

UiO : Institutt for informatikk

Trygg infrastruktur og sikre datasystemer

IN1020 – Introduksjon til datateknologi
18.09.2026

Kristin Skar
kritisk@ifi.uio.no

Datateknologi og sikkerhet

Tema for tema:

1. Datasikkerhet - Er det så viktig da? (19. aug)
2. Å innfri sikkerhetsmål: Autorisert og uautorisert tilgang (21. aug)
3. Hvordan hackes vi? Trusselaktører og angrepsvektorer (26. aug)
4. Kryptografi – nøkkelen til (fungerende) digital samhandling (9.sept)
5. **Trygg infrastruktur og sikre datasystemer (18.sept)**
6. Å skape trygge digitale tjenester krever innsats (23.sept)

I dag: Trygg infrastruktur og sikre datasystemer

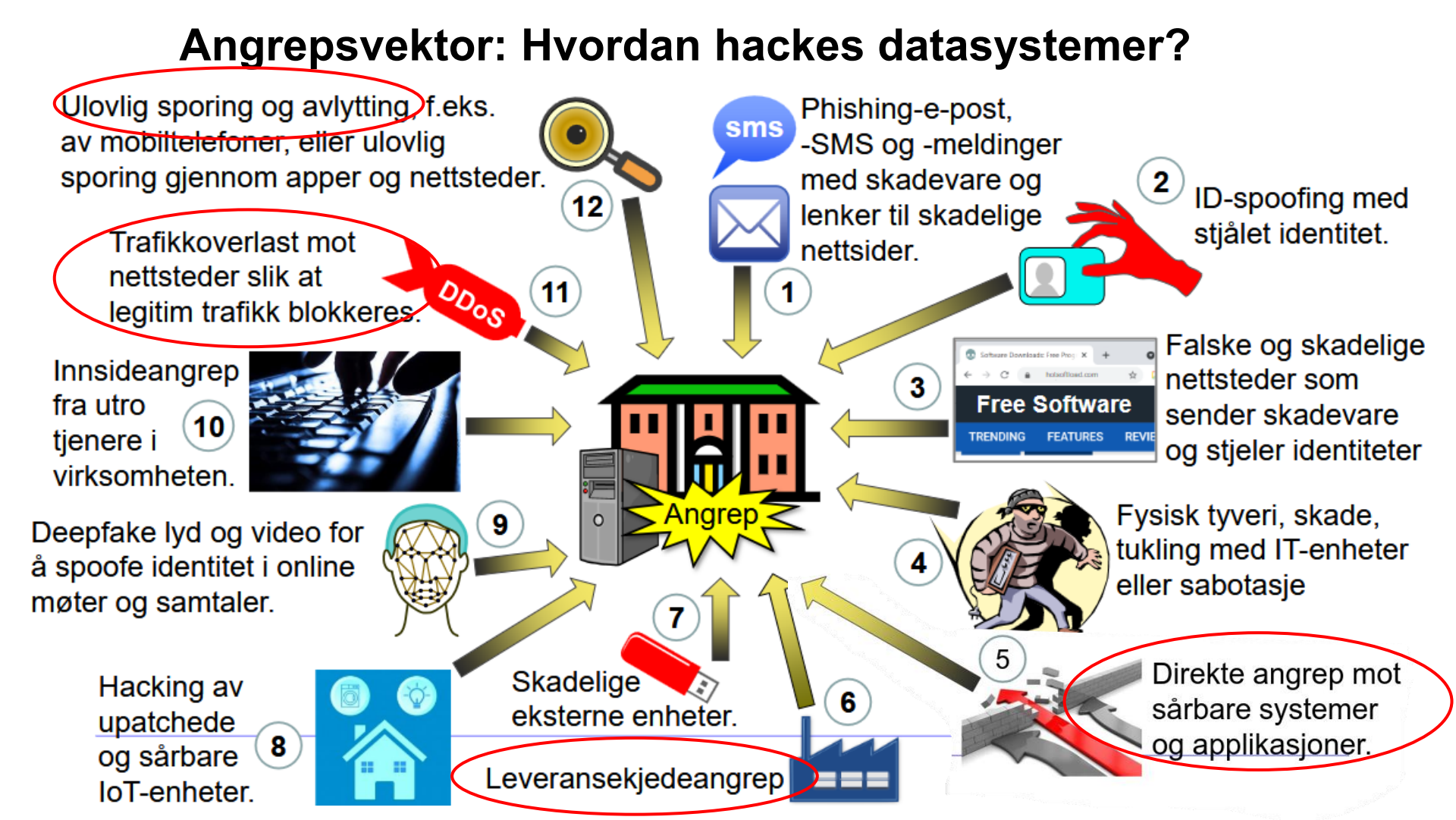
Ressurser:

- Forelesning 18.09.26
- Ukeoppgaver og pensumlitteratur
  - Jøsang: 3.1-3.5 (3.5 er kursorisk)
    6.2-6.5 (6.2.1 – 6.2.4 er kursorisk)
    11.8.1, 11.8.2, 11.9

Nøkkelord:

- Nettverkssikkerhet:
  - Kommunikasjonssikkerhet
  - Datanettsikkerhet
- Systemsikkerhet
  - Buffer-utnyttelser
- Digitale verdikjeder

Angrepsvektor: Hvordan hackes datasystemer?



