Einführung in die Hard- und Software

(Jupp Joachimski)

Was geht eigentlich die Technik den Datenschutz an?

Vieles, denn

- nach § 6 KDO ist die Datensicherheit Teilaspekt des Datenschutzes.
- Insbesondere der betriebliche Datenschutzbeauftragte muss abschätzen können, wie sich Änderungen der Hard- und Software auf die Datensicherheit auswirken.
- Neue Hardware – Rechner, Drucker, Laptops, aber auch Smartphones – verändern sehr schnell die Sicherheitslage von EDV-Systemen.
- Neue Software birgt z.T. noch höhere Risiken.
- Die Eröffnung ganz neuer Arbeitsmöglichkeiten, z.B. Fernzugang, Cloud-Computing findet in immer kürzeren Abständen statt und hat Auswirkungen auf die Zugangskontrolle.

Ganz generell: Das Verständnis für die Zusammenhänge ist entscheidend für eine effektive Gefahrenabwehr.

Die Hardware

Bauformen der Computer:

Die immer noch gebräuchlichste Form ist diejenige des Towers. Seine Nachteile sind Größe und Gewicht, die Vorteile die sehr flexible Erweiterbarkeit und der Umstand, dass bei Funktionsstörungen sehr leicht und preiswert Komponenten ausgetauscht werden können.

Und da gibt es noch ein Zuckerl: Bei Towern/Desktops passen im Prinzip alle Bauteile zu (fast) allen Rechnern. Das ist ein Zustand, von dem man bei seinem Auto nur träumen kann. Von dem Typ meines Autos, den ich fahre, wurden im selben Baujahr sieben verschiedene Wasserpumpen produziert. Es ist klar, dass jede von denen erheblich mehr kostet als wenn es nur einen Wasserpumpentyp in 10 Jahren gegeben hätte.

Eine ähnliche Bauform wie die des Towersist die des Desktops (vollwertiger Computer) bzw. der Workstation (Computer ohne eigene Festplatte):

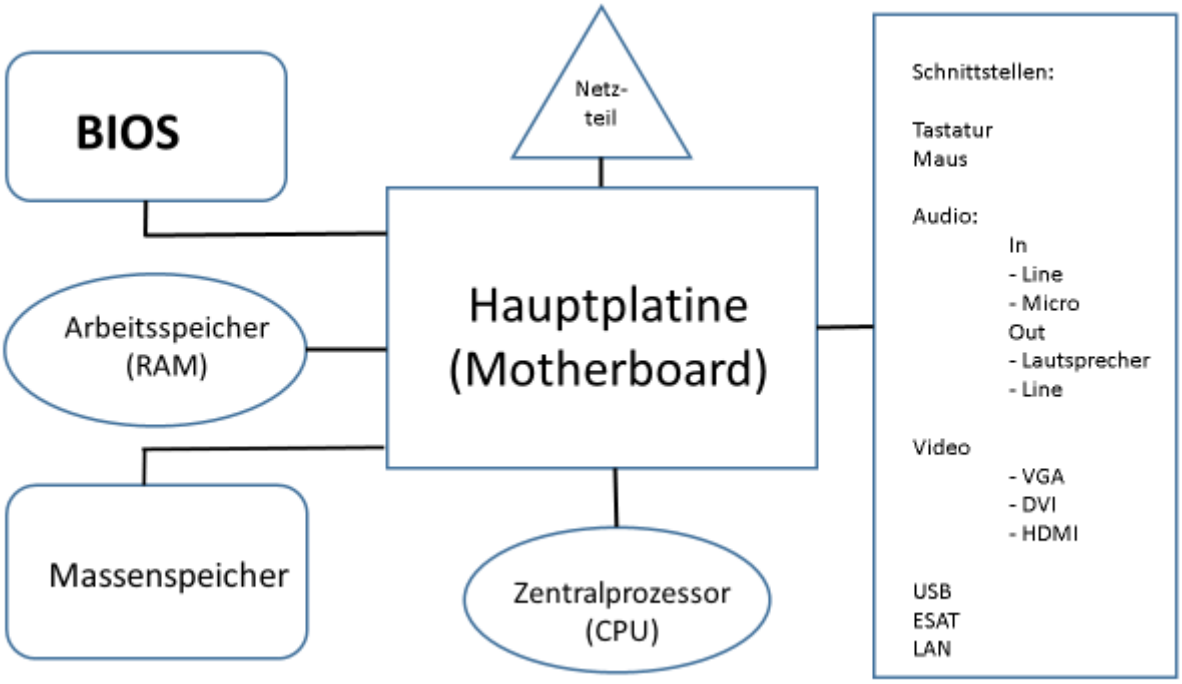
Es geht aber natürlich noch kleiner:

So z.B. mit dem **Barebone**, ein kompletter, aber kleinerer Computer, der die Stereo- und Videoanlage im Wohnzimmer ersetzt und auf Ton- bzw. Videowiedergabe getrimmt ist.

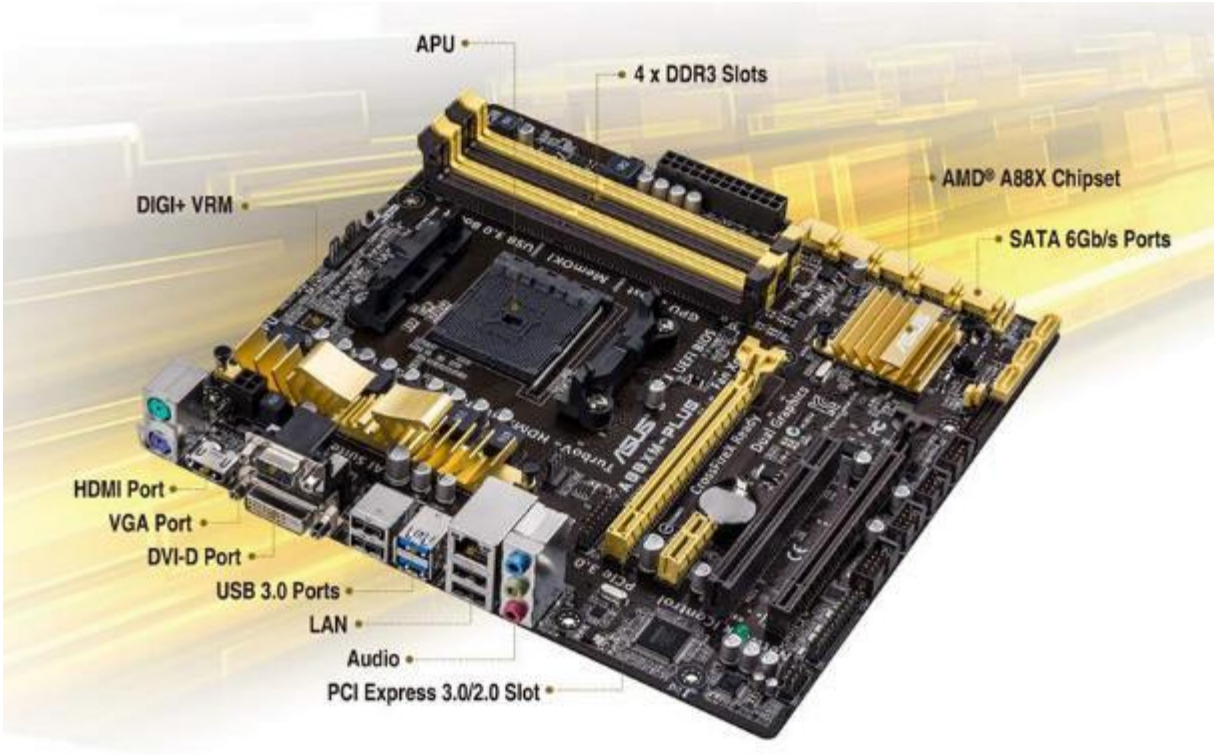
Weitere Bauformen sind Ihnen sicher bekannt:

- Der **All-In-One** vereint Bildschirm und Gehäuse in einem etwas dickeren Monitor, das **Notebook** in einem flachen Gehäuse. Das **Notebook**, auch **Laptop** genannt, zeichnen sich durch Mobilität aus.

