

UiO : Institutt for informatikk

Å skape trygge digitale tjenester krever innsats.

IN1020 – Introduksjon til datateknologi

25.10.2023

Kristin Skar
kritisk@ifi.uio.no

Datateknologi og sikkerhet

Tema for tema:

1. Datasikkerhet - Er det så viktig? (27.sept)
2. Hvem er hvem på internett? Hvordan kunne stole på digitale aktører (28.sept)
3. Kryptografi – nøkkelen til (fungerende) digital samhandling (12.okt)
4. Hvordan hackes vi? (19.okt)
5. Å skape trygge digitale tjenester krever innsats (25.okt)

I dag: Hvordan hackes vi?

Ressurser:

- Forelesning 25.10.23
- Ukeoppgaver og pensumlitteratur
  (Heide/Nätt: Kap. 5 (134-143), 13, 14 (kursorisk))

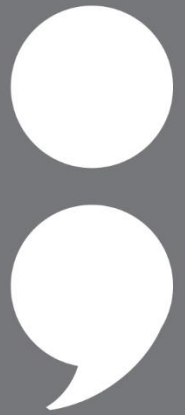
Nøkkelord:

- Lovpålagte krav
- Tjenesteutsetting
- Trusselmodellering og risikoanalyse
- Systematikk og kontinuitet

Lovpålagte krav til personopplysningsvern







UiO : Institutt for informatikk

«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.»



Kilde:
https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-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)
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*
- Prinsipper for behandling av personopplysninger (artikkel 5):
  - *Lovlighet, rettferdighet og åpenhet*
  - *Formålsbegrensning*
  - *Dataminimering*
  - *Riktighet*
  - *Lagringsbegrensning*
  - *Integritet og konfidensialitet*
- Definerer *roller*
  - *Behandlingsansvarlig* - ansvarlig part for at prinsippene overholdes
  - *Databehandler* - behandler personopplysninger på vegne av behandlingsansvarlige
- Krav til *innebygd personvern* og *personvern som standard* (artikkel 25)

Innebygd personvern (artikkel 25)

- Sørge for at programvaresystemene vi bruker oppfyller personvernprinsippene
- Ta hensyn til personvern i alle utviklingsfaser av et system eller en løsning
- Det *minst personverninngripende* alternativet skal være standarden i alle systemer og løsninger:
  - Mengden personopplysninger
  - Omfang av behandling
  - Lagringstid
  - Tilgjengelighet

Sikkerhet ved behandlingen (artikkel 32)

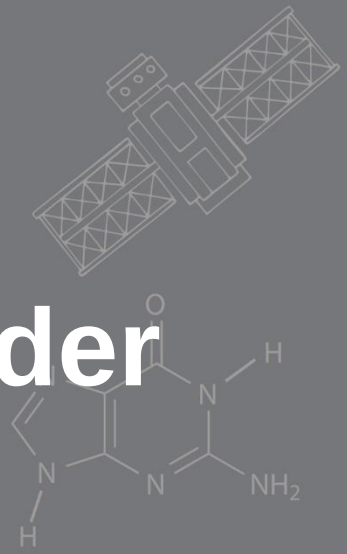
- Ivareta informasjonssikkerhet gjennom hele behandlingsperioden:

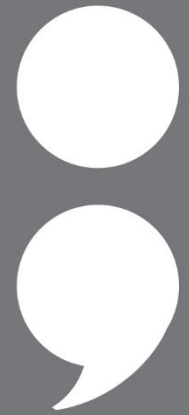
«… gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

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.»

