abgabe eines Angebots in der chemischen Industrie oder in einer Versicherung.

Systeme zur Unterstützung verteilten Arbeitens sind z. B. *Workgroup-Support-Systeme*. Diese werden im Gegensatz zu den WMS zumeist bei der Bearbeitung einer relativ unstrukturierten Aufgabe eingesetzt. Die Kooperation basiert auf Netzwerkarchitekturen mit zugehörigen Kommunikationssystemen, wie:

- Konferenzplanungssystemen: Terminvereinbarung, Ressourcenverwaltung (Besprechungsräume, Präsentationsgeräte),
- Computerkonferenzsystemen: Diskussionen zwischen räumlich getrennten Personen (z. B. Videokonferenzsystem),
- Gruppenentscheidungsunterstützungssystemen (Mehrbenutzerumgebungen, z. B. zur gezielten Kompromissfindung bei Verhandlungen) und
- Mehrautorensystemen (Co-Authoring): Werkzeuge zur gleichzeitigen Bearbeitung von Dokumenten (Texten, Plänen, Konstruktionszeichnungen, Grafiken) durch mehrere Teammitglieder.

2.1.3.2 Individualsoftware

Unter *Individualsoftware* versteht man AS, die für eine spezielle betriebliche Anforderung mit der zugehörigen Hard- und Softwareumgebung individuell angefertigt wurden. Die Individualsoftware wird entweder selbst produziert oder fremdbezogen (zu Kriterien für diese Entscheidung s. ► Abschn. 5.1.4). Die Eigenentwicklung kann sowohl von der IT-Abteilung als auch von den entsprechenden Fachabteilungen, dort i. d. R. mit Tabellenkalkulation und Datenbankabfragen (s. ► Abschn. 3.1.2), durchgeführt werden. Aufgabe ist hier, die Entwicklung von Anwendungssoftware als Einzelfertigung technisch und finanziell zu beherrschen (s. ► Abschn. 5.1.2).

Wegen der hohen Entwicklungskosten von Individualsoftware ist ein zunehmender Trend hin zu Standardsoftware zu beobachten. Demgegenüber wird Individualsoftware häufig eingesetzt, um etwa solche Prozesse zu steuern, mit welchen sich ein Unternehmen von seinen Wettbewerbern positiv unterscheidet.

2.1.3.3 Komponentenarchitekturen

Die zunehmende *Modularisierung* von AS, die aus Gründen der erhöhten Wiederverwendbarkeit und leichteren Veränderbarkeit der Bausteine verfolgt wird, lässt die Grenze zwischen Individual- und Standardsoftware schwinden. Komponentenbasierte AS werden aus einzelnen Bausteinen individuell zusammengestellt. Eine *Softwarekomponente* ist ein *Codebaustein* mit Softwareschnittstellen, Attributen (Eigenschaften) und Verhalten (Funktionalitäten). So können die Komponenten zwar als Standardsoftware bezeichnet werden; da sie jedoch erst in einer spezifischen Zusammenstellung die gewünschte Funktion erfüllen, ist das resultierende AS keine Standardsoftware im eigentlichen Sinne mehr.

Die Integration der Komponenten zu AS erfolgt in Komponentenarchitekturen (auch: Komponentenframeworks). Diese spezifizieren einerseits, wie Schnittstellen der Komponenten aufgebaut sein müssen. Andererseits bieten sie eine Plattform als Laufzeitumgebung (Funktionalität zur Ausführung von Maschinencode), die den Betrieb des AS – also das konsistente Zusammenspiel der Komponenten – steuert und verwaltet sowie u. a. Sicherheitsmechanismen, Datenbankverbindungen, Benutzungsschnittstellen und die Speicherverwaltung bereitstellt. Aus Entwicklersicht besteht die Aufgabe darin, die Anwendungslogik (auch: Geschäftslogik oder Prozesslogik) in Form spezifischer Kombinationen vorgefertigter Bausteine zu programmieren (oder fremd zu beziehen, s. ► Abschn. 5.1.3). Dabei ist es nicht erforderlich, die Komponenten auf dem gleichen Rechner zu betreiben.

Zwei weit verbreitete Architekturen bzw. Plattformen zur Entwicklung komponentenbasierter AS sind die Java Platform Enterprise Edition (Java EE) von Oracle und das.NET-Framework von Microsoft.

Java EE bietet ein *Komponentenmodell* auf Basis der Programmiersprache Java an: Die Anwendungslogik wird in Enterprise Java Beans (EJB) gekapselt. Als Laufzeitumgebung bietet Java EE einen sog. Container, der die Komponenten verwaltet und z. B. die Kommunikation mit Benutzungsschnittstellen ermöglicht.

Das *.NET-Framework* stellt ein mit Java EE vergleichbares Konzept dar, lässt jedoch die Entwicklung in zahlreichen Programmiersprachen zu. Dafür ist dieses Framework jedoch nicht plattformneutral wie Java, sondern auf eine Anwendung im Umfeld von Microsoft-Betriebssystemen ausgerichtet.

2.2 Vernetztes Arbeiten: Rechnernetze und Netzarchitekturen

An sich unabhängig arbeitsfähige Rechner werden über Kommunikationspfade miteinander zu einem *Rechnernetz* verbunden, um mehrere Entscheidungsträger (Menschen oder Maschinen) in gemeinsame verteilte Steuerungs-, Dispositions- oder Planungsprozesse einzubinden. Beispiele sind verschiedene Formen der *zwischenbetrieblichen Integration* (z. B. elektronischer Datenaustausch im Rahmen des Supply-Chain-Managements (SCM) in ► Abschn. 4.8) oder der Zugriff auf externe Datenbanken (z. B. bei der Patentrecherche). Ebenso werden Maschinen, beliebige Endgeräte mit Datenschnittstellen oder Sensoren in Netzwerken eingebunden. Die wichtigsten Komponenten eines Rechnernetzes sind:

- die Rechner selbst, einschließlich der physischen Netzwerkanbindung (Netzwerkkarte oder Modem) sowie der jeweiligen Betriebs-, Netz- und Anwendungssoftware,
- die Verbindungs- und Kommunikationskomponenten in und zwischen Netzen (Switches und Router),
- die Datenübertragungswege sowie
- die Protokolle.

Verbindungs- und *Kommunikationskomponenten* bezeichnen spezielle Geräte, deren Aufgabe in der Einbindung von Rechnern in Netze, der Verknüpfung von Netzen sowie hierauf aufbauend der intelligenten Weiterleitung von *Datenpaketen* liegt. Man bezeichnet sie häufig als Vermittlungsknoten. Switches sind die zentralen Punkte in einem lokalen Netzwerk (s. ► Abschn. 2.2.3.1), die Rechner miteinander verbinden. Die Verbindung erfolgt über eine Reihe von Anschlüssen, sog. Ports. Die in einen Port eingehenden Datenpakete werden über die Switches an den Zielport bzw. Zielrechner übertragen. Router können unterschiedliche Netze miteinander verbinden; z. B. kann ein lokales Netzwerk an das Internet angeschlossen werden.

Daten werden auf Datenübertragungswegen (Leitungen oder Funkstrecken) übermittelt. Die gängigsten Übertragungskanäle sind verdrillte Kupferkabel, Glasfaserkabel, Radiowellen (Mobilfunk, *Wireless LAN* (WLAN), Bluetooth, Infrarot- und Laserwellen (optischer Richtfunk)).

Protokolle definieren sämtliche Vereinbarungen und Verfahren, die zur Kommunikation zwischen Rechnern beachtet werden müssen. Die in der Praxis am weitesten verbreitete *Protokollfamilie TCP/IP* (Transmission Control Protocol/Internet Protocol) spielt v. a. im Internet eine große Rolle (s. ► Abschn. 2.3.1).

2.2.1 Rechnerklassen und mobile Endgeräte

Für die Gestaltung der betrieblichen Rechner- und Netzinfrastruktur sind neben dem PC und den Endgräten zur Datenein- und -ausgabe weitere Rechnerklassen und Endgerätetypen relevant, von denen die wichtigsten im Folgenden vorgestellt werden.

Der *Großrechner* (Host oder auch Mainframe) bietet durch seine großen Rechen- und Speicherkapazitäten eine hohe Verarbeitungsgeschwindigkeit im Multiuser-Betrieb an. In größeren Unternehmen werden oft mehrere Hosts in einem Netz verbunden, z. B. um hohe Leistungsbedarfe der Anwender befriedigen zu können oder eine gewisse Sicherung gegenüber Systemausfällen zu erhalten. Neuinstallationen von Großrechnersystemen werden überwiegend zugunsten von PC-Netzen in Clustern verworfen.

