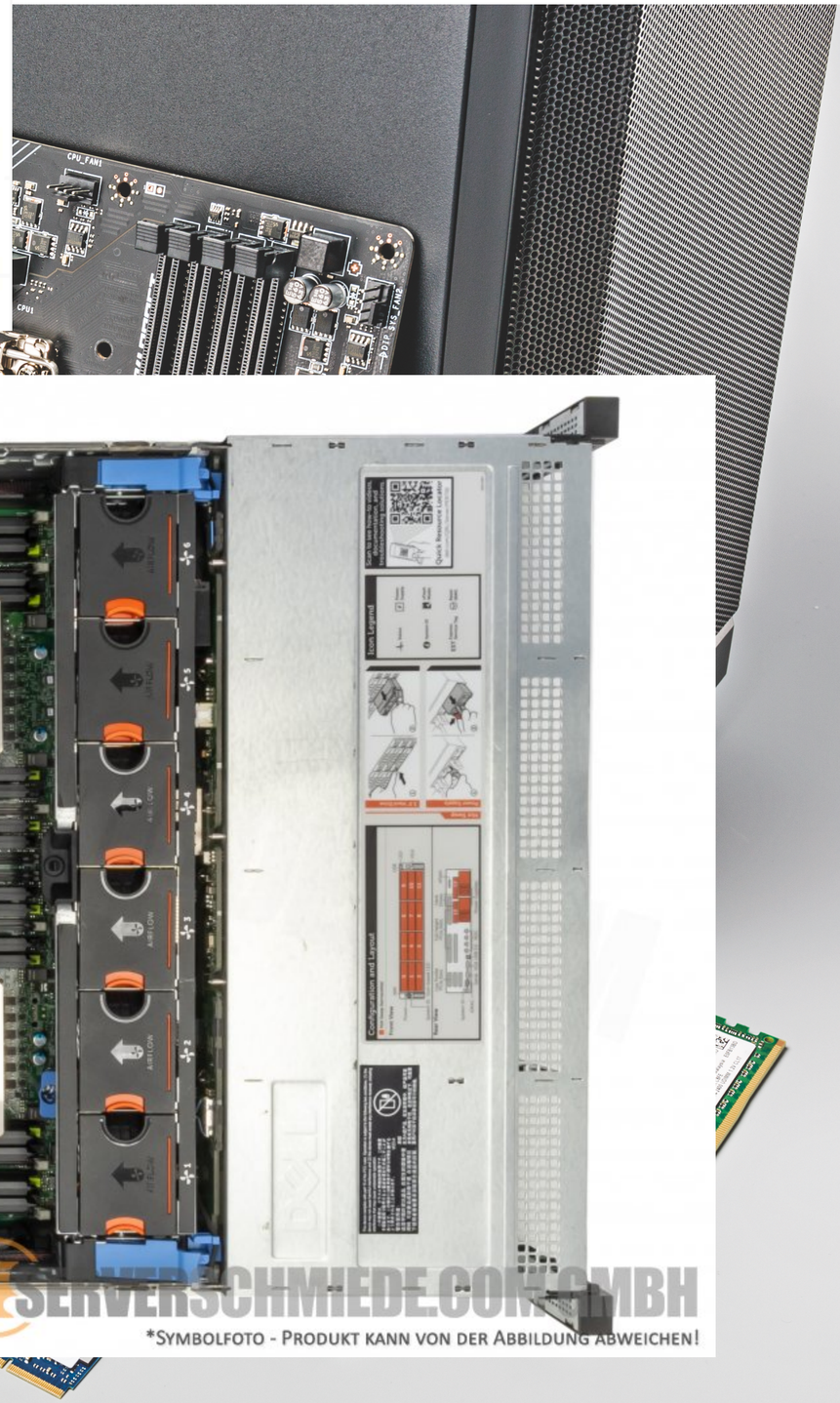
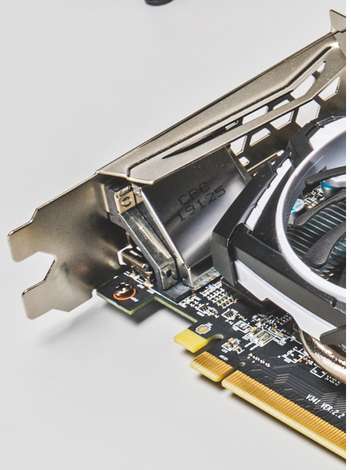
Datensicherheit
Prof. W. Lisiewicz
E-Mail: w.lisiewicz@hs-sm.de