- **Tabletcomputer** sind im Prinzip ganz flache Notebooks und
- **Smartphones** sind noch etwas kleiner und gut bekannt.
- Der kleinste Allround-Computer ist derzeit der **Raspberry-PI** mit einer Größe von 10 x 8 x 3 cm (und einem Preis von weniger als 50 Euro)**.**



So wie auf dieser Grafik dargestellt sehen im Prinzip alle Rechner von innen aus, gleich welche Bauformen sie haben. Allerdings sind die Tower oder Desktop Rechner leichter zu verstehen als Laptops oder gar Smartphones – einfach deswegen, weil sie größer sind. Wir bleiben also im Folgenden bei der Betrachtung dieser beiden Bauformen. Ausgangspunkt dafür ist die Hauptplatine – oder auf Neudeutsch Motherboard bzw. Mainboard. Sie bietet allen Elementen des Rechners Platz und Anschluss. So sieht ein Motherboard dann in Wirklichkeit aus:



Es gibt zahlreiche Hersteller von Hauptplatinen. Maßgeblich dafür, welche Hauptplatine gewählt wird, ist :

- der einzusetzende Zentralprozessor, für ihn ist das Motherboard gebaut.
- die Zahl und Art der Schnittstellen
- die vorhandene (oder fehlende) Integration des Audio- und des Videoprozessors.
  Dafür gilt: Wird eine besonders hochwertige Verarbeitung von Audio- oder Videosignalen angestrebt, ist es sinnvoll, diese Aufgaben besonderen Einheiten – Audio- bzw. Videokarte – zu überlassen und diese Komponenten auf den hierfür vorgesehenen PCIE-Steckplätzen (Peripheral Component Interconnect Express) einzubauen. Das kommt z.B. in Betracht für Tonstudios oder bei Rechnern, die vorwiegend für Videobearbeitung bzw. für Spiele eingesetzt werden.
- Das vorgesehene Gehäuse entscheidet über die Bauform: Hier ist das sog. ATX-Format (Advanced Technology Extented) derzeit die gebräuchlichste Form, die eigentlich zu jedem Gehäuse passt.

Prinzipiell gilt auch für alle PC: Alle Bauteile aller Hersteller passen zu allen Bauteilen aller Hersteller. Die große Ausnahme von dieser Regel ist Apple.

Die Prozessoren:

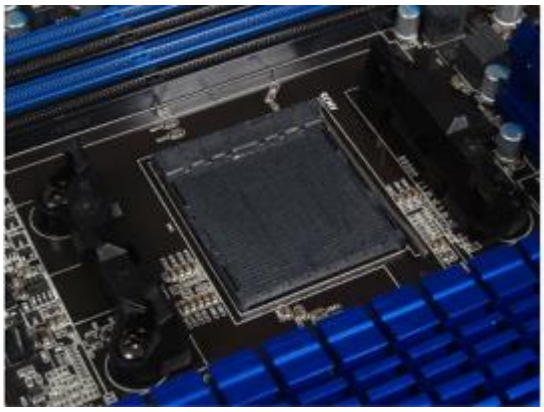
nehmen die zentralen Rechenaufgaben des Computers wahr. Gegenwärtig stellen drei Unternehmen Prozessoren her: INTEL (über 70%), AMD (ca. 23%), Motorola (4%). INTEL und AMD bieten je eine große Palette von Prozessoren unterschiedlicher Leistungsstufen.

Drei Merkmale kennzeichnen die Leistungsfähigkeit eines Prozessors:

- Prozessordesign in Bit:

- Ein Bit ist die kleinste Informationseinheit (ja/nein oder 0/1[1]), ein Byte besteht aus 8 Bit und ist ausreichend zur Definition eines Buchstabens oder einer Zahl.
- Ein 32-Bit-Prozessor verarbeitet 32 Bit = 4 Byte in einem Arbeitstakt. Er kann höchstens 4 GByte Arbeitsspeicher ansprechen (adressieren).
- Ein 64-Bit-Prozessor verarbeitet 64 Bit = 8 Byte in einem Arbeitstakt. Er kann mehr als 4 GByte Arbeitsspeicher adressieren.

- die Zahl der Kerne (interne Prozessoren) und
- die Taktgeschwindigkeit: Ist sie höher, steigt die Gesamtleistung.



Von Bedeutung ist daneben der Stromverbrauch des Prozessors. Mehr Stromverbrauch bedeutet mehr Kühlungsbedarf für den Prozessor und geringere Laufzeit von Akkus tragbarer Computer.

So unscheinbar sieht ein moderner Prozessor aus:

Der Austausch eines Prozessors gegen einen anderen (meist leistungssstärkeren) ist nur in Ausnahmefällen möglich, wenn der Sockel des Mainboards der gleiche ist und die elektischen Daten übereinstimmen. Normalerweise müssen Mainboard und Prozessor in solchen Fällen gemeinsam getauscht werden, um eine Gesamtleistungssteigerung des Rechners zu erzielen.

Arbeitsspeicher

auch RAM (random access memory) genannt, unterlagen wohl der stärksten Entwicklung in Tempo und Preisverfall:

1981 kostete ein Kilobyte RAM ca. 10 DM
2015 die (millionenfache) Größe von einem Gigabyte 5 Euro.
RAM hat zwei wesentliche Kennzahlen:

- die Größe (gegenwärtig 1- 16 GByte)
- die Busgeschwindigkeit: Das ist die maximal von der Hauptplatine zu verarbeitende Taktzahl. Die eigene Taktzahl des RAM-Moduls kann höher liegen.

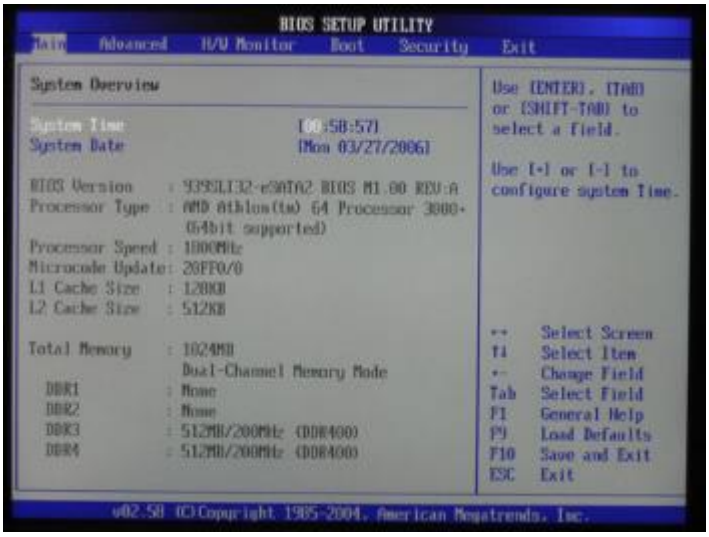
Ein typischer Windows-Rechner ist mit vier Gigabyte RAM ausgestattet; bis zu 16 Gbyte können sinnvoll sein.

BIOS (Basic Input and Output System)

Das BIOS ist in einem (nur kompliziert) austauschbaren Chip auf dem Mainboard untergebracht. Es lässt sich im Rahmen des Startvorgangs des Rechners auf die Bedürfnisse der Nutzer einstellen.

[1] Das wird im Skriptum „Grundlagen der EDV“ erläutert. Sind Sie sich sicher, dass Sie es gelesen haben?

