HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Datensicherheit

Herausforderungen der IT-Technologien und des zunehmenden "cyber crime“ aus interdisziplinärer Sicht

Prof. Dr. iur. Wojciech Lisiewicz

Wintersemester 2020 / 2021

im Netz: http://wdb.fh-sm.de/DatenSicherheitVorlesung

Einige Fragen zum Aufwärmen

Überlegen Sie:

- Welche Informationstechnologien (IT) setze ich persönlich ein? Werden dabei Daten verarbeitet?
- Welche IT und datenverarbeitenden Systeme werde ich vermutlich in meinem beruflichen Leben einsetzen?
- Wann ist für mich die eingesetzte IT sicher?
- Von welchen Bedrohungen für die IT habe ich schon mal gehört?
- Wann sind Daten sicher und wann unsicher?

Warum soll ein Jurist über IT-Security sprechen?

Bisherige Projekte:

- Lernwerkzeuge knowledgeTools
- Bereich Internetdatenbanken und Branchenportale => Webanwendungen, Datenbanken, Webserver (früher MS IIS / ASP, später Linux / Apache) etc.
- Umsetzung eines DMS in der Rechtsabteilung eines Energieversorgers
- aktuell: hochverfügbare Systeme mit Linux / FreeBSD sowie virtualisierte Server/Cluster, inkl. sicherer Cloudanwendungen
- ABER auch: interne und externe Revisionen bei *compliance*-Problemen, Haftungsfälle, Beseitigung der Folgen von Cyberattacken, digitale Gefahren auch sonst (Lernbiologie?)

Warum sollten wir über Datensicherheit sprechen?

2017:

Digitale Angriffe haben bei 7 von 10 Unternehmen Schäden verursacht

vgl.:

https://www.zdnet.de/88372729/bitkom-100-milliarden-euro-schaden-pro-jahr-durch-cyberangriffe/

Warum sollten wir über Datensicherheit sprechen?

2019:

Rekordschäden: Cyberkriminalität kostet deutsche Wirtschaft 100 Milliarden im Jahr

vgl.:

https://www.e-recht24.de/news/strafrecht/11729-cybercrime-schaden-deutsche-wirtschaft.html

A.1. Einstieg: einige Beispiele (1)

Kammergericht Berlin, 2019/2020

- im Nachhinein als „APT 28“ bezeichnete Hackergruppe ist mit einem „emotet“-Angriff auf das Kammergericht erfolgreich
- die „Infektion“ kompromittiert die gesamte IT-Infrastruktur des Gerichts und macht die Arbeit ab Oktober 2019 unmöglich
- bis weit in das Jahr 2020 Arbeit mit Papier und Fax
- es war zumindest möglich, Daten zu verdeckten Ermittlern, Opfern von Verbrechen, Zeugen etc. abzugreifen

im Gegensatz zu den Berichten in der Presse ist „emotet" nicht auf irgendetwas spezialisiert - es ist nur ein Werkzeug, Datenklau oder ihre Verschlüsselung (und dann Erpressung) zu ermöglichen…

A.1. Einstieg: einige Beispiele (2)

Bundestag, 2015

- Trojaner wird auf den Rechnern im Netzwerk des BT installiert
- über weitere Angriffsstufen wurde Zugriff auf mehrere Arbeitsgeräte erlangt und auch auf administrative Funktionen im Netzwerk
- die Geräte waren praktisch durch Angreifer komplett fernsteuerbar - es war Zugriff sowohl auf alle Daten, wie auch auf Funktionen des kompletten Netzwerks möglich
- insgesamt flossen ca. 16 GB an Daten ab

beim Angriff spielte auch eine Fake-Seite der UN eine Rolle, auf die eine (ebenfalls „fake“) E-Mail leitete, die alle Mitarbeiter erhielten

A.1. Einstieg: einige Beispiele (3)

Düsseldorfer Klinik, 2020

- ein Ransomware-Angriff verschlüsselt Daten in einer Düsseldorfer Klinik und legt Datenverarbeitung lahm
- die Behandlung von Patienten ist nich möglich
- auch Notfälle müssen in andere Krankenhäuser umgeleitet werden
- eine schwer erkrankte Frau kann nicht vor Ort notbehandelt werden - die deutlich verlängerte Fahrt in eine entlegene Klinik führt zu ihrem Tod

mittlerweile ist die IT nicht nur eine Frage von effizientem Arbeiten, sondern Bestandteil von lebenserhaltenden Systemen !!!

A.2. Was und warum wird hier behandelt?

unsere Ziele

Überblick über die IT	▸ die sicherheitsrelevanten Aspekte der IT verstehen ▸ sinnvolle und problematische Lösungen unterscheiden können
IT-Fachmann verstehen	▸ blendet er gerade oder ist es plausibel? ▸ sind es seine Lieblings-Spielsachen oder gut konzipierte Lösung?
Weichenstellungen setzen	▸ welche Hard- und Software kann die Sicherheit jahrelang prägen? ▸ wie arbeite ich sicherheitstechnisch nachhaltig?
insbesondere: Bewusstsein schaffen	▸ was sind die Risiken und Gefahren? ▸ was sind die notwendigen Maßnahmen?

auch wenn Sie hier keine Hacker und Programmierer werden können - sie sollten vor dem Problem nicht kapitulieren!