E.1. Computer - Aufbau



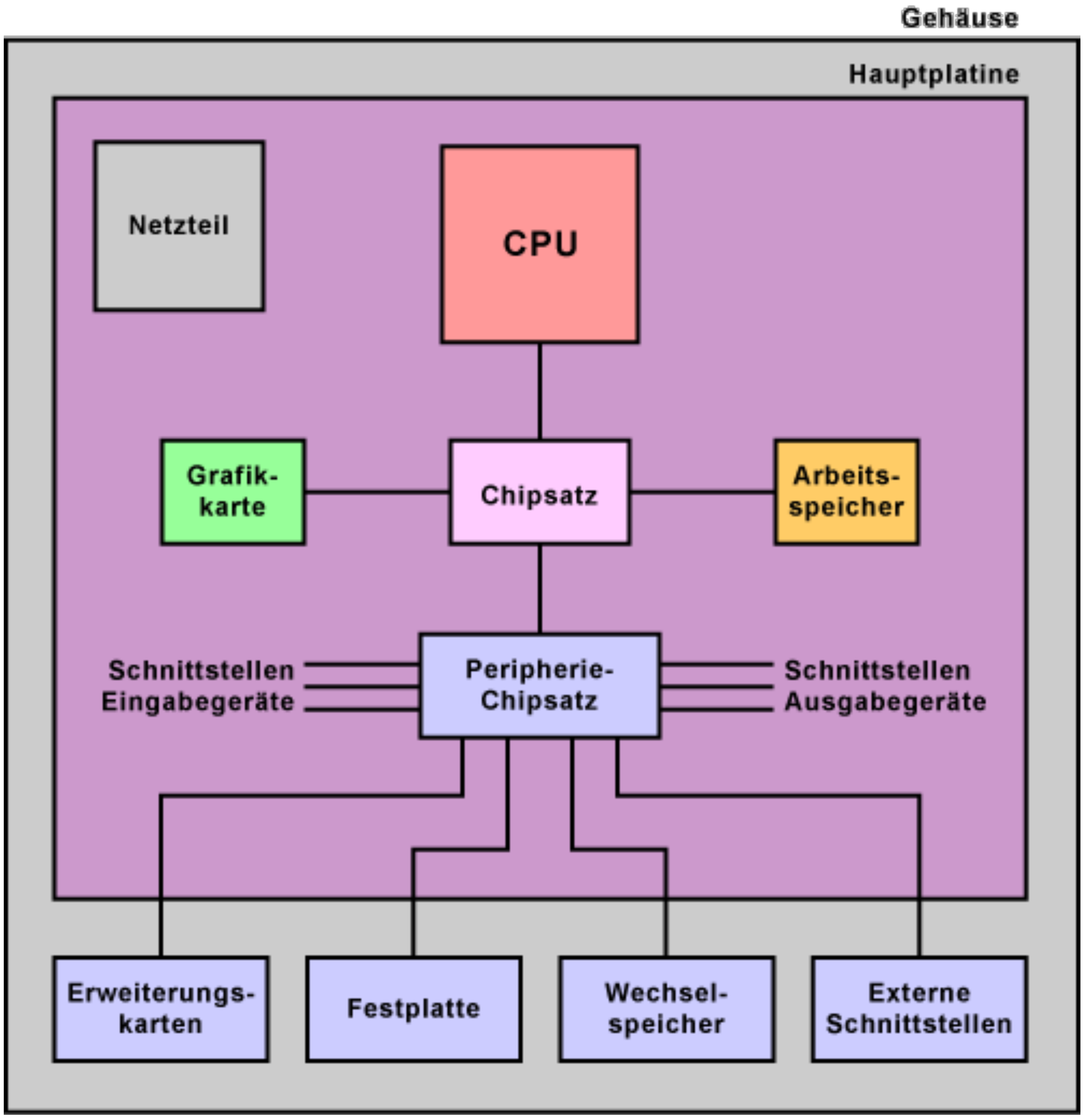


E.1. Computer - Aufbau

Welche Komponenten sind relevant für die Datensicherheit?

- CPU?
- Arbeitsspeicher?
- Netzteil?
- Festplatte?
- Externe Schnittstellen?
- Eingabegeräte?

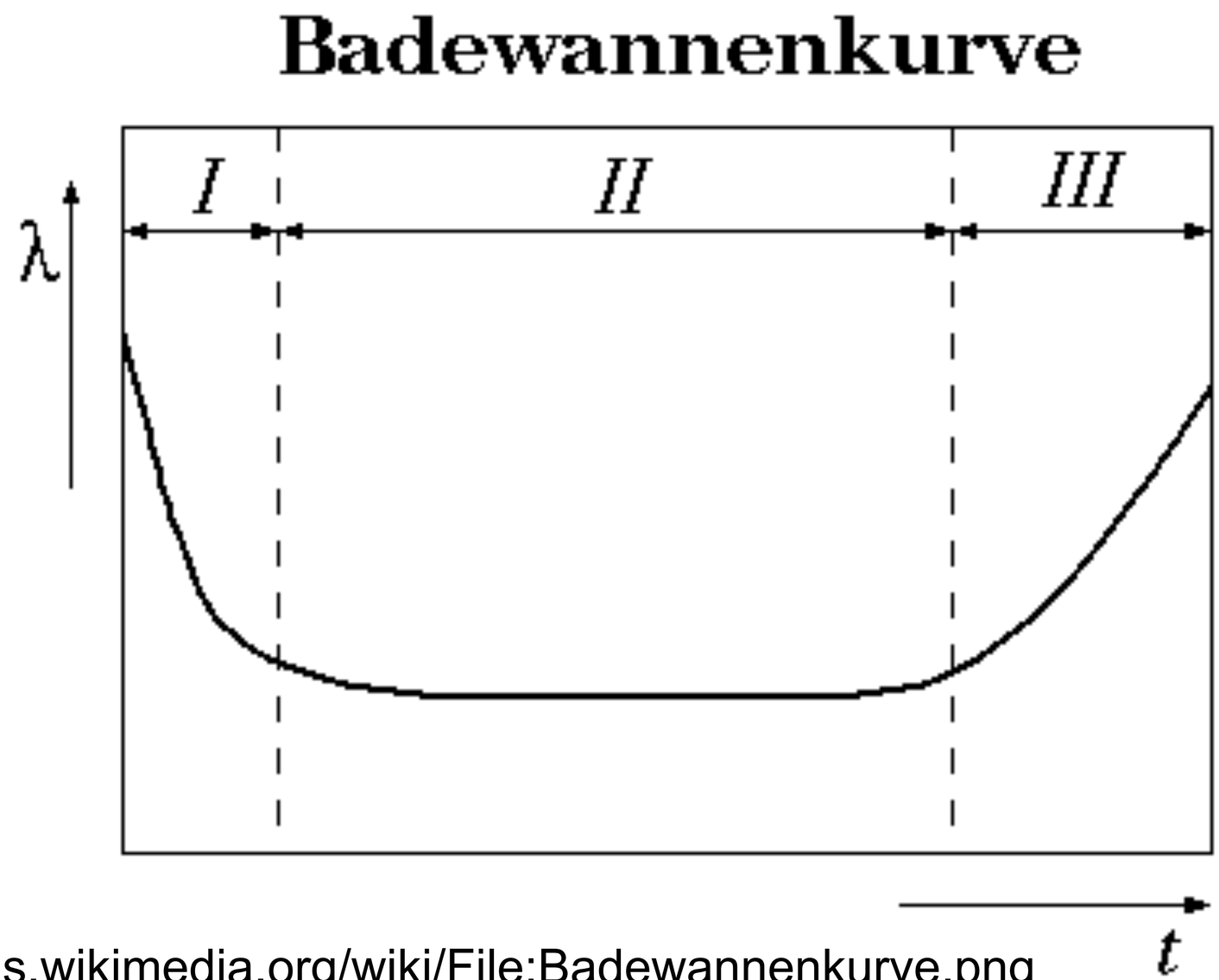
eigentlich alle!



