

UiO : Institutt for informatikk

Å skape trygge digitale tjenester krever innsats.

IN1020 – Introduksjon til datateknologi

24.09.2025

Kristin Skar
kritisk@ifi.uio.no

Datateknologi og sikkerhet

Tema for tema:

1. Datasikkerhet - Er det så viktig? (20.aug)
2. Hvem er hvem på internett? Hvordan kunne stole på digitale aktører (27.aug)
3. Kryptografi – nøkkelen til (fungerende) digital samhandling (10.sept)
4. Hvordan hackes vi? (18.sept)
5. **Å skape trygge digitale tjenester krever innsats (24.sept)**

I dag: Hvordan hackes vi?

Ressurser:

- Forelesning 24.09.25
- Ukeoppgaver og pensumlitteratur
  (Heide/Nätt: Kap. 5 (134-143), 13, 14)

Nøkkelord:

- Lovpålagte krav
- Digitale verdikjeder
- Trusselmodellering og risikoanalyse
- Systematikk og kontinuitet
- Administrative sikkerhetstiltak

Dagens trusselbilde

Bakteppe:

- Sikkerhetspolitiske uroligheter
- Ustabilitet og krig i Europa
- Komplekse digitale verdikjeder
- Profesjonalisering av angrep
- Kunstig intelligens

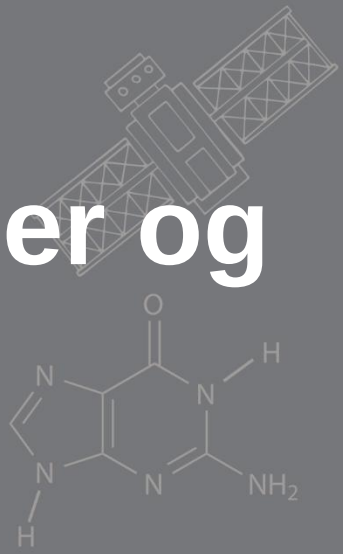
Trender:

- Innsidevirksomhet
- Angrep mot virksomheter underlagt sikkerhetsloven
- Sårbarheter i leverandørkjeden finnes og utnyttes
- Phishingkampanjer (fakturasvindel)
- Nulldagssårbarheter utnyttes
- Tjenestenektangrep

Kilde: Nasjonalt digitalt trusselbilde 2025

Lovpålagte rammer og krav





«Overtredelsesgeby til Østre Toten kommune.

Datatilsynet har ilagt Østre Toten kommune et overtredelsesgebyr på 4 millioner kroner. Kommunen er også pålagt å implementere et egnet styringssystem for *informasjonssikkerhet* og personopplysningssikkerhet.»

Datatilsynet

Kilde:
https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2022/overtredelsesgebyr-til-ostre-toten-kommune/

Personopplysninger (repetisjon)

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson.

Reguleres av «Lov om behandling av personopplysninger» (GDPR - General data protection regulation): https://lovdata.no/dokument/NL/lov/2018-06-15-38

Loven skiller mellom:

- Alminnelige personopplysninger (artikkel 4)
  - Navn, brukernavn, telefonnummer, studentnummer, adresse, IP-adresse, fingeravtrykk, adferdsmønster, …
  - Fødselsnummer – kun når helt nødvendig for en behandling
- Særlige kategorier personopplysninger (artikkel 9)
  - Helseopplysninger, seksuell legning, religion, straffedommer, etnisk opprinnelse, fagforeningsmedlemskap, …

EUs Personvernforordning (20.07.18)

- Virkeområde: EØS samt *virksomheter som tilbyr varer og tjenester til EØS-borgere*
- Definerer *roller*
  - *Behandlingsansvarlig* - ansvarlig part for at prinsippene overholdes
  - *Databehandler* - behandler personopplysninger på vegne av behandlingsansvarlige
- Relevante artikler:
  - Fastsetter prinsipper for *behandling* av personopplysninger (artikkel 5)
  - Krav til *innebygd personvern* og *personvern som standard* (artikkel 25)
  - Krav til *sikkerhet* ved behandlingen (artikkel 32)
  - Pålegger vurdering av *personvernkonsekvens* (artikkel 35)

Prinsipper for behandling (artikkel 5)

- Lovlighet, rettferdighet og åpenhet
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet

Innebygd personvern (artikkel 25)

- Sørge for at programvaresystemene vi bruker oppfyller personvernprinsippene.
- Må ta hensyn til personvern i alle utviklingsfaser av et system eller en IT-løsning.
- Det *minst personverninngripende* alternativet skal være standarden i alle systemer og løsninger:
  - Mengden personopplysninger
  - Omfang av behandlingen
  - Lagringstid
  - Tilgjengelig kun for berettigede personer

Sikkerhet ved behandlingen (artikkel 32)

- Ivareta informasjonssikkerhet gjennom hele behandlingsperioden:

«… gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

a) pseudonymisering og kryptering av personopplysninger
b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,
c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,
d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.»

Hva med annen type informasjon?