Workstations sind prinzipiell als selbstständige Arbeitsplatzrechner konzipiert, deren Leistungsfähigkeit zunächst unterhalb von Großrechnern einzuordnen ist. Die Leistung von Workstations kann durch die Verwendung im Verbund – typischerweise vernetzt zu einem Local Area Network (LAN, s. ► Abschn. 2.2.3.1) – in sog. Workstation-Farmen zur Lastverteilung auf momentan freie Kapazitäten erhöht werden.

Als eine weitere Rechnerklasse werden häufig *Netzwerkcomputer* (NC) und *Thin Clients* diskutiert. Dies sind preisgünstige Rechner mit einer geringeren Leistungsfähigkeit, die man speziell für den (Client-) Betrieb in Netzen (s. ► Abschn. 2.2.2) konzipiert hat. NC bzw. Thin Clients nutzen über das Netz AS, die auf einem entfernten Server ablaufen. Im Idealfall kommt ein solches System ohne Festplatten aus. Durch die zentrale Administration (z. B. in einem Rechenzentrum) werden zudem die Kosten für die Pflege der Systeme reduziert.

Daneben nutzt der Außendienst häufig Notebooks als *transportable Endgeräte* für die Anbahnung der Kundengespräche sowie die Beratung.

Mobile funktionsintegrierte Endgeräte wie Smartphones und Tablets erlauben ortsunabhängiges Arbeiten entkoppelt von stationären Arbeitsplätzen und reglementierten Arbeitszeiten, z. B. bei manuellen Bestandskontrollen in Warenlagern oder außerhalb des Betriebsgeländes im Außendienst sowie auf Geschäftsreisen. Ausgestattet mit einem Touchscreen zur integrierten Datenein- und -ausgabe sowie Schnittstellen zu Datenaustausch und Kommunikation über Mobilfunknetze und WLAN ist dieser Typ Endgerät auf die vernetzte mobile Anwendung ausgelegt, ergänzt durch ein handliches, tragbares und stabiles Gehäuse mit niedrigem Gewicht. Im Vergleich zu konventionellen Rechnern werden in mobilen Endgeräten System-on-a-chip (SOC)-Architekturen verbaut, die Prozessor, Arbeitsspeicher und eine Graphic Processing Unit (GPU) auf einem Chip integrieren. Als Speichermedien werden intern Flash-Speicher genutzt (s. ► Abschn. 2.1.1), zum externen Anschluss sind je nach Hersteller und Produkt Schnittstellen zur Verwendung von microSD-Speicherkarten und USB-Geräten vorhanden. Das meistverbreitete Betriebssystem für mobile Endgeräte ist das auf Linux (s. ► Abschn. 2.1.2) basierende Android, das von einem durch Google gegründeten Konsortium verschiedener Unternehmen entwickelt wird. Apple liefert seine Mobilgeräte mit dem auf Unix basierendem Betriebssystem iOS aus. Seit Windows 10 bietet Microsoft für Mobilgeräte und konventionelle Rechner ein einheitliches Betriebssystem an.

Smartphones sind zum Alltagsgegenstand geworden, da sie sich mit verschiedenen mobilen Dienstleistungen sowie größerem Funktionsumfang vom klassischen Mobiltelefon zu einem vielseitigen tragbaren Rechner einschließlich Internetbrowser, Navigationsgerät und Multimediaplayer entwickelt haben. *Tablet-PCs* erweitern den Vorteil der Tragfähigkeit von Notebooks durch geringeres Gewicht, ein flacheres Gehäuse (Tafel, englisch: tablet) sowie die Entbehrlichkeit von Maus oder Tastatur zur Dateneingabe aufgrund des großflächigen Touchscreens. Wesentliches Merkmal mobiler Endgeräte ist die einfach zu bewerkstelligende individuelle Anpassung der Funktionen durch die Installation von *Apps*. Apps sind Anwendungsprogramme, die mit wenigen, gezielt ausgewählten Funktionen sowie per Touchscreen eine spezialisierte Aufgabe auf einem tragbaren Gerät benutzungsfreundlich und schnell bewerkstelligen. Angeboten werden Apps dem Anwender entweder kostenlos (außer dem Aufwand für mobilen Datenaustausch) oder zum Kauf zumeist auf einem zentralen Online-Marktplatz. Die Funktionseigenschaften von mobilen und stationären Geräten gleichen sich zunehmend einander an, da Rechen- und Speicherleistungen auf technisch immer kleinerem Raum verwirklicht werden.

Im Gegensatz zu den zuvor aufgeführten Rechnerklassen besteht bei mobilen Endgeräten verstärkt die Herausforderung, dass nicht nur betrieblich bereitgestellte Endgeräte, sondern

auch z. B. private Tablets oder Smartphones zunehmend zu betrieblichen Zwecken eingesetzt werden. Die Integration privater portabler Endgeräte in die Rechner- und Netzinfrastruktur von Unternehmen wird als *Bring Your Own Device* (BYOD) bezeichnet (vgl. Disterer und Kleiner 2013). Organisationsrichtlinien regeln, auf welche Art und Weise das private Gerät das Unternehmensnetzwerk sowie Firmendaten nutzen darf, wobei auch rechtliche und sicherheitsbezogene Anforderungen z. B. bezüglich Lizenzrecht oder Datenschutz berücksichtigt werden müssen (s. ► Abschn. 2.4.2). Durch eine gewisse Wahlfreiheit der Geräte kann auf persönliche Bedürfnisse der Mitarbeiter besser eingegangen werden, sodass deren Zufriedenheit und Motivation steigt. Kritisch am BYOD-Ansatz wie an mobilem Arbeiten i. Allg. wird eine mögliche Verschmelzung von Berufs- und Privatleben im Hinblick auf eine ständige Verfügbarkeit gesehen. Zudem wirkt BYOD der Standardisierung, Konsolidierung und Komplexitätsreduktion der IT-Infrastruktur entgegen. Das *Corporate-Owned-Personally-Enabled* (COPE)-Konzept beschreibt den gegenteiligen Ansatz, bei dem ein betriebseigenes Endgerät auch zur privaten Nutzung freigestellt wird.

Embedded Systems sind spezialisierte Rechner, welche Teile eines größeren Systems oder eines Gerätes darstellen und gewisse Aktivitäten in ihrer Umgebung steuern. Charakteristisch für diese Systeme ist, dass sie nicht in erster Linie als Computer wahrgenommen werden, sondern z. B. Komponente eines per Programmüberwachung betriebsoptimierten Verbrennungsmotors sind. Sie sind i. d. R. derart spezialisiert, dass sie kein Betriebssystem benötigen, sondern nur Anwendungsprogramme zur Erfüllung ihrer Funktion beinhalten. Mittels eingebetteter Systeme kann z. B. die Stromqualität in Kraftwerken und anderen Industriebetrieben überwacht werden, um großen Schäden bei Spannungsschwankungen vorzubeugen. Viele Geräte für den alltäglichen Gebrauch sind bereits mit solchen Systemen ausgestattet: Eingebettete Steuerungschips regeln die Kühlleistung in Kühlschränken anstelle mechanischer Regulation, melden den fertigen Waschgang einer Waschmaschine per Vernetzung an ein mobiles Endgerät oder finden sich zur automatischen Steuerung von Antiblockiersystemen (ABS) in Kraftfahrzeugen. Auch diese Systeme sind damit in Netzwerke eingebunden. Gleiches gilt für Fahrzeuge, deren Daten z. B. an Automobilhersteller übertragen werden können oder bei denen das übermittelte Fahrverhalten Einfluss auf die Versicherungsprämie hat (s. ► Abschn. 7.4.1). Selbst Messwerte von Sensoren können so über das Internet ausgelesen werden. Man spricht dabei auch vom „*Internet der Dinge*".

2.2.2 Client-Server-Konzept als Kooperationsmodell

Die Kommunikation zwischen Rechnern setzt die Existenz eines geeigneten *Kooperationsmodells* voraus, das im Hinblick auf die Partner eine eindeutige Rollenverteilung festlegt und die gemeinsamen Protokolle spezifiziert. Im Client-Server-Konzept versuchen auf der Benutzerseite *Clients*, von einem bestimmten Rechner im Netz (Server) angebotene Dienste (z. B. Daten und Transaktionen eines AS) in Anspruch zu nehmen. Aufgaben des Clients sind die Präsentation der entsprechenden Daten und die Interaktion mit dem Benutzer. Dieses Kooperationsmodell lässt sich auch mehrstufig umsetzen. So können etwa Datenbank- und Applikationsserver auf unterschiedlichen Rechnern implementiert werden, um die Arbeitslast zu verteilen. Die Clients nehmen einen Dienst des *Applikationsservers* in Anspruch, der wiederum die benötigten Daten von einem *Datenbankserver* erfragt.