A.3. Prüfung - Inhalt und Form

Die Prüfung des Gesamtmoduls besteht aus zwei Teilen:
- Datenschutz = Teil 1
- Datensicherheit = Teil 2

Prüfungsform in Teil 2

- Klausur
- Ein Szenario mit Darstellung der IT-Architektur in einem Unternehmen / einer Organisation steht im Zentrum.
- Zum Szenario sind Fragen zu Problemen / möglichen Maßnahmen zu beantworten.

Themen im Einzelnen

- Was sind die (im Szenario geschilderten) Probleme / Risiken / Gefahren?
- Wie kann diesen Problemen begegnet werden (Werkzeuge, Techniken, Maßnahmen)?

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Lernmaterial

Skripte

- http://wdb.fh-sm.de/DatenSicherheitVorlesung

Bücher

- **Eckert, IT-Sicherheit, DeGruyter (eBook)**
- Hellmann, IT-Sicherheit, DeGruyter
- Kipker, Cybersecurity - Rechtshandbuch, C. H. Beck

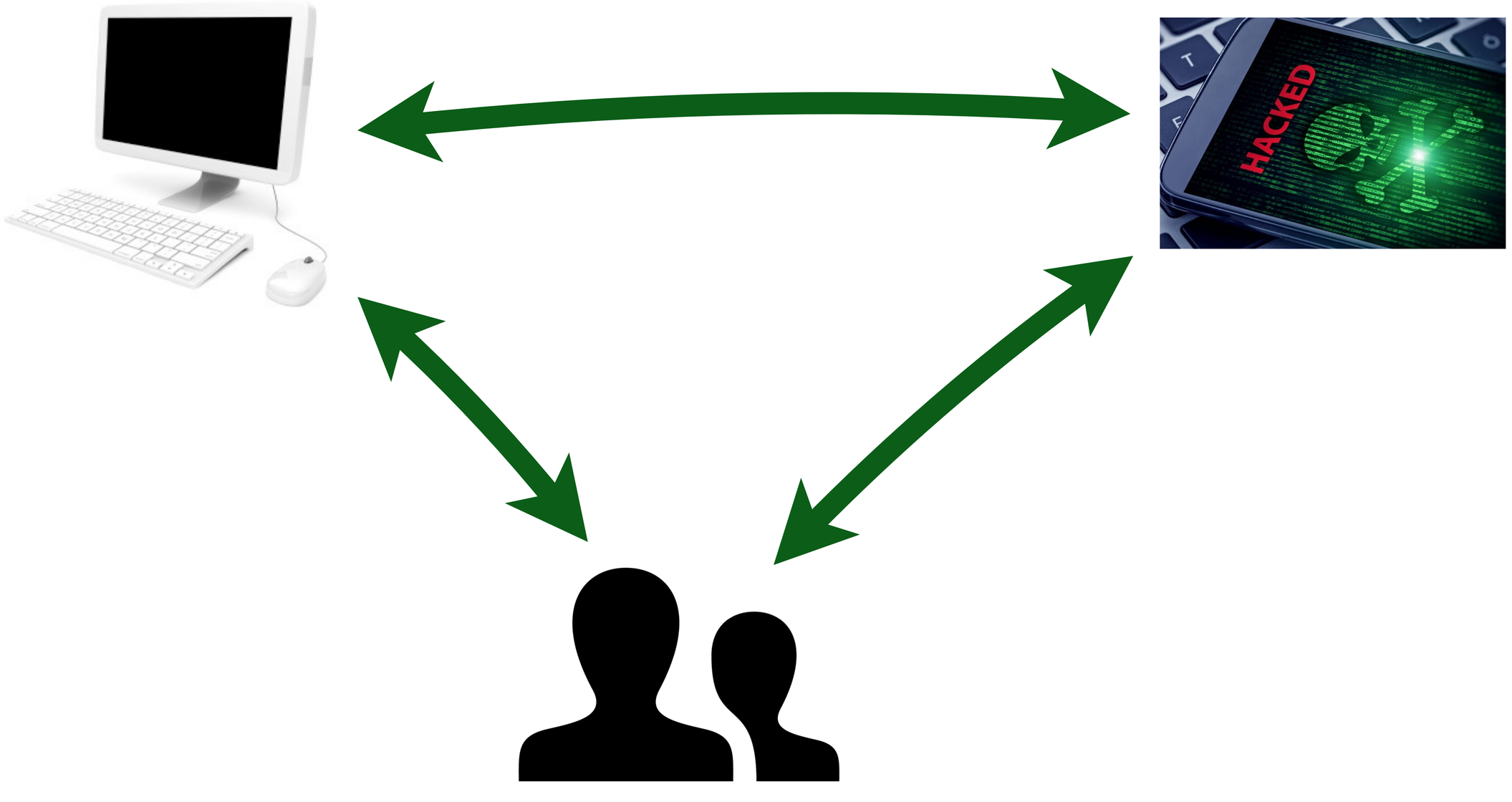
B. Bestandsaufnahme

Wo stehen wir?