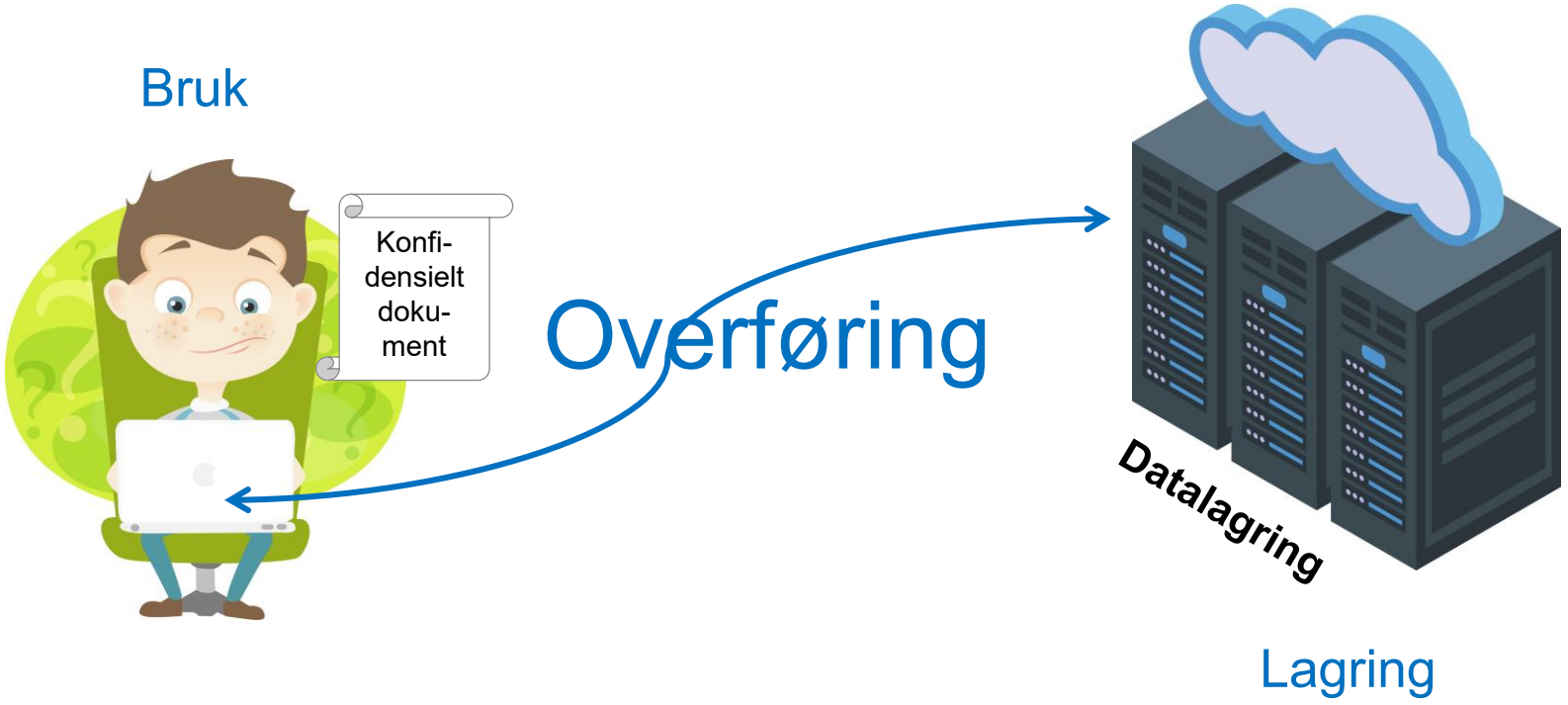


Nettverkssikkerhet

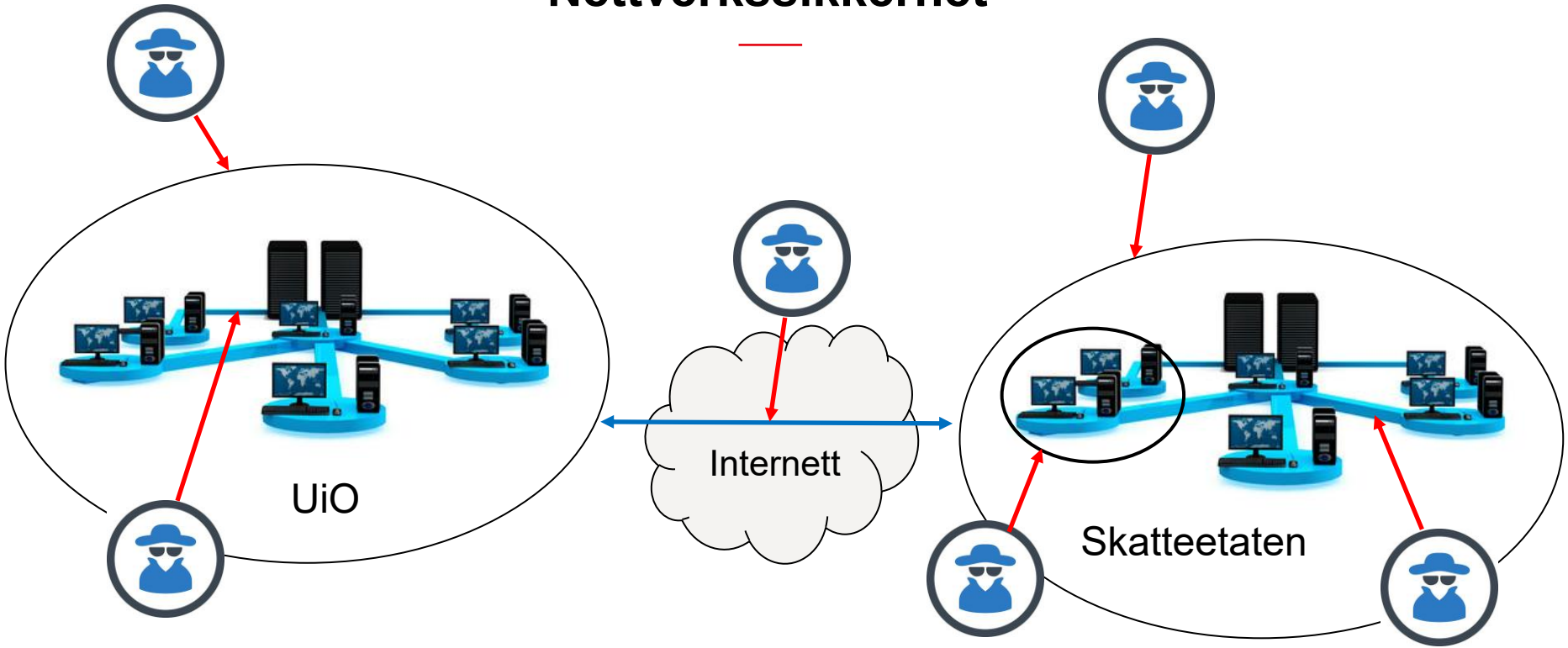


UiO : Institutt for informatikk

Informasjon må beskyttes i alle tilstander



Nettverkssikkerhet





Spørsmål

Hva er vanlige trusler mot nettverkstrafikk i:

1. Trådløse nett
2. Kablede nett

Kommunikasjonssikkerhet

Kommunikasjon i trådløse nett går via radiosignaler:

- «Hvem som helst» kan lytte til signalene.
- Signalforstyrrelser (tilsiktet eller utilsiktet) kan føre til utilgjengelighet.
- Falske aksesspunkter: En trådløs enhet vil koble seg til aksesspunktet med sterkest signal.
- Kompromitterte aksesspunkter, spesielt åpne nett/aksesspunkter.



Kommunikasjon i kablede nett går via fysiske kabler:

- Avlytting krever fysisk tilgang, men er likevel fullt mulig.
- Ødelagt kabel (tilsiktet eller utilsiktet) kan føre til utilgjengelighet.
- Kompromitterte nettverks-endepunkter (routere/switcher).
- Kompromitterte enheter på samme fysiske nettverk.



Hvordan beskytte informasjon under overføring?

Kryptering/sikkerhet i lagene:

- Sikre nettverksprotokoller. Eksempler:
  - Transport Layer Security (TLS) tilbyr kryptering for ende-til ende applikasjoner – f.eks. nettbank eller butikker. Har tatt over for Secure Sockets Layer (SSL).
  - IPSec – kryptografi på IP-pakker (internettlaget).
- VPN (basert på TLS eller IPSec) – kobler to subnett sammen så det fungerer som ett LAN selv om de er fysisk adskilt.
- WiFi Protected Access (WPA) - Kryptering på trådløse nettverk, krypterer forbindelsen mellom deg og aksesspunkt/ruter.

