

Netztechnik +/-

Vorteile und Möglichkeiten von Netzen/ Netzwerken

1. ZENTRALE STEUERUNG VON PROGRAMMEN UND DATEN UND ALSO WENIGER ADMINISTRATIONSaufWAND

- Updates, Treiber, Userverwaltung, Lizenzierung

2. NUTZUNG GEMEINSAMER DATENBESTÄNDE UND ALSO VEREINFACHTE KOOPERATION UND NUTZUNG ZENTRALER DATENBANKEN, DATEIABLAGEN

- Lager eines Shops, Terminverwaltung, Textversionierung,...
- Mandantenfähigkeit: Software sollte mandantenfähig sein

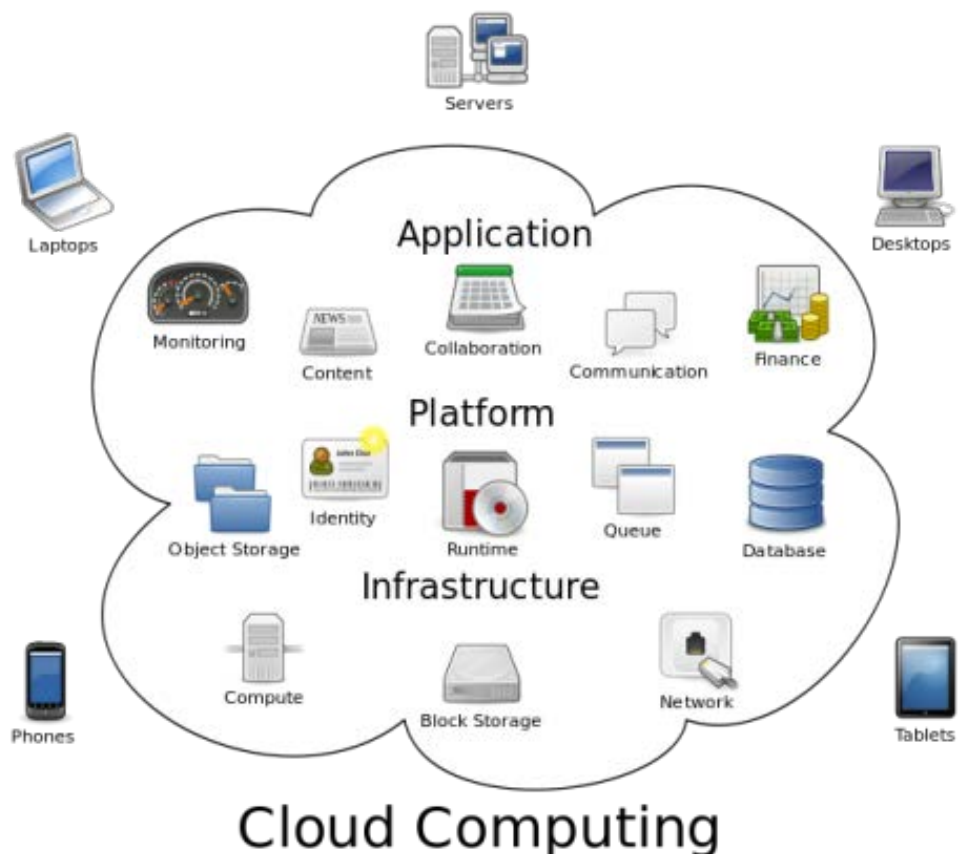
3. ERHÖHTER DATENSCHUTZ UND DATENSICHERHEIT DURCH ZENTRALE USERVERWALTUNG, ABLAGE AN SICHEM ORT, SERVERRAUM MIT BRANDSCHUTZ UND ZUGANGSKONTROLLE

- Fileserver oder LDAP-Server ist in abgeschlossenem Rack in abgeschlossenem Serverraum
- Zugriffskontrolle: unautorisierte Zugriffe werden unterbunden (erschwert) und Zugriffe geloggt/ protokolliert
- zentrale Kontrolle der *Druckquotas* ...
- Zentraler immer aktueller Virens scanner, zentral angestoßene Programmupdates, ...
- Kontrolle der Onlineaktivitäten der Mitarbeiter über einen Proxy

4. GRÖßERE LEISTUNGSFÄHIGKEIT DURCH AUFGABENVERTEILUNG (SPEZIALISIERUNG) UND DISTRIBUTED COMPUTING

- Zuordnung von zentraler Rechenleistung oder Dezentralisierung von Rechenleistung auf verschiedene Rechner/ CPUs (einer Million PS3-TeilnehmerInnen haben Proteinfaltungen analysieren lassen ...)