- immer größere Abhängigkeit von der IT - insbesondere bei jeglicher Datenverarbeitung
- eingesetzte Technik immer komplexer, auch wegen der „Featuritis“
- die Technologie soll und ist angeblich immer benutzerfreundlicher
- hoher Zeit- und Kostendruck => „agil statt stabil“
- immer stärkere Vernetzung von Systemen
- Datenlecks, GAUs, Angriffe, gravierende Ausfälle und sonstige „Desaster“ nehmen stark zu

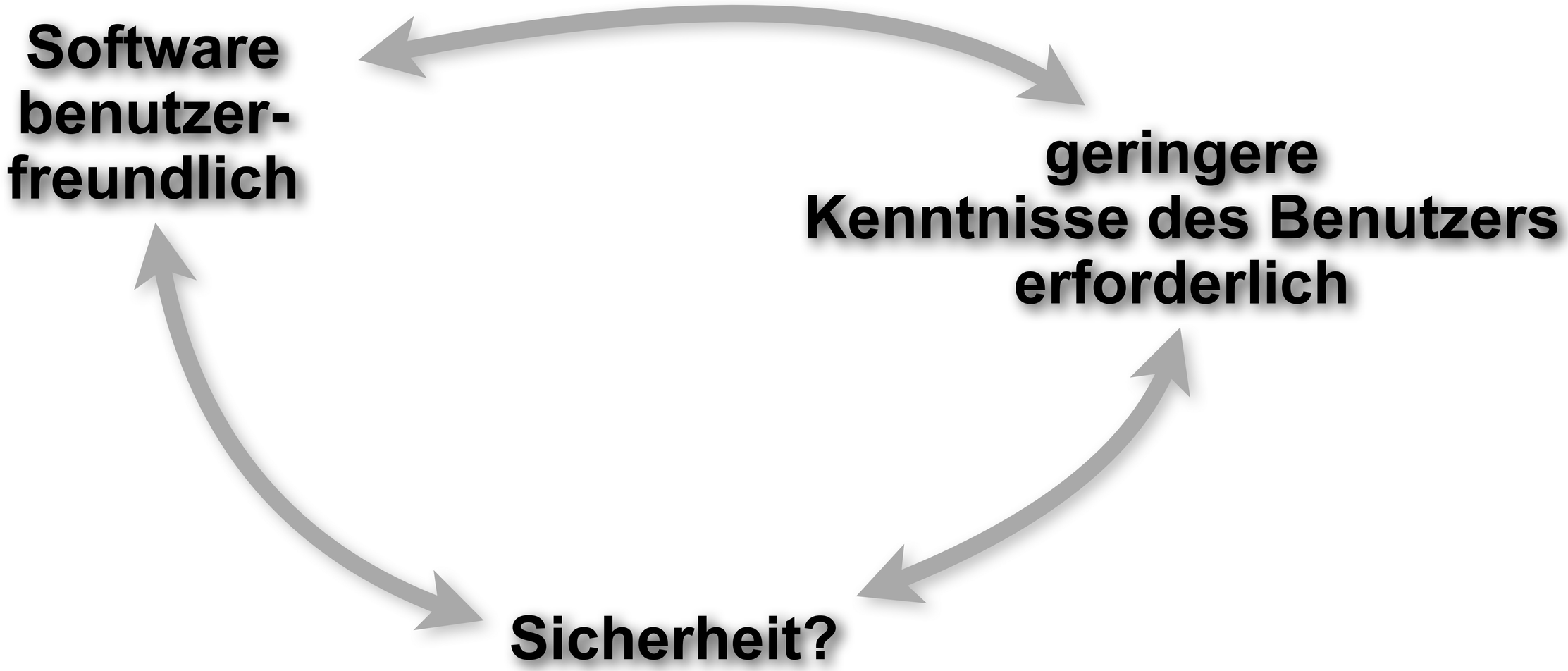
C.1. Mensch als Sicherheitsfaktor

IKT vs. Datensicherheit vs. Mensch



C.2. Spezielles Problem: Benutzerfreundlichkeit

Benutzerfreundlichkeit vs. Datensicherheit



C.2. Spezielles Problem: Benutzerfreundlichkeit

Folgen

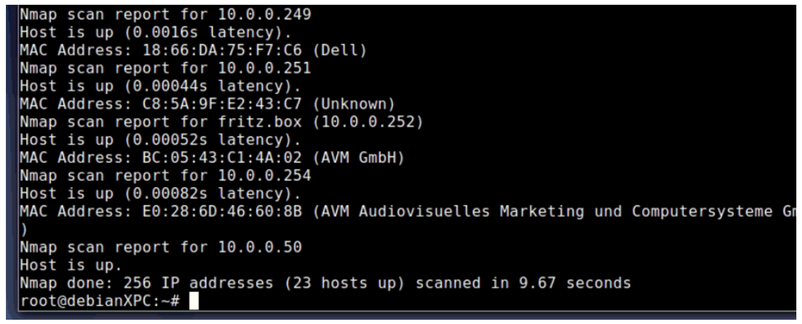
Software benutzer-freundlich

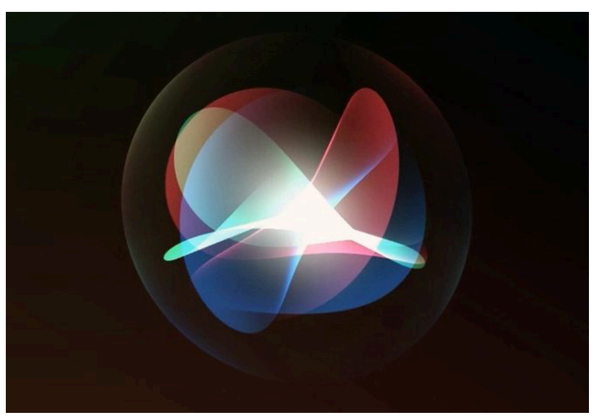
geringere Kenntnisse des Benutzers erforderlich