Oppgave #1 - Nettverkssikkerhet

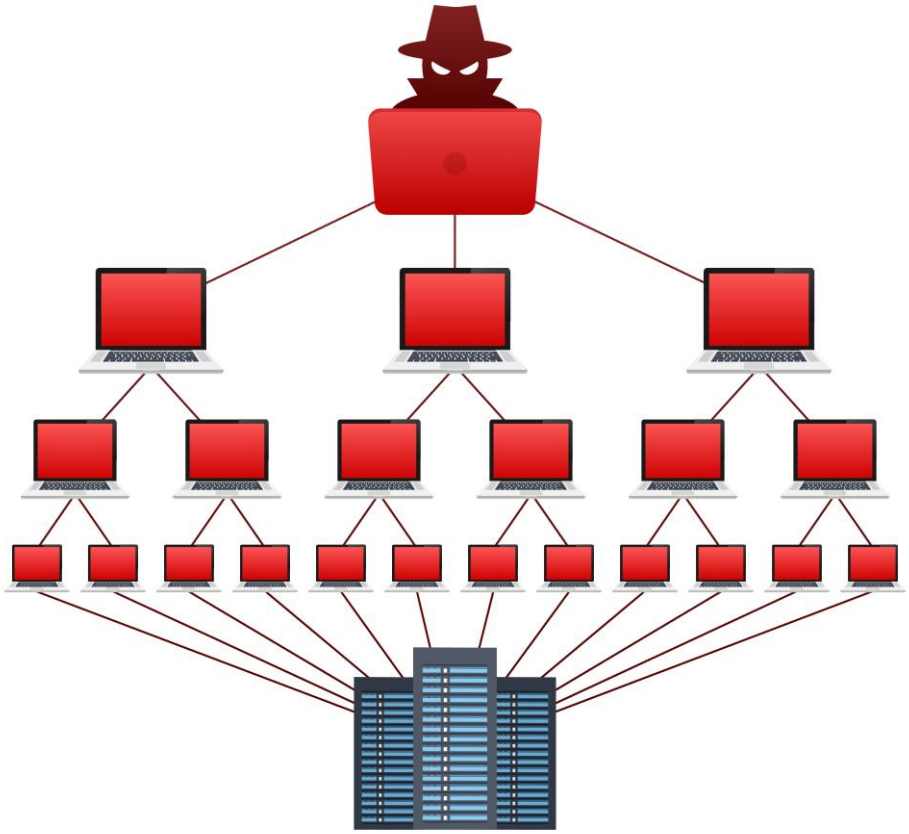
Under utvikling av et nytt nettsted for en organisasjon blir du rådspurt om det er mest fornuftig å benytte protokollen HTTP eler HTTPS for kommunikasjon over nettverk mellom bruker og virksomhetens nettsted.

Oppgave #1 - alternativer

Hvilke av følgende utsagn er sanne hvis man velger HTTP som protokoll:

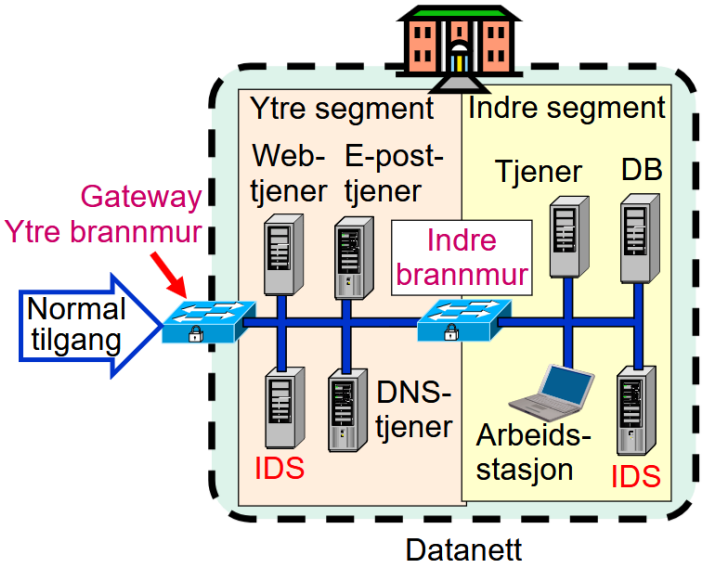
Velg ett eller flere alternativer

- ❑ Hvis en bruker benytter kryptert forbindelse mellom sin datamaskin og sin trådløse hjemme-ruter, hindres både avlytting og modifikasjon av datatrafikken mellom brukerens nettleser og organisasjonens webtjener.
- ❑ Uvedkommende kan være i stand til å avlytte og lese datatrafikk mellom organisasjonens webtjener og en brukers nettleser.
- ❑ Uvedkommende kan være i stand til å modifisere datatrafikk mellom organisasjonens webtjener og en brukers nettleser.
- ❑ Integritet for data sendt mellom organisasjonens webtjener og en brukers nettleser blir ivaretatt.



Hvordan beskytte et *datanett*?

Perimetersikkerhet:



- Brannmur:
  - Sjekkpunkt som slipper inn eller avvise trafikk inn i og/eller ut fra et nettverk basert på forhåndsdefinerte regelsett.
  - Brannmur fungerer som en *tilgangskontroll* for nettverket.
  - Kan være et dataprogram eller maskinvare laget for akkurat dette formålet.

- Inntrengningsdeteksjon (IDS)

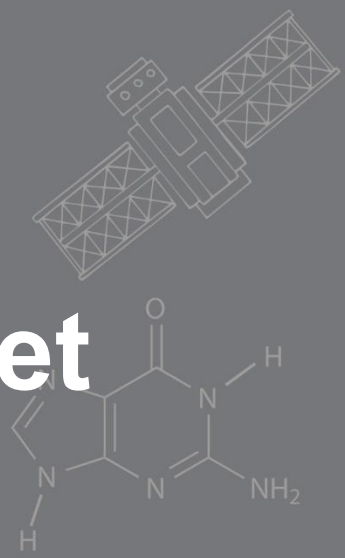
Overvåker nettverkstrafikk, og brukes bl.a. til å detektere:

- Mistenkelig trafikk: Både forsøk på og suksessfulle innbrudd.
- Datavirus og annen ondsinnet programvare.
- Tjenestenektangrep.

Utfordring?