Foreløpig få lovpålagte krav til informasjonssikkerhet generelt. Noe finner man dog i lovverk rettet mot spesifikke bransjer/forvaltningsorganer:

- Sikkerhetsloven (nasjonal sikkerhet)
- Forskrift om IT-standarder i offentlig forvaltning
- eForvaltningsforskriften (elektronisk kommunikasjon i forvaltningsorganer)
- Lov om elektronisk kommunikasjon (ekomloven)
  «Det er ikke tillatt å lagre eller å skaffe seg tilgang til opplysninger i sluttbrukers eller brukers kommunikasjonsutstyr uten at den aktuelle sluttbrukeren eller brukeren er informert om blant annet hvilke opplysninger som behandles, formålet med behandlingen og hvem som behandler opplysningene, og uten at den aktuelle sluttbrukeren eller brukeren har gitt samtykke.»
- Også flere EU (EØS)-direktiver under arbeid.

Personopplysninger til 35 000 bergensere kan være på avveie

Onsdag ettermiddag oppdaget Bergen kommune at uvedkommende har fått tilgang til personopplysninger om opp til 35 000 lærere og elever i kommunen.

Personopplysninger på avveie etter feil hos Studentweb

En feil i Studentwebs driftssystemer gjorde at folk ble logget inn på andres profiler. Kunskapssektorens tjenesteleverandør ser alvorlig på at personopplysninger ble delt med uvedkommende.

Eksamensoppgave

Personopplysningsvern

Behandling av personopplysninger er strengt regulert i norsk og europeisk lovverk gjennom Personopplysningsloven.

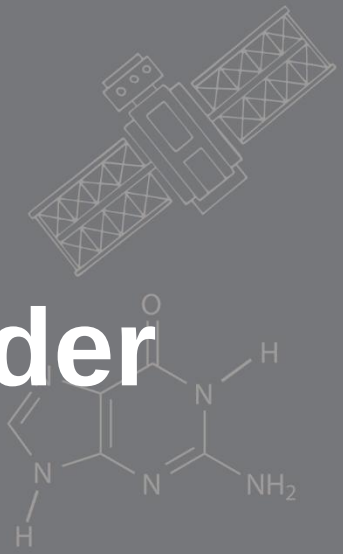
Hvilken gruppe har Personopplysningsloven størst konsekvens for?

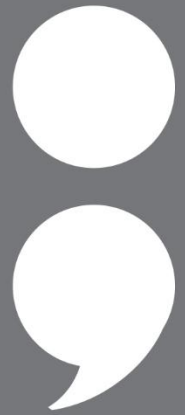
Velg ett alternativ.