5. GEMEINSAME NUTZUNG DER RESSOURCEN DURCH CLOUDCOMPUTING UND ON-LINE-OUT-SOURCING; RESSOURCEN SIND LEICHTER SKALIERBAR (ANPASSUNG AN DEN BEDARF KANN SCHNELL UND FLEXIBEL ERFOLGEN), MAN KANN FLEXIBEL FREMDE DIENSTLEISTER EINBINDEN



- alle können drucken, online gehen, große Dateien abspeichern ... aber es muss keine neue Hardware für alle gekauft werden
- Man kann mit unterschiedlicher Hardware auf die Netzressourcen zugreifen und sich so flexibel den Nutzungsgegebenheiten anpassen (mobiler Einsatz über Laptops oder sogar Smartphones oder zu Hause oder im Büro)

Probleme von Netzen und Netzwerken

1. GROßE STÖRANFÄLLIGKEIT VON NETZEN

- Wenn das Netzwerk ausfällt, dann ist nicht ein einzelner Arbeitsplatz betroffen, sondern möglicherweise die komplette datenverarbeitende Infrastruktur eines Unternehmens, einer Behörde: Anmeldung nicht möglich, Thin Clients ohne jede Rechenleistung, Keine Transaktionen ohne Datenbankzugriff.
- Große Gefährdung weil:
 - Hacker und Cyberkriminelle versuchen permanent Netzwerke anzugreifen, um Zugriff auf die dortigen Daten zu erhalten oder um die Ressourcen zu nutzen (z. B. als Schleudern für SPAM)
 - Hardware wird stark beansprucht; die Fehlermöglichkeiten der Hardware sind groß und die Fehlerwirkungen amorph
 - Ein kleiner Fehler kann gravierende Folgen haben (ein Mitarbeiter geht schlampig mit einem Passwort um, ein Backupsystem hat unbemerkt eine Störung, ein Exploit nutzt eine Schwachstelle der eingesetzten Software ...)
 - Vor allem mit Outsourcing sind Risiken verbunden (Mitarbeiter ohne Firmen-Loyalität und außerhalb der eigenen Kontrolle, unsichere Übermittlungswege ...)

2. ZENTRALISIERUNG ENTWERTET DEZENTRALE KOMPETENZEN, DIE CHAOSQUALIFIKATION DER MITARBEITER SCHADET, STATT ZU NUTZEN

- Zur Behebung von Störungen kann nicht der einzelne vor Ort tätig werden, sondern man muss auf den übergeordneten Spezialisten warten

3. BEDARF AN HOCHQUALIFIZIERTEN (TEUREN) SPEZIALISTEN

- Netzwerke erfordern bei der Anlage und dem Betrieb qualifizierte Spezialisten, die auf dem Arbeitsmarkt teuer sind
- Analyse von Netzwerkfehlern ist zum Teil sehr schwierig: muss aber schnell gehen, weil viele davon betroffen sind

4. BACKUP-LÖSUNGEN UND MAßNAHMEN ZUR DATENSICHERHEIT SIND TEUER UND FEHLERANFÄLLIG

- RAID Level 1-System mit Datenspiegelung verbrennt die Hälfte (RAID 5 immer noch einen großen Teil) der Festplattenkapazität (Hot-Plugging-fähige Hardware ist teuer)
- Backupfehler bleiben oft unentdeckt

5. BIG BROTHER IS WATCHING YOU: SEHR WEIT GEHENDE KONTROLLMÖGLICHKEITEN VON KUNDEN UND MITARBEITERN

- Alle möglichen Zugriffe können geloggt und ‚smart‘ verknüpft ausgewertet werden; so können automatisch Profile der Anwender erstellt werden
- Trennung von privater und beruflicher Netznutzung; Gewährleistung von Datenschutzvorgaben
- Alle Dateien können zugeordnet werden, unsichtbarer zentraler Zugriff auf alle Daten

6. TECHNIKABHÄNGIGKEIT: GROßE ABHÄNGIGKEIT VON RESSOURCEN, ÜBER DIE MAN KEINE WIRKLICHE KONTROLLE HAT: NETZWERKE FUNKTIONIEREN NUR DANN, WENN STROM FLIEßT, DER INTERNETZUGANG FUNKTIONIERT ...

- Es ist wichtiger zuverlässige als billige Provider für Strom, Internet, ... zu haben.
- Strategien zur Überbrückung von Ausfallzeiten
- Haftung klären

Kleine Ursache – große Wirkung:

das gilt im Positiven wie im Negativen!