In großen Netzwerken dienen verschiedene Rechner sowohl als Clients als auch als Server, was als *Peer-to-Peer-Kommunikation* (Kommunikation unter Gleichgestellten) bezeichnet wird und somit eine Kombination beider Rollen darstellt (s. ► Abschn. 4.4.5.1).

2.2.3 Netzklassen

2.2.3.1 Lokale Netze

Befinden sich die miteinander vernetzten Rechner in einem Büro, einem Haus oder einem Betriebsgelände, so spricht man von einem lokalen Netz (Local Area Network, LAN). Dieses wird häufig von unternehmenseigenen Netzabteilungen betrieben. In nicht kabelgebundenen *LANs* (Wireless Local Area Network, WLAN) können mobile Endgeräte wie Notebooks mittels Funktechnik über stationär installierte „Access Points" in einem Netz kommunizieren. Sie sind in der Regel an ein (kabelgebundenes) LAN angeschlossen.

2.2.3.2 Weitverkehrsnetze

Geografisch weit auseinander liegende lokale Rechner oder Rechnernetze können über *Weitverkehrsnetze* (Wide Area Network, WAN) miteinander verbunden werden. Wir unterscheiden zwischen geschlossenen WANs mit Zugangssicherungsverfahren für spezielle Benutzergruppen und öffentlichen WANs wie dem Internet (s. ► Abschn. 2.3). Als technische Infrastruktur nutzt man Kabel- und Funkverbindungen, die innerhalb verschiedener (Netz-) Dienste Anwendung finden.

Asymmetric Digital Subscriber Line (ADSL) ist ein digital arbeitender Telekommunikationsdienst, der auf herkömmlichen Telefonleitungen Daten in Bitform mit einer Empfangsgeschwindigkeit bis zu 16 Mbit/s überträgt. Mit *Very High Speed Digital Subscriber Line* (VDSL) wird ein Verfahren der Datenübertragung bezeichnet, das im Vergleich zu ADSL höhere Übertragungsraten zwischen Vermittlungsstelle und Teilnehmerendeinrichtung (z. B. PC, Workstation) zur Verfügung stellt (VDSL2 bis zu 100 Mbit/s) und für die Verwendung in hybriden Glasfaser- und Kupfernetzen ausgelegt wurde. Die Nutzung von *Mobilfunknetzen* basiert auf eigens dafür entwickelten Systemen. Das weltweit erfolgreichste Mobilfunksystem ist das *Global System for Mobile Communications* (GSM). Die (mobilen) Funknetze der ersten und zweiten Generation bauen auf den Architekturen traditioneller Telefonnetze auf und sind daher vor allem für den leitungsvermittelten Sprachdienst konzipiert. Durch den enormen Erfolg des Internets erhöhte sich auch die Nachfrage nach paketvermittelnden Technologien im Mobilfunk (auf Paketvermittlung wird in ► Abschn. 2.3.1 näher eingegangen). *General Packet Radio Service* (GPRS) stellt einen Zwischenschritt hin zu einer flexiblen und leistungsfähigen Datenübertragung in Mobilfunknetzen dar. *Universal Mobile Telecommunications System* (UMTS) ist die Technologie der dritten Generation 3G, die mobilen Endgeräten durch neue Übertragungsverfahren, wie dem *High Speed Downlink Packet Access* (HSDPA), breitbandige Datenübertragung ermöglicht, sodass auch multimediale Inhalte, wie etwa Videoclips, übertragen werden können. *Long Term Evolution* (LTE) ist die Weiterentwicklung des Mobilfunkstandards 3G mit höheren Datenübertragungsraten bis zu 300 Megabit pro Sekunde.

Als *Hochleistungsnetz* oder Backbone werden zentrale Übertragungsstrecken bezeichnet, die Daten aus unterschiedlichen Subnetzen bündeln und weiterleiten. Sie verfügen über hohe Übertragungskapazitäten und garantieren den reibungslosen nationalen bis transkontinentalen Datenverkehr.

2.2.4 Kommunikationsstandards und Webservices

Die Grundlage jeglicher Interaktion und Koordination betrieblicher Aufgaben und Prozesse ist eine effiziente Kommunikation. Damit diese funktionieren kann, müssen sich Sender und Empfänger einer Nachricht ex ante auf eine gemeinsam genutzte Sprache bzw. einen *Kommunikationsstandard* einigen.

Zum Informationsaustausch hat sich die *Extensible Markup Language* (XML, s. auch ► Abschn. 2.3.2) als Standardstrukturierungssprache etabliert. XML ist eine textbasierte Meta-Auszeichnungssprache, die es ermöglicht, Daten bzw. Dokumente bezüglich Inhalt und Darstellungsform derart zu beschreiben und zu strukturieren, dass sie – v. a. auch über das Internet – zwischen einer Vielzahl von Anwendungen in verschiedensten Hardware- und Softwareumgebungen ausgetauscht und weiterverarbeitet werden können. Dokumente zur Unterstützung von Geschäftsprozessen (wie etwa eine Bestellung oder Fakturierung), die in XML geschrieben sind und bei denen man sich auf eine inhaltliche Struktur geeinigt hat, können so (z. B. im Rahmen des Electronic Data Interchange, EDI) von Systemen verschiedener Geschäftspartner mit einem Minimum an personellen Eingriffen automatisch verarbeitet werden (vgl. Weitzel et al. 2001). Dazu ist es notwendig, dass Syntax und Semantik der Nachricht genau festgelegt sind. Die Syntax beschreibt die Regeln, welche Zeichen verwendet und zu komplexeren Einheiten zusammengefasst werden dürfen. Die Semantik ordnet den Zeichengruppen dann die inhaltliche Bedeutung zu. Es gibt wirtschaftszweig- und branchenabhängig verschiedene EDI-Nachrichtenstandards.

Mit *Webservices* wird das Konzept der komponentenbasierten Softwareerstellung weiterentwickelt hin zu weltweit verteilten und völlig voneinander losgelösten Anwendungsmodulen. Webservices lassen sich verstehen als autonome, gekapselte Dienste, die eine genau definierte Funktion erfüllen und über das Web als Teile übergreifender Wertketten verwendet werden können. Haben zwei AS eine Webservice-Schnittstelle, so können sie über standardisierte Internetprotokolle (s. ► Abschn. 2.3.1) miteinander kommunizieren. Auf diese Weise ist es u. a. möglich, Geschäftsprozesse abzuwickeln, die durch mehrere AS ausgeführt werden, z. B. die Buchung einer Reise, die individuell aus Flug, Hotel und Mietwagen in den AS unterschiedlicher Anbieter zusammengesetzt wird.

Als Basis von Webservices lassen sich wiederum *Serviceorientierte Architekturen* (SOA) definieren. SOA bezeichnet eine Systemarchitektur für eine plattform- und sprachneutrale Nutzung und Wiederverwendung verteilter Dienste, die von unterschiedlichen Besitzern verantwortet werden. Der Entwurf von Services orientiert sich hierbei nicht mehr (wie z. B. Softwarekomponenten im Rahmen einer Komponentenarchitektur) vorrangig an technischen Gesichtspunkten, sondern vielmehr an der Funktionalität im Hinblick auf die zu unterstützenden betrieblichen Funktionen und Prozesse. Ein Service kann z. B. die im Rahmen der Auftragsdatenerfassung durchzuführende Bonitätsprüfung des Kunden über eine Kreditauskunftei sein. Ziel ist es, dass es einem Unternehmen ermöglicht wird, als Antwort auf geänderte geschäftliche Anforderungen durch die Reorganisation von Services, schnelle und kostengünstige Anpassungen der AS-Landschaft vorzunehmen, ohne jede benötigte Funktionalität neu und selbst implementieren zu müssen (vgl. Buhl et al. 2008). Als zentrale Infrastrukturkomponente für die Kommunikation zwischen Anbietern und Nutzern von Webservices dient im Rahmen einer SOA häufig ein sog. Enterprise Service Bus (ESB).

2.2.5 Verteilte Rechen- und Speicherleistung

Mit dem Einsatz von Rechnernetzen werden verschiedene Ziele verfolgt, so z. B. die bessere Ausnutzung von Kapazitäten sowie der parallele Zugriff auf im Netz verfügbare Daten, Programme oder Hardwareressourcen.

Beim sog. *Grid Computing* haben Nutzer oder AS Zugriff auf einen großen Pool von heterogenen, vernetzten IT-Ressourcen. IT-Ressourcen können in diesem Zusammenhang z. B. Server, Speicher, CPUs, Datenbanken oder Services sein (vgl. Berman et al. 2003).