- Enkeltpersoner (de registrerte)
- Virksomheter
- Kriminelle

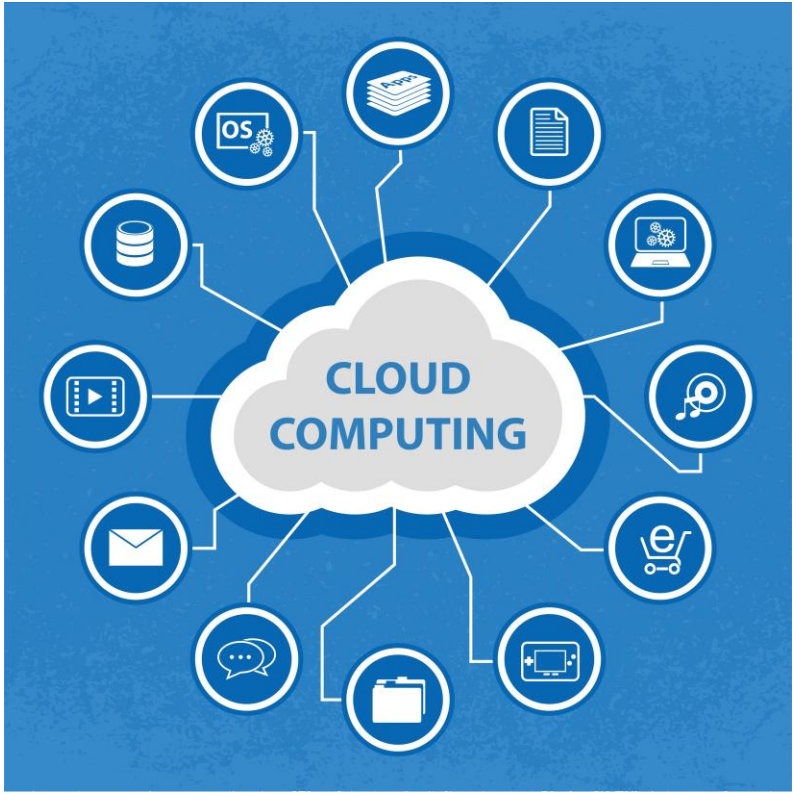
Digitale verdikjeder

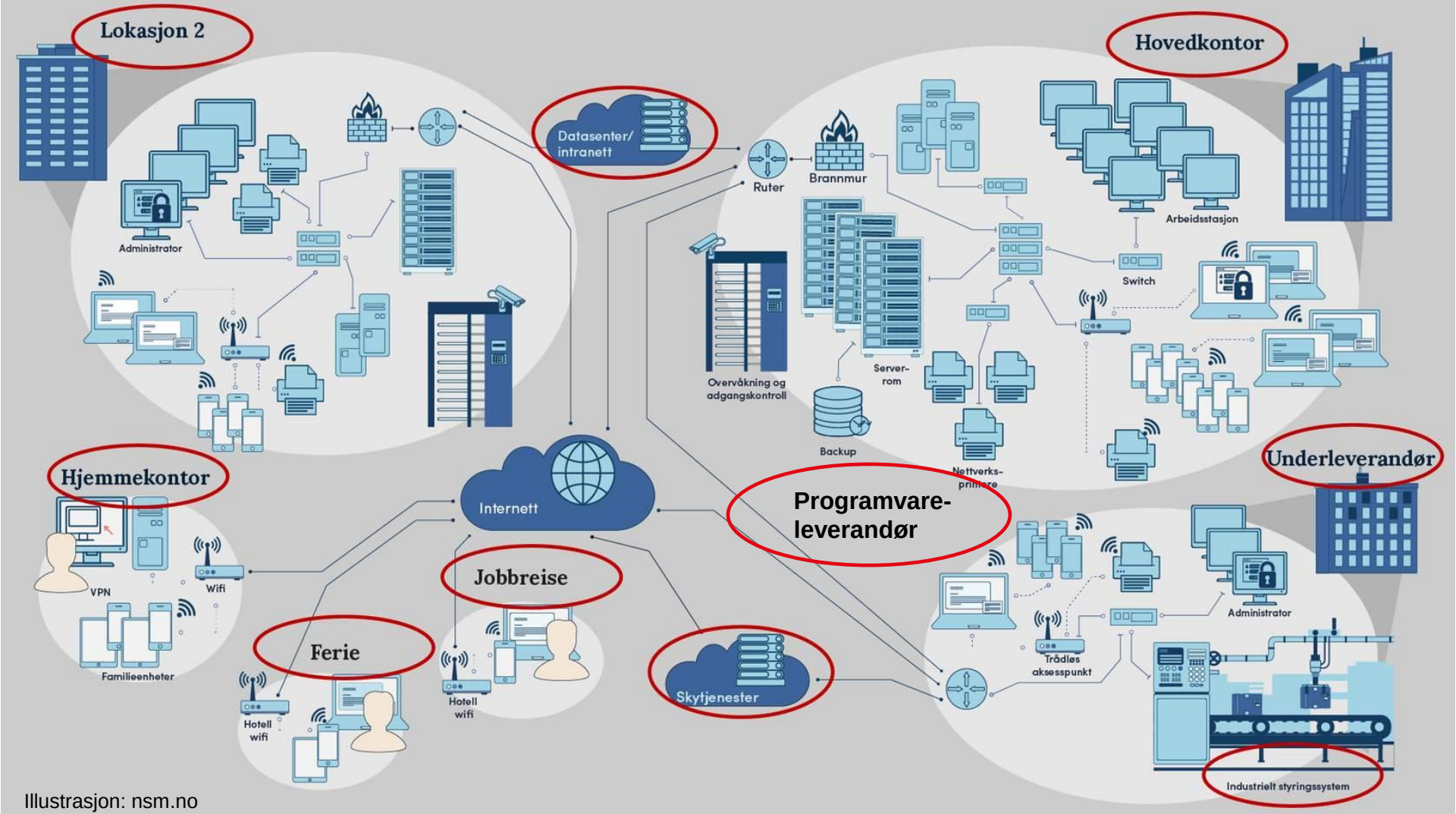




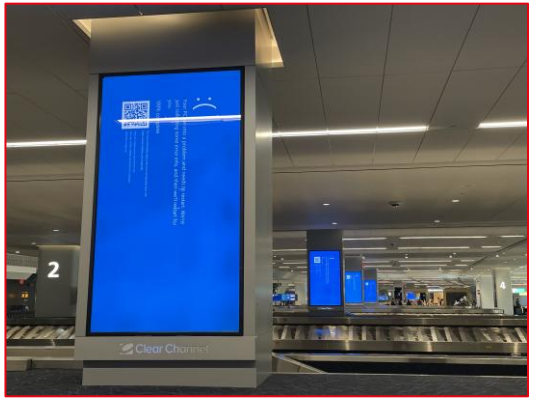


UiO : Institutt for informatikk


OS
CLOUD
COMPUTING



Illustrasjon: nsm.no