Digitale verdikjeder







UiO : Institutt for informatikk

Dagens trusselbilde

Bakteppe:

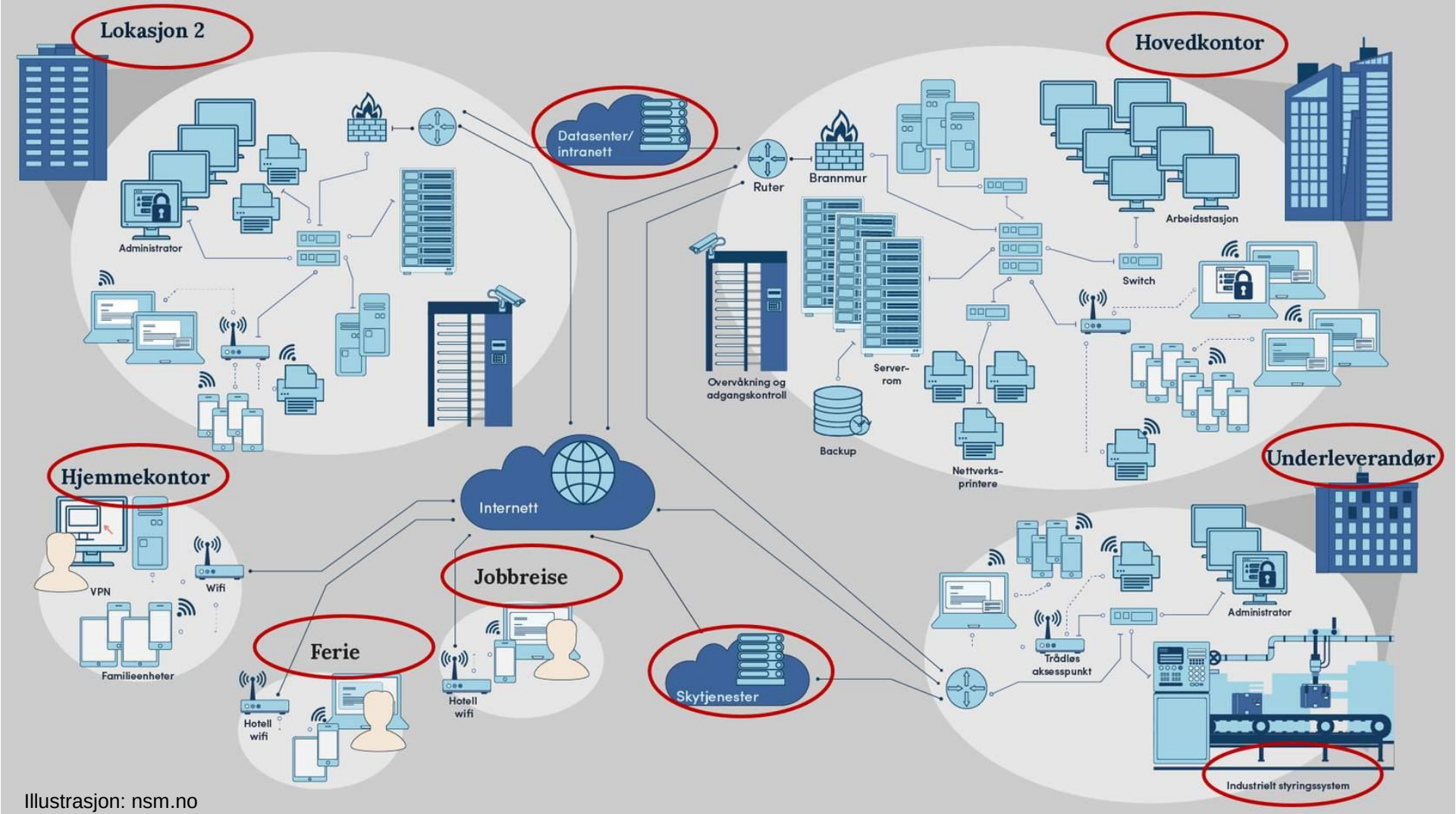
- Profesjonalisering av angrep
- Komplekse digitale verdikjeder
- Kunstig intelligens
- Ustabilitet og krig i Europa



Trender:

- Nulldagssårbarheter
- Tjenestenektangrep
- Digital svindel og utpressing foregår svært målrettet og avansert
- Sårbarheter i leverandørkjeden finnes og utnyttes
- Nye sektorer rammes

Kilde: Nasjonalt digitalt trusselbilde 2023 (NSM, oktober 2023)