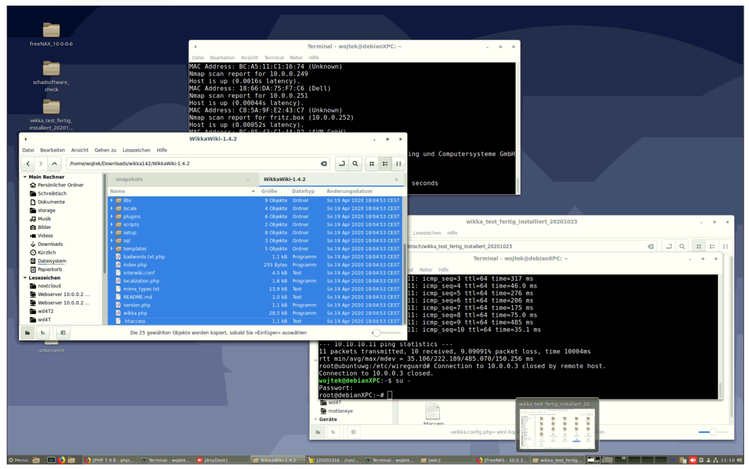
Sicherheit leidet!!!

C.3. Komplexität vs. Benutzerfreundlichkeit

ein sich (selbst) verstärkender Trend







D. Grundbegriffe und ihre Systematik

1. Schutzziele
2. Schwachstelle und Verwundbarkeit
3. Gefährdungsfaktoren
4. Bedrohung vs. Risiko
5. Angriff

die Systematik dieser Begriffe wird in verschiedenen Quellen mitunter etwas chaotisch und unterscheidet sich von Autor zu Autor ein wenig…

D.1. Schutzziele

- Authentizität (glaubwürdige Daten, vom richtigen Subjekt) - und auch Möglichkeit der Nachverfolgung eventueller Änderungen — *authenticity*
- Datenintegrität (nicht unbefugt manipuliert - auch durch technische Fehler nicht!) — *integrity*
- Vertraulichkeit (kein unbefugter Zugriff) — *confidentiality*
- Datenschutz (informationelle Selbstbestimmung) — *privacy*
- Verfügbarkeit (es funktioniert ohne ungeplante Unterbrechung; Zugriff auf notwendige Daten stets möglich) — *availability*

während die ersten drei Punkte eng mit dem Datenschutz verknüpft sind, ist das letzte Thema auf den ersten Blick alt, technisch und wenig spannend - dennoch nach wie vor extrem bedeutsam

D.2. Schwachstelle vs. Verwundbarkeit

„Wird eine […] Schwachstelle ausgenutzt, so kann es zu Beeinträchtigungen der Datenintegrität, Informationsvertraulichkeit oder auch Verfügbarkeit [d. h. der Schutzziele] kommen“

Eckert, IT-Sicherheit

- Schwachstelle = Schwäche eines Systems oder ein Punkt, an dem das System verwundbar werden kann; => allgemein! — *weakness*
- Verwundbarkeit = Schwachstelle, über die ein unautorisierter Zugriff auf das System möglich ist; => speziell im Hinblick auf Angriffe! — *vulnerability*
- Exploit = Möglichkeit der Ausnutzung einer Schwachstelle für einen Angriff — *exploit*

Schwachstellen können über Gefährdungsfaktoren identifiziert werden

D.3. Exploit

Exploit, d. h. die Möglichkeit der Ausnutzung einer **Schwachstelle** für einen Angriff ist - im Hinblick auf die Möglichkeit vorsätzlicher Angriffe - ein bedeutsames Phänomen der IT!

- besondere Kategorie: ***zero day exploit***
- Bedeutung für:
  - Hersteller = Qualitätsmanagement (Wettbewerbe)
  - aber auch: Kriminelle und (?) Geheimdienste
- Typen:
  - lokal vs. remote
  - Art der Schwachstelle:
    - *buffer overflow*
    - Eingabevalidierung
    - *race conditions*
    - *privilege escalation*

D.4. Gefährdungsfaktoren

Die Suche nach Schwachstellen ist anhand der Liste von **Gefährdungsfaktoren** möglich:

- höhere Gewalt
- Fahrlässigkeit, menschliche Fehler
- Angriffe vorsätzlicher Art
- technisches Versagen
- organisatorische Mängel

D.5. Bedrohung vs. Risiko

Verschiedene Schwachstellen können insbesondere Angriffe ermöglichen. Welche Bedeutung die jeweiligen Schwachstellen im konkreten Kontext haben, ist mittels Bedrohung und Risiko zu ermitteln.

- Bedrohung = Schwachstelle / Verwundbarkeit wird ausgenutzt, um die Schutzziele zu verletzen — *threat*
- Risiko = Wahrscheinlichkeit (relative Häufigkeit) des Eintritts eines Schadensereignisses und Höhe des potentiellen Schadens — *risk*
- Gewichtung zwischen dem Wert der Güter, dem Schadenspotential und der Wahrscheinlichkeit des Schadenseintritts erforderlich! — *assets*

darauf basiert ein wichtiges Instrument der Daten- und IT-Sicherheit
=> die Bedrohungs- und Risikoanalyse

D.5. Bedrohung vs. Risiko => Systematik

Zusammenhang zwischen den Begriffen

Vgl. Eckert, IT-Sicherheit, Abb. 1.3

D.6. Angriff

Verschiedene Schwachstellen können insbesondere Angriffe ermöglichen. Da Schwachstellen selten allein in unserer Hand liegen (Softwareanbieter, Dienstleister etc. ist für Anwender immer weniger transparent, der Anwender versteht immer weniger von der IT-Infrastruktur), ist mit Angriffen **immer** zu rechnen:

- Angriff = nicht autorisierter Zugriff / Zugriffsversuch auf das System *attack*

  - passiv = unautorisierte Informationsgewinnung (Verlust der Vertraulichkeit)

    Beispiele: *eavesdropping, sniffing*

  - aktiv = unautorisierte Modifikation von Daten (Verlust der Datenintegrität / Verfügbarkeit)

    Beispiele: *DoS, spoofing*

D.6. Angriff - Ursachen

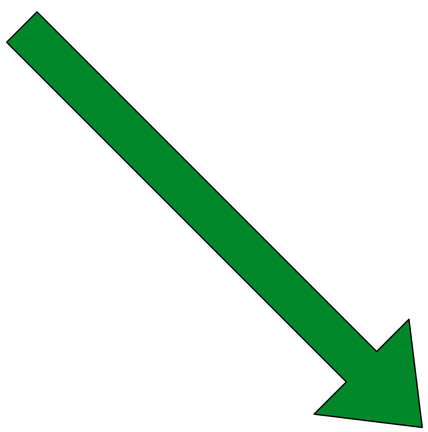
Großteil nach wie vor intern - Bedeutung externer Angriffe steigt aber deutlich an!

Angriffe von Innen

- Mitarbeiter aus Frust
- Korruption
- Whistleblowing

Angriffe von Außen

- Hacker
- Spionage
- Skript Kiddies



D.6. Angriff - Beispiele

- *eavesdropping* = Abhören von Datenleitungen / unautorisiertes Lesen aus Dateien
- *sniffing* = Ausspähen von Passwörtern
- *spoofing* = Datenänderung (insb. zur Identitätsverschleierung) - durch falsche Angabe der E-Mail-Absenderadresse, des DNS-Namens
- *phishing* = Abfangen von Passwörtern (z. B. nach *spoofing*)
- *denial of service* = Störung der Verfügbarkeit von Diensten
- Einschleusen von Schadsoftware (Virus / Wurm / Trojaner) zu verschiedenen Zwecken

Vgl. auch Arten von Schadsoftware nach ihrem Zweck!

D.6. Angriff - Typen von Schadsoftware

Folgende Arten von Schadsoftware sind weit verbreitet - eine zu 100 % eindeutige systematische Einordnung wird hier nicht angestrebt - zunächst einmal erfolgt eine grobe Einteilung nach Funktionsweise der Schadsoftware:

- Virus
- Wurm
- Trojaner

Sollte Schadsoftware nach ihrem konkreten (schädigenden) Zweck identifiziert werden, dann empfiehlt sich folgende Einteilung:

- Rootkit
- Backdoor
- Ransomware
- Spyware
- Scareware
- Adware

D.6. Angriff - Typen externer Angriffe

- Hacker = technisch versiert, sucht nach Exploits, nicht zwingend kriminell aber mitunter illegal — *exploit*
- Skript Kiddies = nutzen bekannte Lücken für Angriffe, nicht zwingend kriminell, verursachen aber Schäden — *script kiddie*
- Spionage = Geheimdienste oder Wirtschaftsspione überwachen massiv Datenverkehr — ***z. B. NSA***
- Kriminelle = Angriffe zum Zwecke der Bereicherung, z. B. durch *Ransomware* — *ransomware*
  - mit Bot-Netzen
  - mit Spyware
  - mit einer *brute-force*-Attacke
  - usw.

E. Technologie im Kontext der Datensicherheit

Um die Aspekte der Daten- und IT-Sicherheit zu verstehen, müssen wir zumindest im Ansatz die Technologie, die zur Datenverarbeitung genutzt wird, verstehen…

1. Hardware: Computer, PC, Device…
2. Software: Betriebssystem und Anwendungen
3. Exkurs: Virtualisierung
4. Netzwerke und Netzwerktechnik
5. Spezielle Netzwerktechnologien
6. Datensicherheit als technische Sicherheit

E.1. Computer - Aufbau

Welche Komponenten sind relevant
für die Datensicherheit?

