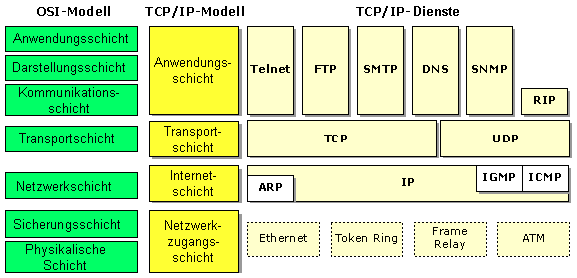
2017-09-18

OSI – Modell & TCP/IP Modell



Schichten auf Englisch!!

1. Kommunikation untereinander

Zum Dateien übertragen brauche ich zb FTP 🡪 file transport protocol.  
Telnet wurde zum Arbeiten irgendwo anders.  
SMTP 🡪 Simple mail transfer protocol

Darauf wurde Arpanet entwickelt

Ab 1985 begann die Vernetzung und ab Mitte der 1990er hat sich das Internet etabliert.

1. OSI-Modell

1. Schicht: Physikal Layer

Manchester Codierung

Nachteil: Jedes Bit zwei Impulse 🡪 nur halbe Bitrate als normal  
Vorteil: Systemfehler (Spannungsfehler werden erkannt)

Doppelstrom Codierung

Cat 5 und 6  
Schaut aus wie ein Zopf 🡪 der Impuls kann durch elektrische Felder verloren gehen, durch die Verdrillung heben sich die Felder auf   
kann ich auf vier bahnen gleichzeitig machen 🡪 Cat 5 auf 100 lässt sich 1 Gigabit übertragen

Schlecht ist wenn die Kontakte kaputt sind oder das Kabel geknickt ist

Normen:

Dosen, usw. (alles was Strom und Spannung ist)

Ethernet ist in Schicht 1 und 2 genormt 🡪 CSMA/CD (Flow Control)

2. Schicht: Link Layer

Wie überprüfe ich ob die Bits richtig sind? Bei 10^7 Bits wird durchschnittlich ein Fehler gefunden

Hamming Distanz

D1 = e+1 🡪 zeigt das Fehler vorhanden sind

D2 = 2e + 1 🡪 erkennt Fehler & weiß an welcher Stelle die Fehler sind

Block Check Character (BCC 🡪 Anwendung der Hamming Distanz und Erweiterung)

Performant

CRC

Am Häufigsten

Restklasse XOR Verknüpfung

1 + 1 = 2 🡪0 Rest 🡪 1+1=0  
1 - 1 = 0 🡪 0 Rest 🡪 1-1=0  
1 + 0 = 1  
0 + 0 = 0

1010010:1001 🡪 shiften 🡪 1010010  
 1011000  
 ------------  
 0001010  
 1011  
 ------------  
 0001 🡪 die Stelle, an welcher der einer steht ist falsch

Hamming Codierung

**Codierungen stehen alle genau in der Mappe!!!!!**

Protokoll

Verbindungsorientiert:  
Verbindungslos: keine Durchgehende Verbindung 🡪 virtuelle Verbindung, physische Wege werden erst gesucht,  
 wenn eine Leitung ausfällt dann kann sich das Paket einen anderen Weg suchen, viel mehr  
 Kapazität da die Leitungen nur besetzt bzw das Netz ausgenutzt werden wenn ein Paket  
 verschickt wird 🡪 zB Voice over IP

QoS = Quality of Service (nur bei Firmenzugängen, fixe Zusage von Bandbreite 🡪 Business Account kostet mehr als Private Account) 🡪 wird bei IPv6 besser  
LT hat kein QoS

Wie Weihnachtsgeschenke vorstellen: Wenn ich das Ethernetpaket auspacke komme ich zum IP Paket wenn ich das wiederum auspacke komme ich zum TCP oder UDP Paket und so weiter

Internet Protokoll (= IP, Schicht 3)

IP-Kopf steht auf Seite T6 in der Mappe🡪 Ergänzungen:  
Paketlänge: in Byte (Kopf + Daten)  
Identifikation: Counter um Paket einordnen zu können, erhöht sich immer um die Anzahl der Gesendeten Bytes  
DF: Dont Fragment 🡪 bei 1 darf es nicht Fragmentiert werden (geteilt) 🡪 bei IPv6 nicht mehr  
MF: Multiple Fragment 🡪 bei 1 wurde es Fragmentiert  
Fragmentabstand: vom Beginn des Pakets weggezählt die Position des Fragments  
Transport: welches Protokoll ist in der nächsten Schicht  
Optionen:   
 - Source Route (auf dieser Route muss das Paket gesendet werden)   
 🡪 Strict: die Route ist fix  
 🡪 loure: es müssen alle Knoten durchlaufen werden aber auch Stützknoten  
 - Record Route: zeichnet den Weg der Knoten auf mit Zeitstempel

1. IPv4

**128 64 32 16 8 4 2 1**

Nat  
lokale Adressen bleiben immer innerhalb des Netzes   
Präfix: es können 254 Rechner pro 8 Bit vergeben werden

Subnetzmaske eine AND Verknüpfung.

192.168.10.0/24  
Subnet Maske: 255.255.255.0  
1. Subnetz: 192168.10.001 00001  
2. Subnetz: 192.168.10.

Private Adresse:

* 10.0.0.0 – 10.255.255.255 🡪 10.0.0.0/8 🡪 Weglassen der 10.0.0.0/24
* 172.16.0.0 – 172.31.255.255 🡪 172.16.0.0/12
* 192.168.0.0 – 192.168.255.255 🡪 192.168.0.0/16

TCP (Schicht 4)

Duplexfähig: kann senden und empfangen gleichzeitig  
Portnummern: 0 – 1023 sind statisch zB smtb  
 1024 – unendlich sind dynamisch zB skype

TCP Kopf: Mappe T6 Rückseite

Sender Port: wichtig   
Empfänger Port: wichtig  
Sequenznummer: erhöht sich immer um die Daten  
Quittungsnummer: Überprüfung ob alle Daten angekommen sind  
Flags: Steuerbits  
 - Urgent Pointer Flag: der UrgentPointer ist aktiv  
 - ACK: Bestätigungsflag   
 - Push: übergib die Daten sofort an die Applikation  
 - RST: setzt Zählerzustand bis zur letzten Bestätigung zurück  
 - SYN: Verbindungsaufbauwunsch  
 - FIN: Verbindungsabbauwunsch

Fenstergröße: wie viel darf ich senden ohne zu eine Bestätigung zu bekommen max. 16.000 Bit  
 wenn diese ausgereizt ist dann kann nichts mehr gesendet werden

Prüfsumme:  
Urgent Pointer: zeigt auf die zunächst verarbeitenden Daten innerhalb des Pakets

1. Protokollablauf

Nur Syn und Fin Flag erhöhen die eigene Sequenznummer um 1.

