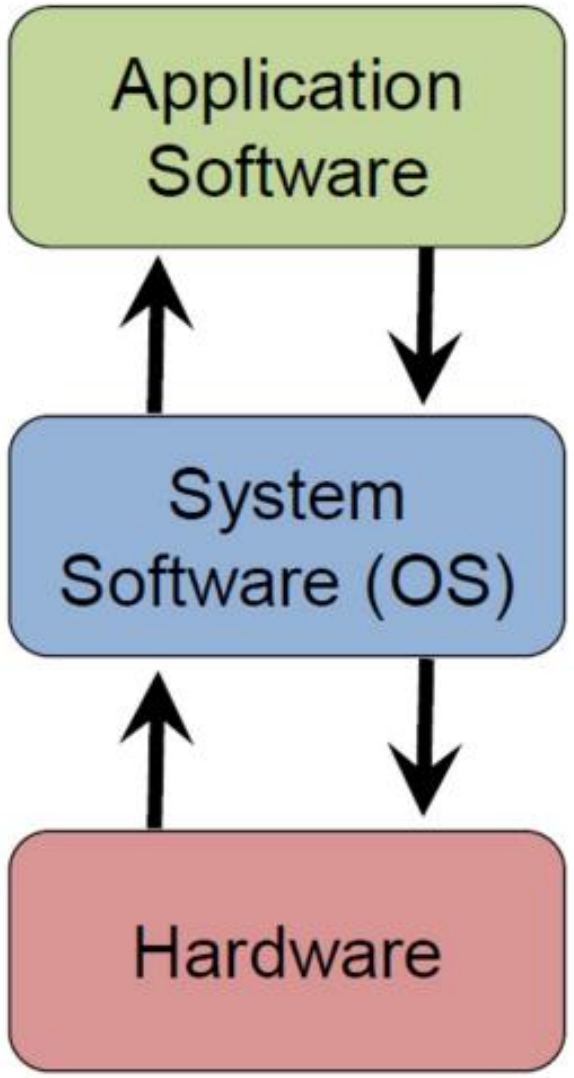
Intro til operativsystemer og sikkerhet

Shahi Ftah

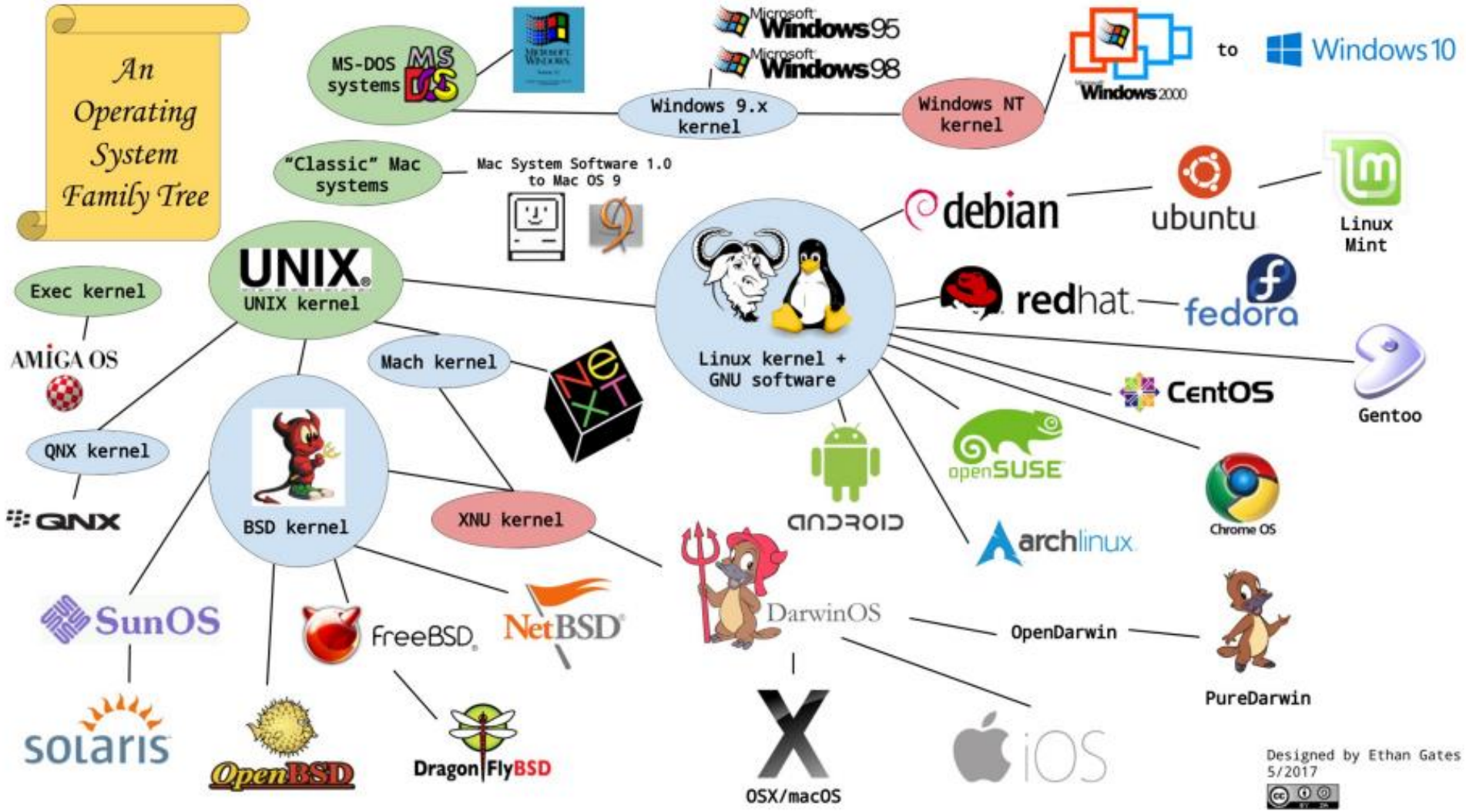
shahiaf@uio.no

Hvordan fungerer en datamaskin?

- Trenger programvare får å kjøre noe
- Operativsystem – dirigent i datamaskinen
- Mellomnivå – programvare og maskinvare