So sieht das herkömmliche (bis 2013 standardmäßig verbaute) BIOS auf dem Bildschirm aus:



Seit 2014 erhielten neue Rechner das sog. UEFI-BIOS (Unified Extensible Firmware Interface), das sich so präsentiert:

Und das tut das BIOS nach dem Einschalten des Rechners:

- Power On Self-Test (POST)
- Initialisierung der Hardware
- Aufforderung zur Eingabe eines BIOS-Passworts (falls konfiguriert)
- Aufforderung zur Eingabe eines Festplatten-Passworts (falls konfiguriert)
- Darstellung eines Startbildschirms
- Möglichkeit, ein BIOS-Konfigurationsmenü („BIOS-Setup“) aufzurufen
- Aufrufen von BIOS-Erweiterungen einzelner Subsysteme, die entweder auf Steckkarten untergebracht sind oder direkt auf dem Mainboard integriert sind, z. B.:
    - Grafikchip
    - Netzwerkchip
    - Massenspeicher-Controller
- Feststellen, von welchem Datenträger gebootet werden kann und soll
- Laden des Bootsektors; meistens ist das ein Bootloader.

Das Netzteil:

Netzteile enthalten in einem (insgesamt austauschbaren) Gehäuse

- Transformator
- Gleichrichter
- Kühlgebläse für den gesamten Rechner sowie
- Schalter und Anschlusskabel.

Kenngrößen sind

- Leistungsabgabe in Watt
- Geräuschentwicklung in Sone

Das Netzteil gehört zu den preiswertesten (ab ca. 25 €) Komponenten eines Rechners, aber auch zu den anfälligsten. Es muss am häufigsten ausgetauscht werden.

Interne Massenspeicher:

enthalten alles, was der Rechner an Software zum Betrieb braucht. Der erste weit verbreitete Massenspeicher war die Diskette. Sie verlor in den 90er Jahren an Bedeutung, da die Festplattenlaufwerke immer preiswerter, schneller und zuverlässiger wurden. Rechts sind die verschiedenen Bauformen dargestellt:

Diskettenlaufwerke finden sich heute in Rechnern nicht mehr.

Magnetspeicher-Festplatte: Sie ist – im Prinzip – noch aufgebaut wie eine Diskette. Auf einer rotierenden magnetisierbaren Fläche sind die Informationen in Spuren magnetisch gespeichert.

Solid State Drive (SSD): Sie arbeitet nach dem Prinzip einer Speicherkarte oder eine USB-Sticks. Die Informationen werden in Halbleitern dauerhaft gespeichert, ohne dass bewegliche Teile nötig sind. Die SSD ist gegenwärtig noch acht Mal teurer als die „normale“ Festplatte, aber auch achtmal schneller. Eine kostengünstige Kombination aus einem kleinen SSD (für das Betriebssystem) und einer größeren Datenplatte nennt man Hybrid-Festplatte.

Optische Laufwerke:

Basierend auf der Technik der Compact Disc, bei der durch einen Laserstrahl digitalisierte Informationen auf eine empfindliche Metalloberfläche gebrannt werden, gibt es drei in der Kapazität unterschiedliche optische Datenträger:

- CD-ROM bzw. CD-RW bis ca. 700 Megabyte
- DVD bzw. DVD-RW bis 4,6 GByte in der einfachen Form, bis 8,6 GByte in der Form des Zweischichtverfahrens (Double Layer).
- Blue-Ray -Blue-Ray-RW bis 25 GB, bis 50 GByte in der Form des Zweischichtverfahrens (Double Layer).

Alle Bauformen gibt es als ROM- (Read Only Memory=Nur Lesen) oder RW- (Read-Write=Lesen und Schreiben) Varianten.

Bedeutung haben die optischen Laufwerke vor allem

- in der Unterhaltungselektronik
- zur Installation von Software
- bei der Datensicherung.

Die Anbindung der Massenspeicher

Bis ca. 2003 erfolgte die Verbindung zwischen Mainboard und Massenspeicher ausschließlich über das sog. IDE-Kabel (Integrated Development Environment), das parallele Datenübertragung ermöglichte.

Seit 2004 setzte sich immer mehr die sog. SATA-Verbindung (Serial Advanced Technology Attachment) durch. Sie arbeitet mit serieller Übertragung.

Warum seriell? Mit der Erhöhung der Taktgeschwindigkeit von Prozessoren wurde es bald möglich, die Signale nacheinander genauso schnell hintereinander zu übermitteln wie zuvor nebeneinander (parallel). Auf diesem Gedanken beruht auch die wichtigste Schnittstelle des Rechners, der **U**niverselle **S**erielle **B**us „USB“. Der Begriff „Bus“ hat in diesem Zusammenhang nichts mit dem Öffentlichen Personennahverkehr zu tun, sondern bezeichnet einfach eine Leitung.

Bei Nachrüstung bzw. Ersatz von Massenspeichern muss auf die richtige Bauform, welche vom Mainboard vorgegeben wird, geachtet werden.

So versammeln sich die SATA-Buchsen auf dem Mainboard:

Peripherie: Die Tastatur

Tastaturen werden entweder über

- besondere Stecker (PS/2) oder
- USB oder
- drahtlos angeschlossen.

Ihr Layout ist

- vor dem Laden des Betriebssystems, z.B. bei Einstellung des BIOS, amerikanisch:
  QWERTY
  …..
  ZXCVBN
- nach dem Laden des Betriebssystems einstellbar, z.B. Deutsch
  QWERTZ
  …….
  YXCVBNM

Peripherie: Die Maus

Maus-Eingabegeräte unterscheiden sich durch den Anschluss:

- Kabel (PS/2, USB)
- drahtlos (Bluetooth oder WLAN-Frequenz)
- die Tastenzahl:
    - mindestens 3 Tasten
    - zusätzlich Rollrad (mit integrierter Taste) und weitere – frei belegbare – Tasten
- die Abtastmethode:
    - Gummikugel oder
    - Laser
- die erreichbare Minimalbewegung, angegeben in Dots per Inch; üblich 300 - 1200

Neben den normalen Mäusen existieren Sonderformen für Präsentationen und Zeichnungen (Grafiktablett).

Ton-Ein- und Ausgang

Bei einer hochwertigen Audiokomponente eines für Tonbearbeitung besonders konzipierten Rechners bestehen mehrere – häufig frei konfigurierbare – Ein- und Ausgänge für

- Mikrofon
- Line In
- Line Out
- Subwoofer
- mehrere Lautsprecher

Die Konfiguration erfolgt über ein Programm des Soundkomponenten-Herstellers.

Videoausgang

Je nach der Eingangsbuchse des Monitors wird das Signal ausgegeben über

- VGA (Video Graphics Array)
- DVI (Digital Visual Interface)
- HDMI (High Definition Multimedia Interface), überträgt auch Ton

Die Grafikkomponente des Rechners ist bei modernen Mainboards meist auf diesen fest untergebracht. Für mehr Leistung bei speziellen Aufgaben, z.B. Videobearbeitung, empfiehlt sich die Verwendung einer speziellen Grafikkarte, die dann wie auf dem Bild links u.U. sogar eine aktive Kühlung haben kann.

Die Leistungsfähigkeit einer Grafikkomponente bemisst sich nach deren

- Arbeitsspeichergröße
- Taktfrequenz

Der Monitor

ist mittlerweile nahezu ausschließlich in LCD-Technik (Liquid Crystal Display) ausgeführt.
Unterscheidungsmerkmale:

- Größe (meist in Zoll Diagonale angegeben)
- Auflösung in Pixel (je mehr, desto besser; Full HD = 1920 x 1080 ist ein sehr guter Standard-wert)
- Reaktionszeit in ms (je weniger, desto besser)
- Lautsprecher eingebaut?
- Mikrofon eingebaut?
- Zusätzliche USB-Steckplätze?