Vgl.: https://www.elektronik-kompendium.de/sites/com/1309121.htm

E.1. Computer - Verfügbarkeit - Alterungsprozess

Hardwarealter vs. Ausfallwahrscheinlichkeit



Vgl.: https://commons.wikimedia.org/wiki/File:Badewannenkurve.png

Datensicherheit
Prof. W. Lisiewicz
E-Mail: w.lisiewicz@hs-sm.de

E.2. Software

Anwendungen

Die eigentliche Arbeit erledigen, Geschäftsprozesse ermöglichen:

- Geschäftssoftware
- Kommunikation
- Datenbanken
- etc. etc.

Betriebssystem

Anwendungen ermöglichen:

- Grundlage für Anwendungen
- Hardware, Ressourcen nutzen können
- speichern und lesen von Daten

BIOS / Firmware

Systemstart / Hardwareeinstellungen

Hardware

physikalische Geräte

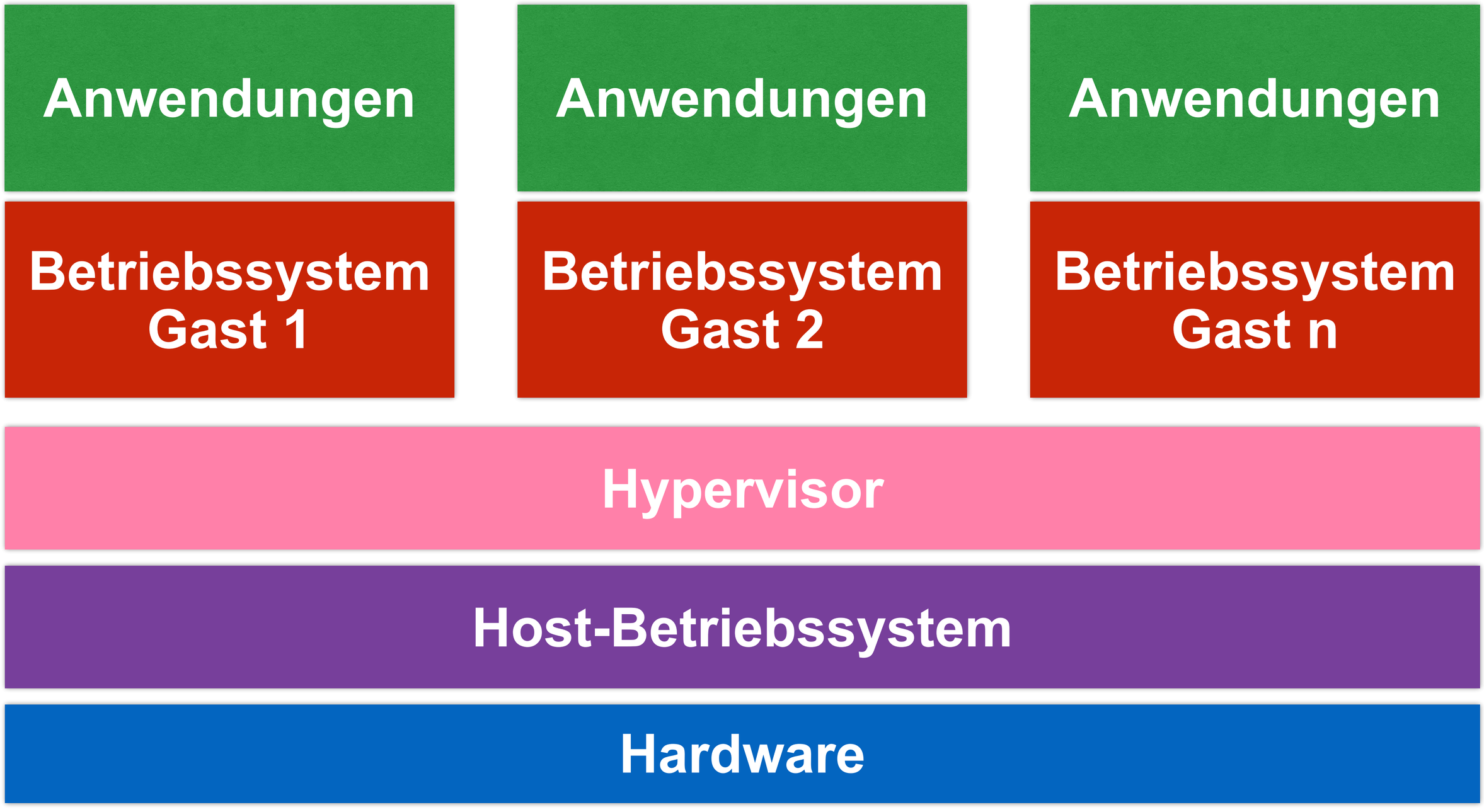
E.2. Software

Betriebssysteme - eine Übersicht

Desktop	mobile Geräte	IoT	Server
DOS, Windows (bis ME), **Windows** NT bis **10** MacOS, Mac OSX (Darwin) OS2, Linux, Android	**Android** iOS, iPadOS (Darwin) PalmOS bada MeeGo Windows Phone Linux	Ubuntu for IoT Contiki Windows IoT Brillo OS RIOT OS	Windows Novell NetWare **UNIX** SunOS/**Solaris** HP-UX, AIX **BSD**: heute Free-Net-, OpenBSD **Linux**

TOP 500 Supercomputer, ISS: Linux
(2017: letzter AIX IBM rausgefallen);

E.3. Exkurs: Virtualisierung



E.3. Exkurs: Virtualisierung

Einige Sicherheitsprobleme hängen nicht zuletzt mit dem Trend zur Virtualisierung zusammen. Eine durchaus praktische Technologie wendet sich - wie so oft - plötzlich gegen den Anwender, weil mit ihr völlig neue Angriffsformen möglich werden (Stichwort: Meltdown / Spectre). Dies in Verbindung mit Cloud-Anwendungen macht die Fülle der Angriffsmöglichkeiten perfekt!