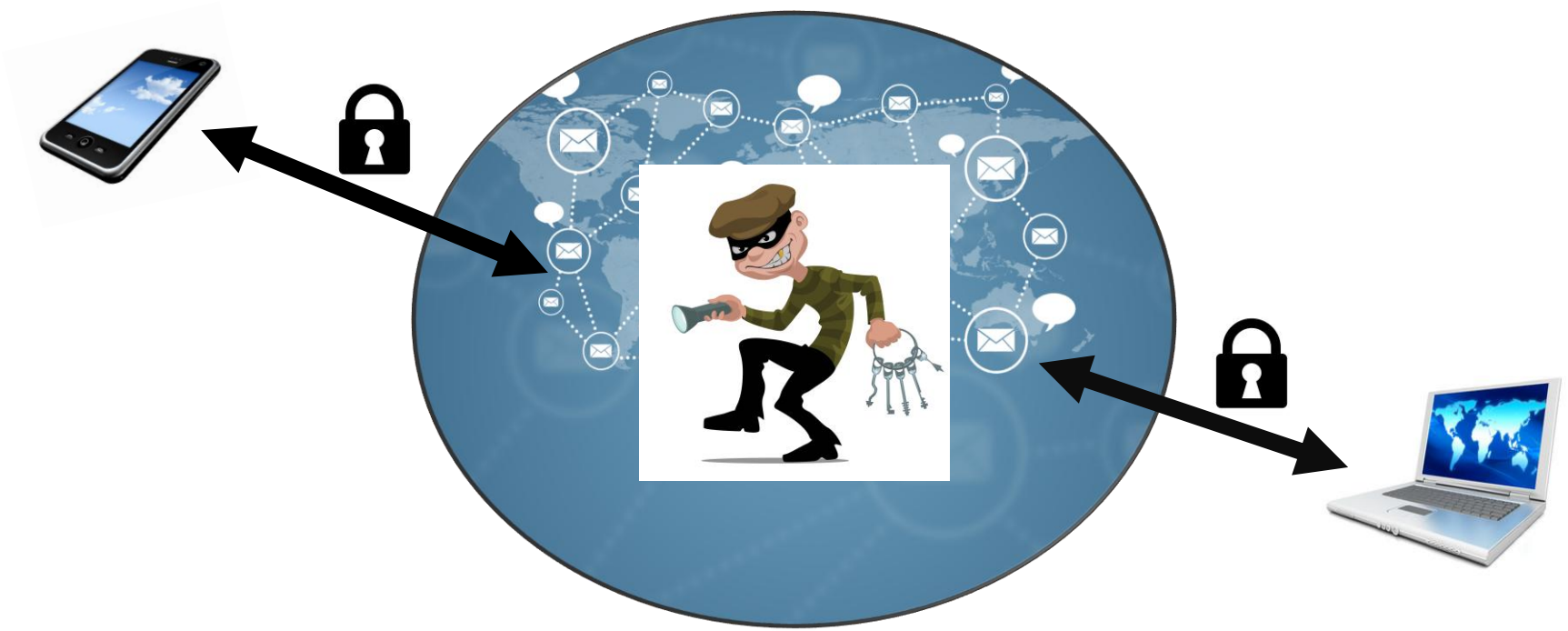
Systemsikkerhet





UiO : Institutt for informatikk

Tradisjonell sikkerhetsmodell:
Stoler på endesystemene, nettverket anses upålitelig.



Programvare:

Applikasjonsprogramvare:

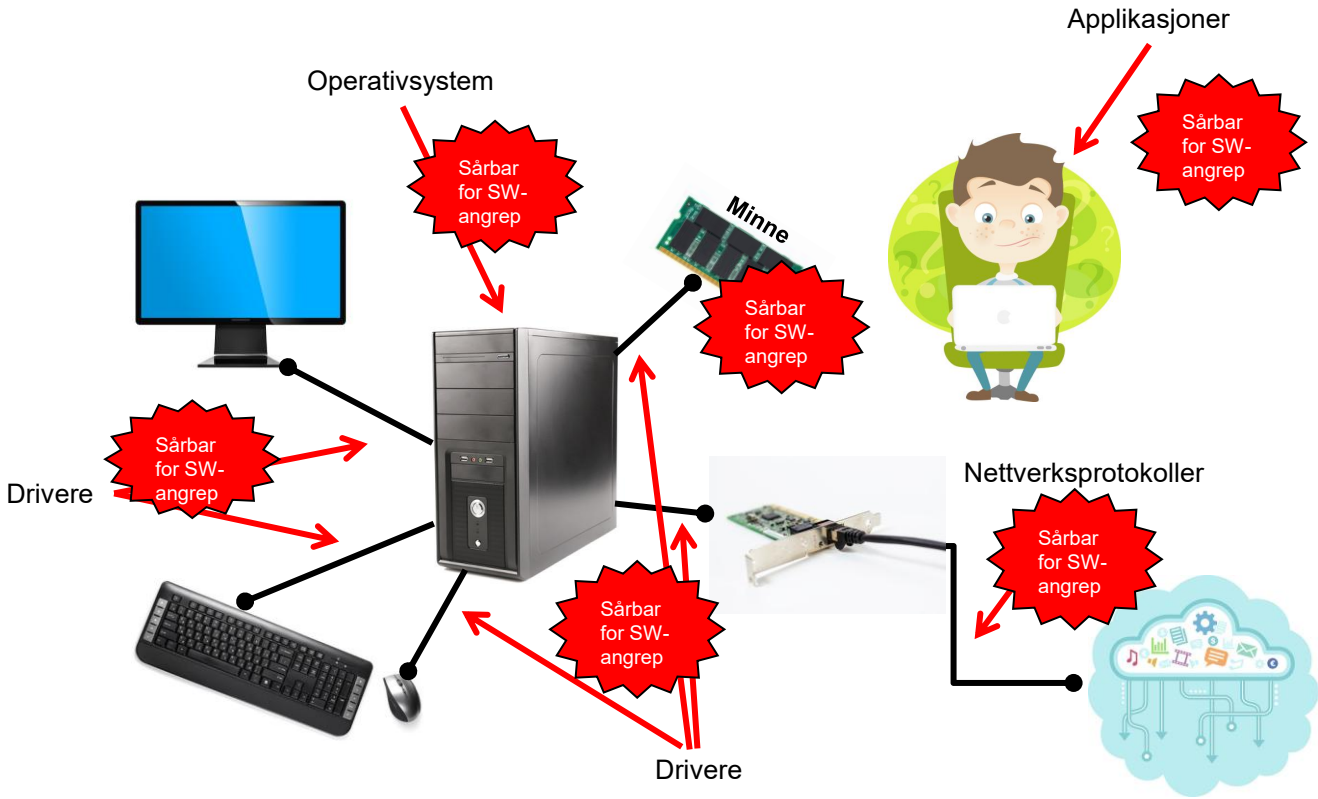


Applikasjonssikkerhet

Systemprogramvare:



Systemsikkerhet


Applikasjoner
Operativsystem
Sårbar for SW-angrep
Sårbar for SW-angrep
Minne
Sårbar for SW-angrep
Sårbar for SW-angrep
Drivere
Nettverksprotokoller
Sårbar for SW-angrep
Sårbar for SW-angrep
Drivere

Sikkerhet i operativsystemet

- OS styrer ulike brukeres tilgang til ressurser (prinsipp om *minste privilegium*)
- *Kjernen* i operativsystemet styrer alt.
- Kjernen kommuniserer med *periferenhetene* i datamaskinen gjennom *drivere*.
- Brukerprosesser kommuniserer via kjernen for å kunne benytte periferenhetene.
- Minnet i en datamaskin benyttes (bl.a.) til mellomlagring.

Sikkerhet i operativsystemet (forts)

1. Kjerne og drivere er dataprogrammer

- Kan inneholde sårbarheter

2. Kjernen kjører i *supervisor mode* og har tilgang til «alt»

- En sårbarhet i kjernen er kritisk

Ekstremt viktig å holde både operativsystem og drivere fri for sårbarheter:

- Sørge for trygg programvare
- Holde programvaren oppdatert vha. *sikkerhetoppdateringer*.