Verbindungsaufbau

A B  
 Seq = 100; Flag = Syn;

A B  
 Seq = 300; ACK = 101; Flag = Syn, Ack

A B  
 Seq = 101; ACK = 301; Flag = ACK

Datenaustausch

A B  
 Seq =101; ACK = 301; Data = 10

A B

Seq = 301; ACK = 111; Data = 20; Flag = ACK

A B  
 Seq = 111; ACK = 321; Flag = ACK

Verbindungsabbau

A B  
 Seq = 111; ACK = 321; Flag = Fin

A B  
 Seq = 321; ACK = 112; Flag = ACK; Data = 10

A B  
 Seq =112; ACK = 331; Flag = ACK

A B  
 Seq = 331; ACK = 112; Flag = Fin

A B  
 Seq = 112; ACK = 332; Flag = ACK

1. Zeitüberwachung

Retransmission Timer

Beim lossenden eines Pakets wird der Timer gesetzt, kommt während der Timer läuft keine Bestätigung wird das Paket erneut gesendet.  
Der Timer ist dynamisch (start ist bei 10 sekunden Wartezeit) und wird nach jeden erfolgreichen Empfangen einer Bestätigung runter gesetzt, bei jeder nicht erfolgreichen Sendung wird der Timer rauf gesetzt.

Persistance Timer

Solang senden bis der Puffer (Window) vom Empfänger voll ist. Sendet Testpaket an Empfänger damit er weiß wie voll der Puffer ist.

Quiet Time

Nach Beendigung der Verbindung muss die Stillhaltezeit von ca. 30 Sekunden eingehalten werden bevor zum gleichen wieder eine Verbindung aufgebaut werden kann.

Keepalive and idletimer

3 Testpakete werden nacheinander ausgesandt um zu Testen ob die Verbindung noch steht sonst wird die Verbindung ordnungsgemäß beendet.

1. Steigerung der Performance

Alle 6 Monate Verdoppelung der Belastung des Internets (am Anfang) 🡪 Wie kann ich das Internet mit SW schneller machen?

Verzögerung der Bestätigung

Der Puffer ist vielleicht schon richtig gerechnet und es gibt Antwortdaten 🡪 viele

Silly Window Avoidance Syndrom (nur Empfänger Seite)

Puffer 🡪 Hier werden Empfangene Daten, welche nicht sofort verarbeitet werden gepuffert, wenn es voll ist können keine Daten mehr angenommen werden 🡪 Bei einer neuen Fenstergröße (erst wenn eine gewisse Änderung der Fenstergröße vorhanden ist) wird diese an den Sender bekanntgegeben

Small Paket Avoidance (Senderseite)

Der Sender wartet bis eine Gewisse Datenmenge vorhanden ist, somit vermeide ich viele, kleine Pakete.  
Kann nur in gewissen Situationen eingesetzt werden 🡪 ZB beim Downloaden, nicht bei Streaming

Jacobson Allgorithmus

Router schickt an Sender, dass sie langsamer senden sollen

UDP

Ersatz von TCP wo es geht zB Lan, sichere Verbindung muss bestehen

Kopf:

1 – 16: Sender-Port 16 - 32: Empfänger-Port  
1 – 16: Länge 16 – 32: Prüfsumme

Prüfsumme wird nicht ausgewertet, keine Reihenfolge er Pakete, muss drauf vertrauen dass die Daten in der richtigen Reihenfolge ankommen  
Privaten Netzwerken,

ICMP

1 – 8: Typ 8-16: Code 16 - 32: Prüfsumme  
1 – 32: Verschiedenes  
+ IP-Kopf + 8 Data Byte

Typ: unreachable, timeexited  
Code: untertypen  
Verschiedenes: Pausen zwischen den Paketen, …

Internet Working

Besteht aus vielen Selbständigen Netzen die miteinander kommunizieren,  
Autonome Zone: Voll arbeitsfähig 🡪 DNS, Gateway nach außen  
Von einer Zone zur nächsten wird geroutet  
Die Vermaschung ist so eng das man mit max 3 Hops zur Zielzone kommt, meist über Seekabel wenn Überkontinental vernetzt werden soll (weniger Verzögerung, günstiger)

1. Router

Selbe wie Gateway bloß muss das Protokoll dasselbe bleiben 🡪 nur Adressen umsetzten  
Wohin sende ich das Pakte?

Routing

Optimaler Weg 🡪 schnellstmöglicher Weg 🡪 5 – 6 Hops  
Routingfaktor: wie nahe bin ich am optimalen Weg  
Vorteil bei IPv6 🡪 2 – 3 Hops

Statisches Routing

Lan 🡪 fixe Routing Tabellen

Dynamisches Routing

permanent werden Routing Pakete losgeschickt um die Verbindung zu testen 🡪 Performance der Einzelnen Leitungen wird festgehalten 🡪 einkommendes Paket wird auf den schnellstmöglichen weg geschickt

Average Routing

die Pakete werden an alle gesendet außer an dem von dem es kommt 🡪 das Paket, welches als erstes ankommt hat „Gewonnen“, die anderen werden gelöscht. Somit kann der schnellste Weg ermittelt werden 🡪 wird heute nicht mehr verwendet wurde aber am Anfang des Internets verwendet

1. Gateway

Kommunikationsrechner, welcher verschiedenen Rechennetze miteinander verbindet. Kann Protokoll umsetzten (übersetzten)

1. Bridge

Verbindung von Zwei Netzen, Entfernung überbrücken

Ethernet (Schicht 1 & 2)

Kollisionsdomäne:  
5-4-3 Regel: max 5 Kabel, max 4 Repeater, max 3 Stationen 🡪 alte Regel

1. CSMA

Alt! Nun mehr aus kompatibilitätsgründen, Bussystem (nur ein Signal/Paket auf der Leitung)

Carrier Sense multiple exces

CA: Prüft ob Spannung auf der Leitung ist…

MA: Es können mehrere darauf zugreifen

CD: collision Detection … die ersten 64 Bit dürfen sich nicht verfälschen

Bei Coax Kabeln oder Hubs  
Übergang in Flow Control

Prüfbits heißen Präambel

Standartkabel: 100Base-TX

Ethernet || tagged: Inter Frame Gap 9,6 mikro-s werden gebraucht um 100m zurückzulegen

Auto-Negotiation: Switches stellen sich auf die geminsamen niedrigsten Standard.