Crowdstrike juli 2024

SOLARWINDS®

Taper millionar etter hacking – har sendt permitteringsvarsel til 35 tilsette

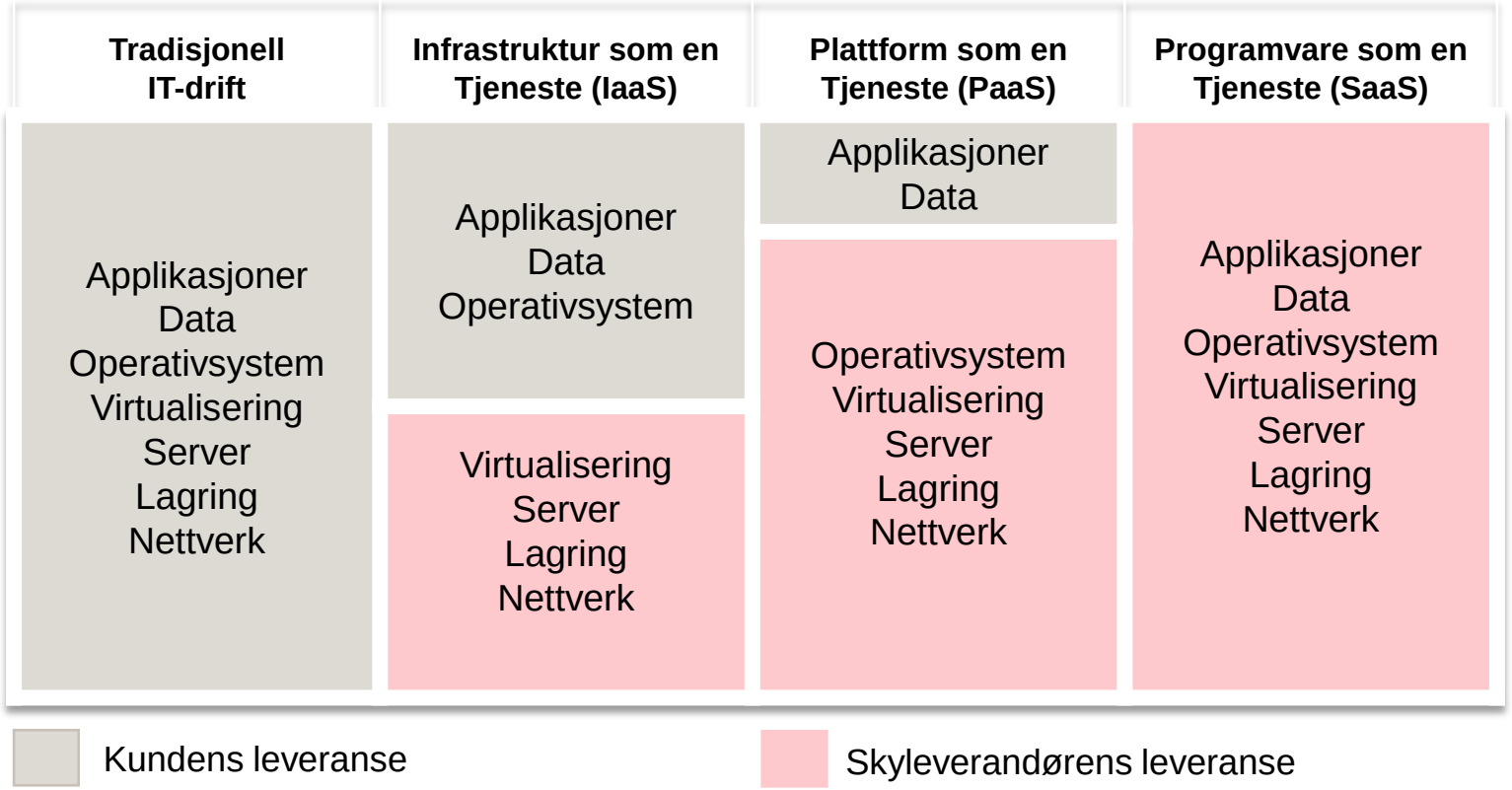
Eit røyrleggjarfirma på Gjøvik kan ha tapt opp mot ti millionar kroner etter at dataleverandøren vart hacka for ei veke sidan.