Cloud Computing folgt der Idee, dem Kunden bedarfsabhängig, jedoch zeit- und ortsunabhängig, standardisierte IT-Ressourcen, wie z. B. Server oder AS, als Dienste zur Verfügung zu

stellen. Auf Nutzerseite werden also Teile der IT-Landschaft (z. B. Rechenzentren) nicht mehr selbst betrieben, sondern in die „Rechnerwolke" eines Anbieters ausgelagert (s. ► Abschn. 6.3). Die Reservierung, Nutzung und Wiederfreigabe der Cloud-Ressourcen erfolgt je nach Bedarf und automatisiert über einen Netzwerkzugriff und wird nach flexiblen Bezahlmodellen, ähnlich dem Strom- oder Telefonnetz, abgerechnet.

Die dynamische Ressourcenbereitstellung ermöglicht der Einsatz von Server-Virtualisierung und mandantenfähigen Systemen. Virtualisierung bezeichnet grundsätzlich die virtuelle (d. h. nicht-physikalische) Nachbildung von Computern, um eine Abstraktionsschicht zwischen dem Benutzer (z. B. einem Betriebssystem) und den physikalischen Ressourcen (z. B. den Hardwarekomponenten eines Rechners) zu erzeugen. Beim Cloud Computing werden nun mehrere virtuelle Server auf mehreren vernetzten physikalischen Servern betrieben und eine virtuelle Maschine wird einem gerade freistehenden Server oder Speicher aus dem Pool zugeordnet. Die tatsächlich eingesetzte IT-Ressource kann vom Kunden oft nicht mehr physikalisch lokalisiert werden (vgl. Marston et al. 2011). Cloud-Anbieter wollen durch die gemeinsame Verwendung von Ressourcen Skaleneffekte für ihr Geschäftsmodell ausnutzen. So ermöglicht Cloud Computing z. B. rasant wachsenden Internetfirmen wie Amazon, aktuell freie Kapazitäten ihrer Cloud-Ressourcen (etwa am frühen Morgen amerikanischer Ostküstenzeit) fremden Nutzern, die sich über das Internet verbinden, im Rahmen einer serviceorientierten Architektur anzubieten und durch den Verkauf von Cloud-Lösungen Erlöse zu erzielen.

Der Zugriff auf die derart abstrahierte IT-Infrastruktur findet bei Rechnerwolken für die breite Öffentlichkeit, sog. „Public Cloud", i. d. R. über das Internet statt. Daneben kann die Bereitstellung z. B. über ein unternehmensinternes Intranet erfolgen, sodass der Zugang zu den entfernten Systemen einer „*Private Cloud*" nur der eigenen Organisation vorbehalten ist (vgl. Armbrust et al. 2009). Die „*Community Cloud*" bietet einem spezifischen eingeschränkten Nutzerkreis, beispielsweise mehreren Universitäten oder Betrieben mit ähnlichen Interessen, Zugang an. Eine kombinierte Cloud aus Private, Community und Public Cloud, die sog. „*Hybrid Cloud*", ermöglicht es, auf unterschiedliche Nutzerbedürfnisse und Anwendungsanforderungen einzugehen. Kritische Anwendungen können z. B. in der unternehmensinternen Private Cloud betrieben werden, während gleichzeitig auch auf Dienste der öffentlichen Cloud zugegriffen werden kann. Schnelle und zuverlässige Breitbandverbindungen sind also für den Einsatz und die Verbreitung von Cloud Services zwingend notwendig, sodass kein Unterschied zwischen lokaler und entfernter Datenverarbeitung und -speicherung wahrgenommen wird (vgl. Mell und Grance 2011).

Mit zunehmenden Grad an Abstraktion stellen Cloud-Anbieter Infrastruktur-, Plattform- und Softwaredienste zur Verfügung:

- „*Infrastructure as a Service*" (IaaS) beinhaltet Rechenkapazität und Speicherplatz auf virtuellen Cloud-Servern zur Kapazitätserweiterung der unternehmensinternen IT-Infrastruktur auf Abruf, z. B. Amazon Web Services.
- „*Platform as a Service*" (PaaS) liefert eine Software-Plattform in der Cloud zum Entwickeln, Testen, Nutzen und Verwalten von individuellen Webanwendungen, z. B. Google App Engine. Diese Dienste basieren auf den Leistungen der IaaS-Schicht.
- „*Software as a Service*" (SaaS) bietet komplette Anwendungsprogramme, z. B. salesforce.com für das Kundenbeziehungsmanagement. Diese Dienste basieren in der Regel auf Leistungen der PaaS-Schicht.

Angebot und Nutzung dieser Cloud-Dienste erfolgen über Netzwerkverbindungen, Protokolle sowie über lokale Anwendungsprogramme. Der Kunde hat somit keine Kontrolle mehr über die zugrunde liegende Technik, etwa die Serverplattform, was Bedenken bzgl. der Datensicherheit

mit sich bringt. Neben dem Wegfall von Vorabinvestitionen, Flexibilität bei der Ressourcennutzung und Kosteneinsparungen aufgrund von Ressourceneffizienz können durch die Virtualisierung auch erhebliche Hardware-Einsparungen realisiert werden. Insofern ist Cloud Computing bzw. Virtualisierung eine wichtige sog. *Green-IT*-Maßnahme mit einem potentiell positiven Umwelteffekt.

Green IT beschäftigt sich mit der Fragestellung, wie IT-Systeme zu einer Reduktion des Energieverbrauchs und höherer Energieeffizienz einen Beitrag leisten können. Als relativ neuer und stetig wachsender Anwendungsbereich der betrieblichen IT ist es die primäre Zielsetzung, Organisationen zur Erreichung ökologischer Ziele und mehr Nachhaltigkeit zu befähigen. Während sich ein eng gefasster Ansatz von Green IT primär auf die Verbesserung des Energieverbrauchs von Hardwaresystemen sowie deren Auslastung bezieht, umspannt eine weiter gefasste Sichtweise die planmäßige Entwicklung und den Einsatz von IT zur Verbesserung der Nachhaltigkeit in der Wirtschaft (vgl. Dedrick 2010). Themenfelder von Green IT behandeln Theorie und Praxis der effizienten Entwicklung, Herstellung, Nutzung sowie Entsorgung von Computern, Servern und den dazugehörigen Systemen mit möglichst keinem oder minimalen negativem Einfluss auf die Umwelt. In diesen Kontext fallen Bereiche wie beispielsweise energieeffiziente IT, Stromüberwachung, Entwurfsgestaltung für Rechenzentren, Ansätze zur Virtualisierung von Servern oder eine Standortwahl die vorhandene Ressourcen zur Klimatisierung nutzt oder die Abwärme an anderer Stelle nachnutzt. Ebenso werden die verantwortungsbewusste Entsorgung und Wiederverwertung von Altgeräten, die Einhaltung von Gesetzen und Richtlinien, die Nutzung erneuerbarer Energien sowie Verwendung von Umweltzeichen und Ökosiegeln für IT-Produkte betrachtet. Auch die Veränderung und Neugestaltung eines Geschäftsprozesses (Business Process Redesign, s. ► Abschn. 6.1.1) kann mit der Beachtung von Gesichtspunkten ökologischer Nachhaltigkeit unter Einbeziehung von Umweltkennzahlen, etwa Energieverbrauch und CO_2-Emissionen, erfolgen (vgl. Tenhunen und Penttinen 2010).

2.3 Weltweite Vernetzung: Das Internet

Das Internet bezeichnet den Zusammenschluss tausender lokaler Netzwerke, bestehend aus Millionen Rechnern, die Informationen über die Protokollfamilie TCP/IP (s. ► Abschn. 2.3.1) austauschen. Darüber hinaus bietet es eine Reihe von Diensten und Techniken, die nicht nur seine Funktionalität sichern, sondern neben institutionellen Netzbetreibern auch kommerziellen Telekommunikationsanbietern im Aufbau und Erhalt technischer Infrastrukturen Verdienstmöglichkeiten eröffnen, wie z. B. bei interkontinentalen Datenleitungen. Die Entwicklung des Internets kennzeichnet das Bestreben, durch Verbindung von Netzen den jederzeitigen Zugriff auf weltweit verfügbare Informationsressourcen preiswert zu ermöglichen, um Kooperationsvorteile zu erzielen.

2.3.1 Protokollfamilie TCP/IP

Die Protokollfamilie TCP/IP setzt sich aus zwei Teilen, dem Transmission Control Protocol (TCP) und dem Internet Protocol (IP), zusammen. Das TCP zerlegt Nachrichten, z. B. eine E-Mail, in verschiedene Datenpakete und versieht jedes Datenpaket mit der IP-Adresse des Senders und Empfängers.