Dagens operativsystemer



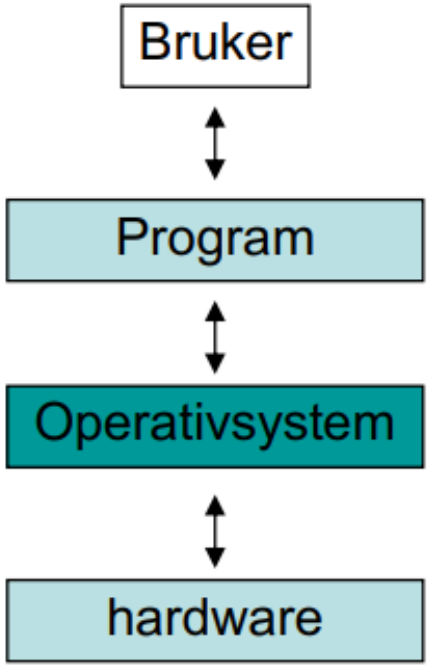
Hvordan fungerer de?

Hvem skal bestemme hvordan maskinen skal kjøre?

Mange ulike lag som «kommuniserer»

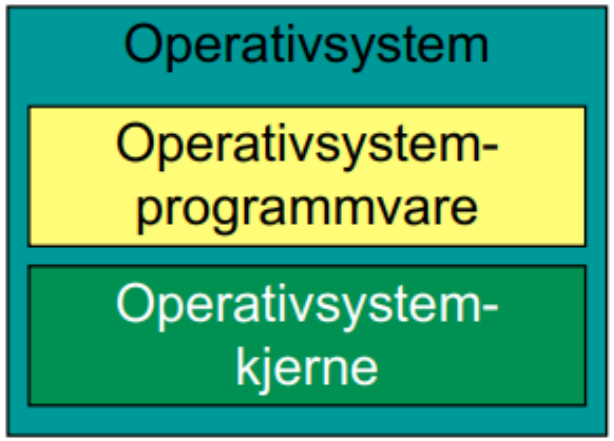
Menneske – Er en virtuell maskin, skjuler detaljer