Die meisten Flachbild-Fernseher sind auch als Monitore zu verwenden.

USB (Universal Serial Bus)

bietet eine universelle Verbindung des Rechners zu Massenspeichern und allen Arten externer Geräte, sogar zur Verbindung zweier Rechner. USB hat eine stetige Entwicklung hinter sich und wurde mit jeder Entwicklungsstufe schneller:

- USB 1.0 12 MBit/sec
- USB 2.0 400 MBit/sec
- USB 3.0 4 Gbit/sec
- USB 3.1 (in Entwicklung) 10 Gbit/sec

Die Technik ersetzte mit der Zeit die serielle und die parallele Schnittstelle, Firewire und ESATA
Und erlaubt die sehr einfache Schnittstellenvervielfachung durch USB-Hubs. Inzwischen werden nahe alle Peripheriegeräte über USB angebunden.

Apple hat eine Eigenentwicklung: Thunderbolt, nutzt aber daneben auch USB.

Die Software

Die Betriebssysteme

Betriebssysteme stellen sozusagen die Schnittstelle zwischen Mensch und Rechner dar. Die jetzt noch gebräuchlichen Betriebssysteme leiten sich nur von zwei Entwicklungslinien ab:

- UNIX ist aus einem Mehrbenutzersystem hervorgegangen, das von den Bell-Laboratories 1969 entwickelt wurde. Den entscheidenden Schub für die Verbreitung erhielt es 1991 von Linus Torvalds, der es als LINUX weiterentwickelte. Auf diesem Betriebssystem basiert seit 2001 das Apple-Betriebssystem MacOs. Auch das von Google für Smartphones (kostenlos) auf den Markt gebrachte Android enthält einen LINUX-Kern.
- DOS (Disk Operating System) von Microsoft hatte seinen Ursprung 1860 in einer IBM-Entwicklung, die später auch von Commodore und Atari übernommen wurde. Die ersten drei Windows-Versionen basieren direkt auf MS-DOS, während die späteren Windows-Varianten ab NT weitgehend Neuentwicklungen waren. Im Unterschied zu früheren Varianten unterstützen sie die parallele Verarbeitung von 64 Bit.

Die Aufgaben eines Betriebssystems:

sind

- Starten und Beenden des Rechnerbetriebs
- Organisation und Verwaltung des Arbeitsspeichers
- Steuerung der Hardwarekomponenten
- Organisation und Verwaltung der Speichermedien

- Organisation der Bildschirmanzeige
- Laden und Kontrollieren der Anwenderprogramme, Weitergabe von Benutzereingaben, Behandlung von Fehlern, Verwaltung von Benutzerrechten
- Bereitstellung von Dienstprogrammen für verschiedenste Zwecke: Datensicherung, Texteingabe, Telekommunikation, Spracheingabe, Zeichnen, Rechnen etc.

Am Beispiel von Windows: Ein typischer Startvorgang

1. Selbsttest der Hardware (**POST** = **P**ower **O**n **S**elf **T**est)
2. Startprozess initialisieren
3. Bootprogramm laden (Das Bootprogramm legt fest, was von wo geladen wird)
4. ggfs. Auswahl des Betriebssystems
   Überprüfen der Hardware
5. Auswahl der Konfiguration
6. Kernel (Betriebssystemkern) laden
7. Kernel initialisieren
8. Einloggen der Benutzer

Das Betriebssystem Windows und seine kostenlosen Alternativen:

Das Betriebssystem Windows basiert auf dem Ausgangs-Betriebssystem DOS und wurde ursprünglich seit 1987 entwickelt, um den Zugang zum Computer für einen größeren Nutzerkreis zu ermöglichen. So standen am Anfang der Entwicklung die Bedienung mit der Maus und die leichte Ansprechbarkeit der Datenträger im Vordergrund. Mit der Zeit kamen weitere Ziele hinzu, nämlich die

- Implantierung einer echten Mehrplatzfähigkeit mit einer Abgrenzung der Benutzerkonten,
- Anbindung von Cloud-Speichern (vgl. S.18)

Windows 7 ist seit 2009 in den meisten Dienststellen der Kirche eingeführt worden. Windows 8 fand bei seiner Einführung 2013 nur wenige echte Freunde, was auch daran liegt, dass es als „eierlegende Wollmilchsau“ für PCs, Tabletcomputer und Smartphones gleichermaßen programmiert war und zur Vorgängerversion zu viele Brüche vorhanden waren. Windows 10, die – nach Auskunft von Microsoft „letzte“ – Betriebssystemversion, vermeidet die meisten Fehler der Version 8.

Unix lebt als LINUX gut weiter. LINUX gibt es mittlerweile in 10 verschiedenen kostenlosen Distributionen, je nach Verwendungszweck. Einen Überblick finden Sie unter: http://www.pcwelt.de/ratgeber/Aktuelle_Linux-Distros_im_PC-WELT-Check-Linux-Distributionen-7971293.html

Office-Programme

Ein kostenpflichtiges Programm: **MS-Office 2013** ist im Handel als

- Home and Student mit Excel, Word, Powerpoint, One Note
- Home and Business: zusätzlich Outlook
- Professional: zusätzlich Publisher, Access, Outlook
  - auch als 2-Platz-Version erhältlich -

Es besteht keine Preisbindung, daher ist ein Preisvergleich besonders zu empfehlen; sehr günstig sind Download-Versionen bei Ebay.

Von Office 365 für 5 Plätze als Mietmodell für 99 €/Jahr muss abgeraten werden, weil das Programm eine standardmäßige Speicherung auf dem cloudbasierten (vgl. S. 18) Programm Onedrive mit dem physikalischen Speicher außerhalb des Bereichs der Europäischen Union vorsieht. Office 2016 ist angekündigt, kann aber noch nicht beurteilt werden.

Will man Microsoft Office durch sogenannte Freewareprogramme ersetzen, genügt es nicht, nur eines zu installieren. Zwar enthält Libre Office die wesentlichen Elemente der Textverarbeitung, Datenbank, Tabellenkalkulation, Präsentation und eines Zeichenprogramms, doch fehlen Mail Clients (zur Bearbeitung von E-Mails) und ein Publizierprogramm. Als freier Mail Client ist Thunderbird zusammen mit der Komponente Lightning sehr empfehlenswert; beide zusammen ersetzen ohne weiteres Outlook. Statt des MS Publisher kann das Programm Scribus installiert werden. Alle mit MS Office Produkten erzeugten Dateien sind mit diesen Programmen zu öffnen; umgekehrt können alle MS Office Dateien damit geschrieben werden.
Fundstellen: http://de.libreoffice.org http://www.mozilla.org

Virenschutzprogramme:

Als beste käufliche Virenschutzprogramme wurden getestet:

- Eset Smart Security (35 €)
- G Data Internet Security (35 €)
- Avira Internet Security (40 €)

Die genannten Preise beziehen sich jeweils auf eine Jahreslizenz und einen Arbeitsplatz. Unbedingt empfehlenswert ist immer noch ein zusätzlicher Trojanerschutz, z.B. www.malwarebytes.de
Die kostenlose Version davon reicht.

Virenschutz kann auch kostenlos installiert werden.

- Avira Free Antivirus
- Avast Free Antivirus

Die beiden Programme erkennen Viren gleich gut wie die käuflichen, haben aber keine Firewall (= Verhinderung unbefugter Aufnahme einer Verbindung mit dem Web). Die ist aber

- in vielen Routern vorhanden
- in Windows 7/8/10 eingebaut
- z.B. von Zoner Free kostenlos zu haben.