Beispiele für Virtualisierungslösungen:

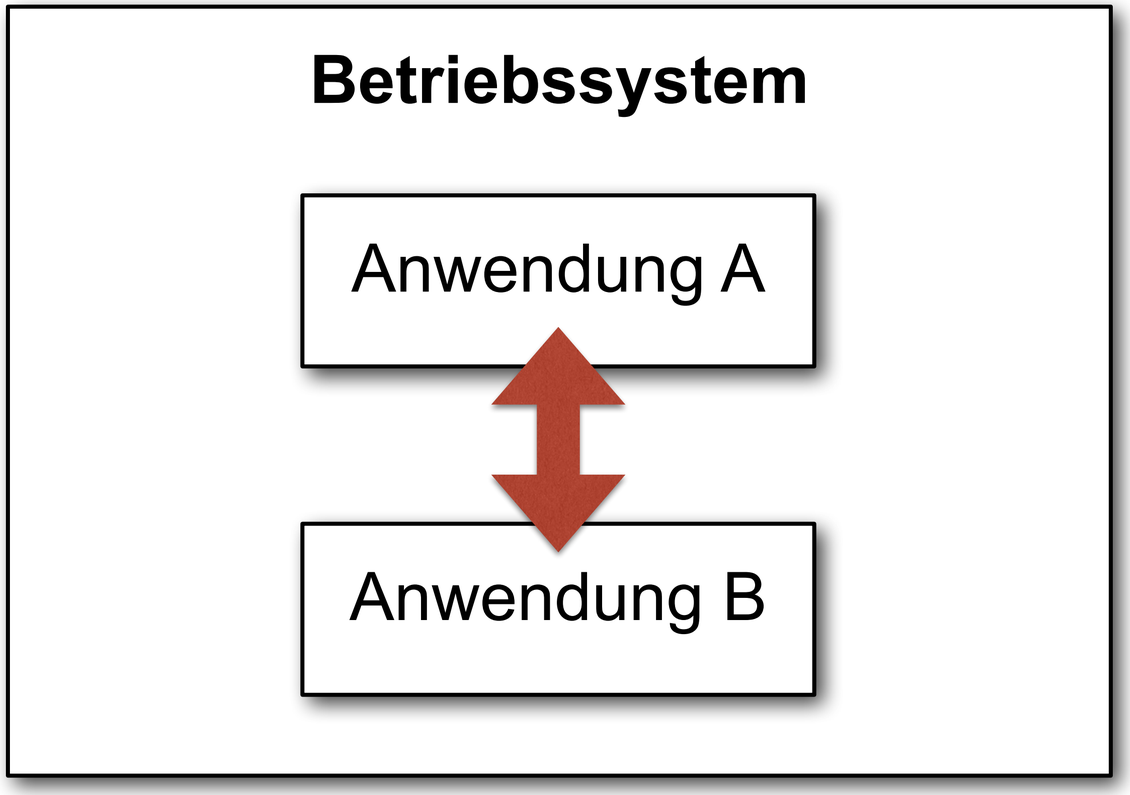
- Typ-1-Hypervisor: „bare metal“
  - ESXi von VMware
  - XEN aus der Linux-Welt
  - Hyper-V von Microsoft
- Typ-2-Hypervisor
  - VMware Player / Workstation / Fusion
  - Virtualbox (plattformunabhängig)
  - bhyve auf BSD-Systemen (insbesondere FreeBSD)

Aber nicht nur Problem - teilweise auch interessanter Lösungsansatz für Herausforderungen der IT-Security!

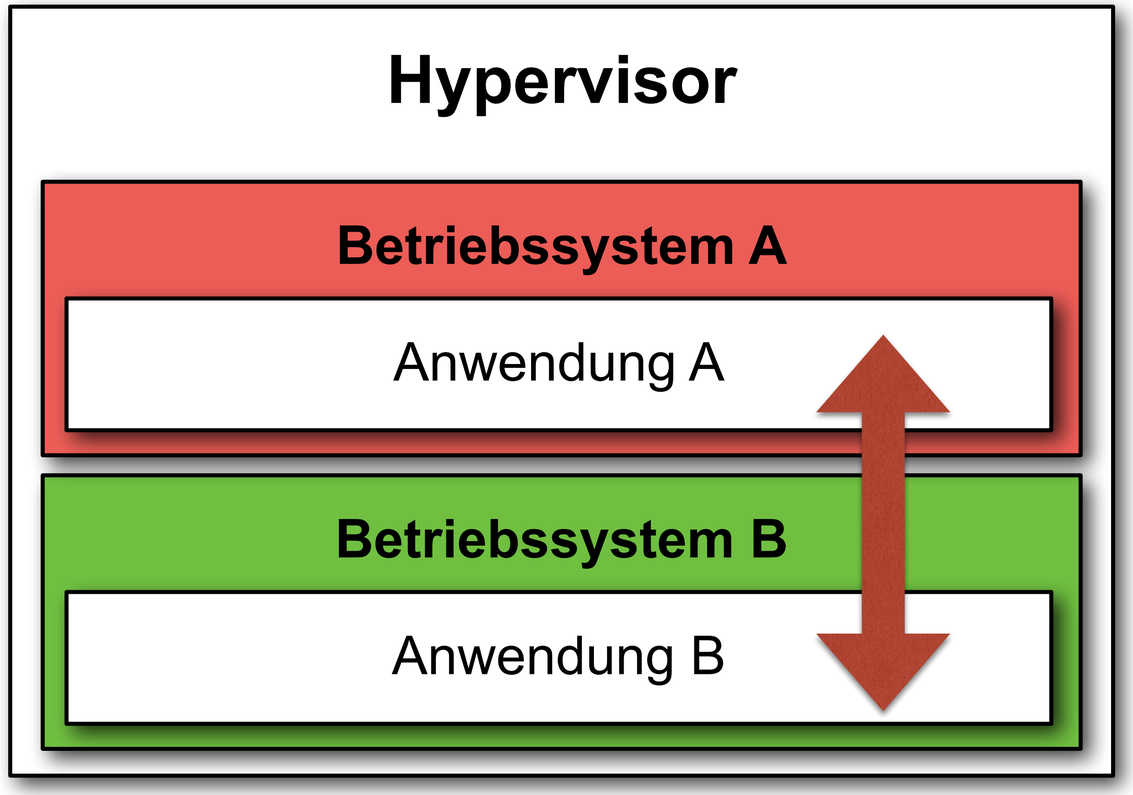
E.3. Exkurs: Virtualisierung

kostengünstige Trennung von Anwendungen in VMs

herkömmliche Lösung



Virtualisierung



E.4. Netzwerke und Netzwerktechnik

Eine der wichtigsten Funktionen computergesteuerter Systeme in heutiger Zeit ist - neben der Verarbeitung von Daten selbst - die Kommunikation. Die Datenkommunikation erfolgt über Netzwerke - allen voran das Internet.
Diese Kommunikation weist einige bedeutsame Folgen für die Datensicherheit auf.