Maskin – hver program har sin tid/plass



Kjerne – starte systemet, håndtere oppg, kommunisere med maskinvare, tildeling av CPU-tid til kjørende prosesser

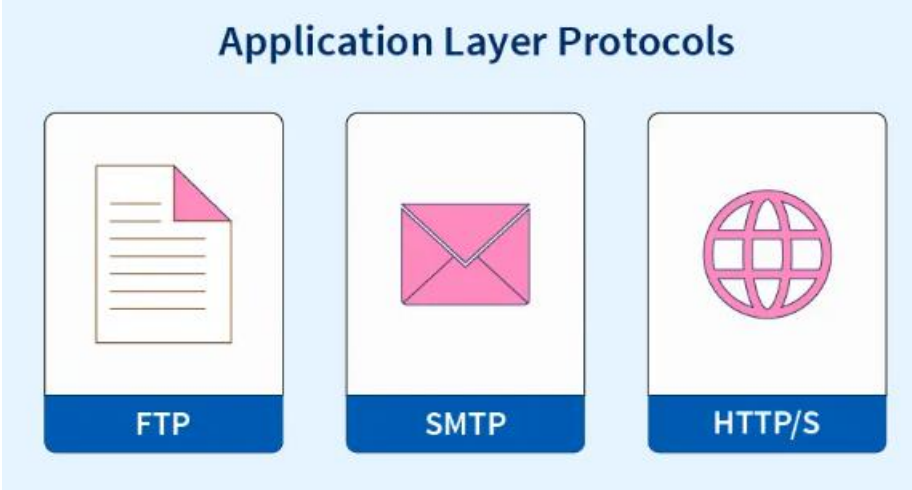
OS – Sett av programmer som gir tjenester på raskest mulig måte



Application layer

- Synlig for oss
- Mange prosesser kjører samtidig
- Flere samtlige brukere

- Sikkerhet
- Rettferdighet



Hvor finner vi et operativsystem?