Webbrowser

- **Internet Explorer** (Microsoft): Nicht sehr komfortabel, vielfach als unsicher eingestuft, künftige Updates ungewiss; Nachfolger **Edge** kam mit Windows 10; kann noch nicht beurteilt werden;
- **Firefox** (Mozilla): Z. Zt. der am häufigsten verwendete Browser mit vielen Erweiterungen, als sehr sicher bezeichnet;
- **Chrome** (Google): Sehr flexibel und komfortabel; Datensicherheit zumindest fragwürdig;
- **Iron** (SR-Ware): basiert auf der Chrome-Technik, aber ohne dessen Datenprobleme – die derzeit sicherste Lösung;
- **Opera**: schnell und innovativ; Datenschutzprobleme nicht bekannt;
- **Safari** (Apple): Windows-Version des Apple-Standardbrowsers; inzwischen ausgereift und ausreichend schnell.

Alle Webbrowser sind kostenlos.

Kommunikationsprogramme für verschiedene Plattformen

- VOIP-Telefonie und Chatting: Skype (Microsoft). Voice Over IP – Telefonie unter Nutzung des Internetprotokolls - bringt Sicherheitsprobleme und ist deswegen für die Übertragung vertraulicher Informationen bzw. besonderer personenbezogener Daten nach § 2 Abs. 10 KDO ungeeignet.
- Messenger erlauben Schrift, Ton- und z.T. Videoverbindungen der gerade eingeloggten Benutzer, z.B. ICQ, Trilian. Auch sie sind nicht gerade sicher. Interessant sind aber die automatisch verschlüsselten Systeme, z.B. Cryptocat.
- WhatsApp ist ein internetbasierter, plattformübergreifender Instant-Messaging-Dienst für den Austausch von Textnachrichten, Bild-, Video- und Ton-Dateien sowie Standortinformationen zwischen Benutzern von Mobilgeräten wie Smartphones. Die Datensicherheit ist schon deswegen gering, weil das Programm von Facebook vertrieben wird. Allerdings ist eine Verschlüsselung angekündigt, wenn auch noch nicht durchgehend eingeführt. Das gibt unter Umständen Anlass dafür, die Einschätzung in einigen Monaten zu überprüfen. Eine derzeit bereits verfügbare sichere Alternative wäre Threema.

Grafikprogramme – Bearbeiten von Digitalfotos

Kaufprogramme:
PhotoShop CS 6 in der aktuellen Version für ca. 1000 € - wird in aller Regel nur von professionellen Bildbearbeitern ausgenutzt; völlig ausreichend in den meisten Fällen: PhotoShop Elements (ca. 100 €)
Raw-Bild-Entwicklung Lightroom
Freeware:
Äquivalent zu Photoshop CS6: GIMP
Meist ausreichend jedoch: Photoscape, Picasa
Dazu jedenfalls sinnvoll die kostenlosen Programme SHIFTN und Exifer
Raw-Bild-Entwicklung Photivo oder Raw Therapee

Diese Freeware-Programme braucht man normalerweise außerdem:

Advanced Renamer	sehr flexibles Umbenennen von Dateien
Speccy	Informationen über die Hardware des Rechners
Crystal Disk Info	Auskunft über den Gesundheitszustand der Festplatte
Fences (Version1.0!)	Schafft Ordnung auf dem Desktop
Foxit Reader	Lesen von PDF - sicherer als Adobe Reader)
Autostart Administrator	gestattet einen Eingriff in den Autostart von Programmen
Tera Copy	besonders leistungsfähiges Kopierprogramm
Unstoppable Copier	zum Kopieren von beschädigten CDs und DVDs
Recuva	Wiederherstellen von Dateien
GetFolderSize	zeigt die Ordnergröße im Explorer an
Multi Commander	sehr guter Ersatz für den Explorer
Don‘t Sleep	verhindert die Abschaltung des Rechners durch die Energieoptionen
CCleaner	räumt den Rechner regelmäßig auf
Paragon Personal Backup	sehr gutes Datensicherungs-Programm
Teamviewer	erlaubt die Fernwartung des Rechners
Irfanview	zur Anzeige und Organisation von Bildern
ImgBurn	Brennen von CDs, DVDs und BLU-Rays
Locate 32	(Desktopsuche)
oder Google Desktop Search	
PDF Creator	produziert PDF Dateien
Adware Cleaner	beseitigt unerwünschte Werbedateien

Grundregeln für die Installation von Freeware

- Download nur von CHIP, PC-Welt, Computerbild oder Heise, nicht von Anbietern, die Ihnen ein besonderes Downloadprogramm installieren wollen wie z.B. Softonic.
- Immer die benutzerdefinierte Installation wählen (auch bei Download von Chip; dort als manuelle Installation bezeichnet!). Sehen Sie sich genau an, wozu Sie ihre Zustimmung geben!
- Achten Sie darauf, dass Sie nie der Installation von Toolbars, Suchhilfen (z.B. „Ask“) o.ä. zustimmen! Deaktivieren Sie unbedingt die entsprechenden Kästchen für das Einverständnis.
- Prüfen Sie nach der Installation des Programmes unter Systemsteuerung – Programme, was sonst noch heute installiert wurde (auf Änderungsdatum klicken). Deinstallieren Sie gleich, was Sie nicht wollten!
- Wenn doch einmal etwas hängengeblieben ist: EmsiSoft Emergency Kit oder Malwarebytes herunterladen, ebenso vorsichtig installieren und zum Säubern hernehmen.

Netzwerke

Hardware-Voraussetzungen

Netzwerke können prinzipiell drahtgebunden oder drahtlos sein. Nahezu jeder handelsübliche Desktop-PC hat einen LAN- (Local Area Network) Anschluss, der auf dem Mainboard integriert ist. An drahtloser Kommunikation kommen in Betracht ein WLAN (Wireless LAN) – Empfänger, ausgeführt als

- PCIe-Karte
- USB-WLAN-Empfänger
- Bluetooth-Empfänger

Der Netzaufbau am Beispiel eines kleinen Netzes:

In der einfachsten Variante werden PC und Telefon über ein Patch-Kabel an den Router angeschlossen. Der Router besorgte bis 2015 bei Telekomanschlüssen die Trennung des Telefonnetzes vom Datennetz; er benötigte in diesen Fällen auch noch einen sogenannten Splitter. Seit die Telekom ihre Anschlüsse auf Datenleitungen umstellt, ist dieses Bauteil nicht mehr erforderlich. Ein Beispiel ist der in Deutschland meistverkaufte Router, die FRITZ!Box 7490:

Die Grafik zeigt die vielfältigen Anschlussmöglichkeiten eines solchen Routers. Jeder Router enthält wiederum einen eigenen Computer, der typischerweise auf dem Betriebssystem Unix läuft. Wie

ein Computer kann sein Betriebssystem Updates erhalten und sich so einer Veränderung der Umgebung anpassen.

Bis 1.11.2015 mussten die Kunden der Internet-Provider den von ihrem Provider gestellten Router verwenden. Seither kann jeder Kunde sich einen eigenen Router seiner Wahl anschaffen.

Die meisten Router sind bereits für die Verbindung zu 4 Netzgeräten gebaut. Wenn mehr Netzgeräte an einen Router geschaltet werden müssen, verwendet man einen sogenannten Switch (s. rechts). Switches für kleine Netzwerke werden mit 5-13 Netzanschlüssen gebaut; für große Netzwerke gibt es Geräte mit bis 256 Anschlüssen.