RJ45 Stecker für die Kabel  
CAT 6 ist dicker statt CAT 5 e Standard um die 100m zu schaffen (Gigabit-Ethernet)

10 Gigabit-Ethernet: CAT 7

Jumbo-Frame: größere Pakete 🡪 mehr Fehler

Glasfaser: Kunststoffader 🡪 Licht wird hin und her gleitet (Totalreflektion), Enden werden poliert = optisch sauber und nicht reflektieren 🡪 die Kabel werden zusammengelegt und mit einem Harz verbunden (Splice)

1. Switch

Jeder hat seine eigene Leitung, kann aber auch in den Hub-Modus schalten bei großer Überlastung

Kaskadieren: Switch mit Switch mit Switch Verbinden (max 100 m Leitungen) dann erst Rechner  
Performance leidet

Switching

Cut Through

Analysiert sofort das Paket, sobald er die Zieladresse hat wird das Paket weitergeleitet 🡪 keine Vollständige Analyse (keine Fehler Analyse während dem senden 🡪 erst beim Ziel)  
Sinn: gute Qualität, weniger Fehler

Store and Forward

Gesamtes Paket empfangen und analysieren 🡪 kein Fehler dann wird es weiter geschickt

Adaptive Cut Through

Kombi aus cut through und store and forward 🡪 Preis Richtung 1000€  
Kombinieren teilweise während dem senden

FragmentFree Cut Through

Cisco 🡪 in den 1. 64 Byte treten am häufigsten Fehler auf 🡪 64. Byte werden analysiert

Latenzzeit

Cut through und store forward werden verschieden gemessen (FIFO und LIFO - Verfahren)

1. MAC (Maschine Access Control) – Adresse

MAPPE: T3  
In Schicht 1, muss weltweit eindeutig sein, vom Hersteller Codiert

Flow Control, Back-Pressure, Auto-Negotation (einstellen auf gleiche Bandbreite 🡪 sonst Head of Line Blocking)  
Quality of Service, Classes of Service, Jitter, VoIP (muss mit QoS zusammenspielen) 🡪 unterstützen SIP,

VLAN

Switch, welcher SW mäßig getrennt

Prioritäten: zb VoIP höhere Priorität

NFS

Von Firma SAN  
zuerst für UNIX  
damit bin ich kompatibel zB von Windows auf Linux

Setzt auf UDP auf

1. Einteilung der Zugriffstechniken (Zugriffsverfahren, Netzwerkintegration):

Stufe 1: Time Sharing

Eine CPU jeder Task bekommt einen kurzen Zeitabschnitt

Stufe 2: File Transfer

Es gibt einen Dateiserver 🡪 nur für unstrukturierte Dateien

Stufe 3: NFS

Blockweise übertragen 🡪 Festplatten unabhängig 🡪 auch nur für unstrukturierte Dateien zB Videostreaming

Stufe 4: Client-Server-System (Thick Client)

Man benötigt viel Bandbreite, wenn ich einen Datensatz brauche (Anfrage) bereitet sie der Server auf, schickt sie zurück und bildet sie in einer Maske ab

Stufe 5: Terminal Server RDP (Thin Client) (vorher ICA)

Gedanklich wie Stufe 1: einen Zentralen Server der alles Verwaltet 🡪 nur mehr komprimierte Bildschirme werden übertragen, auch Maus und Tastatur eingaben werden komprimiert übertragen  
Vorteile: Remote (über Internet hinweg) Verbinden (mehrere Standorte auf einen Server zugreifen), Central Point of Administration (brauch nicht zu jedem Computer hinlaufen & neu Installieren, Server verteilt), brauch nicht so viel Leistung

Stärken: Performant  
Schwächen: bei Absturz bleiben offene Dateien offen, Zusätzlichen Server für Sicherheit (zB Login),

FTP unsicher 🡪 Passwort wird im klartext übertragen

IPv6

Panik IPv4 Adressen gehen aus  
von 32 auf 128 Bit lange Adressen  
Vorteile: halbe Anzahl der Hops (3-4) (Routing), QoS (Bandbreite zuweisen), Verschlüsselungsfunktion, genug Adressen,

Nachteile: Hardware muss eingetauscht werden

* Header: Basis + Optionale (Baumstruktur)
* Klassifizierung der Datenströme 🡪 Prioritäten setzen 🡪 höchste Priorität hat am meisten Bandbreite
* Performantere Kommunikation innerhalb des Netzwerkes
* Manuelle Konfiguration erheblich vereinfacht
* Benutzung anderer Protokolle statt TCP wird unterstützt
* Engpässe werden erkannt 🡪 Flow Control
* Router werden automatisiert konfiguriert 🡪 Pakete erkennen, welcher Weg am schnellsten ist
* Handynetz und Datennetz werden fusioniert

1. Adressen

Variante 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 Bit | 13 Bit | 8 Bit | 24 Bit | 16 Bit | 64 Bit |
| 001 | TLA | reserviert | NLA | SLA | Lokal |

TopLabelAggregation 🡪 Provider, verwalten Backbones (Datenautobahnen (Highspeedverbindung))  
NextLevelAggregation 🡪 Local Provider zum Versorgen der Kunden  
SiteLevelAggregation 🡪   
Lokal

Führende null nicht schreiben

123.0:0.ABC / 60  
1234:0000:0000:0000:0000:0000:0000:0ABC / 60  
1234::ABC / 60  
:F143 / 64

UNICAST: ein einzelner Empfänger

ANYCAST: aus einer Gruppe von Empfänger werden spezielle ausgewählt

MULTICAST = Broadcast

|  |  |  |  |
| --- | --- | --- | --- |
| 8 Bit | 4 Bit | 4 Bit | 112 |
| 1111 1111 | Typ | Bereich | Gruppe |

Es gibt auch andere Adressierungsarten 🡪 zB für kleinere Provider 🡪 seit 2005

Bestreben: streaming verbessern, lokale Adressen abschaffen  
DHCP ist nicht mehr notwendig 🡪 anderes Verfahren IEEE

Institute of Electrical and E Electronics Engineers 🡪 Dachorganisation der Elektrotechniker 🡪 Standard EVI 48 und EVI 64

Mac-Adresse: 34 56 78 9A RC DE  
EVI 64: 34 56 78 9A FF EE 9A RC DE

Link local Adresse: (lokaler privater Bereich)

|  |  |  |
| --- | --- | --- |
| 10 Bit | n Bit | m Bit |
| 1111 1110 10 | 00..00 | Adressen |

Geht nicht über Router hinaus (in IPv4 lokale Adressen)

Loopback:

127.  
0::0

127.0.0.1 🡪 0:0:0:0:0:0:0:1 (= ::1)

Host ID (64 Bit)

Variante 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 Bit | 1 Bit | 1 Bit | 48 Bit | 16 Bit | 64 Bit |
|  |  |  | Globaler Präfix | Subnetz | Lokale |

Multicast 🡪 Gruppe 2^12 Teilnehmern

Adressenunterschiede

* 1. Auf IPv4 abgebildete Adressen 🡪 0:0:0:0:0:FFFF:a.b.c.d
  2. IPv4 kompatible Adressen 0:0:0:0:0:0:a.b.c.d

Socket Adresse

Netz IP – Host IP - Portnummer

Firewall

Gerät das ein sicheres Netz vom einem unsicheren Netz schützt.