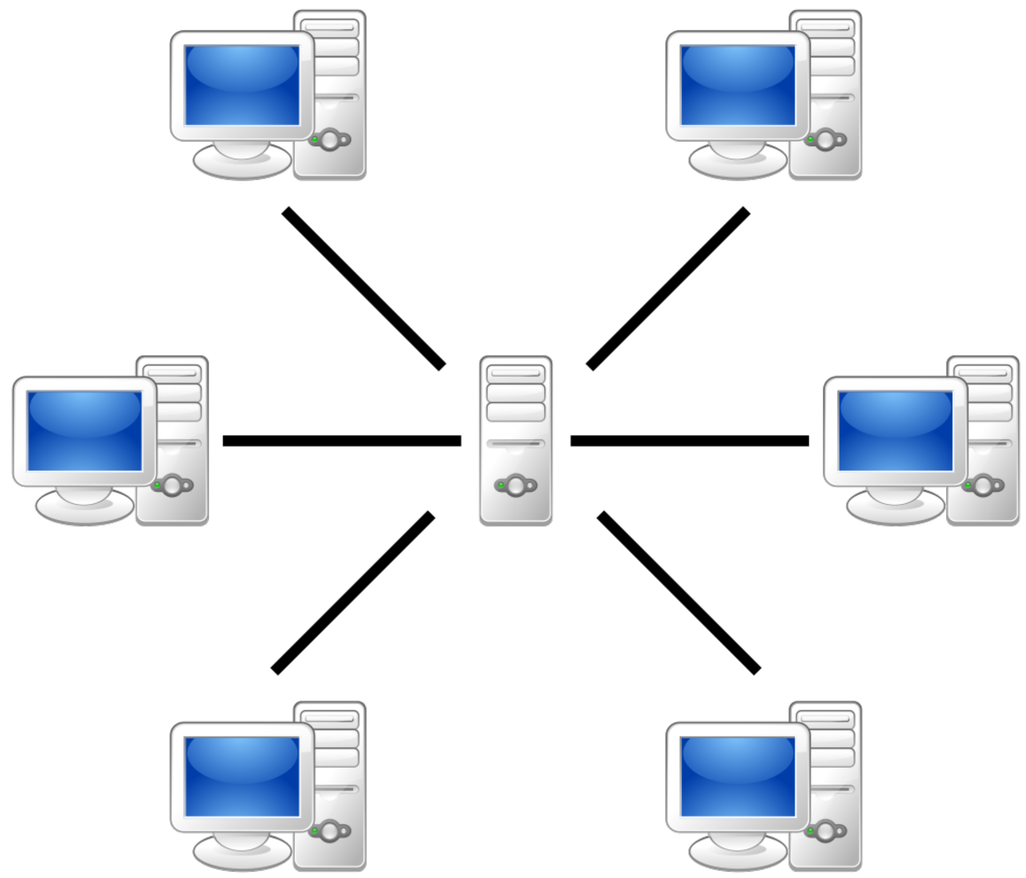
Folgende Begriffe der Netzwerkkommunikation sind dabei hervorzuheben:

- TCP/IP und einzelne Ports / spezielle Anwendungsprotokolle
- WWW vs. Internet?
- DNS - Adressen und Namen
- E-Mail
- Routing / NAT und Firewall
- sonstige Netzwerkprotokolle: NFS, SMB

E.4. Netzwerke und Netzwerktechnik

Warum Netzwerke?

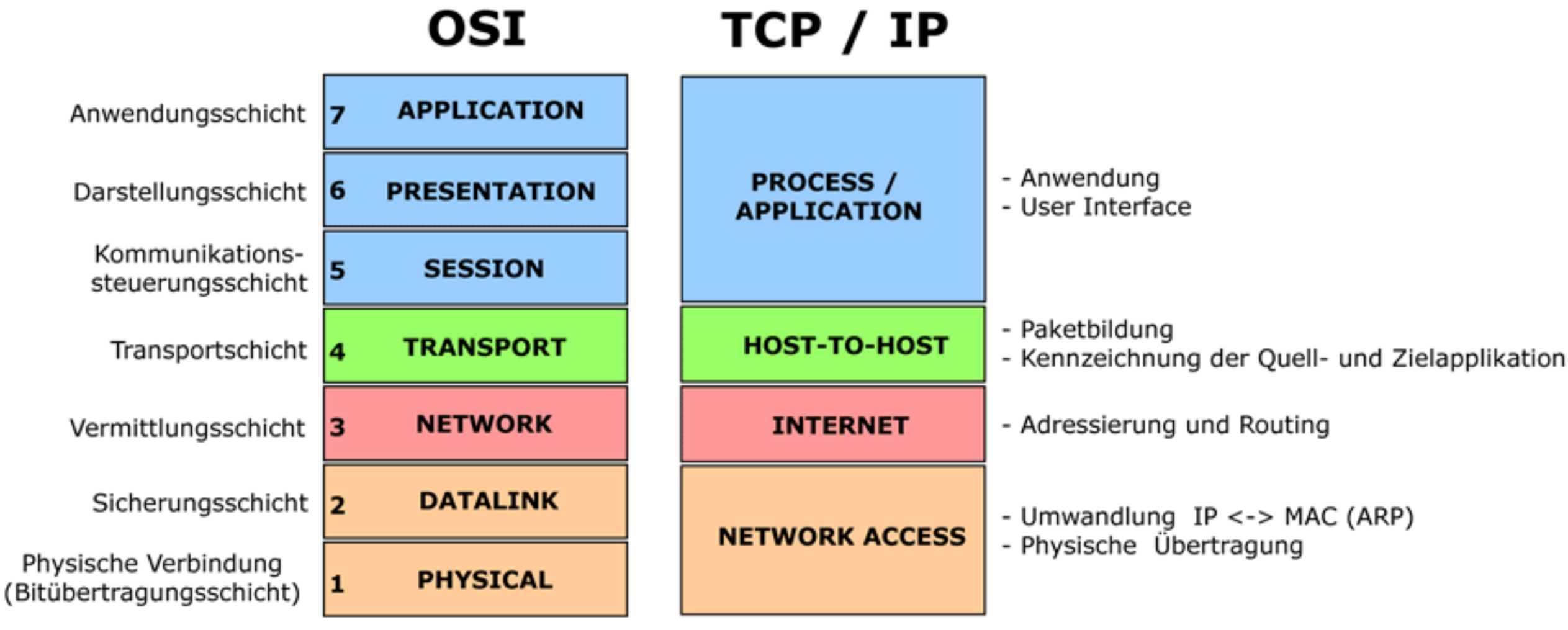
- Standortunabhängigkeit
- Datenaustausch
- auch automatisiert
- Client-Server-Architektur => (= Zugriff und Arbeit an einer gemeinsamen Datenbasis von mehreren Arbeitsplätzen aus)