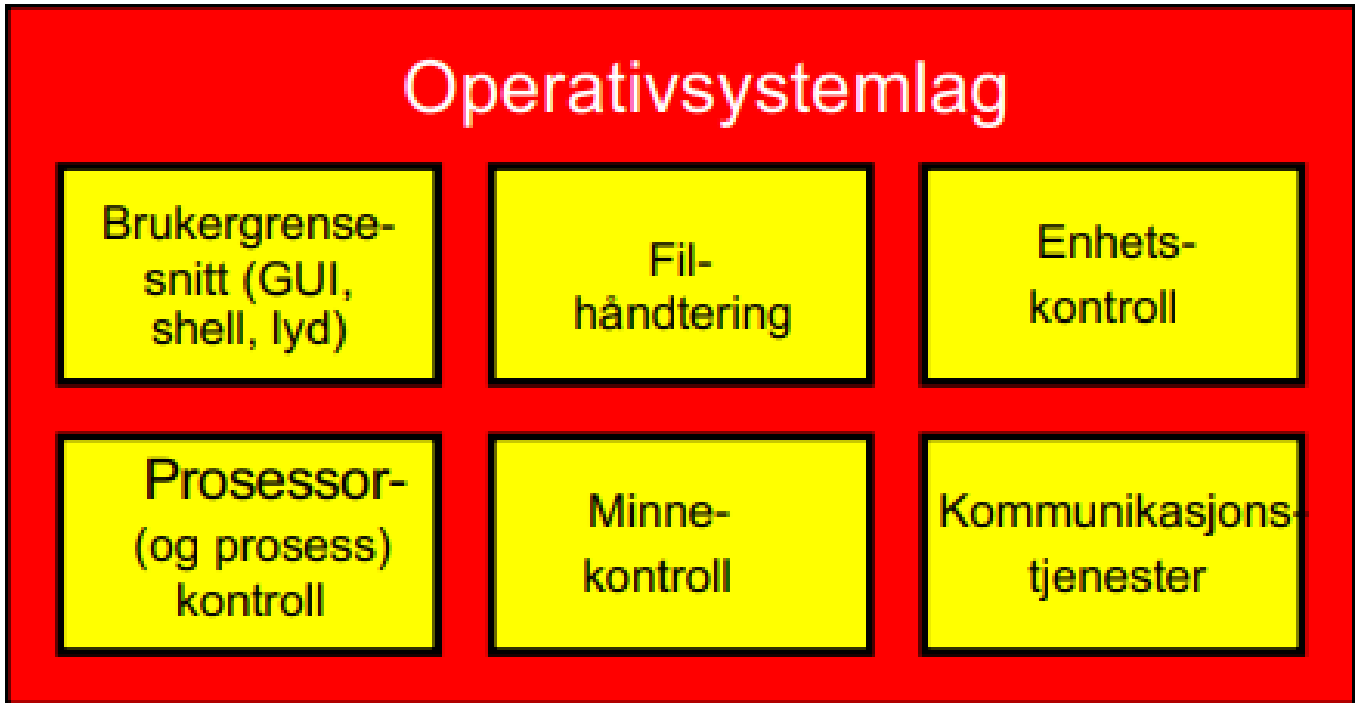


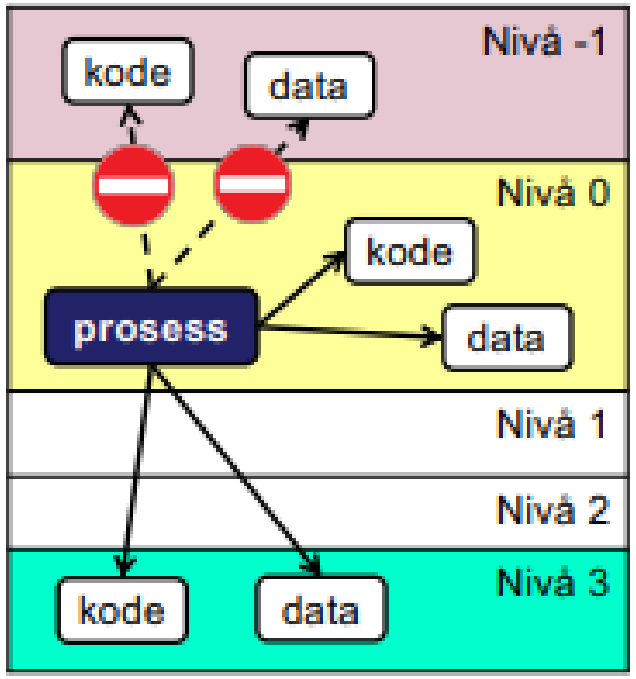


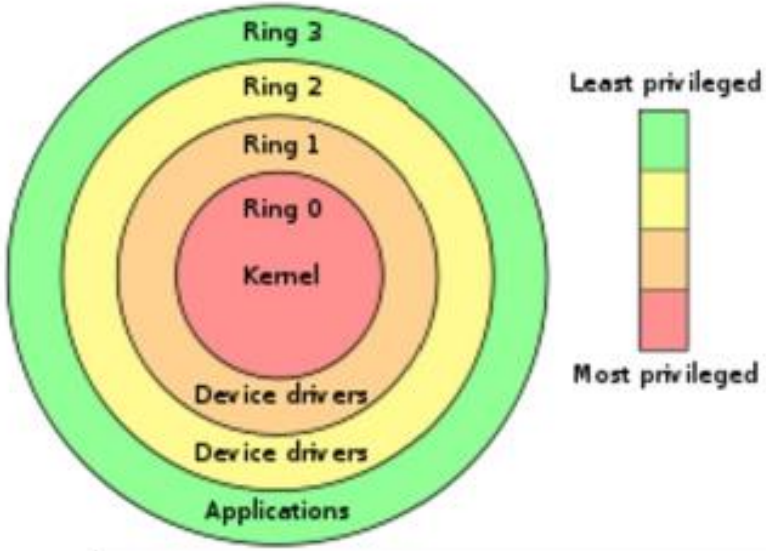


Hva ligger i et operativsystem

- Skiller mellom brukernivå og kjernenivå pga sikkerhet og beskyttelse
- Operativsystemet kjører i kjernemodus
- Brukernivå – protected mode