Sicheres Netz – FIREWALL – unsicheres Netz

1. Personal Firewall

Direkt am Server installiert

Kann dinge die externe Firewall nicht kann weil es die Apps kennt 🡪 Calling Home kann man sperren

Sollte man immer belassen und konfigurieren

1. Externe Firewall

Rechner oder eine eigene Box/Hardware die dafür entwickelt wurde

Rechner braucht viel zu viel Strom und ist nich ausfallsicher

Eigene Hardware werden geflasht statt aufgesetzt haben keine festplatte sondern arbeiten mit internem Speicher 🡪 reine Funktion der Firewall

Ethernet Router ist eine Firewall auf sehr niedriger Ebene

* NAT (wichtigste Funktion einer Firewall)

Komponenten:

* Statische Paketfilter (alles blocken was von außen kommt)
* Dynamische Paketfilter (über 1023 und ergeben sich während des Aufbaus)
  + Stateful inspection (alles was auf icmp läuft wird gefiltert)
  + Verbindung als ganzes überwacht
  + Filterung passiert durch das anschauen des icmp paketes
  + ftp sperren 🡪 sperre ich die ports
* application Firewall
  + erkennt das Programm das verwendet wird
  + kann skype, whatsapp herausfiltern
  + erkennt die Software dahinter
* PROXY (Form der Application Firewall)
  + Geht statt meinem Rechner ins internet und liefert mir die Ergebnisse
  + Nicht so angreifbar wie mein Rechner

Standard:

Alles was von außen kommt ist verboten 🡪 alle Ports sind geblockt

Von innen ist alles frei 🡪 kann man sagen was von innen geblockt wird

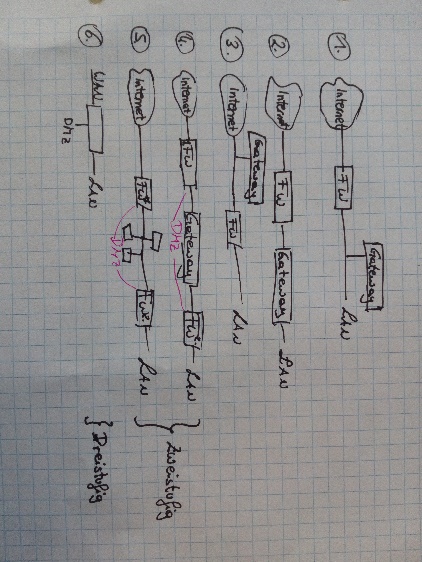
1. Angriffe auf Netzwerk und Computer:

meiste Angriffe von unzufriedenen Mitarbeitern  
von außen Nutz man Pucks, falsch konfigurierte Firewalls oder Trojaner (häufigste Methode)

* Angriffe auf interne Systeme: Server, PCs (Clients) 🡪 gezielter Geräteangriff (ausspionieren) um Daten zu stehlen oder zu manipulieren
* Angriff auf Verbindungen:
  + Man-in-the-middle 🡪 man hängt sich zwischen Sender und Empfänger, Daten laufen über eigenen Rechner 🡪 abhören und sabotieren von Daten
  + Umleiten 🡪 Daten laufen über Server 🡪 Pakete werden umgelenkt bevor sie zum Empfänger gelangen
  + Denial of Service 🡪 Verbindung lahmlegen damit sie nicht mehr arbeiten kann 🡪 Hacker übernehmen Rechner um Pakete gleichzeitig loszuschicken (für große Firmen) 🡪 nur Provider kann etwas dagegen unternehmen (ist Mühsam)
* Viren 🡪 Verbindungen lahmlegen 🡪 2 – stufig (Virenschutz auf Firewall und auf Computer)
* Verschlüsselungstrojaner: Trojaner verschlüsselt Daten, die nur entschlüsselt werden wenn zB ein Geldbetrag bezahlt wird

Lösung Zonen schaffen 🡪

Sicherung muss offline sein und in Generationen vorhanden sein um wirklich immer eine zu haben

Etwa 30 % werden in den nächsten Jahren für Lösungen und Behebungen von Angriffen gezahlt

1. Mehrstufige Firewalls

1. Für Mailrelay  
2. Rechenleistung des Gateways wichtig um effizient arbeiten zu können  
3. Virenscanner, Mailrelay 🡪 kein Schutz des Gateways  
4. Doppelte Sicherung des Lans und Gateway getrennt von Lan 🡪 zwei verschiedenen Hersteller bei den FWs um eventuelle Bucks abzusichern  
5. Rückverfolgung (Thornetz, nur wenn online) und Dummynetz = Fallenserver (simuliert Firmennetz, lukrativ 🡪 Datenschutzverletzung auch nur beim Anschauen der Daten)  
6. Dreiarmige FW 🡪 kombinierbar mit 5. zB zur 1. FW ( = zwei DMZ und drei FW) 🡪 alles in einem Gerät

Übung Firewall

DMZ 🡪 spezielles VLan 🡪 alles von außen ist gesperrt bis auf die Ports, welche notwendig sind 🡪 von DMZ in Lan alles geschlossen von Lan in DMZ Zugriff möglich

SQID 🡪 Proxy http Server 🡪 statische Seiten caschen, Proxy statt Rechner ins Internet schicken   
Proxy eher in eine zweite DMZ (mehr Sicherheit)

CustomerPrimisisEquipment 🡪 Komponenten, die dem Provider gehören aber in der Firma stehen 🡪 kein Zugriff auf Gerät 🡪 BlackBox verfahren