Quelle: https://commons.wikimedia.org/wiki/File:Server-based-network.svg

E.4. Netzwerke und Netzwerktechnik

Referenzmodell



Vgl. https://kompendium.infotip.de/netzwerktechnologie2-referenzmodelle-und-protokolle.html

E.4. Netzwerke und Netzwerktechnik

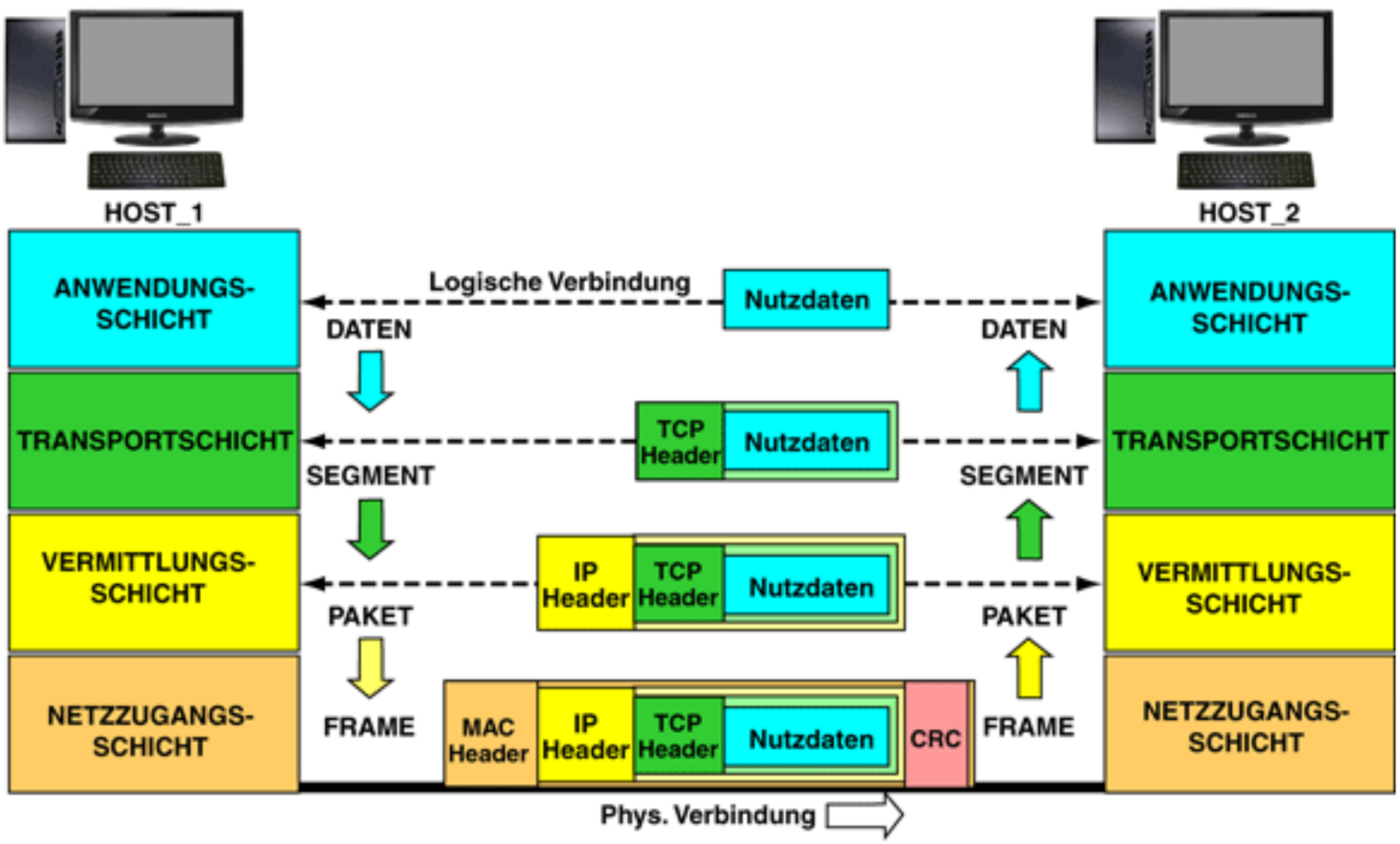
OSI und einzelne Technologien / Protokolle

Schicht 7	**Anwendung**	Telnet, **FTP, HTTP, SMTP**, NNTP
Schicht 6	**Darstellung**	Telnet, **FTP, HTTP, SMTP**, NNTP, NetBIOS
Schicht 5	**Kommunikation**	Telnet, FTP, HTTP, SMTP, NNTP, NetBIOS, TFTP
Schicht 4	**Transport**	**TCP, UDP**, SPX, NetBEUI
Schicht 3	**Vermittlung**	IP, IPX, ICMP, T.70, T.90, X.25, NetBEUI
Schicht 2	**Sicherung**	LLC/MAC, X.75, V.120, ARP, HDLC, PPP, IEEE 802.11 WLAN
Schicht 1	**Übertragung**	Ethernet, Token Ring, FDDI, V.110, X.25, Frame Relay, V.90, V.34, V.24

Vgl. https://www.elektronik-kompendium.de/sites/kom/0301201.htm

E.4. Netzwerke und Netzwerktechnik

Kommunikation über TCP/IP im Detail



Vgl. https://kompendium.infotip.de/netzwerktechnologie2-referenzmodelle-und-protokolle.html

E.4. Netzwerke und Netzwerktechnik

OSI und einzelne Technologien / Protokolle

Schicht 7	**Anwendung**	Telnet, **FTP, HTTP, SMTP**, NNTP
Schicht 6	**Darstellung**	Telnet, **FTP, HTTP, SMTP**, NNTP, NetBIOS
Schicht 5	**Kommunikation**	Telnet, FTP, HTTP, SMTP, NNTP, NetBIOS, TFTP
Schicht 4	**Transport**	**TCP, UDP**, SPX, NetBEUI
Schicht 3	**Vermittlung**	IP, IPX, ICMP, T.70, T.90, X.25, NetBEUI
Schicht 2	**Sicherung**	LLC/MAC, X.75, V.120, ARP, HDLC, PPP, IEEE 802.11 WLAN
Schicht 1	**Übertragung**	Ethernet, Token Ring, FDDI, V.110, X.25, Frame Relay, V.90, V.34, V.24