In ein Netzwerk lassen sich außer Computern noch andere Geräte integrieren, die dann für sämtliche Computer des Netzwerkes oder einen Teil derselben zur Verfügung stehen, so z.B.:

- gemeinsam genutzte Festplatten (NAS = network attached storage); Information hier
- Drucker
- Faxgeräte

In der Regel ist der Router selbst in der Lage, auch drahtlose Verbindungen herzustellen und enthält dann ein sogenanntes WLAN-Modul. Damit können auch Computer angebunden werden, die nicht über einen ständigen Netzanschluss in den Räumen verfügen. Die meisten unserer Dienststellen wurden in Gebäuden errichtet, deren Bauzeit schon länger zurückliegt. Zur Zeit des Baues dachte man noch nicht daran, Leitungen für Computerkabel vorzusehen. In solchen Fällen hilft das WLAN, wirft aber auch Sicherheitsprobleme auf, wie später noch darzustellen sein wird. Es wurden daher in den letzten 15 Jahren Übertragungstechniken entwickelt, die es erlauben, die Computer Informationen über das Stromkabel zu versenden. Die sogenannte Powerline Technik arbeitet mit Adaptern, die in die Elektro-Steckdose gesteckt werden. Was im Einzelfall günstiger, ist muss abgewogen werden.

WLAN	**Powerline**
• Preiswerter als Powerline zumindest ab 3 Gegenstellen • Übertragungsgeschwindigkeit theoretisch bis 1300 MBit/s, praktisch nur 100 Mbit/s • Relativ unsicher • Messbare Elektrosmogbelastung 	• Teurer , jedenfalls ab 3 Gegenstellen • Übertragungsgeschwindigkeit tatsächlich bis 1000 MBit/s • Sehr sicher • Kein Elektrosmog 

Das WLAN

Prinzipiell ist ein WLAN für jedermann zugänglich. Der gesamte Verkehr auf dem Netz kann damit ausgespäht werden. U. U. ist auch ein Zugriff auf die angeschlossenen Computer von außen möglich. Deswegen muss das WLAN verschlüsselt werden. Dazu gibt es mehrere Wege:

- WEP (Wired Equivalent Privacy) bietet nur wenig Schutz vor sog. „Brute Force"-Angriffen, also solchen, bei denen einen ganzes Wörterbuch innerhalb weniger Sekunden als Passwort ausprobiert wird.
- AES (Advanced Encryption Standard) arbeitet zusammen mit der technischen Ergänzung WPA2 (WI-FI Protected Access) und bildet gegenwärtig eine ausreichend hohe Sicherheit.

Besser noch wäre ein Schutz durch einen sog. VPN-Tunnel (Virtual Private Network): Dabei wird innerhalb eines Netzes ein anderes so geknüpft, dass die beiden Netze voneinander zwar nicht physikalisch, aber logisch getrennt sind.

Die Anbindung an das öffentliche Netz

erfolgt bei stationären Routern jetzt nur mehr in der Form eines Breitbandanschlusses in folgenden Leistungsvarianten:
6 MBit/s 16 MBit/s 50 MBit/s 100 MBit/s 200 Mbit/s

Werte über 16 Mbit/s lassen sich nur mit Glasfaserkabeln realisieren. Bei allen Werten handelt es sich um theoretische Maximalwerte in der Richtung zum lokalen Netz hin (Download). Der Uploadwert (entgegengesetzte Richtung) beträgt nur einen Bruchteil dessen.

Bei drahtloser Übertragung ist der Durchsatz nicht nur von der Leistungsfähigkeit des Netzes, sondern auch von der Zahl eingebuchter Geräte abhängig. Typische Werte sind:
3,8 MBit/s bei Edge 7,6 MBit/s bei GPRS 50 – 300 (theoretisch) MBit/s bei LTE

LTE (Long Term Evolution) soll in Zukunft nicht nur die mobile Datenverarbeitung gewährleisten, sondern auch die Versorgung mit Breitbandanschlüssen außerhalb der Ballungsgebiete sicherstellen.

Die Anforderungen an einen guten Router

können wir also jetzt zusammenstellen:

- Updatefähigkeit der Software
- Anschüsse mindestens
  - 4 LAN (am besten 1000 MBit/s)
  - 1 USB
  - 3 Telefon
- Eingebaute Basiseinheit für schnurlose Telefone vorhanden
- Telefonbuch- und/oder Kurzwahlfunktion; Durchwahlfunktion
- Eingebaute Fax- und Emailfähigkeit
- WLAN mit 1300 MBit/s, WPA2-Sicherung (**W**i-Fi **P**rotected **A**ccess),
  WPS (**W**ireless **P**rovisioning **S**ervice), Nacht- und Gastnetzschaltung, Unterstützung mehrerer Frequenzen
- Möglichkeit des Fernzugangs

Das World Wide Web

entstand durch den Zusammenschluss einzelstaatlicher Datennetze. Seine Internationalität wird auch durch den an sich nicht zutreffenden Begriff Internet gekennzeichnet. Es basiert auf drei Kernstandards:

- HTTP (**H**yper**t**ext **T**ransfer **P**rotokoll) ist ein gemeinsames Protokoll, mit dem der Browser (= das Empfangsprogramm in jedem Rechner) Informationen vom Webserver anfordern kann.
- HTML (**H**yper**t**ext **M**arkup **L**anguage) als Dokumentenbeschreibungssprache, die festlegt, wie die Information gegliedert ist und wie die Dokumente verknüpft sind (Hyperlinks). Nur dank

HTML sind alle Rechner auf der Welt in der Lage, im Prinzip alle Internetseiten aufzurufen und zu lesen.

- URLs (**U**niform **R**essource **L**ocator) als eindeutige Bezeichnung einer Ressource, die in Hyperlinks verwendet wird. Jede Webseite hat eine eindeutige Bezeichnung, unter der sie im WWW gefunden werden kann.

Im Prinzip gilt für das WWW alles, was auch für ein lokales Netz gilt, entsprechend. Allerdings erfolgt die Vergabe der IP-Adressen nicht zentral durch einen Router, sondern gebietsbezogen, aber auf internationalen Absprachen beruhend.

Die IP (Internetprotokoll) – Adresse

ist eine auf dem Internetprotokoll basierende eindeutige Ziffer, die ein bestimmtes Gerät als Anschrift verwendet. Noch ist die Verwendung der sog. „IPv4"-Adressen mit 32 Stellen die geläufige Bezeichnung. Eine IPv4-Adresse besteht aus vier Oktetten (Im Ergebnis enthält sie also vier Bytes) und sieht z.B. bei einem Router in einem Heimnetz wie folgt aus: ***192.168.178.1***

Im Heimnetz verteilt der Router die IP-Adressen; das Verfahren heißt DHCP (Dynamic Host Configuration Protocol). So erhält jedes Gerät, das sich im LAN und/oder WLAN dieses Routers angemeldet hat, eine eigene Adresse, z.B.
192.168.178.51 für den ersten Computer
192.168.178.52 für den zweiten Computer
192.168.178.53 für den dritten Computer usw. und zwar jeweils in der Reihenfolge der Anmeldung.

Die Ziffern 192.168.178.02 - 192.168.178.50 sind typischerweise für andere Geräte reserviert, zum Beispiel für Drucker. 192.168.178.01 ist die interne Adresse des Routers selbst. Der Nummernkreis 192.X.X.X ist speziell für interne Netzwerke gedacht. Extern hat jeder angemeldete Router wiederum eine andere Nummer, die vom jeweiligen Internet-Provider nach einem allgemeinen Schema vergeben wird. Was die Sache noch weiter kompliziert, ist, dass der Internet-Provider die Leitung bei Privatleuten und kleinen Dienststellen jeden Morgen um 5:00 Uhr trennt und eine neue IP-Adresse vergibt. Nehmen wir einmal an die IP-Adresse extern würde ***213.112.144*** lauten. Der Router verwaltet Intern-IP und Extern-IP, weiß beide und kennt die Unterschiede.

Bei den Internetprotokoll-Adressen muss ich Ihnen gleich wieder zumuten, sich auf eine Änderung einzustellen. Noch ist die Verwendung der IPv4-Adressen mit 32 Stellen die geläufige Bezeichnung; die Umstellung auf IPv6 mit 128 Stellen ist aber im Gange.IPv4 ermöglichte nämlich nur ca. 4 Mrd. Anschriften, IPv6 ein Vielfaches davon. Die Provider haben bereits beide Adressen und verwalten sie ebenfalls intern. Wann es dazu kommen wird, dass nur noch die IPV6-Adressen zu verwenden sind, ist noch nicht zu sagen.