IP-Adressen sind Zifferncodes, die zur Identifikation von Informationsstandorten dienen. In der aktuell noch verbreiteten Protokollversion IPv4 haben sie eine Länge von 32 Bit (4 Byte)

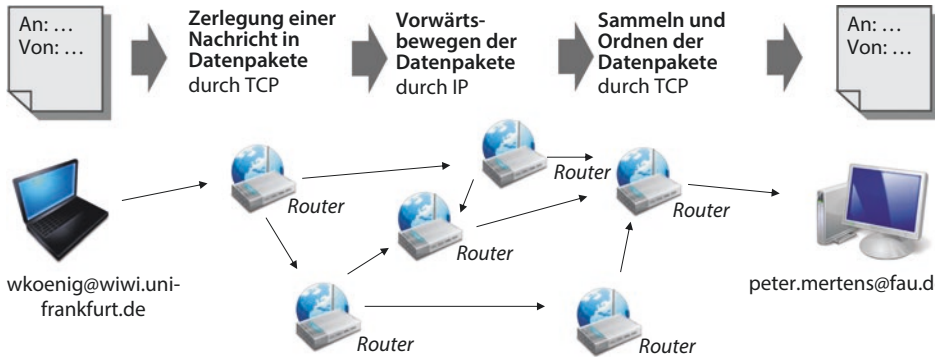

Abb. 2.2 Datenübertragung im Internet

und werden in Form von vier durch Punkte getrennten Dezimalzahlen angegeben, welche jeweils Werte aus dem Intervall von 0 bis 255 annehmen können. Für Menschen ist es i. Allg. leichter, mit Namen anstelle von Zahlenkolonnen umzugehen. Der sog. Domain Name Service (DNS) übersetzt diesen Namen in die zugehörige IP-Adresse (z. B. www.wiwi.uni-frankfurt.de in 141.2.196.151).

Abbildung 2.2 verdeutlicht die *Datenübertragung im Internet*. Die Pakete werden an einen *Router* geschickt (z. B. an den des Internetproviders), dessen Aufgabe in der IP-gesteuerten Weiterleitung der Informationen liegt. Innerhalb des Routernetzwerks versuchen z. B. Telefongesellschaften, momentane Belastungstäler in der verfügbaren Streckeninfrastruktur aufzufüllen, indem ein Paket über den am wenigsten ausgelasteten Weg in Richtung Ziel geleitet wird. Jedes Datenpaket einer Nachricht kann einen anderen Weg im Internet nehmen (man spricht von einem Packet Switching Network). Am Ziel werden die Pakete – gesteuert durch TCP – in die ursprüngliche Reihenfolge gebracht.

Jeder Dienst, der das TCP/IP-Protokoll nutzt, verwendet fest im Netzwerkprotokoll spezifizierte Ports zur Kommunikation. Dieser Zusatz erlaubt es, dass mehrere AS über eine Internetverbindung gleichzeitig Daten austauschen können. Anhand der Portnummer erkennt das System, für welches AS die ein- und ausgehenden IP-Pakete bestimmt sind. Die Kombination aus IP-Adresse und Port ermöglicht die eindeutige Identifizierung des Dienstes auf einem spezifizierten Rechner.

Da die Anzahl der verfügbaren IPv4-Adressen nahezu ausgeschöpft ist, löst eine neue Protokollversion, die als IPv6 bezeichnet wird, die 32-Bit-Version des IPv4 schrittweise ab. Mit der Version 6 werden 128 Bits für die Adressierung verwendet, was einer Anzahl von $3{,}4 \times 10^{38}$ Adressen entspricht. Im Gegensatz zu IPv4 bezeichnet man die Adressen bei IPv6 in Form von acht durch Doppelpunkte getrennte 16-Bit-Werte in hexadezimaler Schreibweise (z. B. 2BA:0:66:899:0:0:459:AC39). Neben der Erweiterung des Adressraums soll IPv6 das Routing vereinfachen und zu einer höheren Datensicherheit beitragen sowie die Reservierung von Ressourcen, etwa für eine dauerhafte Verbindung, ermöglichen.

2.3.2 Dienste und Technologien der Vernetzung

Das Internet verfügt heute über eine Vielzahl von Diensten, die es einem Anwender ermöglichen, Informationen zu empfangen bzw. zu senden. Zu den populärsten Diensten zählt das World Wide Web (WWW).

Das *Hypertext Transfer Protocol* (HTTP) ist das Standardprotokoll des WWW. Über dieses Protokoll werden die Webseiten übertragen. Der Webbrowser stellt einen HTTP-Client dar, der Anfragen generiert und diese an einen Webserver sendet. Der Server enthält einen sog. HTTP-Daemon, der auf HTTP-Anfragen wartet und diese bedient.

Zentraler Baustein von Webanwendungen sind in der *Hypertext Markup Language* (HTML) geschriebene Dokumente. Der Begriff Hypertext bezeichnet die Verknüpfung von Wörtern oder Textabschnitten mit anderen Informationsquellen. Durch Anklicken eines solchen Verweises (Link) kann das referenzierte Dokument aufgerufen werden. Durch den Erfolg des WWW sind die Grenzen des HTML-Konzepts vielfach sichtbar, da z. B. die inhaltliche Struktur der ausgegebenen Daten nicht expliziert ist und damit deren Weiterverarbeitung erschwert wird. Eine Lösung dieses Problems bringt die *Extensible Markup Language* (XML). XML erlaubt es, die Inhalte und ihre Struktur von der Darstellung (Layout) zu trennen, sodass z. B. ein Dokument für unterschiedliche Endgeräte jeweils grafisch angemessen visualisiert werden kann (z. B. PC-Monitor vs. Mobiltelefon-Display).

Für Client-seitige Anwendungen ermöglicht Java die Entwicklung von *Applets*, die als portable Programme vom Server auf den Client übertragen und dort im Browser ausgeführt werden. Dies erlaubt auch die Verlagerung der Ressourcenbeanspruchung (Prozessor, Speicher) vom stark beanspruchten Server auf die Client-Rechner.

Neben dem WWW und HTTP existieren weitere anwendungsbezogene Dienste auf der Grundlage von TCP/IP wie z. B. FTP (*File Transfer Protocol*) für die Dateiübertragung oder Voice-over-IP zur Übertragung von digitalisierten Sprachinformationen über das Netz.

2.3.3 Intranets und Extranets

Die beschriebenen Internettechniken sowie die vielfach kostenfreie Verfügbarkeit entsprechender Software attrahieren deren breiten Einsatz im Unternehmen in sog. Intranets und Extranets.

Intranets sind selbstverantwortlich betriebene und gegenüber Außenstehenden abgesicherte Netze auf der Basis von TCP/IP sowie den darauf aufsetzenden Protokollen und Diensten. Der Aufbau von Intranets ist insbesondere aus Gründen der Integration mit den Diensten im Internet attraktiv, sodass Anwender beide Netze mit der gleichen Oberfläche benutzen können. Häufig bietet man interne Handbücher, Rundbriefe, Adressverzeichnisse, Organisationsrichtlinien und nicht-öffentliche Teilekataloge in Intranets an. Bestehen Schnittstellen zwischen einem geschlossenen Netz und dem Internet, so werden üblicherweise *Firewalls* (s. ► Abschn. 2.4.1) implementiert, die den internen Bereich vom öffentlichen Netz abschotten.

Ein *Extranet* bezeichnet demgegenüber ein geschlossenes Netz von über das Internet verbundenen Unternehmen mit entsprechenden Zugriffsrechten (z. B. die Zulieferunternehmen eines Automobilherstellers oder die eines Produzenten mit seinen Logistikpartnern). Wie Intranets basieren Extranets auf der Nutzung von Internettechniken. Häufigen Einsatz finden *Virtual Private Networks* (VPNs), in welchen über ein Tunneling-Protokoll Informationen beim Übergang vom privaten LAN in das öffentliche Netz verschlüsselt und beim Eintreffen am Empfangspunkt entsprechend decodiert werden. Darüber hinaus kann diese Technik auch in Intranets zum Einsatz kommen.

2.3.4 Rechner- und Netzinfrastrukturen

Unternehmen und andere netzbetreibende Organisationen setzen, logisch gesehen, aus den vorgestellten Bausteinen ihre Rechner- und Netzinfrastruktur zusammen und verbinden diese mit dem Internet. Bei großen Betrieben verläuft die Entwicklung einzelner Beschaffungs- und

Erweiterungsentscheidungen im Zuge der zunehmenden Integration von Betriebswirtschaft und Technik in vielen Fällen ausgehend von zentralen Großrechnern zu dezentralen Architekturen. Dabei führen kurzfristige Einflüsse bisweilen dazu, dass derartige Systemstrukturen unkoordiniert wachsen. Einen Beitrag zur gezielten Entwicklung kann die Anwendung von u. U. recht komplizierten IT-Architekturmodellen leisten (s. ► Abschn. 6.2.1).