Digitale verdikjeder

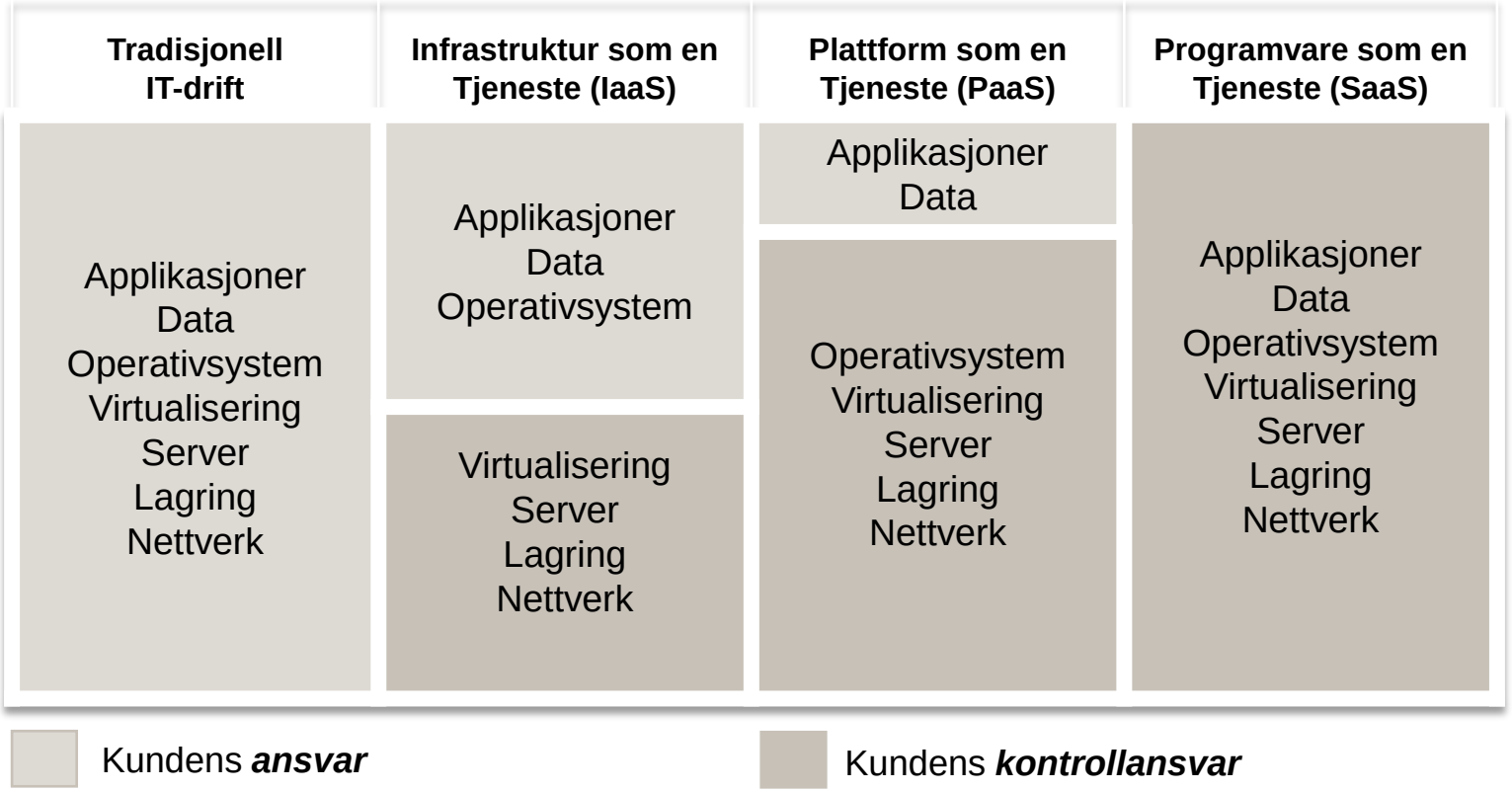
Virksomheter anskaffer digitale tjenester, funksjoner eller varer fra eksterne leverandører istedenfor å gjøre jobben selv – det oppstår en *digital verdikjede.*

- Programvare: Andre utvikler og vedlikeholder *programvare* som tas i bruk
- Tjenesteutsetting: Andre utvikler og vedlikeholder *IT-tjenester* som tas i bruk
  - Enkel tilgang til et sett med IT-ressurser, lett tilgjengelig overalt
  - Rask anskaffelse og tilgjengelighet
  - Men: Vet du hvor «skyen» befinner seg?

Ulike modeller for tjenesteleveranser



Men: Hvem har ansvar for *sikkerhet*?



Er tjenesteutsetting smart?

- Fordeler:
  - Reduserte driftskostnader til kompetanse + infrastruktur
  - Besparelser i form av betaling for faktisk bruk
  - **Sannsynligvis god informasjonssikring**

- 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)

Gebyr til Ålesund kommune for bruk av Strava

Datatilsynet har vedteke å gje Ålesund kommune eit overtredelsesgebyr på 50 000 kronar for deira bruk av treningsappen Strava.



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.

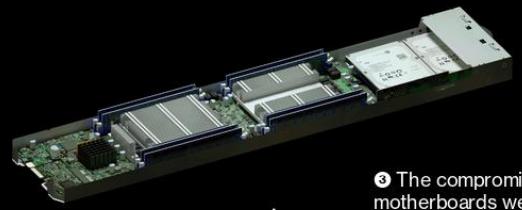
How the Hack Worked, According to U.S. Officials

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.



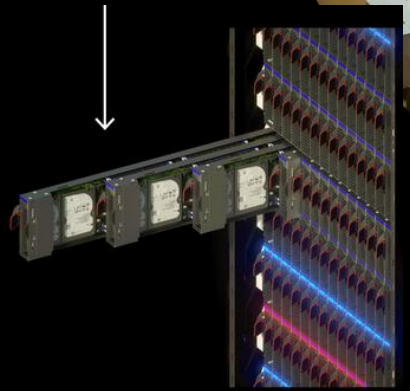


❸ The compromised motherboards were built into servers assembled by Supermicro.