IP-Adressen und Webseitenaufruf

Sehen wir uns doch einmal an, was passiert, wenn eine bestimmte Webseite angewählt wird.
Der Benutzer wählt eine bestimmte Webseite an,
z.B. **www.tagesschau.de**
Die Anwahl wird zu einem sog. DNS-Server (Domain Name Server) geleitet.
Der sieht in der Datenbank nach und stellt fest:

www.tagesschau.de hat die IP-Adresse 112.136.201.23

Dies wird dem Ausgangsrechner mitgeteilt.
Dessen Browser wählt nun die bezeichnete IP-Adresse an.

Die Manipulation oder Sperre des Internets in einem teildemokratischen Land kann dadurch erfolgen, dass die dortigen DNS-Server angewiesen werden, nicht oder auf die falsche Webseite – zum Beispiel die des Zentralkomitees der herrschenden Partei – weiterzuleiten.

Die Sache mit der täglich wechselnden IP-Adresse hat einen Haken: Wenn man sich in seinen häuslichen Rechner oder den seiner Dienststelle einwählen will, weiß man nicht die richtige IP-Adresse. Nur große Unternehmen haben feste IP-Adressen, alle anderen Webteilnehmer haben täglich wechselnde, weil der Provider ja jeden Morgen eine neue IP-Adresse zuteilt. Um trotzdem eine Einwahl in bestimmte Rechner, zum Beispiel solche, in denen die eigenen Daten auf EU-Gebiet gespeichert sind, zu ermöglichen, wählt man das Verfahren der dynamischen DNS. Das funktioniert so:

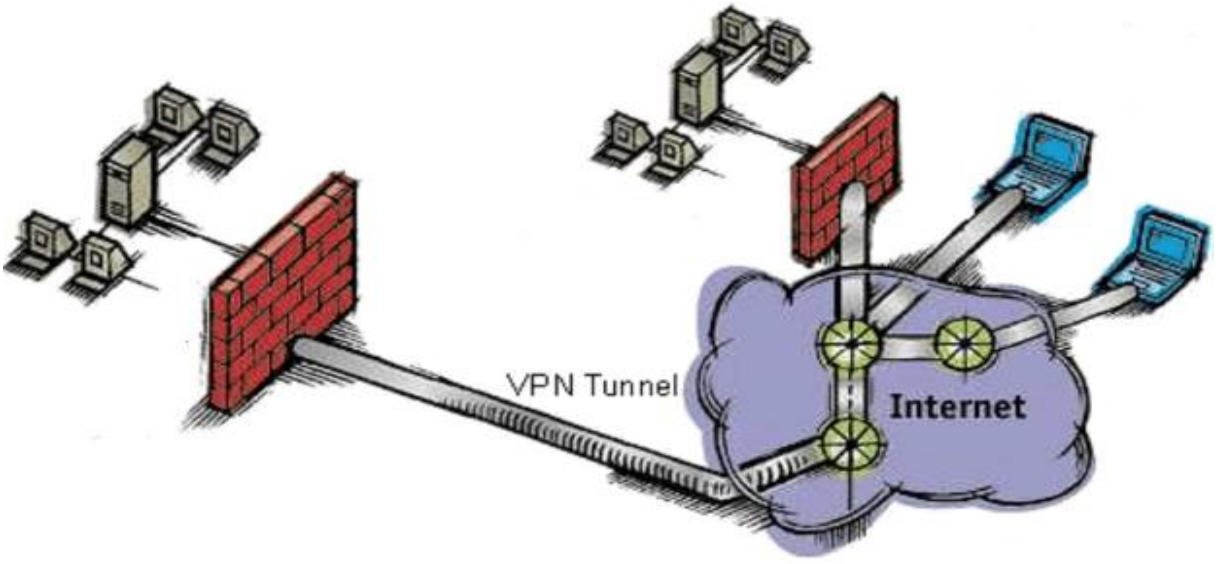
- Rechner Joachimski bekommt um 3:00 Uhr die IP-Adresse 113.17.187.212
- Router Joachimski teilt dies der Webdatenbank dyndns.org mit; wird gespeichert.
- Jetzt kommt die Anfrage eines Nutzers: Ich will Joachimski direkt anwählen, um von seinem Rechner etwas herunterzuladen.
- Antwort von dyndns.org: Nimm doch 113.17.187.212
- Der Nutzer wählt dies an und loggt sich mit Benutzername und Passwort ein.

Dafür gab es früher einen kostenlosen Service, dyndns.org. Leider verlangt das Unternehmen inzwischen etwas dafür, aber es gibt reichlich Ersatz:
http://www.pcwelt.de/ratgeber/DynDNS-Alternativen-kostenlos-5680355.html

Virtuelles Privates Netzwerk

Nehmen wir an, Sie befinden sich auf Dienstreise und wollen auf das Netzwerk Ihrer Dienststelle zugreifen, um dort Unterlagen abzurufen. Sie stellen eine Verbindung zum Internet her und wählen sich anschließend mittels der Software in das VPN-Netzwerk ein. Nun können Sie so arbeiten als ob Sie im Büro wären, obwohl Sie hunderte Kilometer entfernt sind.

VPN bezeichnet also ein virtuelles privates - in sich geschlossenes - Kommunikationsnetz, das ein bestehendes Kommunikationsnetz als Transportmedium verwendet. Es dient dazu, Teilnehmer des bestehenden Kommunikationsnetzes an ein anderes Netz zu binden. Sobald ein Teilnehmer eine VPN-Verbindung aufbaut, ist die Auswirkung vergleichbar mit dem Umstecken seines Netzwerkkabels an das per VPN zugeordnete Netz. Machen wir ein Beispiel: Ein Unternehmen will seine Heimarbeitsplätze in das eigene lokale Netzwerk integrieren. Das sieht dann so aus:



Der sogenannte VPN Tunnel „untergräbt“ das öffentliche weltweite Netz und schafft per Software ein eigenes Netz, das gegenüber dem öffentlichen abgegrenzt ist. Kein Teilnehmer des öffentlichen Netzes kann in das VPN hineinsehen. Sehr praktisch ist das auch, wenn man zum Beispiel auf den Rechner seiner Dienststelle von einem Internetcafé aus zugreifen muss. Die WLAN Verbindung eines Internetcafés ist regelmäßig nicht mit Sicherungen versehen, so dass im Prinzip jeder, der dort eingewählt ist, alle Eingaben lesen könnte. VPN verhindert das und schafft auf diese Weise auch die notwendige Sicherheit. VPN Tunnel ermöglichen also einen virtuellen Anschluss eines Rechners an ein bestimmtes Netz. Sie sind relativ einfach einzurichten und bieten höchstmögliche Sicherheit. Selbst für den Privatgebrauch lässt sich dies nutzen:

- Download und Installation von „hotspot shield“ (kostenlos, werbefinanziert) z.B. auf dem Laptop
- Bei Einwahl im Zug oder Internetcafe baut die Software eine VPN-Verbindung direkt zur gewünschten Webseite auf, die – relativ – sicher ist.
- Ein oft nicht unerwünschter Nebeneffekt: Es lässt sich eine IP-Adresse des US-Bereichs wählen.

Cloud-Computing

ist eine Sammelbezeichnung für die Speicherung persönlicher Daten (Dokumente, Bilder, Musik, Video) auf entfernten Servern, die vom Nutzer über das WWW erreicht werden.