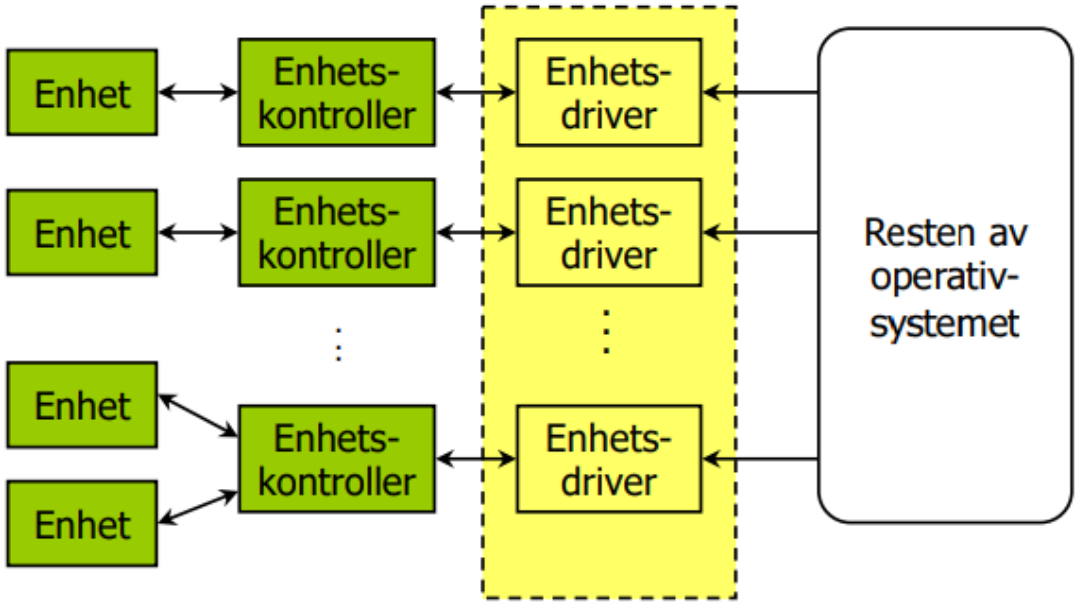


Brukernivå og kjernenivå

- - Buffer Overflow
- - Minnet overskrives og blir korrupt

Enhetskontroll

- Synlig for bruker
- Kontrollerer enheter tilkoblet til maskinen, alt som er koblet til systemet: tastatur, minne, skjermer osv
- Oversette instruere kommunikasjonen mellom inn- og utgangsenheten, ved å oversette 1/0 instruksjoner
- Stor forskjell på hastighet

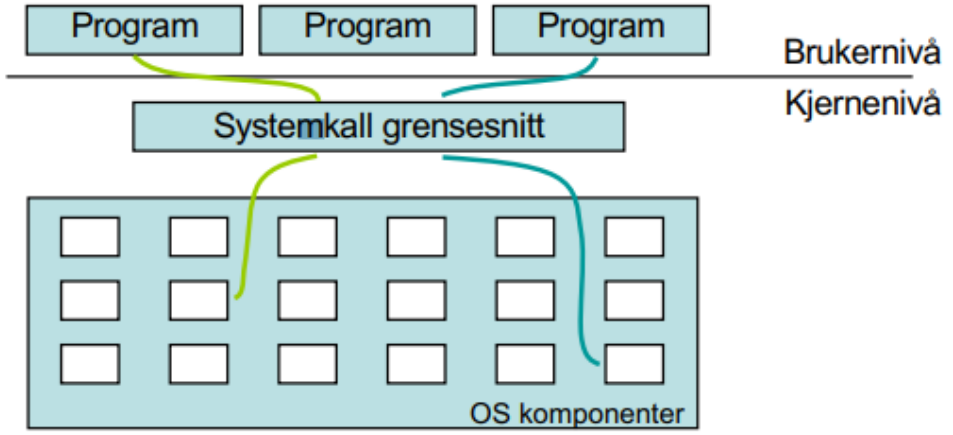


Brukergrensesnitt og systemkall

- Koblingen mellom bruker og datamaskin
- Det som er synlig/tilgjengelig på pc
- GUI



- Mellom operativsystem og bruker
- Henter og utfører en kall som vi har bedt om.



