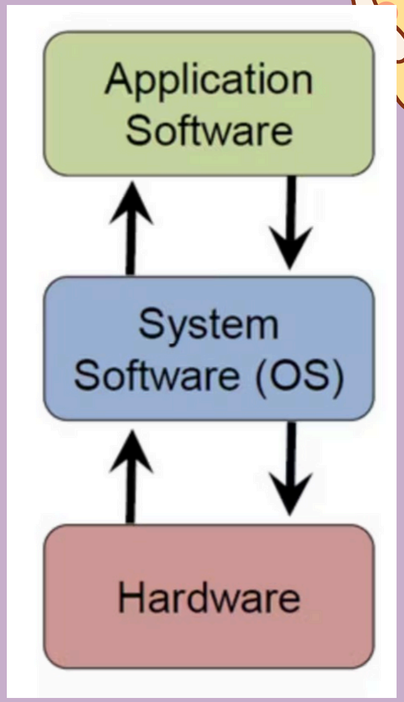
INI020
OS & SIKKERHET

AV ELISE
OG MATHEA

HVA ER ET OS?

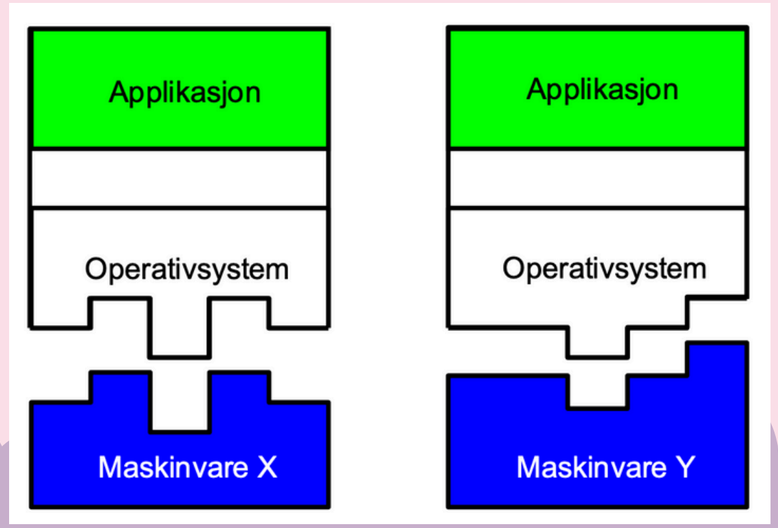
- Dirigenten i maskinen
- Sørger for at flere personer kan bruke datamaskinen
- Sørger for at flere prosesser kan kjøre samtidig
- Fungerer fom et mellom nivå mellom maskinvare og programmet



HVOR FINNER VI OPERATIVSYSTEMER?