Praktisches Beispiel

Die comdirect bank AG ist Marktführer unter den Online-Brokern Deutschlands und die führende Direktbank für Anleger. Mehr als 1,8 Mio. Privatkunden nutzen deren Dienste für Wertpapiergeschäfte (Brokerage) und andere Bankdienstleistungen (z. B. Kreditvergabe und Beratung, s. auch ► Abschn. 4.4.3). Insgesamt bedient die comdirect-Gruppe in den Geschäftsfeldern B2C und B2B über 2,8 Mio. Kunden.

Im Zentrum steht die Website www.comdirect.de – mit 2015 monatlich rund 200 Mio. Seitenaufrufen eine der meistbesuchten Finanz-Websites in Deutschland – mit dem Transaktionssystem Direct-Brokerage, über das die Kunden der Direktbank Wertpapieraufträge erteilen können. Neben dem Direct-Brokerage-System stellt comdirect ihren Kunden den größten europäischen Börseninformationsdienst im Internet, den sog. Informer der Firma Interactive Data Managed Solutions AG in Frankfurt am Main, zur Verfügung (integriert in http://www.comdirect.de). Dieses System ist über Standleitungen mit den Zentralsystemen der Commerzbank AG verbunden, etwa für das Konsolidieren der Konten, bietet z. B. kostenlose aktuelle Informationen zum weltweiten Börsengeschehen und stellt unterschiedliche Oberflächen für Anfänger und Experten zur Verfügung. Der Informer bediente im Jahr 2015 über das Internet ca. 200 Mio. Seitenabfragen (page impressions) pro Monat. In der Spitzenlast beantwortete das System ca. 250.000 Datenbankabfragen pro Minute.

Die Leistungen werden von den beiden Häusern gemeinschaftlich erbracht. Die Interactive Data Managed Solutions liefert alle im öffentlichen Bereich des Informer-Angebots zugänglichen Informationen über das Netzwerk der Commerzbank an die comdirect bank. Dort werden die Informationen, angereichert und zu vollständigen Seiten zusammengesetzt, an den Kunden ausgeliefert. Neben zwischen den Häusern redundant ausgelegten Standleitungen mit jeweils 150 Mbit verfügt die comdirect hierfür über zwei 200 MBit-Anbindungen an das Internet. Die Anwender greifen auf Frontend-Server zu, welche die Anwendungslogik enthalten und sich zur Seitenerstellung zusätzlicher Backend-Funktionen bedienen (z. B. standardisierte Kursabfragen oder individuelle Marktübersichten). Der Datenaustausch zwischen den Anwendungsebenen wird hierbei über sog. Middleware (s. ► Abschn. 4.2.4) ermöglicht.

Die Anwendungssoftware läuft unter dem Betriebssystem Linux (s. ► Abschn. 2.1.2) und ist komplett eigenerstellt, um die hohen Durchsatzanforderungen zu befriedigen. Da die Dienste Direct-Brokerage und Informer im Webbrowser integriert sind, ist für den Anwender die Trennung der beiden Systeme nicht erkennbar. Das Rechenkontingent der comdirect bank ist in der Spitze zu etwa 50 % ausgelastet. Die Transaktionsleistung wird von einem nach Bedarf ausbaufähigen Zusammenschluss von momentan 250 Intel-basierten Hochleistungsservern erbracht, die ebenfalls über ein Breitbandnetz kommunizieren.

2.4 Sicherheit vernetzter Systeme

Stärkere Vernetzung und zunehmende Automatisierung der Geschäftsprozesse führen zu einer wachsenden Abhängigkeit des Geschäftsbetriebs von der IT. Geschäftsausfälle durch zufällig oder über gezielte Attacken korrumpierte AS sind ein Risiko, auf das Betriebe sowohl mit technischen, organisatorischen sowie rechtlichen Sicherheitsmaßnahmen in Bezug auf die Nutzung von Hard- und Software reagieren. Vorsorge, Sicherung und Schutz (*Prävention*), das Erkennen einer Störung oder eines Angriffes (*Detektion*) sowie mögliches Eingreifen (*Reaktion*) gegenüber Bedrohungen von außen sowie betriebsinternen Gefahren, die gängigerweise bis zu 70 % aller bekanntgewordenen, gezielten Korruptionen in einem Unternehmen ausmachen, sind Aufgabe des IT-Sicherheits- und Risikomanagements.

Die IT-Sicherheit betrachtet traditionell insbesondere den Schutz der technischen Systeme vor Ereignissen und Angriffen. Neben der IT-Infrastruktur eines Unternehmens sind auch die darin gespeicherten Daten und Informationen (s. ► Kap. 3) sowie betriebliche Transaktionen und die Kommunikation gegen Bedrohungen zu schützen, die folgende Qualitäten der IT gefährden:

- Vertraulichkeit der in den Systemen verarbeiteten Informationen
- Integrität der Daten und erbrachten Dienstleistungen
- Verfügbarkeit der Systeme und ihrer Dienste

Vertraulichkeit beschreibt die Wahrung von Geheimnissen und den Schutz vor Informationsweitergabe an unbefugte Personen, Organisationen oder Systeme. Vertraulichkeit ist notwendige Grundlage zur Aufrechterhaltung der Privatsphäre sowie zur Wahrung von Geschäftsgeheimnissen. Integrität steht für die Gewährleistung der Konsistenz und Genauigkeit von Daten und stellt sicher, dass Daten nicht unautorisiert bzw. unentdeckt modifiziert und manipuliert werden. Der Begriff Verfügbarkeit umfasst die Eigenschaft eines technischen Systems, seinen eigentlichen operativen Zweck zur Verfügung zu stellen (König et al. 2014).

Aufgrund der wachsenden Abhängigkeit des Geschäftsbetriebs von IT finden die Analyse und das Ergreifen von Maßnahmen der Sicherheit der IT Beachtung im Rahmen der IT-Governance (s. ► Abschn. 6.4). IT-Sicherheit gehört zumindest in Unternehmen mittlerer Größe zu den Aufgaben der IT-Abteilung. Alternativ ist es möglich, derartige Aufgaben an einen betriebsexternen Dienstleister zu vergeben. Nicht nur in Bezug auf externe Dienstleister sind notwendige Leistungen vertraglich durch Service Level Agreements (SLAs, s. ► Abschn. 5.1.1.3) festzuschreiben, um das notwendige Maß an Sicherheit, Verfügbarkeit, Wiederanlauf und Reaktionszeiten zu gewährleisten.

Der Realisierung von Sicherheits- und Gegenmaßnahmen geht eine Risikoanalyse voraus, die relevante Bedrohungen identifiziert. Betrachtet wird die Wahrscheinlichkeit, mit der ein Schaden eintreten kann, und das zu erwartende Ausmaß des Schadens. Die potenzielle monetäre Schadenshöhe wird den Kosten der Maßnahmen gegenübergestellt, die zur Verhinderung notwendig sind.

Bedrohungen für betriebliche IT bestehen durch Faktoren innerhalb des Betriebs (intern) sowie von außen (extern). Sowohl interne wie externe Ereignisse können mit krimineller Intention als Angriff durchgeführt werden sowie als nicht-intendiertes Ereignis wie zufälligen technischen Ausfällen oder fahrlässigen menschlichen Handelns stattfinden. Die vier möglichen Kombinationen werden nachfolgend erläutert.

Interne zufällige Gefahren bestehen durch technische Störungen wie dem Ausfall von Hardwarekomponenten, Spannungsschwankungen und Abbruch der Stromversorgung. Ebenso können Störungen in den lokalen Netzen des Betriebes zur Beeinträchtigung des Geschäftsbetriebs führen. Nicht-intendierte Ereignisse können auch in externen Bedrohungsszenarien wie Naturkatastrophen (Erdbeben, Überflutungen oder Brände) ihren Ursprung haben.

Nicht-intendierten Vorfällen wird im Bereich der IT mit Maßnahmen der Ausfallsicherheit begegnet. Um den Verlust von Daten in einem Schadensfall zu verhindern, werden redundante Systeme und Subsysteme angelegt. Redundant bedeutet, dass die Daten an mindestens einem weiteren Ort „gespiegelt" gespeichert werden, um im Schadensfall von mehreren physischen Orten aus abrufbar zu sein. Bei Ausfall einer Hardwarekomponente wird möglichst automatisiert ein Ersatz bereitgestellt. Um sich gegen einen Stromausfall abzusichern, müssen Notstromaggregate genutzt werden. Ferner sollte ein Katastrophenhandbuch ausgearbeitet werden, welches das Vorgehen im Notfall (z. B. Brand im Rechenzentrum) beschreibt und die notwendigen Schritte umfasst, um basierend auf den bisherigen Sicherheitsmaßnahmen den Betrieb der IT bzw. Unternehmung binnen kürzester Zeit fortzuführen.