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

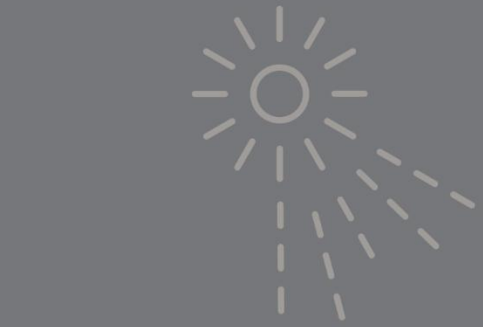
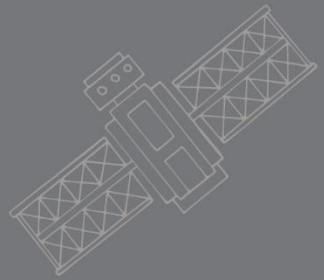
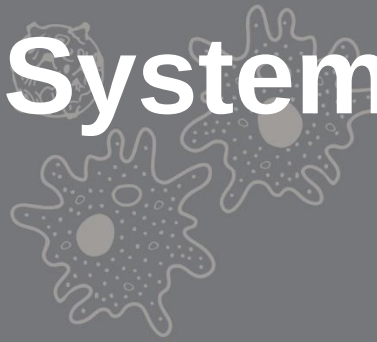
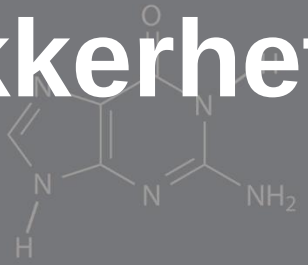


❺ When a server was installed and switched on, the microchip altered the operating system's core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.

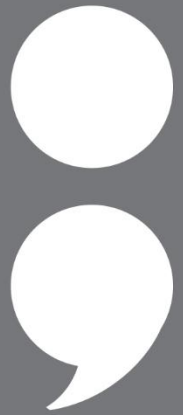


Kan vi stole på leverandørkjeden?

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

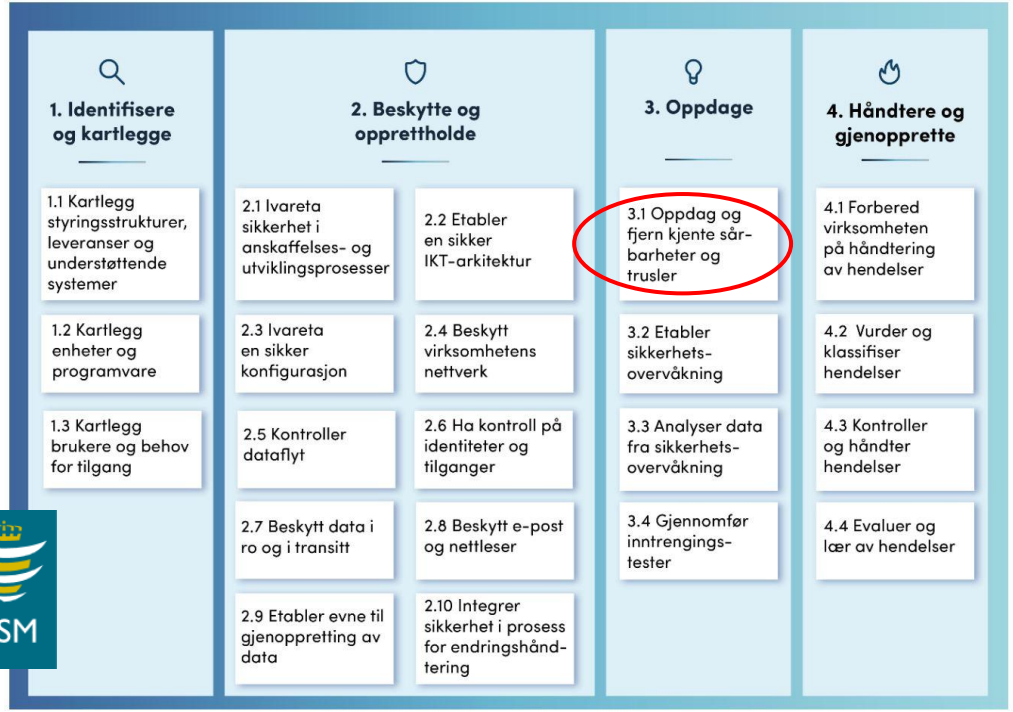
Systematisk datasikkerhet



UiO : Institutt for informatikk

Behov for *systematikk og rammeverk*

- Rammeverk for informasjonssikring:
  - Svært mange ulike rammeverk
  - NSMs grunnprinsipper for informasjonssikkerhet er tilpasset norske forhold.
- Kjente sårbarheter?
  Abonner og følg med på varslinger.
  (f.eks. https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/)



https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/ta-i-bruk-grunnprinsippene/