Vgl. https://www.elektronik-kompendium.de/sites/kom/0301201.htm

E.4. Netzwerke und Netzwerktechnik

Kommunikation über TCP/IP - Adresse

IP

IPv4

Beispiel:

`194.94.84.191`

IPv6

Beispiel:

`2001:0db8:85a3:0000:0000:8a2e:0370:7344`

IP = eindeutige Adresse im IP-Netzwerk bzw. in einem abgetrennten Netzwerkbereich

E.4. Netzwerke und Netzwerktechnik

IPv4 => Adressbereiche

Alle (öffentliche und private) Adressen: 1.1.1.1 - 255.255.255.255 => 2^{32} = ca. 4 Mrd.

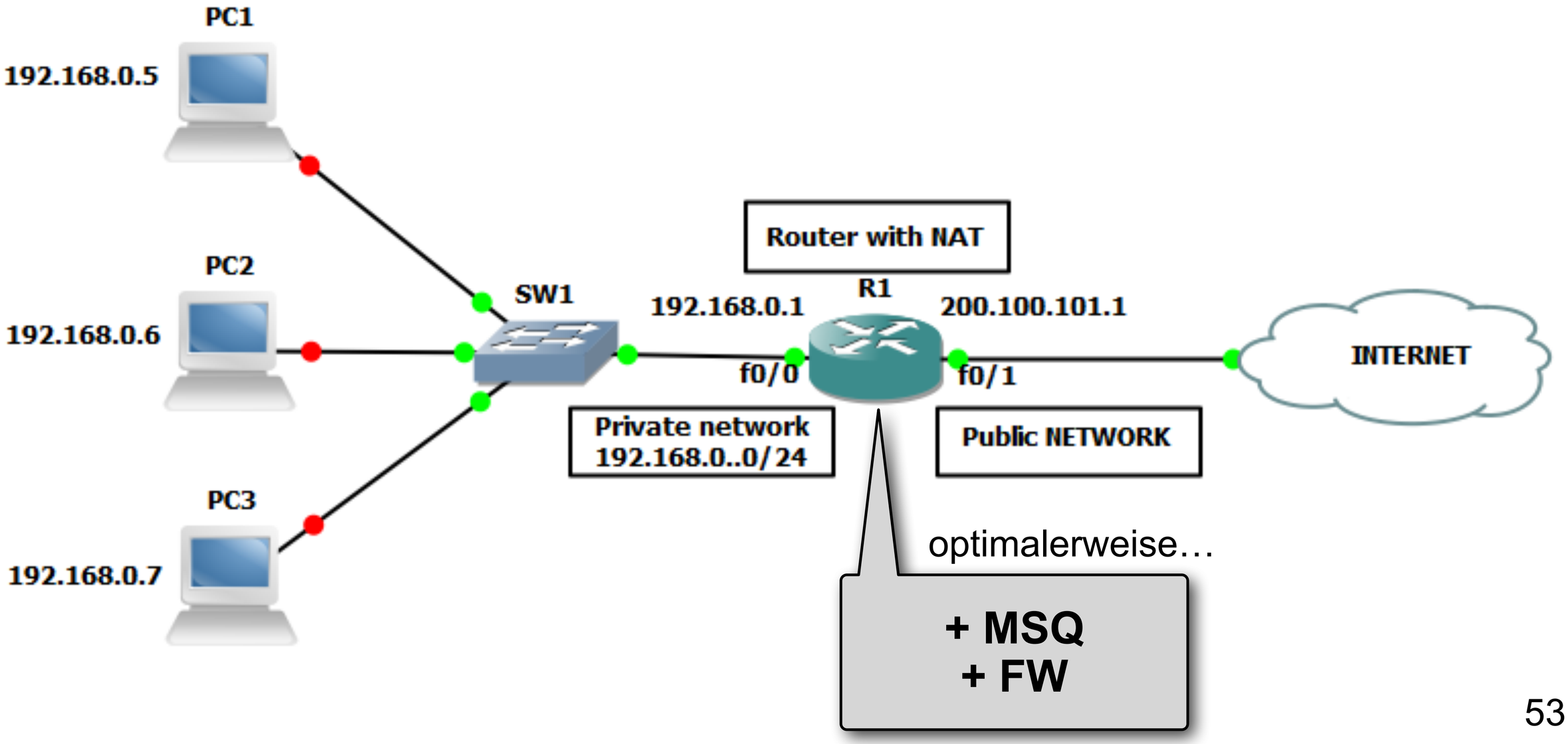
Adressbereich	Beschreibung	größter CIDR-Block	Anzahl IP-Adressen
10.0.0.0–10.255.255.255	privat, 1 **8-Bit**-Netz	10.0.0.0/8	2^{24} = 16.777.216
172.16.0.0–172.31.255.255	privat, 16 **16-Bit**-Netze	172.16.0.0/12	2^{20} = 1.048.576
192.168.0.0–192.168.255.255	privat, 256 **24-Bit**-Netze	192.168.0.0/16	2^{16} = 65.536
169.254.0.0–169.254.255.255	link local, 1 **16-Bit**-Netz	169.254.0.0/16	2^{16} = 65.536

Kommunikation zwischen Adressbereichen = Routing

da IP-Adressen nicht für alle Geräte ausreichen => Trennung von privaten Netz-Adressbereichen zwingend

E.4. Netzwerke und Netzwerktechnik

NAT und IPv4



E.5. Einzelne Netzwerktechnologien

einige Netzwerktechnologien im Detail

Dateien / Inhalte senden / empfangen	▸ Internet: FTP, **HTTP**(S), WebDAV ▸ lokal: CIFS, SMB, **NFS**, AFP (läuft aus), RSYNC
Kommunikation zwischen Geräten	▸ NetBIOS, Finger, (SSH), SNMP, etc.
(sichere) Verbindung ins Internet	▸ Routing und NAT ▸ Firewall, Content Filter, Intrusion Detection etc.
elektronische Post	▸ **SMTP** ▸ IMAP; POP3
sonstige	▸ DNS, DHCP ▸ VNC, **RDP**