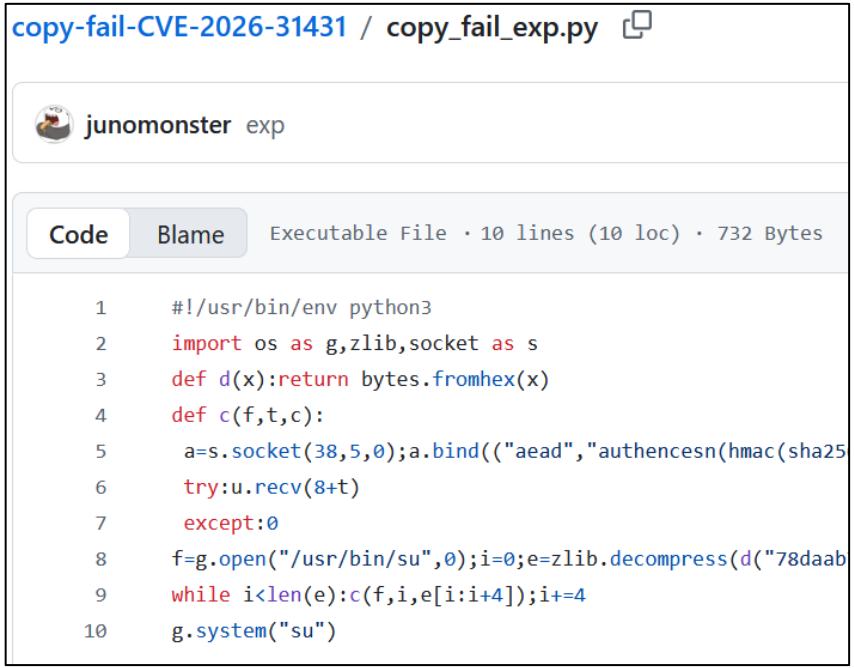
Eksempel: «Copy Fail»

Copy Fail: 732 Bytes to Root on Every Major Linux Distribution

*“Copy Fail (CVE-2026-31431) is a logic bug in the Linux kernel's **authencesn** cryptographic template. It lets an unprivileged local user trigger a deterministic, controlled 4-byte write into the page cache of any readable file on the system. A single 732-byte Python script can edit a setuid binary and obtain root on essentially all Linux distributions shipped since 2017.”*

https://copy.fail/

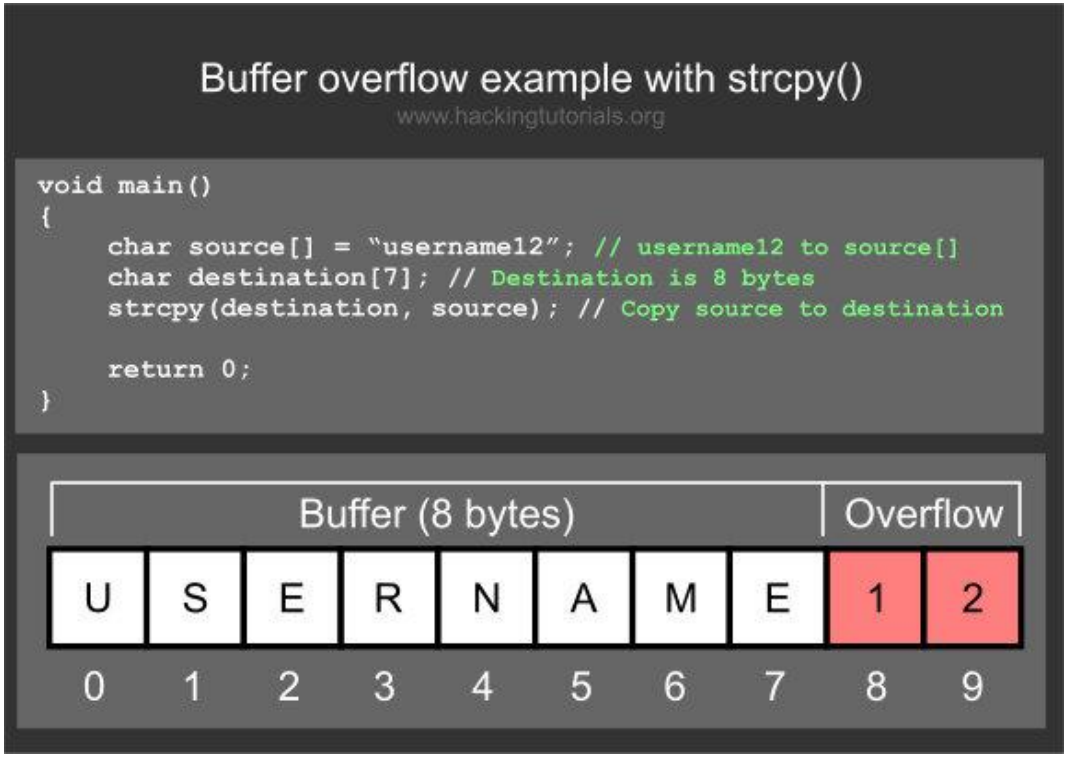
nsm.no: CVE-2026-31431



Utfordring: Kan minnet i en datamaskin «hackes»?



Et buffer er en sammenhengende seksjon i minnet i datamaskinen, avsatt til å inneholde data.

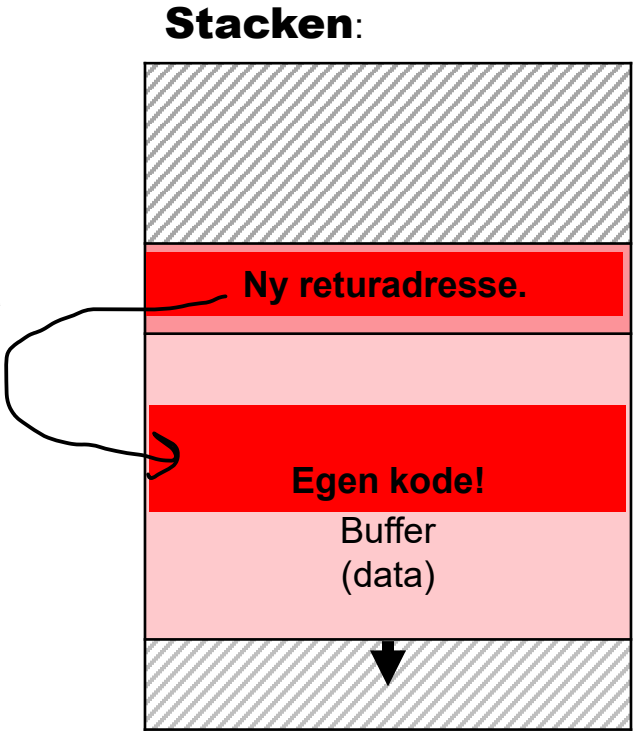


Kan dette brukes kreativt?

- JA – gjennom å kjøre slike sårbare programmer *kan* man skrive uhemmet til minnet i datamaskinen:
  1. Plassere egen programkode på steder i minnet hvor det ligger *kjørbar kode.*
  2. Endre en funksjons returadresse til å isteden peke til adressen i minnet der din kjørbare kode er plassert.

➢ For den interesserte (Computerphile):
https://www.youtube.com/watch?v=1S0aBV-Waeo

- Finnes det sikkerhetstiltak?