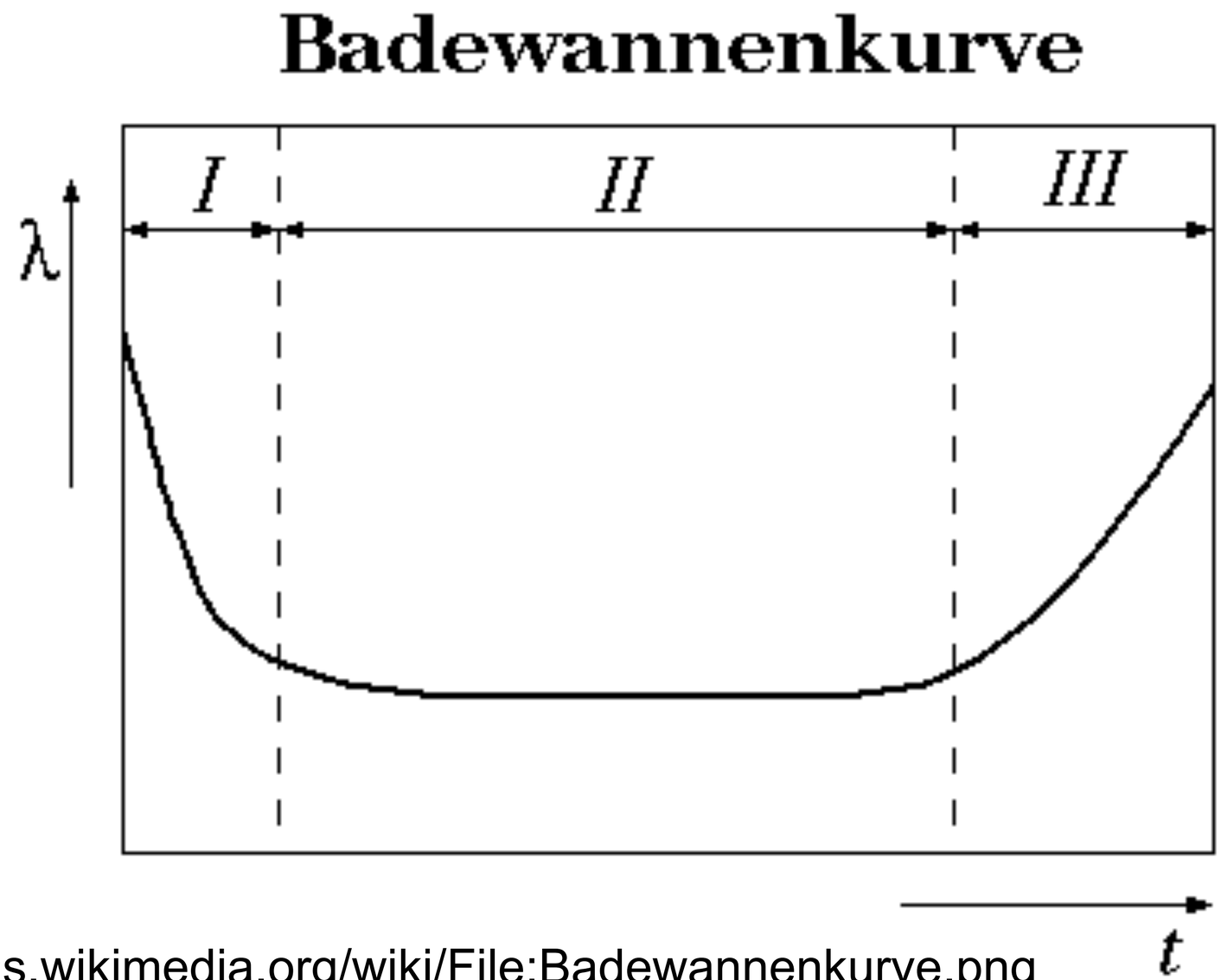
- CPU?
- Arbeitsspeicher?
- Netzteil?
- Festplatte?
- Externe Schnittstellen?
- Eingabegeräte?

fast alle!