E1 (Europäisch)/T1 (Amerikanisch) 🡪 Standleitungen vom Provider zur Verfügung gestellt 🡪 für Firmen nützlich 🡪 garantierte Bandbreite 🡪 sonst nur das maximale angegeben 🡪 fixe IP (beim Betreiben des Servers notwendig) 🡪 ohne eigene IP Adresse von draußen Zugriff über Port forwarding (der Port des Servers ist bekannt)

POP 🡪 Point of presence 🡪 Modem 🡪 Entfernung ausschlaggebend  
Land 🡪 über Hyprid 🡪 Leitung und Funk

x.21 🡪 Data xl 🡪 Leitung von Telekom 🡪 eine Art Standleitung mit x.21 Protokollen 🡪 Gateway zur Übersetzung in TCP/IP 🡪 heute nicht mehr notwendig 🡪 VPN

Radius Server 🡪 Authentifizierungsserver 🡪 nicht mehr Stand der Technik 🡪 VPN (LzTPoverIPsec = läuft auf allen Betriebssystemen 🡪 hohe Sicherheit da zwei VPN Techniken)

Frontend, Backend 🡪 SQL Server mit ERP System, Kunden & Lieferanten wollen auf Teile zugreifen 🡪 kein Zugriff auf den Server im Rechenzentrum 🡪 Server wird auf Frontend in DMZ gespiegelt & dort auch verändert & auch wieder zurück aktualisiert

IP Adresskonzept 🡪 verschiedene Verwendete Adressen 🡪 Private Adresse (nicht ins Internet geroutet)

Verbesserung Übung Anwaltskanzlei:

Netzwerkmaske angeben. 192.168.0.1 sollte nicht verwendet werden 🡪 wird von vielen Providern verwendet

Zusätzlich werden noch die Dosen, die Kabel und die Ports dazu geschrieben zu dieser Beschreibung damit Fehler schneller gefunden werden.

IT-Techniker und Elektriker

1. Konfiguration einer Firewall ZyWall von Zyxel

Wir machen eine Intranet Firewall

Web basierend 🡪 Profis Console Oberfläche

1. Einloggen
2. Zusätzlich mit Antivirus erweitern (kann) 🡪 einfach weiter
3. Bild von Vorderseite der FW
4. Menü Konfiguration
   1. Reiter Portrollen (aufteilen welcher Port soll für welche Aufgabe bereitstehen): Switch wird erspart, wenn Ports auf der gleichen Ebene 🡪 1 LAN, 4 DMZ
   2. Reiter Ethernet: DHCP WAN 1(bereitgestellt 🡪 automatisch bezogen durch Provider)  
       LAN 🡪 jedes Netz muss Konfiguriert werden 🡪 Name, Lan: LAN1, IP  
       Adresse eingeben, DHCP (Startpunkt + 50 sind DHCP), DNS, 8.8.8.8 Google  
       DNS Server)  
       DMZ 🡪 192.128.1.1
5. Menü FW 🡪 Regeln für den Durchlass
   1. Gewisse Adressen und Ports freigeben / sind vorgegeben
   2. DMZ muss von außen erreichbar sein & darf alles nach außen 🡪 allow, verbunden, verbieten
   3. Regel einstellen:  
      from – to – user: any –
   4. Regeln werden von unten nach oben durchgearbeitet 🡪 wenn ich unten was verbiete und oben erlaube ist es erlaubt
6. Menü Objects  
   Oberfläche ist Objektorientiert
   1. Reiter Adress: alle Adressen müssen vorher angelegt werden  
      User: nur gewisse oder alle  
      Interface: was kommt über den Port herein  
      LAN1:   
      DSCP Code: Klassifizierung von IP-Paketen 🡪 any
7. Menü Nat  
   Schirmt alles ab was hinter der Firewall
   1. SMTP-Server:

Datenschutzverordnung Mai 2018 (DSGVO)

Schärfe Datenschutzrichtlinien 🡪 Schutz muss nachweisbar sein

ZB Klassenfoto 🡪 jeder der am Bild ist hat ein Recht nicht so wie bis her

Daten dürfen erst nach Einwilligung verarbeitet werden auch Suchen

Schutzniveau erhöht & Strafen erhöht

Computertechnik

Lithiumtechnik am Ende 🡪 max Abstand am Prozessor 4-6 Nanometer 🡪 sonst treten Quantenmechanische phenomene auf

Parallelisierung 🡪 mehr Kerne 🡪 nicht alle Apps & Programme können alle Kerne verwenden 🡪 Threads warten auf Ergebnisse von anderen Threads

Neue Technologie 🡪 C60 Ringe 🡪 brauchen weniger Energie beim Schalten

Erste Computer mit Prozessoren 1970

Mikrorechner: alle Prozessoren auf IC

Minirechner (ausgestorben):

Hostrechner (im Verschwinden):

Supercomputer: Wetterberechnungen, dynamische Anzeigen

1. Leistung eines Rechners erfassen

MIPS 🡪 Millionen Instruktionen per Sekunde 🡪 nicht rückrechenbar auf die Leistung

Catch 🡪 kann Geschwindigkeit beeinflussen 🡪 Einkaufswagen fährt durch Geschäft Catch trägt Produkte zu

Compiler 🡪 unterschiedliche Anzahl generierten Maschinenbefehle

FLOPS

CLIPS 🡪 logische Schlussfolgerungen pro Sekunde 🡪 Praxis gerecht

Benchmarks 🡪 machen Rechner vergleichbar zb über die Graphikkarte 🡪 nur auf eine bestimmte Anwendung zugeschnitten 🡪 Graphikkarte, Festplatte etc.

1. Arten von Prozessoren

* CISC 🡪
* RISC 🡪 schneller einfachere Befehle 🡪 kann zB nicht multiplizieren

Prozessrechner 🡪 muss nicht Booten (gleich Ready nach Start) 🡪 beim Auto 🡪 Embedded Betriebssystem (im Ram schon vorhanden) 🡪 gegen Umwelteinflüsse geschützt (Erschütterungen, Magnetfelder), Robust, Staubgeschützt, Ausfallsicherheit (im Flugzeug zB redundant),

Mikrocontroller 🡪 kriegt noch weiter Periphäre Funktionen 🡪 Ausgabe usw 🡪 weiterentwickelte Mikroprozessoren

Je Maschinen näher desto schneller und Fehlerunanfälliger

Skalar-Rechner: herkömmlicher Rechner 🡪 Schritt für Schritt Abarbeitung

Vektor-Rechner: kann Aufgaben parallel durchführen 🡪 Nummerische Aufgaben lösen

Analog-Rechner: Anfangszeit 🡪 riesen Rechner mit Schaltrechner  
Hybrid-Rechner: weiterentwickelte Analog-Rechner