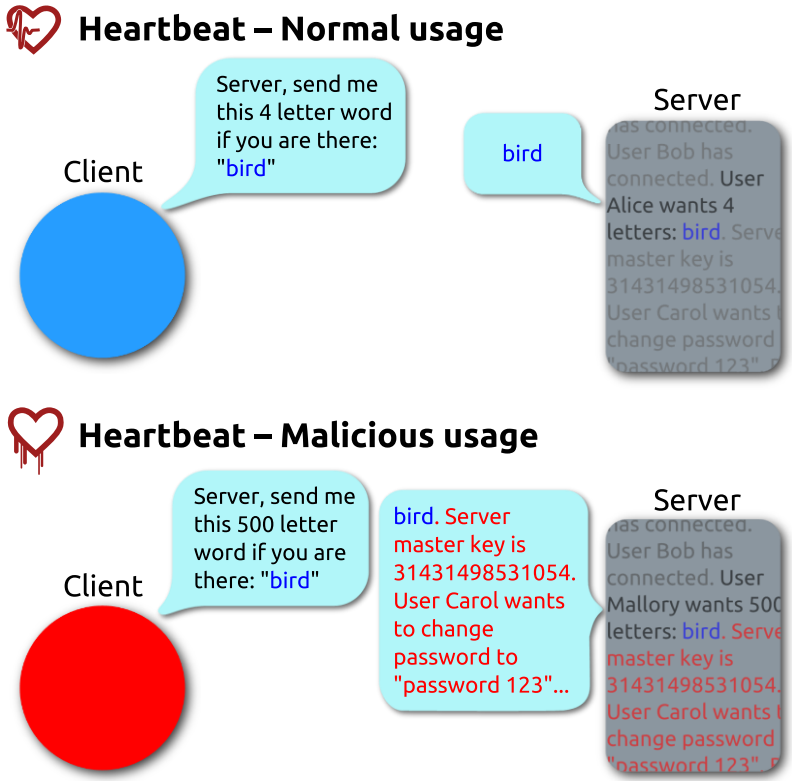


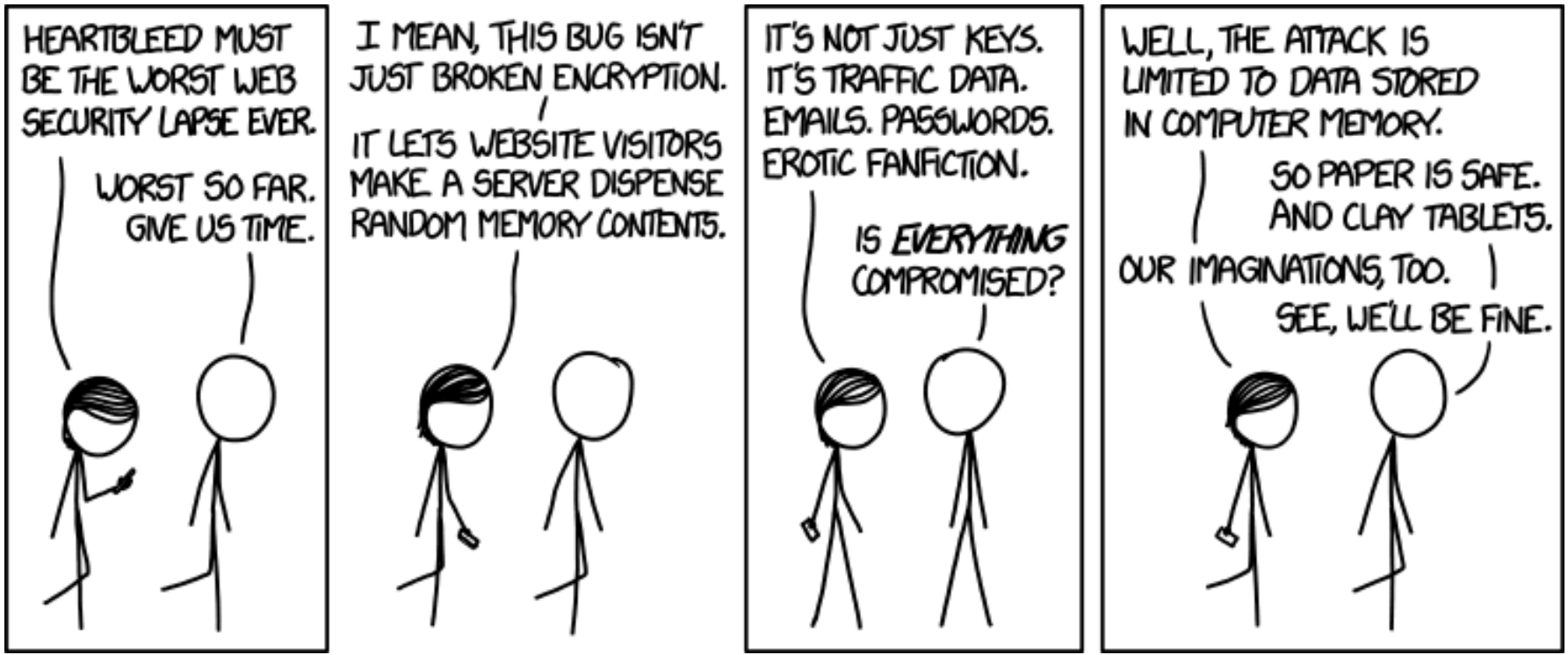
Eksempel: OpenSSL sårbarheter

OpenSSL er *åpen kildekode, og er et* bibliotek kodet i C som *implementerer* protokollen Transport Layer Security (TLS).

Brukes i millioner av applikasjoner, operativsystem, IoT-enehter og servere.

Men likevel: [Heartbleed]