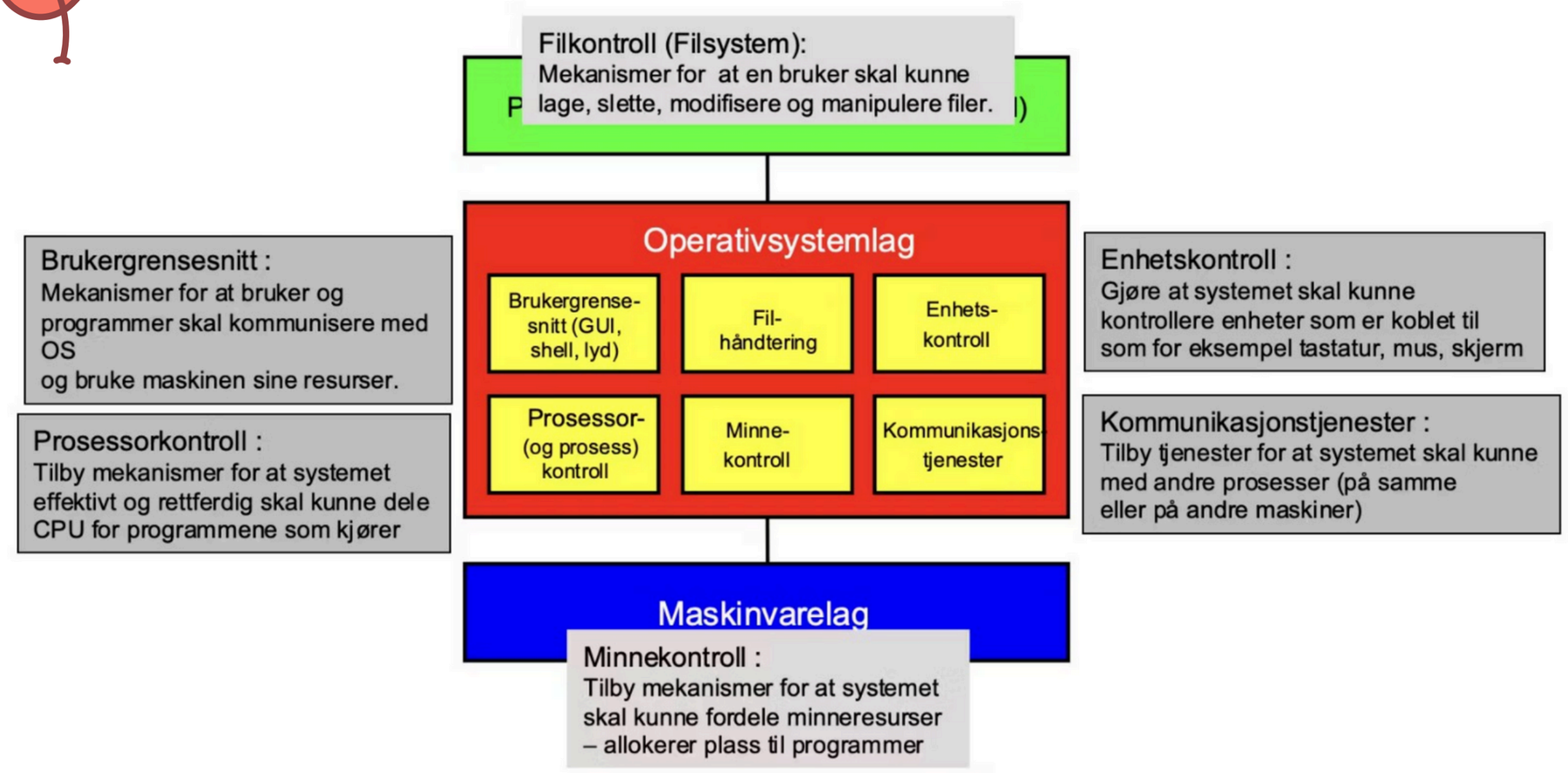


- Overalt
  - Linux, Mac, Windows
- Trenger ikke være stort, mange systemer kan inneholde OS som bare styrer en spesifikk funksjon
  - Vaskemaskiner, Tesla, IoT
- Hva skjer hvis operativsystemet i en vaskemaskin eller en bil blir hacket?
- Er det mindre viktig enn et PC-angrep, eller kan konsekvensene være vel så store?








Filkontroll (Filsystem):
Mekanismer for at en bruker skal kunne lage, slette, modifisere og manipulere filer.
Operativsystemlag
Brukergrense-snitt (GUI, shell, lyd)
Fil-håndtering
Enhets-kontroll
Prosessor- (og prosess) kontroll
Minne-kontroll
Kommunikasjons-tjenester
Maskinvarelag
Brukergrensesnitt :
Mekanismer for at bruker og programmer skal kommunisere med OS
og bruke maskinen sine resurser.
Prosessorkontroll :
Tilby mekanismer for at systemet effektivt og rettferdig skal kunne dele CPU for programmene som kjører
Enhetskontroll :
Gjøre at systemet skal kunne kontrollere enheter som er koblet til som for eksempel tastatur, mus, skjerm
Kommunikasjonstjenester :
Tilby tjenester for at systemet skal kunne med andre prosesser (på samme eller på andre maskiner)
Minnekontroll :
Tilby mekanismer for at systemet skal kunne fordele minneresurser – allokerer plass til programmer

DATASIKKERHET



HACKERE ER UTE ETTER:

HVA:

- Tilgang til informasjon
- Endre forfalske informasjon
- Utilgjengeliggjøre informasjon.