Heutige Prozessoren sind ein MischMasch

|  |  |  |  |
| --- | --- | --- | --- |
| F(etch) | P(rozessing) | O(Output) |  |
|  | F(etch) | P(rozessing) | O(Output) |

* Multiskalar  
  Maschinenbefehl braucht mehrere Taktzyklen  
  Taktfrequenz ist weniger geworden
* Multipipeline  
  mehrere Kerne (Rechenwerke) 🡪 Pipes können nebeneinander laufen

Busse beim Großrechner heißen Kanäle  
IOT & Sicherheitstechnik werden immer mehr gefragt  
Internet of Things 🡪 große Sicherheitslücken

Datenerfassung/träger

Jede Tastatur, jede Maus

* Offline Datenerfassungsgeräte:
  + Kamera
  + Papier (eingescannt und ausgewertet)
  + Barcode (EAN, 13 Codierte Zahlen \* 2) 🡪 auf Verpackung, gute Druckqualität
  + Nachfolgetechnologie EAN: RFID (Liftkarten, Hotelkartenzimmer, neue Supermärkte)
  + Klarsichtbelege 🡪 OCR optical character reconition
  + Pattern Matching
  + Feature Reiognition

Magnetische Speicherung

* Disketten 🡪 ausgestorben 🡪 zu klein
* Streamerbänder 🡪 terabyte 🡪 günstig goße Datenmengen sichern und Speichern

HDD 🡪 günstiger als SSD 🡪 ende der physischen Laufbahn 🡪 Spuren zu eng aneinander daten können nicht ordentlich gespeihcert werden

Vorstellung Torte mit Sektoren in denen die Spuren sind  
Interleaf faktor 🡪 Elektronik ist nicht schnell genug 🡪 Sektor ist zu schnell vorbei und ich brauche noch eine Umdrehung

Low level formatieren 🡪 Struktur einstellen 🡪 Bios weiß wo was 🡪 Adressierung: Spur, Sektor, Kopf (Plattenoberfläche)

Spur in jedem Sektor die gleiche Länge 🡪 Kontroller virtualisiert interne Struktur 🡪 translation mode (native mode im inneren wird übersetzt) 🡪 größe der Platte Schlagartig erhöht 🡪 AT Bus

Schichten, Mechanik verbessert 🡪 Terabyte bereich

Parallele Leitungen höher Takten 🡪 mehr Fehler

(Serielle Busse )Serialatra 🡪 weniger Parallele Kabel die höher getaktet sind

SCSI (SAS) 🡪 Soll Computer System Interface 🡪 Host adapter 🡪 Controller welcher in der Mitte sitzt welcher einen Bus zum Pc und einen Bus zur Festplatte hat (seriell) 🡪 kleiner Computer der automatisch sachen von der Festplatte holt 🡪 gebraucht bei Server (RAID Systeme) für interne Kommunikation

Magnetoptische Datenträger  
Die Stelle wo der Laser auftritt wird bis kurz unter dem Kyriepunkt erhitzt

Preis war zu teuer deswegen ist es abgesetzt

DVD/CD 🡪 Es wird erhitzt beim raufschreiben 🡪 wiederverwendbar

DVD/CD ROM die gebrannt werden sind anders beschichtet

SSP 🡪 Produkte richtig Planen und bewerten

Heute spricht man nicht mehr von Hardware sondern von Diensten/Services  
Dienste sind vernetzt 🡪 ein Ausfall kann einen anderen nach sich ziehen 🡪 Was kostet ein Ausfall?

* File Server
* Email
* Internet
* ERP
* Netz
* LAN
* Active Directory
* ERP
* CloudSystem
  + IAAS: Infrastructure as a Service 🡪 Virtuelle Rechnerleistung (CPU) 🡪 zB zum Austellen eines Windows Server 🡪 Service Level Agreement 🡪 Vertragsgrundlage
  + PAAS: Plattform as a Service
  + SAAS: Software as a Service
  + Vorteile: von überall aus erreichbar, man muss nicht in der Firma sitzen
  + Nachteil: nicht mehr in der eignen Hand
  + Ausprägungen:
    - Public Cloud: offenes System (Dropbox), flexibel, gratis bzw. geringe Kosten
    - Private Cloud:

Sicherheit (Ausfall)

Rechenzentrum (bietet viele Dienste an) 🡪 kann auch Ausfallen 🡪 Wahrscheinlichkeit dass dieses Ausfällt 99,9999 ab dem dritten neuner verdoppelt sich mit jedem weiteren des Preises

Netzwerke

**Warum kann ein Netzwerk ausfallen?**

Schleifen, Stromausfall, Sabotage

Kosten:

* Umsatz: 750 Mio
* Umsatz pro Stunde: 288.000
* Kosten pro Stunde: 50.000

**Wie kann ich einen Ausfall verhindern?**Core Layer 🡪 Distribution Layer 🡪 Excess Layer (Cisco Aufbau Netzwerk)

1. Layer 2

Spanning Tree

Vom Core Switch aus gehen Leitungen in die Etagenswitches (Distribution Layer) der einzelnen Stockwerke, wo wiederum Switches mit Pc’s (Excess Layer) dranhängen.  
Er hat einen bevorzugten und einen Redundanten weg.  
Nachteil: zweite Leitung wird nicht benutzt  
Umschaltzeit: 30s  
beim Rapid Spanning Tree: max 1s 🡪 Resilent Link  
Switch muss Norm unterstützen (für Spanning Tree: IEEE 802.10)  
Autoconfiguration

Basierend auf Layer 2 (auch wenn Gerät Layer 3 kann)

Linked Aggregation (=Trunking)

Bündeln von Leitungen = vom zb Server gehen mehrere psychische Leitungen zum zb Switch/Router  
eine IP-Adresse wird für mehrere Leitungen verwendet.  
max 8 Leitungen können genutzt werden  
Protokoll: IEEE 802.300

MAN KANN AUCH SPANNING TREE UND TRANKING VERBINDEN 🡪 der Hauptast wird zb verstärkt

Resilent TCMP

Multipoint Linked Aggregation = MPLA

Switches kommuniziere über eine HighSpeed Verbindungen 🡪 sind Redundant 🡪 alle Server sind an alle Switches angebunden 🡪 bei Ausfall wird sofort auf anderen geschalten  
können nur Hochleistungsswitches 🡪 Wenn Netzwerkübertragungsgeschwindigkeit gesteigert werden soll und eine Sicherheit sein soll ´