Nicht-intendierte Handlungen von Mitarbeitern können interne Gefahrenquellen darstellen, indem diese der IT fahrlässig, aber unbeabsichtigt Schaden durch mangelnde Aufmerksamkeit oder Missachtung von Dienstanweisungen zufügen (s. ► Abschn. 2.4.2). Auch Mitarbeiter können beabsichtigt mit krimineller Intention vorgehen.

Der Schutz vor intendierten externen Angriffen, wie z. B. Malware oder Cyber-Attacken, ist integrale Aufgabe der IT-Sicherheit. Hier besteht ein bewusster Antrieb, dem Unternehmen zu schaden, indem Daten entwendet und manipuliert oder Betriebsausfälle provoziert werden. Der Begriff *Malware* ist von „malicious software" abgeleitet und eine Sammelbezeichnung für schädliche Softwareprogramme wie Computerviren, Computerwürmer oder Trojanische Pferde. In betriebliche Netzwerke kann Malware beispielsweise während der Internetnutzung durch Mitarbeiter gelangen, indem Skripte auf Webseiten eingegebene Daten des Nutzers unbemerkt an den Angreifer weiterleiten (Cross-Site-Scripting). Ebenso mag Malware aus geöffneten Anhängen von E-Mails eingeschleust werden, durch Hackerangriffe oder durch sogenannte *Schatten-IT* (engl. shadow IT). Letztere bezeichnet die unerlaubte oder unkontrollierte Nutzung von Hardware durch Mitarbeiter im Firmennetzwerk – eine substantielle Gefahrenquelle ist das BYOD (s. ► Abschn. 2.2.1) – oder die unberechtigte Installation von Software auf Betriebshardware. Mögliche Folgen von Malware sind der Verlust sowie Diebstahl vertraulicher Daten (z. B. Kreditkartendaten), die Verlangsamung oder der Ausfall von Unternehmensnetzwerken sowie das Blockieren von Rechenzeit oder Speicherplatz.

2.4.1 Technische Maßnahmen

2.4.1.1 Prävention

Vorbeugende technische Maßnahmen reichen von der physischen Trennung von Systemen, dem Einsatz von Firewalls, der Vergabe und Kontrolle von Zugriffsrechten auf Daten und Prozesse bis zur Verwendung verschlüsselter Protokolle (vgl. König et al. 2014). Auch das Verhalten der Mitarbeiter ist ein sicherheitsrelevanter Faktor, dem durch vorbeugende Maßnahmen begegnet wird (s. ► Abschn. 2.4.2).

Zuverlässiges Vorgehen zur Prävention gegen einen Schadensfall ist die *logische oder physikalische Trennung von Systembereichen*. Bereiche, die für einen externen Angriff leichter erreichbar sind, werden abgeschottet von solchen, die zum Aufrechterhalten des Geschäftsbetriebs unerlässlich sind oder aus Datenschutz- oder Wettbewerbssicht sensible Daten enthalten, z. B. Mitarbeiter- und Kundendaten oder Ergebnisse der Forschungs- und Entwicklungsabteilung. E-Mail-Server, die mit dem Internet kommunizieren, können z. B. von Systemen getrennt werden, die eine vollautomatisierte Produktion steuern. Die Aufspaltung in Intra- und Internet (s. ► Abschn. 2.2.3) vermindert die Wahrscheinlichkeit, dass interne Daten nach außen weitergegeben werden.

Externe Angriffe werden durch *Firewalls* abgehalten. Die Verbindung von außen wird durchbrochen und der komplette Datenverkehr von der Firewall anhand zuvor festgelegter Regeln

überprüft, ob Datenpakete passieren dürfen oder nicht. Freie Ports (s. ► Abschn. 2.2) und festgelegte IP-Bereiche werden blockiert. Aufgrund der vorgegebenen Regeln eignen sich Firewalls nur zur Vorbeugung und nicht zur Erkennung bereits erfolgter Einbrüche. Personal Firewalls arbeiten in Rechnern (oftmals als Teil des Betriebssystems (s. ► Abschn. 2.1.2)). Dedizierte Hardware-Firewalls schützen ganze Netzwerkbereiche und weitere Netzwerkbestandteile wie z. B. Router. Es kann zwischen zwei Arbeitsweisen unterschieden werden: Bei IP-basierter Prüfung betrachtet die Firewall den Sender und Empfänger eines Datenpaketes, während bei Analyse des Anwendungsprotokolls die Firewall die Datenstruktur der Datenpakete auf bösartige Strukturen (sog. Deep-Packet-Filter) untersucht. Um unerwünschte Werbe-E-Mails (Spam) und die damit verbundenen Sicherheitsrisiken zu vermeiden, müssen Mailfilter definiert werden.

Ebenso sind die Software und der Zugang zu Daten durch die Vergabe von *Passwörtern* und *Zugriffsrechten* zu sichern. Zu den Kontrollen zählen eine Identifikation der Benutzer, die Überprüfung der Benutzerrechte sowie die Protokollierung der Aktivitäten. Gegenüber Mitarbeitern sowie als Schutz gegen Außenstehende soll damit erreicht werden, dass nur die Berechtigten auf jeweilige Geschäftsprozesse und Datenbereiche zugreifen können. Dies dient sowohl dem Datenschutz als auch der Sicherung von Geschäftsgeheimnissen.

Sowohl bei der Datenübertragung in internen als auch mit externen Netzen sollten SSL (*Secure Socket Layer*) *verschlüsselte* Protokolle verwendet werden. Mit solchen *kryptografischen Verfahren* werden bei einer Anwendung bei der Datenübertragung Geheimhaltungs- und Authentifizierungsziele verfolgt. Die geforderten Qualitäten der Vertraulichkeit werden durch Verschlüsselung, die Integrität durch kryptographische Protokolle sowie die Authentizität eines Kommunikationspartners durch *digitale Signaturen* umgesetzt. Man kann hierbei *symmetrische* und *asymmetrische Verschlüsselungsmethoden* unterscheiden.

Bei der *symmetrischen Verschlüsselung* wird eine Nachricht durch den Sender mit einem Schlüssel chiffriert und beim Empfänger durch die umgekehrte Anwendung desselben Schlüssels dechiffriert. Ein Problem ist, dass zuvor Sender und Empfänger den Schlüssel über einen sicheren Kanal transportieren müssen. Bei der *asymmetrischen Verschlüsselung* dagegen hält jeder Kommunikationsteilnehmer ein eng aufeinander bezogenes Schlüsselpaar (bestehend aus einem öffentlichen Schlüssel und einem privaten Schlüssel), wobei sich der eine Schlüssel nicht ohne Weiteres aus dem anderen (z. B. durch Umkehrung) herleiten lässt. Die *asymmetrische Verschlüsselung* wird z. B. bei der Erstellung einer digitalen Unterschrift (*Elektronische Signatur*) angewendet, durch welche die Urheberschaft einer Nachricht (z. B. eine per E-Mail versendete elektronische Rechnung) sichergestellt werden kann.

Zusätzlich sind Schulungen zu *Security-Awareness* zu empfehlen, um die Mitarbeiter zu sensibilisieren, auf welche Gefahren im täglichen Arbeitsalltag geachtet werden sollte (s. ► Abschn. 2.4.2), z. B. Anhänge von E-Mails oder an externe Hardwareschnittstellen angeschlossene USB-Sticks.

2.4.1.2 Detektion

Mit der wachsenden Komplexität und stetigen Weiterentwicklung der technischen Systeme lassen sich Sicherheitslücken und Systemschwächen nie ganz verhindern, die zum Angriff und zur Schwächung der Funktionsfähigkeit betrieblicher IT ausgenutzt werden können. Eine Störung wird als Unterschied zum Normalbetrieb definiert. Mit Monitoring-Werkzeugen werden die normalen Betriebsparameter erfasst und Probleme erkannt, wenn diese Parameter unerwartet abweichen. Die Netzwerküberwachung misst die Menge des Datenverkehrs und zeigt dem Netzwerkadministrator den Grad der Auslastung eines Servers an. Beim Angriff einer Dienstblockade (engl. Denial of Service) wird bspw. die normale Kapazität eines Servers durch übermäßige Anfragen überfordert; reguläre Anfragen kann der Server in der Folge nicht mehr bearbeiten. Da auch

normale betriebliche Nutzung zu bestimmten Zeiten z. B. zu erhöhter Nutzung der IT-Infrastruktur führen kann, müssen zur Unterscheidung von böswilligen Angriffen verschiedene Betriebszustände berücksichtigt werden. In Realumgebungen sind diese Zusammenhänge komplex und werden mit technischen Systemen analysiert.