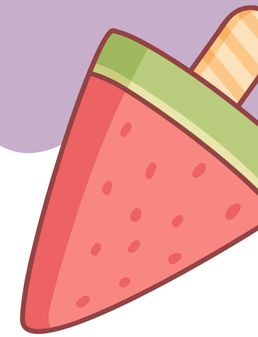
HVORDAN:

- ID-tyveri
- Utnytte sårbarheter i årogramvare
- Få noen til å gi deg hva du vil ha



SIKKER DATALAGRING





Data lagres på mange medier: laptop-disk, servere, skytjenester, USB.

- **Risiko:** Manglende tilgangskontroll, stjålne/miste enheter, datainnbrudd
- Sikkerhetsmålene:
  - Konfidensialitet, integritet og tilgjengelighet må ivaretas

Tiltak:

- Kryptering av filer, databaser og disker
- Tilgangskontroll
- Regelmessig backup
- Sikker sletting





ULIKE TYPER ANGREP

	Virus	Kjennetegnes ved at det sprer seg hver gang en fil med virus blir åpnet av bruker eller systemet.
	Dataorm	Skadevare som på egenhånd er i stand til å spre seg og finne nye ofre.
	Trojaner	Skadevare som utgir seg for å være et nyttig program.
	Bakdør	En ubeskyttet og ukjent åpning inn i et datasystem, laget av en angriper.
	Spionvare	Programvare for å spionere på en bruker i håp om å få tak i f.eks. informasjon, passord, kontoinformasjon.
	Tastelogger (Keylogger)	En enhet eller programvare som er koblet til tastatur eller maskin og som lagrer eller videresender alle tastetrykk. En variant av spionvare.
	Rootkit	Skadevare som endrer eller erstatter funksjoner i OS eller applikasjoner, med mål å ta kontroll over en maskin eller et system.
	Exploit	Et program, en sekvens med data, eller en oppskrift på hvordan en sårbarhet kan utnyttes.

TJENESTENEKTANGREP

Gjør en tjeneste utilgjengelig for brukere

DoS-angrep (Denial of Service)

- En angripende maskin
- Angriperen overstrømmer systemet med trafikk eller forespørsler
- Resultat: Tjenesten krasjer eller blir treg

DDoS-angrep (Destributed Denial of Service)

- Samme prinsipp som DoS mend med mange maskiner samtidig
- Botnet brukes ofte

Redundante systemer og bannmurer kan hjelpe!



SIKKERHET I OPERATIVSYSTEMET OG APPLIKASJONSIKKERHET

SQL-injeksjon

Spørrespråk som brukes til å hente ut eller manipulere data i relasjonsdatabaser.
Angriperen injiserer skadelig SQL-kode, f.eks. i et felt for brukerinput på en nettside.

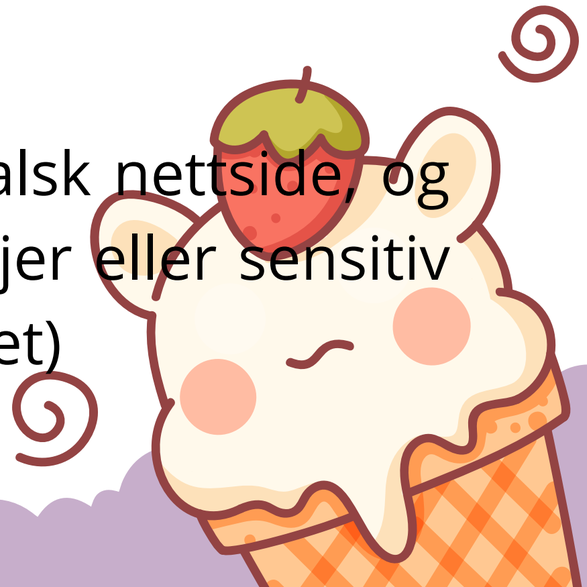
= Kan gi hackeren uautorisert tilgang til data i databasen.

Tiltak?

XXS - Cross-Site Scripting

Angriper injiserer skadelig kode (ofte JavaScript) på et nettsted.
Når et offer besøker siden vil risikoen være at den skaldelige koden kjøres. **- Drive-by-angrep.**

= brukeren blir overført til falsk nettside, og stjeler f.eks innlogningsdetaljer eller sensitiv informasjon (uten å merke det)



Tiltak?