https://xkcd.com/1353/

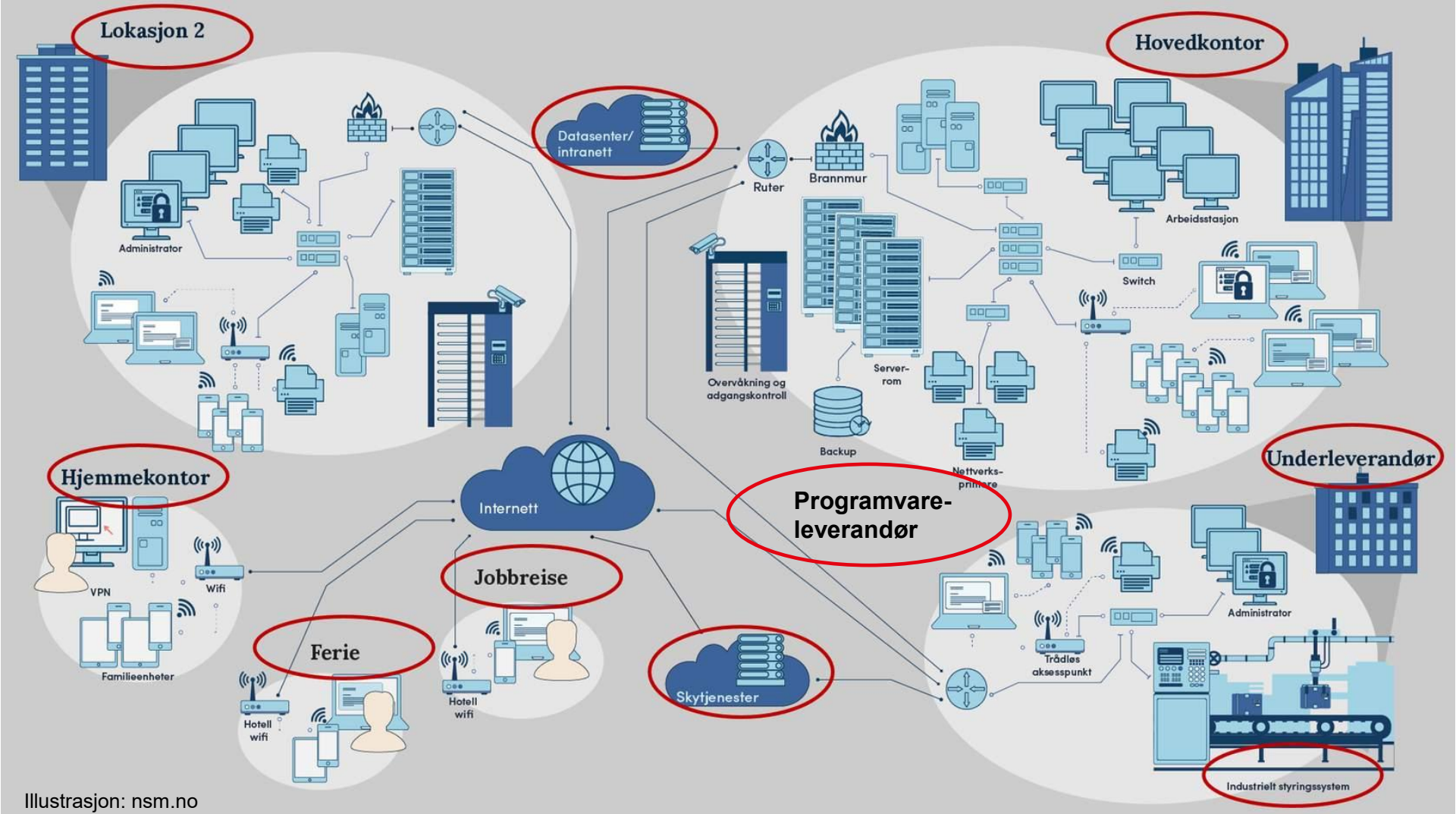


Digitale verdikjeder





UiO : Institutt for informatikk



Illustrasjon: nsm.no

Digitale verdikjeder

Digitale tjenester, funksjoner eller varer fra eksterne leverandører tas i bruk istedenfor å gjøre jobben selv – det oppstår en *digital verdikjede.*

- **Programvare**: En tredjepart utvikler og vedlikeholder *programvare* som ditt system bruker:
  - Programvare
  - Programvarebiblioteker
  - Slipper å finne opp hjulet på nytt hver gang
- **Tjenesteutsetting**: En tredjepartpart utvikler og vedlikeholder *IT-tjenester* som din virksomhet tar i bruk:
  - Enkel tilgang til et sett med IT-ressurser, lett tilgjengelig overalt: Applikasjoner, lagring, beregningstjenester, osv.
  - Rask anskaffelse og tilgjengelighet

Ruters egne tester viser:
Oslo-elbusser kan stoppes og slås av fra Kina.



- Ruter tok bussene fra hverandre og undersøkte dem i et rom der signaler ble isolert.

Der fant de ut at de kinesiske elbussene kan tas kontroll over av produsenten.

Ifølge Ruter har produsenten fjerntilgang til dette på hver enkelt buss:

- Programvareoppdatering
- Diagnostikk
- Styringssystem for batteri- og kraftforsyning

«I teorien kan bussen derfor stoppes eller gjøres ubrukelig av produsenten,» melder Ruter.