E.5. Einzelne Netzwerktechnologien

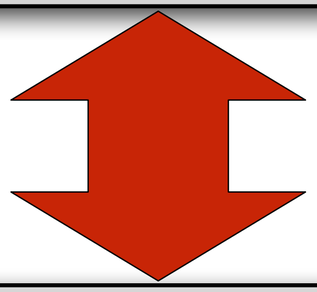
Netzwerktechnologien lokal und öffentlich (Internet)

TCP/IP und einzelne Protokolle

lokale Netzwerke

- SMB (früher CIFS), NFS, AFP (veraltet)
- NetBIOS / NetBUI
- VNC / RDP

DHCP



Routing / NAT / Firewall

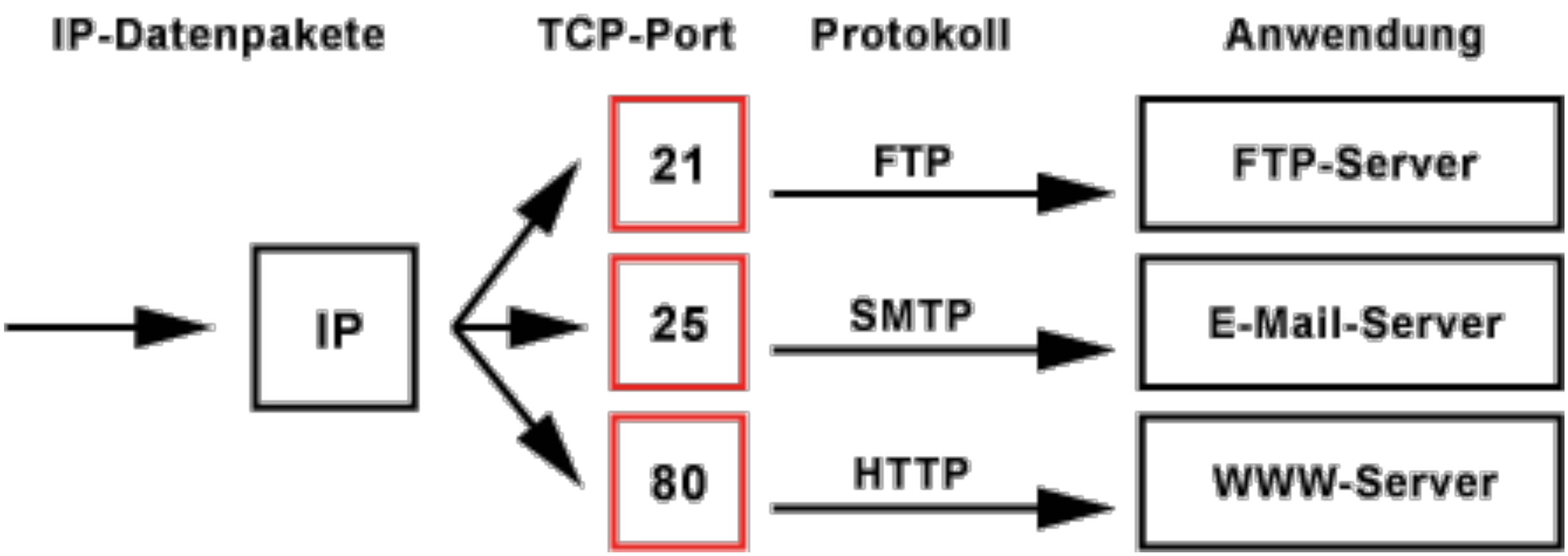
Internet

- E-Mail => SMTP etc.
- DNS
- WWW => HTTP

DHCP

E.5. Einzelne Netzwerktechnologien

Ports



Vgl.: https://www.elektronik-kompendium.de/sites/net/1812041.htm

E.5. Einzelne Netzwerktechnologien

Port	TCP	UDP	Beschreibung
20	TCP	–	FTP – Datenübertragung
21	TCP	UDP	FTP – Verbindungsaufbau und Steuerung
22	TCP	UDP	Secure Shell (SSH) verschlüsselte Fernwartung/Dateiübertragung/ getunnelte Portweiterleitung
25	TCP	–	Simple Mail Transfer Protocol (SMTP) => E-Mail
53	TCP	UDP	Domain Name System (DNS), meist über UDP
80	TCP	–	Hypertext Transfer Protocol (HTTP)
109	TCP	–	Post Office Protocol v2 (POP2)
110	TCP	–	Post Office Protocol v3 (POP3)
123	–	UDP	Network Time Protocol (NTP) => Zeitsynchronisierung
137	TCP	UDP	NetBIOS NetBIOS Name Service
138	TCP	UDP	NetBIOS NetBIOS Datagram Service
139	TCP	UDP	NetBIOS NetBIOS Session Service
143	TCP	UDP	Internet Message Access Protocol (IMAP) – Mail-Management
3389	TCP	UDP	Microsoft Terminal Server (RDP)

E.5. Einzelne Netzwerktechnologien

Cloudanwendungen

Warum?

- Outsourcing
- Abgabe großer Teile der IT an „Profis“
- Fokus auf Kernkompetenzen
- Kostensenkung
- Modern

Probleme

- Daten stets im Internet
- Kommunikation ebenfalls über öffentliches Internet
- Datenverarbeitende Systeme in fremder Hand
- keine physikalische Macht über Daten

E.6. Datensicherheit als technische Sicherheit

- Ursache für Datenverlust / Ausfall der IT ist häufig technisches und menschliches Versagen!
- viele „Feinde“ der Datensicherheit sind gar nicht Hacker oder Cyberkriminelle, sondern:
  - Blitzschlag, Feuer, Überschwemmung etc.,
  - Strom- oder Hardwareausfall,
  - Fehlfunktion von Hardware oder Software.
- Insbesondere im Hinblick auf die **Verfügbarkeit** (als Schutzziel der IT-Security) ist ein genauer Blick auf die Technik und ihre Zuverlässigkeit notwendig;
- **Vorkehrungen gegen technischen Ausfall zahlen sich auch für den Fall eines Cyberangriffs aus!**

E.6. Datensicherheit als technische Sicherheit

Gegenüberstellung von verschiedenen Ansätzen

modernste Technik	vs.	**bewährte Lösungen**
günstige Hardware	vs.	**Markenhardware**
beliebige Systeme	vs.	**passende Lösungen**
beliebige Kompatibilität	vs.	**geprüfte Treiber**