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

E.1. Computer - Aufbau

Hardwarealter vs. Ausfallwahrscheinlichkeit



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

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

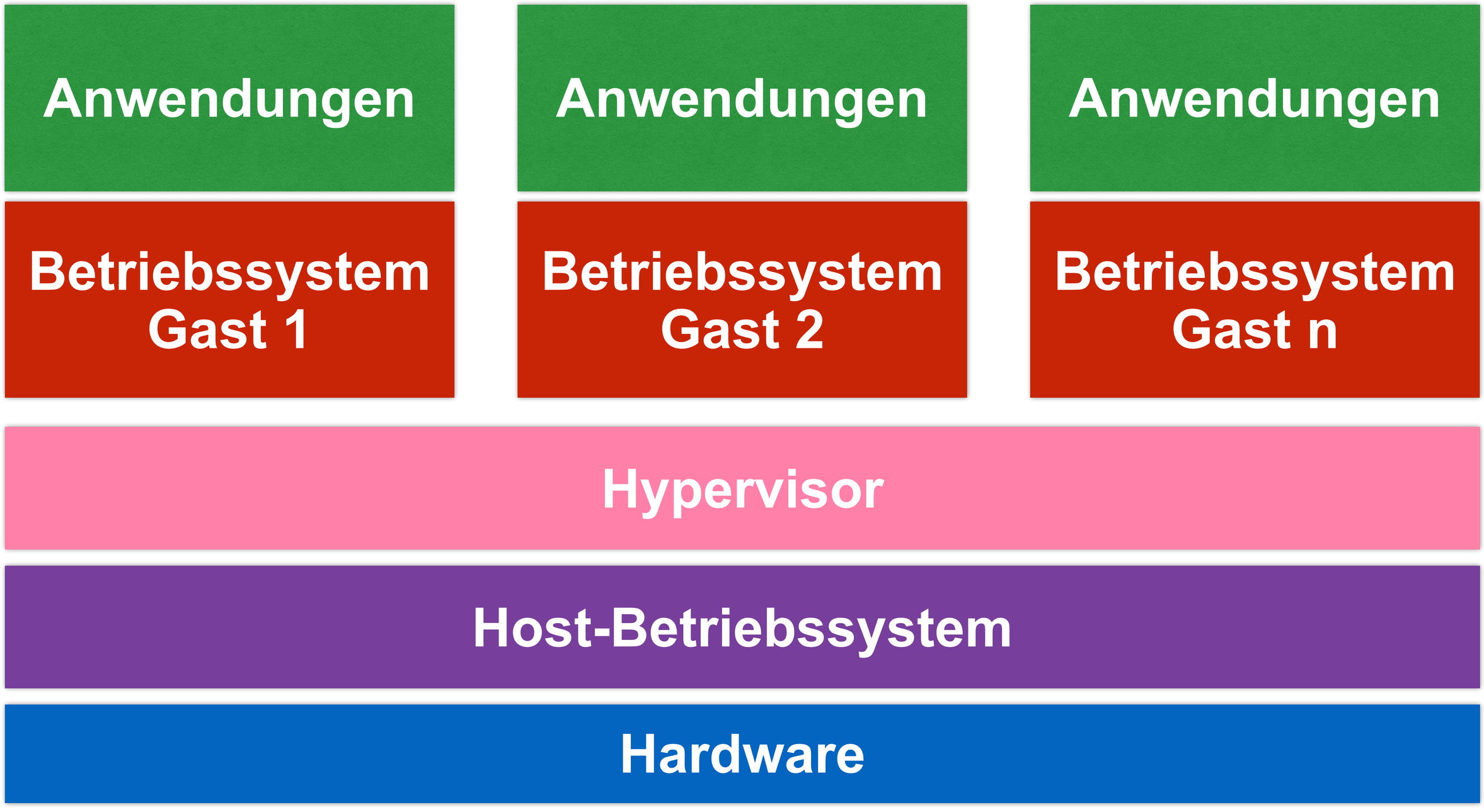
E.2. Software

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 perkekt!

Beispiele für Virtualisierungslösungen:

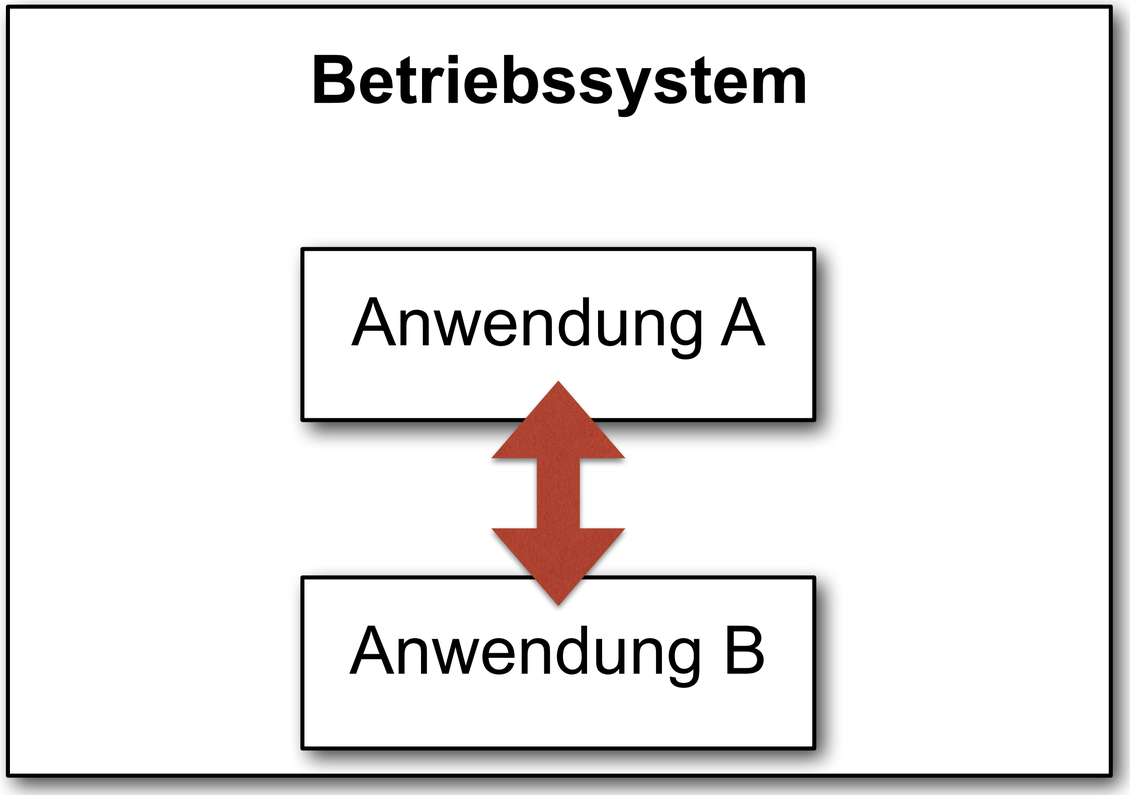
- Typ-1-Hypervisor: „bare metal“
  - ESXi von VMware
  - XEN aus der Linux-Welt
  - Hyper-V von Microsoft
- Typ-2-Hypervisor
  - VMware Player / Workstation / Fusion
  - Virtualbox (plattformunabhängig)
  - bhyve auf BSD-Systemen (insbesondere FreeBSD)