1. Layer 3

A und B sind über Knoten miteinander Verbunden 🡪 über mehrere Knoten 🡪 Routing

Statisch

Örtlich beschränkt ab 10 wird es mühsam  
Routingtabellen mit allen Wegen existieren 🡪 die Besten Wege werden immer genommen  
in allen Firmen, wenn Router mit Switches gemischt

dynamisch

Routingtabelle wird ständig aktualisiert 🡪 es werden Testpakete geschickt um die Verbindung zu prüfen 🡪 eigene Protokolle (zB virtual Router Redundancy Protokoll)

1. WAN Redundanz

2 WAN Ports 🡪 neue Verbindungen werden immer bei der Leitung eröffnet, wo am meisten Bandbreite dahinter ist 🡪 Load Palancing kann bei IPv4 nur vor dem Aufbau der Verbindung (nur mit Einschränkungen möglich) und bei IPv6 sogar während aufgebauter Verbindung erfolgen

1. HW Redundanz

1 Server ist in Bereitschaft wenn der andere ausfällt🡪 Fail Over

Cluster (Server)

Nach oben hin wird virtualisiert damit eine Plattform bereitgestellt werden kann 🡪 erweiterbar im Betrieb 🡪 Plaid-Systeme (Schränke wo Server hineingeschoben sind)

Festplatten

Raid Systeme 🡪 verhalten sich nach außen wie eine

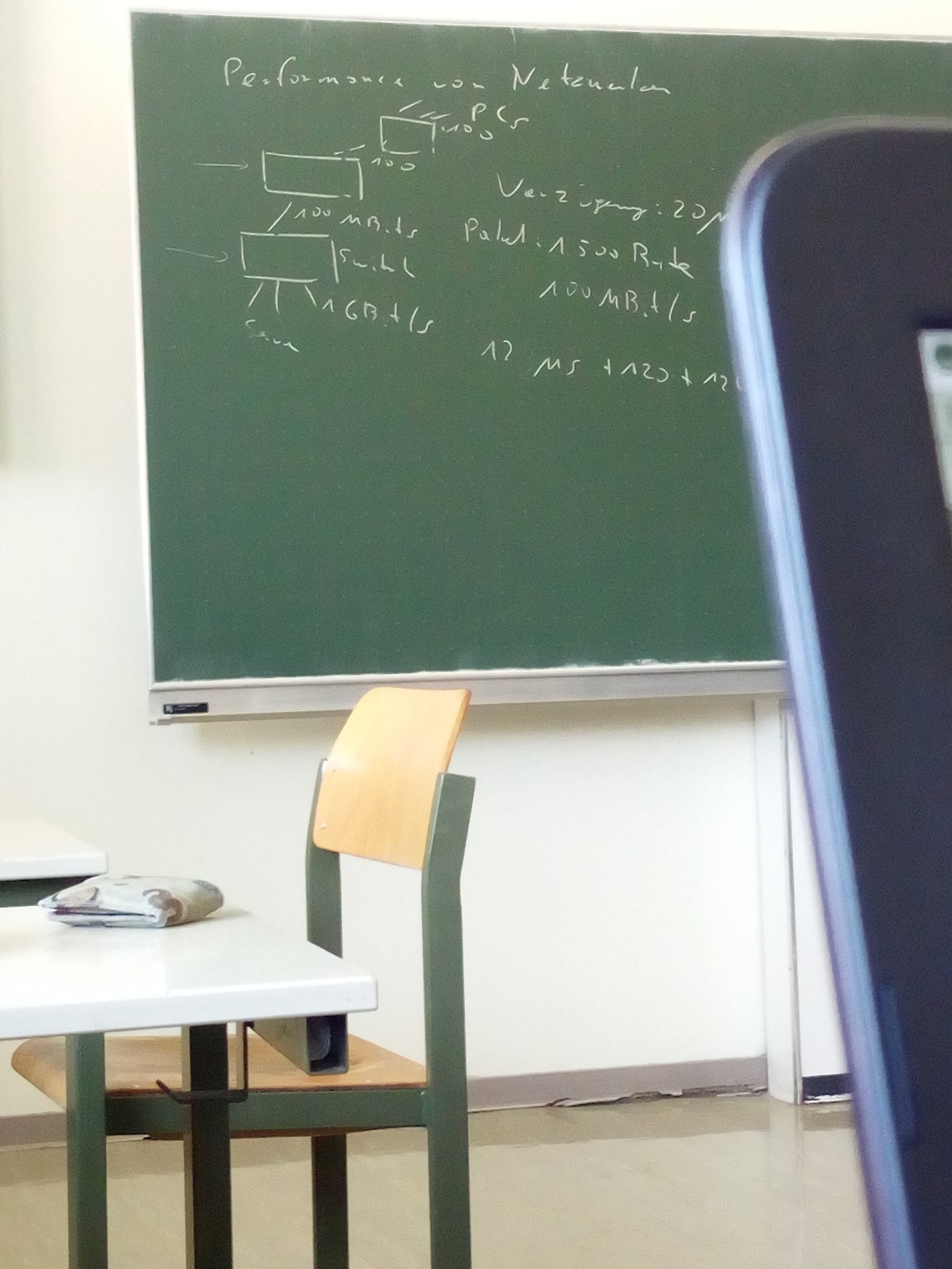
Raid 0: 2 Festplatten 🡪 jede beinhaltet eigene Daten  
Raid 1: 2 Festplatten gespiegelt 🡪 schnellerer Zugriff ¼ Umdrehung  
Raid 5: Stripping 🡪 max 5 Festplatten: 4 beinhalten Datenstreifen nd eine beinhaltet einen Paritätsstreifen 🡪 der Paritätsstreifen befindet sich immer auf einer anderen der Platten  
Raid 5: minimum 4 Platten min 2 Paritätsplatten

Kombinationen zb 5 0 🡪 jeweils 2 \* 3 Festplatten welche nach außen wie ein Raid 0 System funktionierten

Performance von Netzwerken

Mehr Daten werden übertragen durch zB dynamische Websites 🡪 bei Cloudsystemen ist es nicht so gigantsich

Switch Latenzzeit: 20μs   
Paket: 1500 Byte  
 100Mbit/s  
120μs von einem zum Anderen Switch 🡪 120+120+120+120+3\*120=552 μs



Was kann ich tun um in einer Firma das Netzwerk zu gewissen Zeiten einbricht?  
Zuerst suchen zB mittels Messen wo die Schwachstelle ist  
Wenns an einer Leitung liegt kann man zB Trunking einsetzen  
bei den PC’s kann es zB über ein VLAN laufen damit der Traffic nicht aufs ganze Netz geht  
beim untersten Switch (welcher zum Server geht) brauche ich einen Layer 3 Switch, auch auf der mittleren Ebenen ist ein Layer 3 Switch notwenig