2.4.1.3 Reaktion

Das Erkennen und Reagieren auf Fehler ist der Bereich des Fault-Managements. Der physische Ausfall einer Ressource führt zu einer Störung, die durch redundante Systeme abgefangen werden kann. Auf intendierte Angriffe wird in vielen Fällen versucht, mit gezielten Systembeschränkungen zu reagieren. Angriffe über *Bot-Netze* z. B. können einen großen Umfang haben und gehen meist mit sinnloser Kommunikation einher. Um die ausgenutzte Sicherheitslücke zu schließen, lassen sich Anfragen aus einzelnen Netzbereichen des Internets mit einer dem Angriff angepassten Änderung der Filterregeln der Firewall abblocken. Da nur schwer zwischen legitimem und illegitimem Datenverkehr unterschieden werden kann, bspw. zwischen tatsächlichen Kunden eines Webshops und dem Verkehr von Angreifern, mag die Reaktion auf den Angriff auch (ahnungslose) Kunden treffen und verärgern. Das Ziel ist, die Filterung möglichst früh in Richtung der Quelle des Angriffs vorzunehmen. Mit Intrusion-Detection-Systemen wird u. a. versucht, auf unberechtigte Zugriffe wie z. B. Passwort-Phishing (Abfragen des Passworts, z. B. durch falsche Internetseiten) zu reagieren. Wurden Daten unbemerkt ausgelesen, wird dies oftmals erst nachträglich durch den Missbrauch der Daten erkannt, z. B. durch ungewöhnlich häufige Verwendung eines Passwortes oder Anmeldung eines Nutzers. Bei veruntreuten Passwörtern muss ein neues Passwort gesetzt werden.

2.4.2 Organisatorische und rechtliche Maßnahmen

Technische Schutzmaßnahmen betrieblicher AS können unterlaufen werden, falls Mitarbeiter unachtsam handeln. Wenn Daten in betriebsexternen Umgebungen hinterlegt und dadurch missbräuchlich verwendet werden können oder Passwörter im Klartext ausgeschrieben und abgespeichert werden, gefährdet dies die Sicherheit des Unternehmensnetzwerkes. Um Mitarbeitern die sichere Beherrschung der verbundenen Systeme bewusst zu machen, sind entsprechend gestaltete Organisationsabläufe notwendig (vgl. Haag und Eckhardt 2014).

Aus Organisationssicht sind zunächst geeignete Sicherheitsrichtlinien zu definieren, welche die angemessene Nutzung der betrieblichen IT-Ressourcen sowie den sicheren Umgang mit vertraulichen Firmendaten regeln. Diese formellen Regeln zu nutzerbezogenen Themen wie etwa *Passwortsicherheit* oder BYOD (s. ► Abschn. 2.2.1) schreiben die Rolle und Pflichten des Personals in Bezug auf die IT-Sicherheit und den Datenschutz fest und sollen bewusstem und unbewusstem internen Computermissbrauch entgegenwirken.

Das Verständnis und die Einhaltung der Sicherheitsrichtlinien wird durch sog. „*Security Education, Training and Awareness* (SETA)-Programme" gesteigert (vgl. Bulgurcu et al. 2010). In Trainingsprogrammen und Schulungen wird mittels Sicherheitsexperten, Gruppenarbeit oder Rollenspielen das Bewusstsein der Nutzer für die Wichtigkeit eines adäquaten Umgangs mit den IT-Systemen verbessert und das nötige Know-how vermittelt, um die erforderlichen Sicherheitsmaßnahmen im Arbeitsalltag korrekt durchzuführen. Das Hauptziel von SETA-Programmen ist die positive Beeinflussung der Gewohnheiten der Nutzer, alle IT-basierten Arbeitsschritte regelkonform und sicher auszuführen. Informationskampagnen, z. B. über das Intranet, via E-Mail-Newsletter, Poster oder Flyer, ergänzen die Schulungen und machen Mitarbeiter regelmäßig auf Änderungen der Sicherheitsrichtlinien sowie aktuelle Gefahren und Entwicklungen in der

IT- und Internetsicherheit aufmerksam. Entscheidend für den Erfolg ist, das SETA-Programm genau auf die Sicherheitsbedürfnisse, Mitarbeiter und Unternehmensziele abzustimmen. Das Arbeitsumfeld soll dabei positiv das Verhalten der Mitarbeiter in Bezug auf Sicherheit beeinflussen. Um die Wirksamkeit der Maßnahmen zu überprüfen, engagieren einzelne Unternehmen auch professionelle „Hacker".

Eine Kultur des mitdenkenden Handelns und entsprechender Fähigkeiten der Mitarbeiter wird durch das Konzept der organisatorischen Achtsamkeit (engl. Organizational Mindfulness) beschrieben. Organisationen, die eine solide Achtsamkeit im Arbeitsumfeld etablieren und belohnen, reagieren auf unvorhergesehene Fehler- sowie Schadensituationen wie Sicherheitsattacken und Systemausfälle schneller und geschickter; sie arbeiten darüber hinaus mit IT-Systemen sicherer und erfolgreicher.

Zur gesetzlichen Grundlage zum Schutz von IT-Systemen in Deutschland gehören das *Bundesdatenschutzgesetz* (BDSG), *Telemediengesetz* (TMG) sowie das *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* (IT-Sicherheitsgesetz, IT-SIG) (s. ► Abschn. 6.5.2).

Für IT-Sicherheit existieren weitere Normen, die AS und Geräte durch allgemeingültige Standards einheitlich und vergleichbar bewertbar machen. Die International Organization for Standardization (ISO) in Genf definiert international gültige ISO-Normen wie ISO 15408 und 18045, mit denen Hersteller produzierte Systeme, Geräte und Komponenten für die Eignung im Einsatz zur technischen Sicherung von Informationssystemen zertifizieren lassen können. Die Standards mit den Bezeichnungen ISO 27000 und 27001 legen einheitliche Beschreibungen für Aktivitäten von Unternehmen und Organisationen fest, um Maßnahmen für die Informationssicherheit zu bewerten. In Deutschland vergibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Zertifizierungen, die an den *ISO-Standards* ausgerichtet sind. Im Rahmen des IT-Grundschutzes hat das BSI die ISO-Normen in sogenannte *BSI-Standards* umgearbeitet.

Literatur

Berman F, Fox G, Hey A (2003) Grid Computing: Making the Global Infrastructure a Reality. Wiley, New York

Buhl HU, Heinrich B, Henneberger M, Krammer A (2008) Service Science. WIRTSCHAFTSINFORMATIK 49(2): 129–132

Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quart 34(3):523–548

Dedrick J (2010) Green IS: concepts and issues for information systems research. Commun Assoc Inf Syst 27:11–18

Disterer G, Kleiner C (2013) BYOD – Bring Your Own Device. HMD Praxis der Wirtschaftsinformatik 50(2):92–100

Haag S, Eckhardt A (2014) Sensitizing Employees' Corporate IS Security Risk Perception. In: Proceedings of the 35th International Conference on Information Systems, Auckland

Keller G (1999) SAP R/3 prozessorientiert anwenden: Iteratives Prozess-Prototyping mit Ereignisgesteuerten Prozessketten und Knowledge Maps. 3. Aufl. Addison-Wesley, München

König W, Popescu-Zeletin R, Schliesky U (2014) IT und Internet als kritische Infrastruktur – vernetzte Sicherheit zum Schutz kritischer Infrastrukturen. Lorenz-von-Stein-Inst. für Verwaltungswiss. an der Christian-Albrechts-Univ Kiel

Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A (2011) Cloud computing – the business perspective. Decis Support Syst 51(1):175–189

Mell P, Grance T (2011) The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. Special Publication 800–145, Gaithersburg

Tanenbaum AS (2009) Moderne Betriebssysteme. Pearson, München

Tenhunen M, Penttinen E (2010) Assessing the carbon footprint of paper vs. electronic invoicing. In: Proceedings of the Autralasien conference on Information Systems (ACIS 2010)

Weitzel T, Harder T, Buxmann P (2001) Electronic Business und EDI mit XML. dpunkt, Heidelberg

http://www.springer.com/978-3-662-53361-1

Grundzüge der Wirtschaftsinformatik

Mertens, P.; Bodendorf, F.; König, W.; Schumann, M.; Hess, Th.; Buxmann, P.

2017, X, 218 S. 91 Abb., Softcover
ISBN: 978-3-662-53361-1