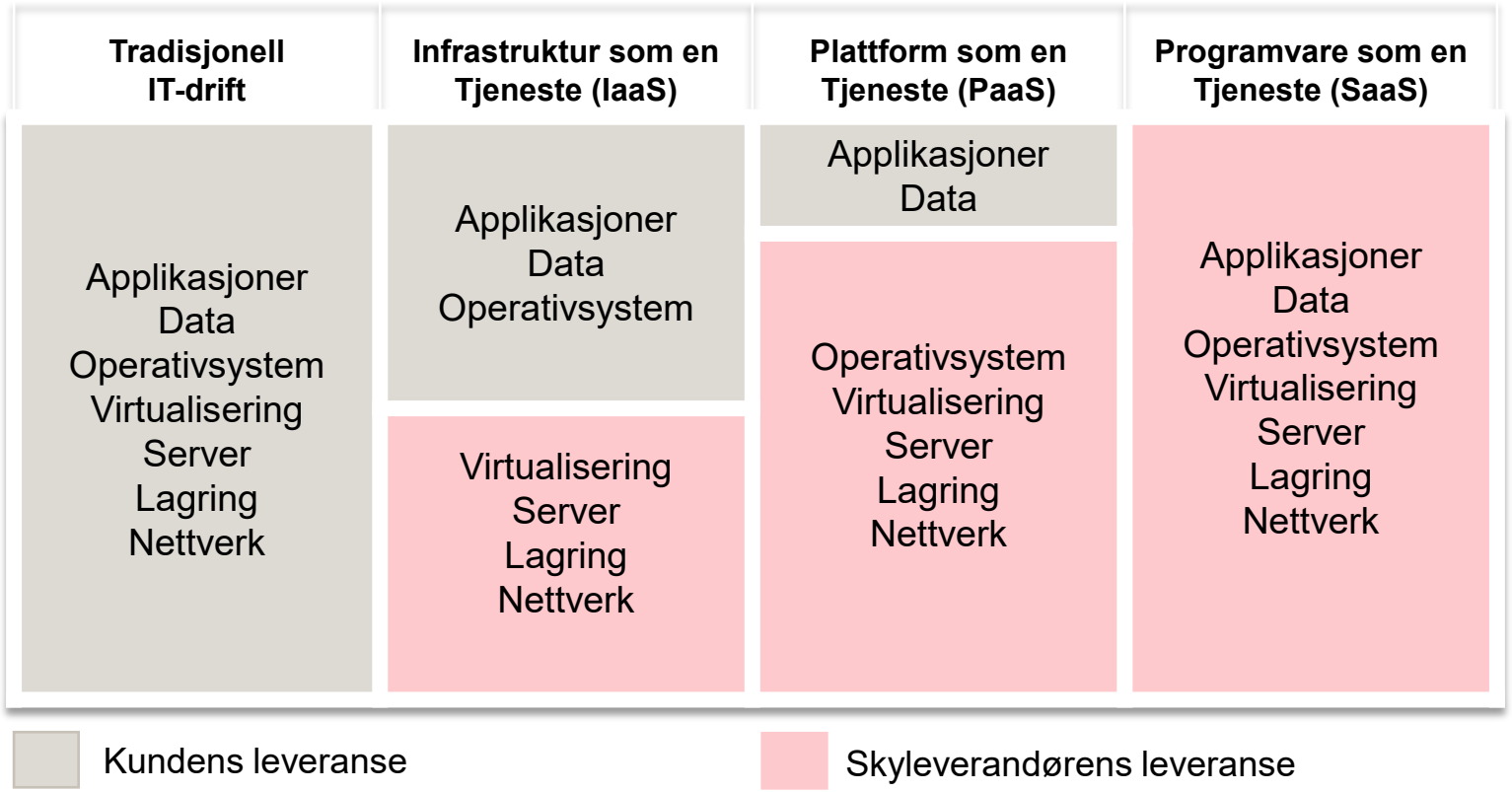
Crowdstrike juli 2024

SOLARWINDS®

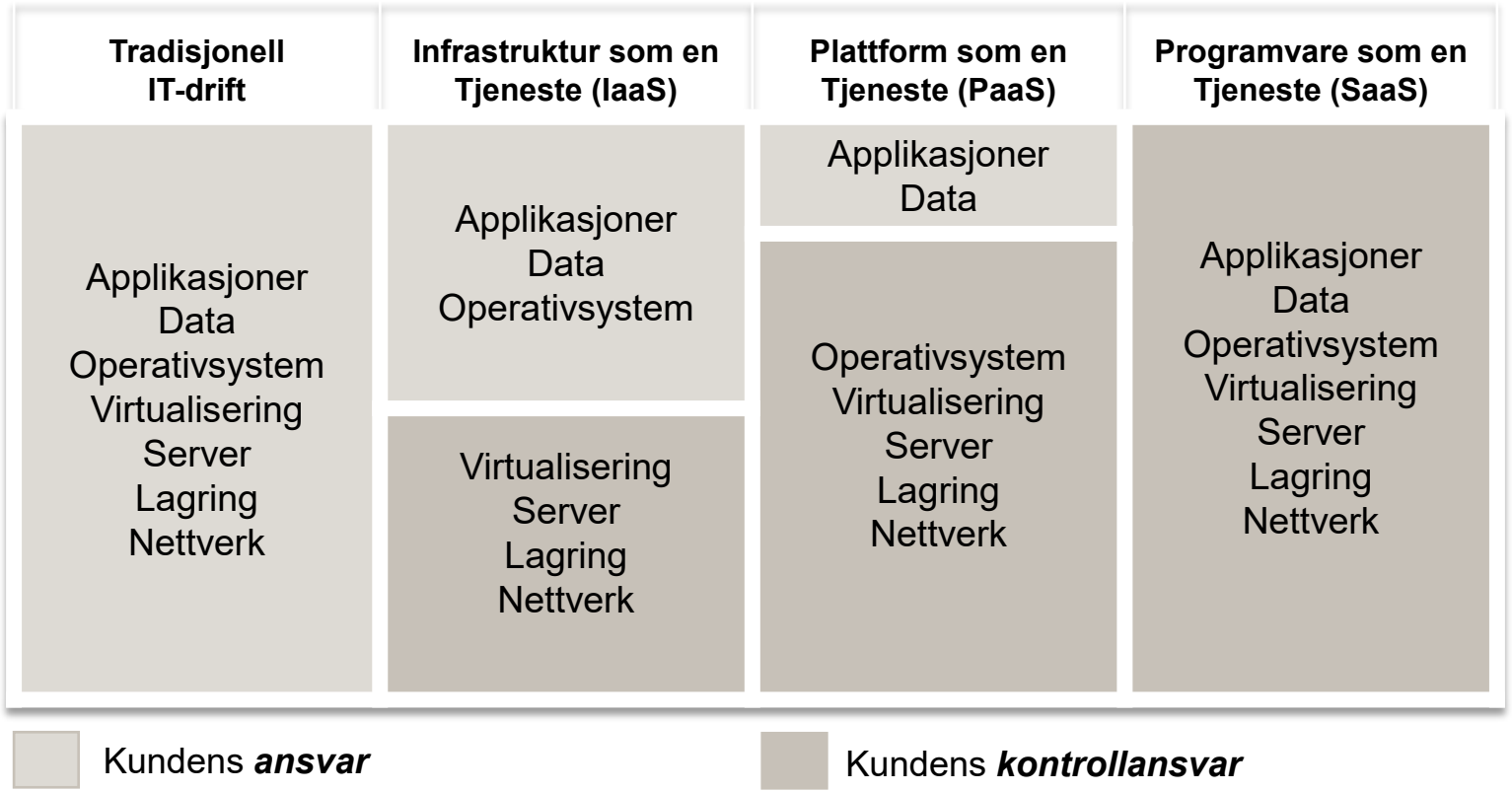
Taper millionar etter hacking – har sendt permitteringsvarsel til 35 tilsette

Eit røyrleggjarfirma på Gjøvik kan ha tapt opp mot ti millionar kroner etter at dataleverandøren vart hacka for ei veke sidan.

Ulike modeller for tjenesteleveranser



Men: Hvem har ansvar for *sikkerhet*?



Er *tjenesteutsetting* smart?

Fordeler:

- Reduserte driftskostnader til kompetanse + infrastruktur
- Ofte besparelser i form av betaling for faktisk bruk
- **Sannsynligvis god informasjonssikring**

Men: Vet du hvor «skyen» befinner seg?

Og hva med personopplysningsvern?

> *«Hvis en virksomhet benytter eksterne skytjenester til behandling av personopplysninger, er det virksomheten som er juridisk ansvarlig for at personopplysningene behandles i samsvar med personvernregelverket.»*

Pålagt å inngå en *databehandleravtale* (artikkel 28 i GDPR).

Oppgave #2

En helseinstitusjon har valgt å bruke en ekstern leverandørs skyløsning for å lagre pasientdata. Alle data (også personopplysninger) lagres på den eksterne leverandørens datautstyr som er fysisk plassert i et EU-land. Overføring av data går over internett.

Hvilke utsagn nedenfor stemmer overens med føringer i Personopplysningsloven (GDPR) for helseinstitusjonens behandling av personopplysninger?

Oppgave #2 - alternativer

Velg ett eller flere alternativer

- ❑ Helseinstitusjonen er juridisk ansvarlig for at data om pasienter behandles i samsvar med personopplysningsloven.
- ❑ Personopplysningsloven stiler krav til informasjonssikkerhet.
- ❑ En pasient har aldri rett til innsyn i hvilke helseopplysninger som er lagret om seg.
- ❑ All behandling av personopplysninger skal skje med egnede tekniske og organisatoriske tiltak.
- ❑ Når personopplysninger lagres hos et eksternt firma kan helseinstitusjonen se bort fra personopplysningsloven for sin behandling av personopplysninger.



ÅLESUND
KOMMUNE

Elevane måtte bruke treningsapp i gym, no får kommunen bot

Elevar ved to skular i Ålesund blei pålagt å bruke treningsappen Strava i kroppsøving. Grovt aktlaust, seier Datatilsynet og gir kommunen 50.000 kroner i gebyr.

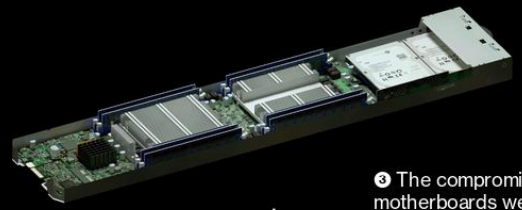
How the Hack Worked, According to U.S. Officials

❶ A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.



❷ The microchips were inserted at Chinese factories that supplied Supermicro, one of the world's biggest sellers of server motherboards.



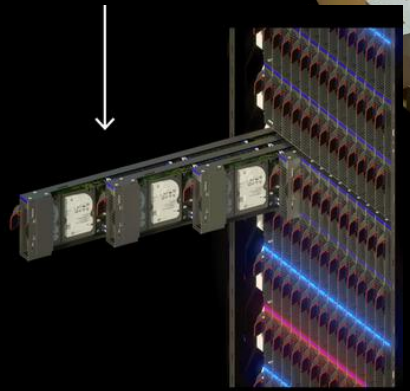


❸ The compromised motherboards were built into servers assembled by Supermicro.

❹ The sabotaged servers made their way inside data centers operated by dozens of companies.



❺ When a server was installed and switched on, the microchip altered the operating system's core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.



Kan maskinvare «hackes»?

Kilde:
https://www.digi.no/artikler/kina-kan-ha-infiltrert-nettverket-til-naermere-30-amerikanske-selskaper/447913

Læringsmål

- Kjenne til hovedprinsippene for *nettverkssikkerhet, kommunikasjonssikkerhet* og *datanettsikkerhet,* inkludert vanlige sikkerhetstiltak.
- Forstå viktigheten av å holde *endesystemer* fri for svakheter og sårbarheter.
- Kjenne til vanlige sårbarheter knyttet til *systemprogramvare.*
- Forstå sikkerhetsutfordringene knyttet til digitale verdikjeder, leverandørkjeder og tjenesteutsetting.

Takk for i dag!

mn.uio.no/ifi