Rechte

1. Urheberrecht

Literatur (zB Programme), bildende Künste, Filmkunst, Singkunst  
geistige Wertschöpfer ist Urheber  
Sammlungen von Urheberschaften zB bei CD (CD-Erzeuger, Komponist, Sänger, Textschreiber)

70 Jahre nach dem Tod des Urhebers erlischt das Urheberrecht 🡪 Folgerecht sind vererbbar

Kein Mindestalter um Urheberrecht

**Wer entscheidet was Urheberrechtlich geschützt ist?**ist automatisch bei einer Neuschaffung Urheber 🡪 kein Register 🡪 ersichtliche Kennzeichnung wann und wo ich etwas erfunden habe 🡪 Beweisen das ich Urheber bin copyright allein zählt nicht

**Kann eine Zusammenstellung von Werken auch Urheberrechtlich geschützt sein? (zB eine Liste)**Auch Datenbanken oder Sammlungen zB Köchelverzeichnis (Alle Werke von Mozart aufgelistet) sind Urheberechtlich geschützt

**Schutzrechte**Wenn ich ein Programmschreibe darf ich es verkaufen bzw. vervielfältigen 🡪 kann aber Rechte weiter geben

**Gebrauchsmusterschutz**unter Patent aber stärker geschützt als Urheberrecht 🡪 Eintragung in DB

**Logo**bildende Künste 🡪 wie Gebrauchsmusterschutz wird aber als Marke eingetragen 🡪 nennt man Markenrechtlicher Schutz 🡪 nicht nur Schriftzug sondern auch Marke ist geschützt 🡪 ca. 3.000€

**Foto**Fotograf Urheber des Fotos  
Recht der eignen Person ist Stärker als Urheberrecht 🡪 wenn ich auf einem Foto bin dann habe ich das Recht zu sagen ich will nicht veröffentlicht werden.  
Aber wenn eine Gruppe fotografiert wird und nicht ich im Fotomittelpunkt stehe kann ich nichts machen  
Keine Fotos von Websiten fotografieren 🡪 klagbar

**Filme**mit dem Drehen des Filmes werden alle Urheberrechte an den Produzenten abgetreten

**Programme**Urheberrecht kann nicht abgetreten oder verkauft werden  
wichtig sind die Folgerechte 🡪 Vervielfältigung, Publikation 🡪 treten wir an die Firma ab (wird abgegolten durch den Gehalt 🡪 steht in Arbeitsvertrag) 🡪 Wenn der Erfolg des Unternehmens durch den Code so groß ist kann der Programmierer eine Sonderzahlung verlangen

Datenbank Urheberrecht erlischt 15 Jahre nach dem Tod des Urhebers

**Websiten**Urheberrechte gelten auch für Menüs oder neue Strukturen

Vervielfältigungsrecht, Vortragsrecht = Aufführungsrecht, zur Verfügungsstellungsrecht  
Covern kann ich nur wenn es mit dem Komponisten abgestimmt ist  
Kopieren 🡪 nicht erlaubt außer für den eigenen Bedarf (Sicherheitskopie erlaubt 🡪 auf neuen Rechner installieren nicht erlaubt)  
CD: darf ich kopieren und 5 freunden geben (nur wenn ich Original besitz)

1. Lizenzrecht

Unterkapitel vom Urheberrecht

Lizenz ist Nutzungsrecht 🡪 man Besitzt nicht zB die Software

Kann überprüft werden 🡪 wenn einfach jedemand überprüft wird ist etwas faul 🡪 Anzeige etc

Überprüfungen werden normal angesagt

Strafen: 10 fache des Wertes der eingesetzten Lizenzen

Software ist nicht Eigentum des Users

Proprietäre Software

Hersteller hat SW geschrieben und vertreibt sie egal ob gegen Geld oder nicht  
Vorkompiliert, Quellcode nicht einsehbar, meist gegen Geld  
Hersteller muss zur Verfügung stehen um zu Helfen  
Datenschutz ist durch Hersteller gegeben

**Freeware Shareware**

Meist einen Monat verwendbar (Tests) dann zu zahlen

**Crypleware**

Funktion eingeschränkt bist zur zahlung 🡪 sonderform von freeware shareware

OpenSource SW

Quellcode ist veröffentlicht 🡪 meist ein Einzelner Entwickelt  
Recht auf Anpassung, Einsehbarkeit und veränderte kostenpflichtige Weitergabe mit Quellcode erlaubt  
muss nicht immer kein Geld kosten  
darf ohne Einschränkungen benutzt werden  
darf nicht proprietäre werden

Privatisierung soll verhindert werden

Weniger Kosten, freie Auswahl, Binde mich zu keinen

Freie SW

Public Domain

Ist komplett frei 🡪 autor verzichtet auf copyright 🡪 stellt code allgemeinheit zur Verfügung  
kann auch meinen Namen drauf geben und Verkaufen

Folgerechte komplett frei 🡪 auch in eigenen code einbauen

Freie SW

**BSD Lizenz**

älteste Freie SW 🡪 code muss nicht mitgegeben werden

**GNU = GPL**

Hier muss Quellcode verfügbar bleiben und copyleft Prinzip  
geht in Bereich OpenSource

Copyleft 🡪 vererbe es weiter 🡪 muss Quellcode wenn er vorhanden war dann muss er mitgegeben werden

Frei SW 🡪 kein Hersteller dahinter kann aber auch was Kosten

1. Lizenzmodelle im Propräterbereich

* Einzelplatz: nur für einen Computer bzw Laptop
* Netzwerklizenz: Lizenz beliebig oft Installierbar aber darf nur einmal zum gleichen Zeitpunkt genutzt werden 🡪 Programm mit Lizenz auf zwei oder mehr rechner installierbar aber nur eine Person auf einem Rechner kann sie nutzen
* Subscription, Dauerlizenz: Updateservice, Wartung nur mit Subscription mit Wartung
* Mietlizenz, Desktop\_Lizenz: Nutzungsbediengung läuft nach dem im Vertrag geregelten Zeitraum ab
* Cloudlizenz: Nur mehr Nutzung zB pro Monat/Aufruf wird bezahlt
* Volumenlizenzen: ein Vertrag wird pro Jahr abgeschlossen zB für 50 Plätze 🡪 brauche nur einen Lizenzschlüssel
* Schullizenzen: sind komplett kostenfrei oder sehr wenig kosten 🡪 rein für Schulische Zwecke