Sikkerhet

Mange grener fra sikkerhet:

- Datasikkerhet
- Cybersikkerhet
- Nettverkssikkerhet
- Informasjonssikkerhet

I praksis betyr alle det samme, men deres popularitet har endret seg

Beskytte verdier mot skadelig hendelser





Sikkerhetsmål

En egenskap man kan ønske å oppnå eller tilby

Noe man retter frem mot å ha oppnådd

Definisjon:

Beskyttelse av informasjonens Konfidensialitet, Integritet og Tilgjengelighet.

I tillegg kan andre egenskaper, f.eks. autentisitet, sporbarhet, ubenektelighet, personvern og pålitelighet omfattes. (ISO/IEC 27000:2018

Sikkerhetsmål

- K- Informasjonen ikke tilgjengeliggjøres for annet en de som er autorisert for tilgang
- I- Stole på at data ikke er slettet eller endret uautorisert
- T- Info er tilgjengelig til enhver tid for den som har tilgang

- Autentisitet – Du er personen som du utgir for å være
- Sporbarhet – Hvem har utført handlingene?
- Uavviselighet – Bekrefte at data er sendt og mottatt
- Personvern – Sikre dine data og dine rettigheter til bruk

Autentisitet

- Autentisitet bekrefter identitet:
- Brukerautentisering
- Organisasjonsautentisering
- Systemautentisering
- Dataautentisering

- Men hvordan kan vi stole på at brukeren er autentisk?
- Autentiseringsfaktor – Noe du vet, noe du har, noe du er
- Flerfaktor-autentisering



Sikkerhetstiltak

- Gjøre noe for å oppnå sikkerhetsmålene
- Deles i 3 grupper:

Organisatoriske tiltak
- ISMS/Styring/Ledelse
- Policyer/Standarder
- Hendelseshåndtering
- Personellsikkerhet
- Sikkerhetskultur
- Øvelser
- etc.

Fysiske tiltak
- Kameraovervåking
- Adgangskontroll
- Skjerming av kabler
- Vektere
- Låser
- Alarmer
- etc.

Teknologiske tiltak
- Brukerautentisering
- Tilgangskontroll
- Systemsikkerhet
- Nettverkssikkerhet
- Sikkerhetskopiering
- Kryptering
- etc.

Sikkerhetsmål:

Konfidensialitet – Integritet – Tilgjengelighet

støtter

Sikkerhetstiltak:

f.eks. låser – kryptering – autentisering - sikkerhetskultur

Verdier og Trusler

- *Hva er en verdi?*
- Informasjonsressurser. Målet er å beskytte verdienes KIT
- *Trussel:* Ønsker å oppnå verdiene, som potensielt kan skade f.eks. organisasjonens verdier.
- *Sårbarheten:* manglende sikkerhetstiltak og evne til å håndtere

- Hvem er trusselen?
- Hvis jeg har tilgang til en ressurs, er jeg da autorisert til ressursen?

Sikkerhetsmål

Sikkerhetsmål er et sentralt begrep innen informasjonssikkerhet. Hvilke av følgende defineres som sikkerhetsmål:

Velg ett eller flere alternativer

 Integritet

Autorisering

 Uavviselighet

Brannmur

 Tilgjengelighet

Orm

Tilgangskontroll

Tofaktor-autentisering

Trusselmodellering

Hvorfor kan bruk av USB minnepinner utgjøre en *sikkerhetstrussel* mot sikkerhetsmå konfidensialitet?

Velg ett eller flere alternativer

- [ ] De kan utilsiktet bli kryptert av for eksempel løsepengevirus.
- [ ] De kan bringe med seg skadevare som omgår andre sikkerhetsmekanismer.
- [ ] De kan bruke for mye strøm og på den måten påvirke en datamaskin negativt.
- [ ] De kan stjeles.