Innebygd informasjonssikkerhet og personvern

- Innebygd informasjonssikkerhet og personvern betyr at det tas eksplisitt hensyn til informasjonssikkerhet og personvern i *hele livssyklusen* til programvare og applikasjoner.
- Metodikken beskrives ofte som en prosess bestående av 7 faser:



- For den interesserte: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/programvareutvikling-med-innebygd-personvern/opplaring/

Behov for systematiske arbeid

*«**Sikkerhetsstyring** er systematiske aktiviteter for å oppnå og opprettholde et sikkerhetsnivå i overensstemmelse med de mål og krav en organisasjon har satt seg»*

- Informasjonssikkerhet må inkluderes i virksomhetsstyringen
- Eksempel: NSMs styringshjul for informasjonssikkerhet



Risikovurdering og tusselmodellering

- Ønsker oss:
  - Forebygge og håndtere sikkerhetsproblemer tidlig
  - Gjøre gode risikovurderinger
  - Effektiv sikkerhetstesting
- Trusselmodellering består i å identifisere, analysere og beskrive relevante angreps-scenarier:
  - Hva kan skje?
  - Hvordan kan våre verdier skades?
  - Hvem kan være interessert i å skade oss?

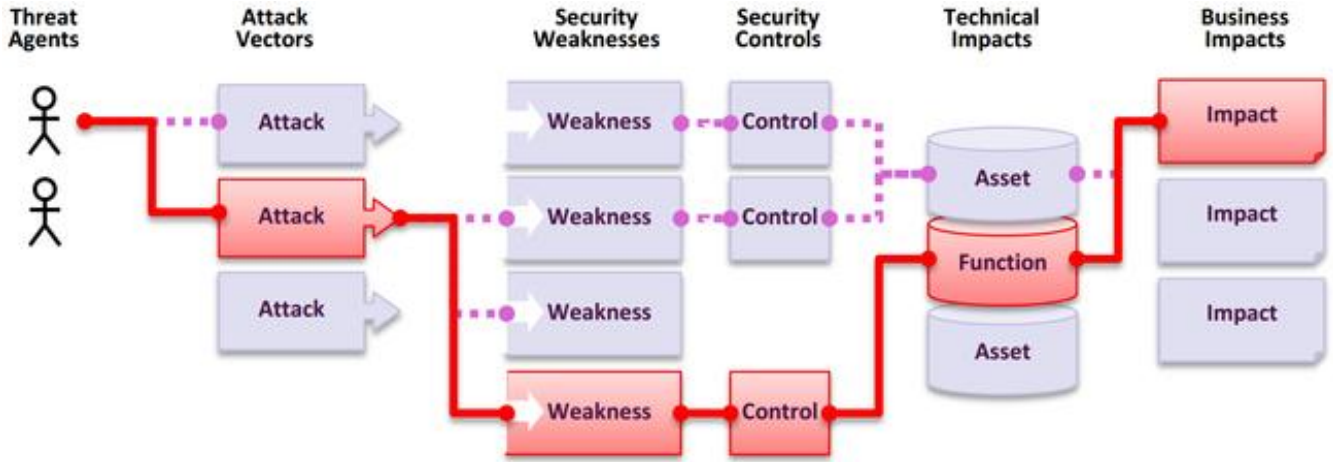
Trusselmodellering

Ulike innfallsvinkler:

- Fokus på **trusselaktør**
  - Identifisere trusselaktørens mål, hvordan går de fram for å oppnå dem, hva er angrepsvektor og angrepsflate.
- Fokus på **system**
  - «Plukke fra hverandre» systemet, identifisere de ulike delene og avdekke hvor og hvordan de kan angripes.
- Fokus på **verdi**
  - Identifisere verdiene i systemet, avdekke hvordan brudd på informasjonssikkerhet kan inntreffe.

➢ Lær av feil! Hva har gått galt tidligere? Men ikke «hvil på laubærene».

Eksempel: «Trusseltre»



Kilde: https://www.owasp.org

Risikoanalyse

- Risiko involverer *konsekvens* (f.eks. målt i kroner og øre).
- Flere definisjoner, men:
  «Risiko er et produkt av sannsynlighet for hendelse og konsekvens knyttet til hendelsen»

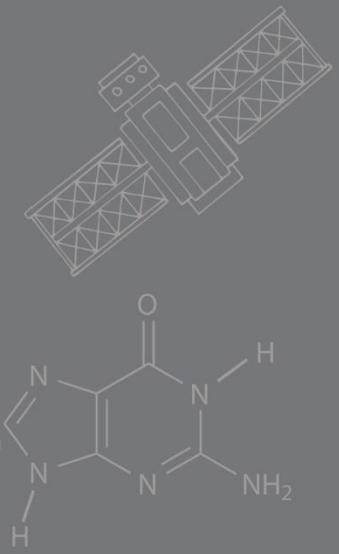
- Hvor skal innsatsen legges?
  - Usannsynlig hendelse som medfører store tap?
  - Sannsynlige hendelser som har lavere kostnad?