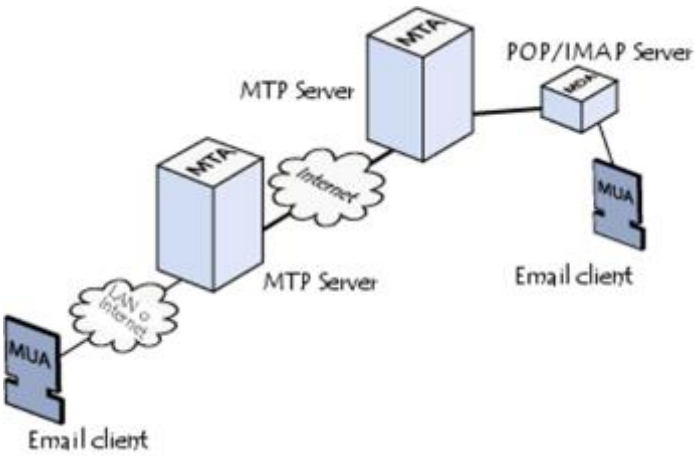
Üblicherweise muss der Nutzer beim Anbieter ein Konto einrichten und erhält einen Benutzernamen. Dann erfolgt eine Anmeldung mit Benutzernamen und Passwort. Auf den Speicher des Anbieters kann der Nutzer so zugreifen, als wäre er in seinem lokalen Rechner vorhanden. Clouddienste sind meist bei geringeren Speichergrößen frei (und ggfs. werbefinanziert), bei größeren aber kostenpflichtig.

Das Hauptproblem bei der Cloud ist die pysikalische Datenspeicherung in Gebieten außerhalb der EU. Dies tritt gerade bei den wichtigsten Anbietern auf: Dropbox, Microsoft Skydrive, Apple

Das Datenschutzproblem kann man vermeiden bei den Anbietern T-Online Mediencenter, Web.de, 1&1, die ihren physikalischen Speicher im Gebiet der Europäischen Union haben. T-Online bietet 25 GB freien Speicherplatz, 1&1 im Zusammenhang mit einem DSL-Vertrag sogar ein ganzes Terabyte.

Die beste Lösung für kleine Dienststellen wie Pfarreien oder Verbände ist aber die eigene Cloud mit einer NAS – gemeinsame Festplatte im eigenen Netzwerk – und dem (freien) Programm „owncloud“ (Installationsanleitung hier).

Der E-Mail-Verkehr



So funktioniert der Versand von E-Mails:

- Client ruft Server
- Server meldet sich bereit
- Client nennt seinen Namen
- Server bestätigt
- Client nennt Absenderadresse
- Server bestätigt
- Client nennt Empfängeradresse
- Server bestätigt
- Client kündigt Inhalt der E-Mail an
- Server bereit für diesen Vorgang

Die Begriffe:

SMTP-Server: Dient dem Versand der Emails
Pop3-Server: Empfangsserver. Auf dem Server bleibt jeweils eine Kopie des Emails gespeichert, auch wenn es im Email-Client gelöscht wird. Die Löschung muss dann im Server explizit oder per Zeitablauf verwaltet werden.
IMAP-Server: Auch Empfangsserver, aber: Die Löschung auf dem Client führt (prinzipiell) zur Löschung auf dem Server

Die Sicherheit des E-Mail-Verkehrs:

Der E-Mail Verkehr über normale Verbindungen ist im höchsten Maße unsicher. Wer die E-Mail-Adresse des Empfängers und den Namen des dazugehörigen Netzknoten weiß, kann E-Mails ganz einfach über Google abfangen. Wir können zwar davon ausgehen, dass der innerdienstliche E-Mail-Verkehr, jedenfalls, soweit er über das Diözesennetz läuft, sicher ist. Der E-Mail-Verkehr mit der Außenwelt ist es aber sicher nicht. Ein Verkehr mit der Außenwelt liegt schon dann vor, wenn eine Pfarrei mit dem dazugehörigen Kindergarten korrespondiert.

Es wurde deswegen vielfach verlangt, personenbezogene Daten überhaupt nicht in E-Mails zu übertragen. Eine derartige Forderung lässt jedoch außer Acht, dass der E-Mail-Verkehr ganz erhebliche Erleichterungen und vor allem eine wirkliche Beschleunigung der Korrespondenz mit sich bringt. Im Rahmen einer Abwägung kann man deswegen folgende Regel aufstellen:

Personenbezogene Daten dürfen auch in E-Mails genannt werden, solange es sich nicht um solche im Sinne des § 2 Abs. 10 KDO handelt. Zumindest gegenwärtig ist eine andere Ansicht auch bei der sogenannten DE-Mail nicht gerechtfertigt, da glaubwürdige Berichte zeigen, dass auch diese Korrespondenz in hohem Maße gefährdet ist. Wenn also Daten im Sinne des § 2 Abs. 10 KDO übertragen werden müssen, bedarf es einer **Verschlüsselung der E-Mails.** Dafür gibt es im Prinzip drei Wege:

- **mit Verschlüsselungsprogrammen, z.B. GpGforWin**:
  - Anton schickt Berta eine E-Mail:
  - Die Verschlüsselung und Signatur der zu versendenden Nachricht übernimmt der E-Mail-Client von Anton. Zur Verschlüsselung wird der öffentliche Schlüssel von Berta verwendet, den sie auf ihrer Webseite stehen hat. Die Signatur erfolgt mit dem privaten Schlüssel von Anton, den er Berta mitteilt.

- Die Entschlüsselung und Signaturprüfung der Nachricht übernimmt der E-Mail-Client von Berta. Die Entschlüsselung erfolgt mit dem privaten Schlüssel von Berta. Die Prüfung der Signatur erfolgt mit dem öffentlichen Schlüssel von Anton.
  Wer eine derartige Lösung sucht, findet hier eine Anleitung.

- **mit einer Webmailer-Lösung:**
  Im Prinzip wird die E-Mail auf einer Webseite der kirchlichen Dienststelle produziert und von dort abgeschickt. Sie verlässt sozusagen nie den Rechner der Dienststelle.

- **mit einer VPN-Tunnel-Lösung**
  Mitarbeiter A schickt seiner Dienststelle vom häuslichen VPN-Rechner aus eine E-Mail.

Ganz generell ist beim E-Mail-Empfang zu Vorsicht zu raten. Gerade über E-Mails werden am häufigsten Viren in fremde Rechner eingeschleust; sie verbergen sich regelmäßig in den Anhängen. Öffnen Sie nie den Anhang eines E-Mails von unbekannten Absendern! Besonders gefährlich sind Dateien mit den Endungen .exe, jpg, doc, docx, pdf. Nun ist leider bei Windows von Haus aus im Explorer unter (Windows 7) **Organisieren Ordneroptionen Ansicht** die Option „*Erweiterungen bei bekannten Dateitypen ausblenden*“ aktiviert. Ich empfehle, das abzuwählen, um Risiken zu vermeiden.

Einige Bemerkungen zum Schluss:

Ich hoffe wirklich, dass ich Ihnen ein paar Zusammenhänge habe erklären können. Wenn dem so ist, wäre es wirklich schade, das frisch aufgebaute Verständnis wieder verkümmern zu lassen. Eine gute Möglichkeit, am Ball zu bleiben, ist das Lesen von Zeitschriften. Haben Sie keine Angst vor Computerzeitschriften! Wenn Sie mich danach fragen, welche, würde ich antworten

Für Anfänger:	*Computerbild* (sehr schön aufgebaut, weil wirklich alles von Anfang an erklärt wird). Durchaus empfehlenswert ist auch der kostenlose tägliche Newsletter.
	PC Go (sehr interessante Artikel, setzt etwas mehr voraus als *Computerbild*)
Für Fortgeschrittene:	*Chip*
	PC-Welt
Für Insider:	*PC-Magazin*

Ich habe mich jedenfalls über Ihr Interesse gefreut und wünsche Ihnen viel Spaß und möglichst wenig Ärger mit der EDV.

Jupp Joachimski