SOSIAL MANIPULASJON

Hva? Psykologisk virkemiddel for å utføre dataangrep og svindel mot brukere av IT-systemer. Utnytter mennesker for svindel forsøk

Hvordan?

- **Spoofing:** Falske avsendere f.eks. e-post eller SMS
- **Phishing:** "Fisker etter opplysninger". Lurer mottakere til å oppgi informasjon de er ute etter.
  - **Masse-phising:** bredt utsendt e-poster
  - **Spear-phising:** Målrettet angrep
  - **Whaling:** Målrettet angrep mot personer med makt og myndigheter.





PHISHING QUIZ

https://phishingquiz.withgoogle.com/

EKSAMENSOPPGAVE

Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin		
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.		
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		
Operativsystemet sørger for at flere programmer kan kjøre samtidig.		
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.		
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.		
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.		

EKSAMENSOPPGAVE

Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin	✔	
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.		
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		
Operativsystemet sørger for at flere programmer kan kjøre samtidig.		
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.		
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.		
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.		

EKSAMENSOPPGAVE

Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin	✔	
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.	✔	
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		
Operativsystemet sørger for at flere programmer kan kjøre samtidig.		
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.		
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.		
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.		

EKSAMENSOPPGAVE

Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin	✔	
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.	✔	
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		✔
Operativsystemet sørger for at flere programmer kan kjøre samtidig.		
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.		
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.		
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.		

EKSAMENSOPPGAVE

Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin	✔	
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.	✔	
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		✔
Operativsystemet sørger for at flere programmer kan kjøre samtidig.	✔	
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.		
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.		
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.		

EKSAMENSOPPGAVE

Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin	✔	
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.	✔	
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		✔
Operativsystemet sørger for at flere programmer kan kjøre samtidig.	✔	
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.	✔	
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.		
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.		

EKSAMENSOPPGAVE

Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin	✔	
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.	✔	
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		✔
Operativsystemet sørger for at flere programmer kan kjøre samtidig.	✔	
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.	✔	
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.	✔	
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		✔
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.		

EKSAMENSOPPGAVE

Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin	✔	
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.	✔	
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		✔
Operativsystemet sørger for at flere programmer kan kjøre samtidig.	✔	
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.	✔	
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.	✔	
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		✔
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.		✔

3.3 Begrepsforståelse

Plasser begrepene under sammen med riktig tekst. Merk: Halvparten av begrepene vil være til overs.

Hjelp

Nulldagssårbarhet	Hash-algoritme	Verdier
Trusselmodellering	Dataorm	Asymmetrisk kryptering
PKI	Leveransekjedeangrep	Risiko
Personopplysninger	Trojaner	Digitale sertifikater

[ ] er en svakhet som ikke er kjent for leverandør av en tjeneste.

[ ] brukes for å sjekke dataintegritet.

[ ] brukes for å sikre ektheten av offentlige nøkler, samt trygg nøkkeldistribusjon.

[ ] har både en nyttig og en skadelig funksjon.

[ ] har lovpålagte krav om konfidensialitet, integritet og/eller tilgjengelighet.

[ ] er en kombinasjon av sannsynlighet for en hendelse og konsekvens av hendelsen.

3.3 Begrepsforståelse

Plasser begrepene under sammen med riktig tekst. Merk: Halvparten av begrepene vil være til overs.

Hjelp

Personopplysninger	Nulldagssårbarhet	Risiko
Digitale sertifikater	Trojaner	Asymmetrisk kryptering
Dataorm	Verdier	Leveransekjedeangrep
Trusselmodellering	Hash-algoritme	PKI

Nulldagssårbarhet ✔ er en svakhet som ikke er kjent for leverandør av en tjeneste.

Hash-algoritme ✔ brukes for å sjekke dataintegritet.

PKI ✔ brukes for å sikre ektheten av offentlige nøkler, samt trygg nøkkel-distribusjon.

Trojaner ✔ har både en nyttig og en skadelig funksjon.

Personopplysninger ✔ har lovpålagte krav om konfidensialitet, integritet og/eller tilgjengelighet.

Risiko ✔ er en kombinasjon av sannsynlighet for en hendelse og konsekvens av hendelsen.

JOBB MED UKESOPPGAVER

SES NESTE GRUPPETIME!