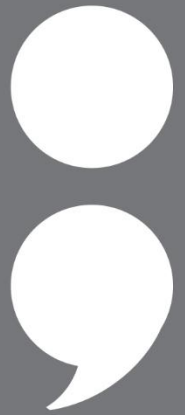
Å redusere risiko:

- Kartlegg alle IT-systemer, få oversikt over sårbarhetsflater
- Reduser sårbarhetsflatene
- Kartlegg egne avhengigheter
- Gjennomfør risikoreduserende tiltak

Administrativ datasikkerhet







UiO : Institutt for informatikk

God informasjonssikkerhet koster

Ressurser til:

- ✓ Kompetanse og bevissthet
- ✓ Styring og kontroll
- ✓ Drift og vedlikehold
- ✓ Tjenesteutsetting
- ✓ Sikkerhetstiltak

Sikkerhet må prioriteres av ledelse og styrer i virksomheter.

Dårlig informasjonssikkerhet koster også…

Marks & Spencer faces £300m impact on profit from cyberattack

Britiske Marks & Spencer utsatt på løsepengevirus i april 2025.

Men på sikt er det kanskje lønnsomt?

Beskytte ressurser = å skape verdi:

- ✓ Forebygge og redusere (økonomiske) tap
- ✓ Skape robusthet og sikre kontinuitet i driften (håndtere hendelser og katastrofer)
- ✓ Økt tillitt (fra kunder, forretningspartnere, investorer, ansatte)
- ✓ Godt rykte, merkevare

Kan bidra til konkurransefortrinn og å øke selskapets verdi.

Administrative sikkerhetstiltak

Hvorfor går det galt?

- Sikkerhet nedprioriteres
- Komplekse systemer
- Utilstrekkelig kompetanse
- Evig kappløp om marked
- Fremdeles ikke full åpenhet om feil

Hvilke tiltak kan gjøres?

- Internkontroll
- Styringssystem
- Policyer / Standarder
- Prosedyrer og praksis
- Bevissthetstrening / opplæring
- Sikkerhetsøvelser
- Rutiner for hendelseshåndtering

- **Lesestoff (men ikke pensum)**
  - Datatilsynet: https://datatilsynet.no
  - Hva betyr personvernreglene for din virksomhet? https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/
  - Programvareutvikling med innebygd personvern: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/
  - Lov om behandling av personopplysninger: https://lovdata.no/dokument/NL/lov/2018-06-15-38
  - Publikasjoner fra Nasjonal sikkerhetsmyndighet: https://www.nsm.no/publikasjoner/

- **Litt på siden** - «How a university got itself banned from the Linux kernel»
  - https://www.theverge.com/2021/4/30/22410164/linux-kernel-university-of-minnesota-banned-open-source

Andre nyttige ressurser:

- OWASP: https://owasp.org/
- NSM Digital sikkerhet og cybersikkerhetssenter: https://nsm.no/fagomrader/digital-sikkerhet/
- Cyber Security Sentre:
  - UK: https://www.ncsc.gov.uk/
  - Norge: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/
  - EU: https://www.enisa.europa.eu/
- NIST: https://www.nist.gov/ og NIST NVD: https://nvd.nist.gov/
- Europeisk sårbarhets-database: https://euvd.enisa.europa.eu/
- CVE (Common Vulnerabilities and Exposures)-database: https://www.cve.org/
- Biblioteksressurser, Oria via Universitetsbiblioteket: https://www.ub.uio.no/

Læringsmål for økten

- Kjenne til **hovedprinsipper** i EUs personvernforordning gjennomgått på forelesning.
- Forstå sammenhengen mellom personvernregelverk og krav til informasjonssikkerhet.
- Kjenne til sikkerhetsutfordringer knyttet til leverandørkjeder og tjenesteutsetting.
- Vite at datasikkerhet må være en integrert del av en virksomhets styring.
- Vite at datasikkerhet og sikring av verdier og ressurser er en kontinuerlig prosess.
- Vite hva trusselmodellering og risikoanalyse innebærer, samt nytteverdi av gjennomføring.

I mål: Kunne *anvende* kunnskapen til å *ta gode valg* profesjonelt (og privat).

Bitt av basillen?

- Institutt for informatikk:
  - IN1030: Systemer, krav og konsekvenser (vår)
  - IN2100: Logikk for systemanalyse (vår)
  - IN2120: Informasjonssikkerhet (høst)
  - IN3210: Network and Communications Security (høst)
  - IN4180: Cyber Operations (vår)
  - IN5080: Sikkerhets- og risikostyring (vår)
  - IN5130: Uangripelige IT-systemer (høst)
  - IN5290: Ethical Hacking (høst)

- Institutt for teknologisystemer (Kjeller):
  - TEK4500: Innføring i kryptografi (høst)
  - TEK5510: Sikkerhet i operativsystemer og programvare (høst)
  - TEK5520 – Cybersikkerhet i industrielle systemer (høst)
  - TEK5530 – Målbar sikkerhet for tingenes internett (høst)

Takk for i dag!

mn.uio.no/ifi