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

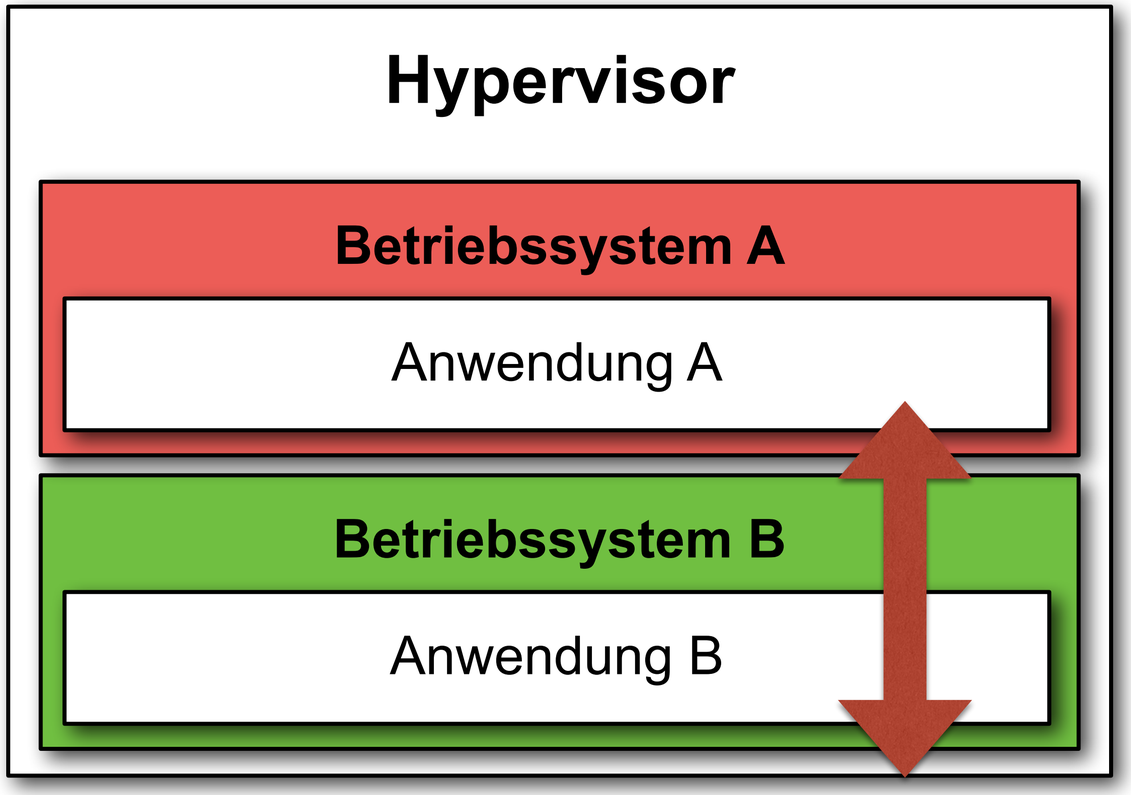
E.3. Exkurs: Virtualisierung

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.

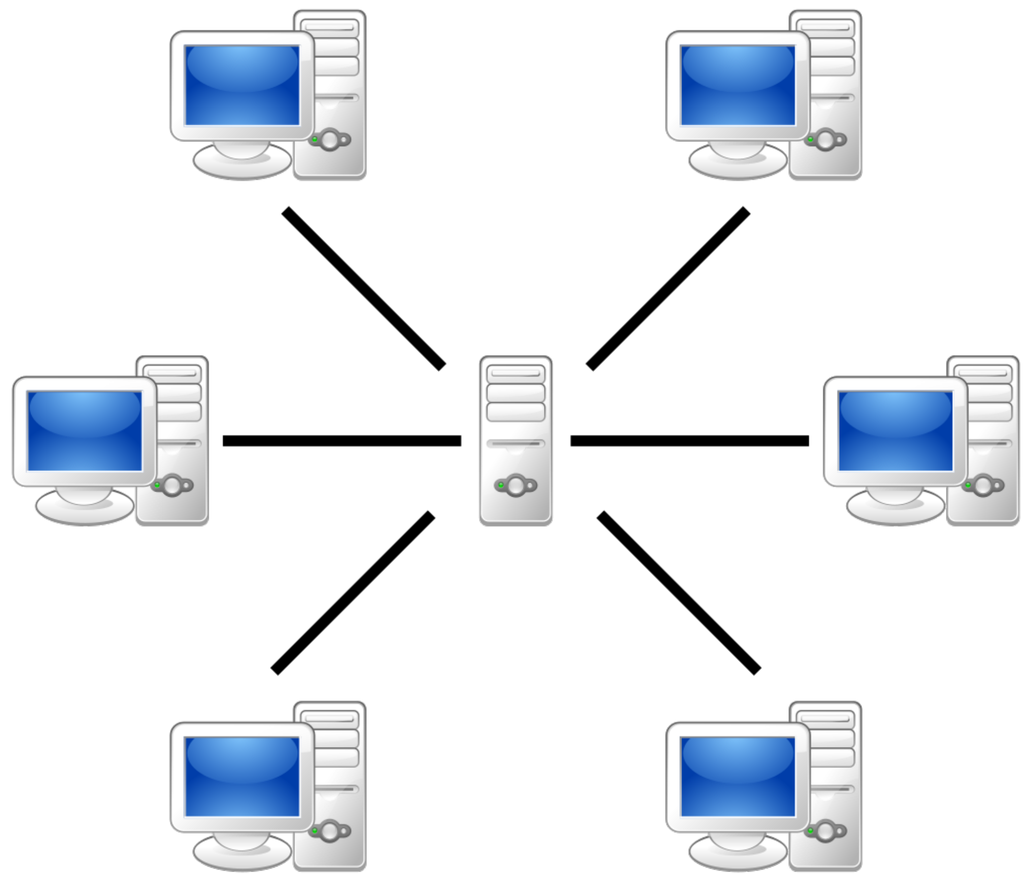
Folgende Begriffe der Netzwerkkommunikation sind dabei hervorzuheben:

- TCP/IP und einzelne Ports / Protokolle
- 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

OSI vs. TCP/IP

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

Datenverarbeitung zwischen 2 Hosts

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

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

TCP/IP und einzelne Ports / 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

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

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

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**