Illustrasjon: nsm.no

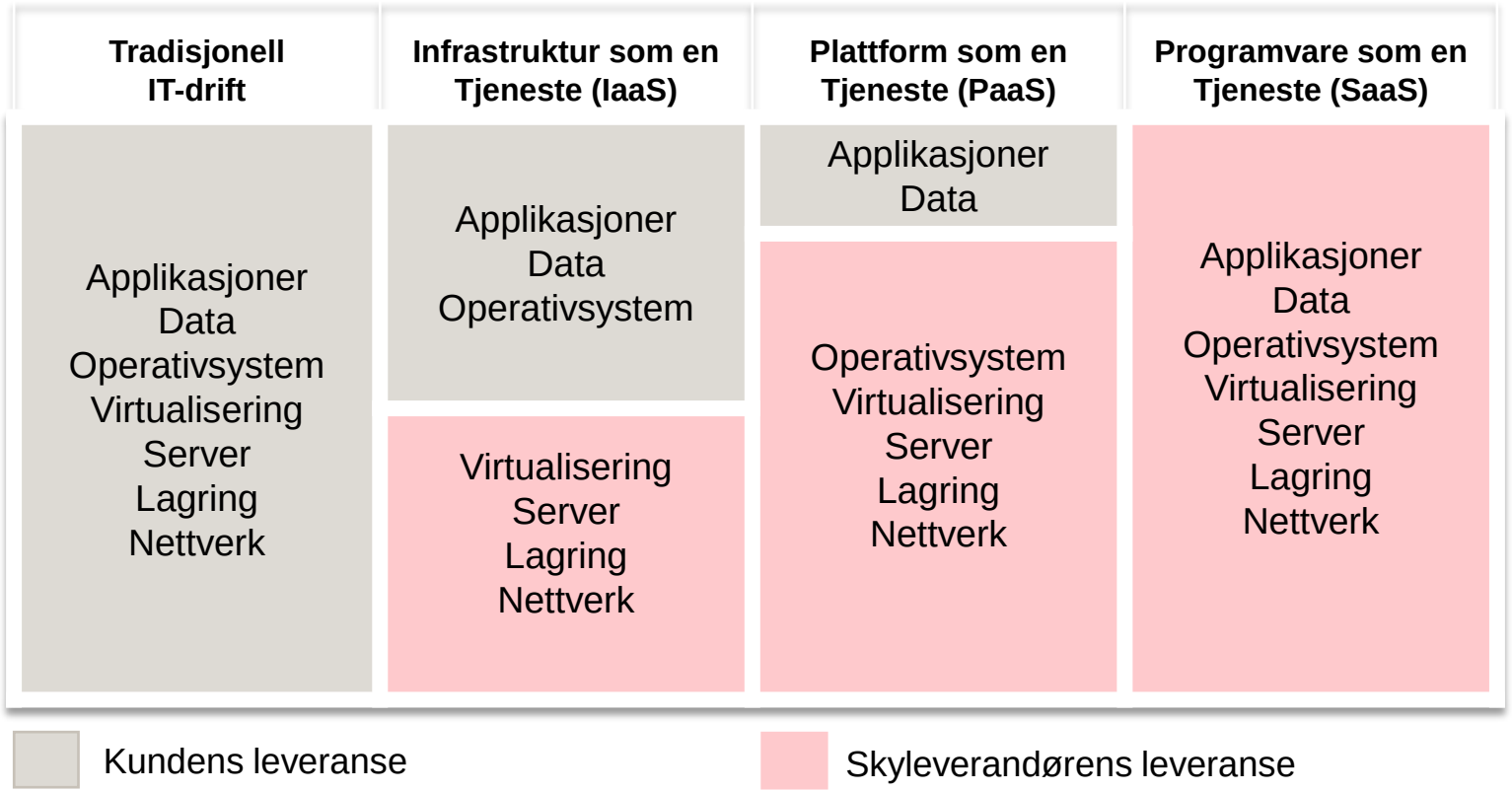

Hey
http://
RSS
Hey
http://
RSS
Hey
Wow
www.

Tjenesteutsetting

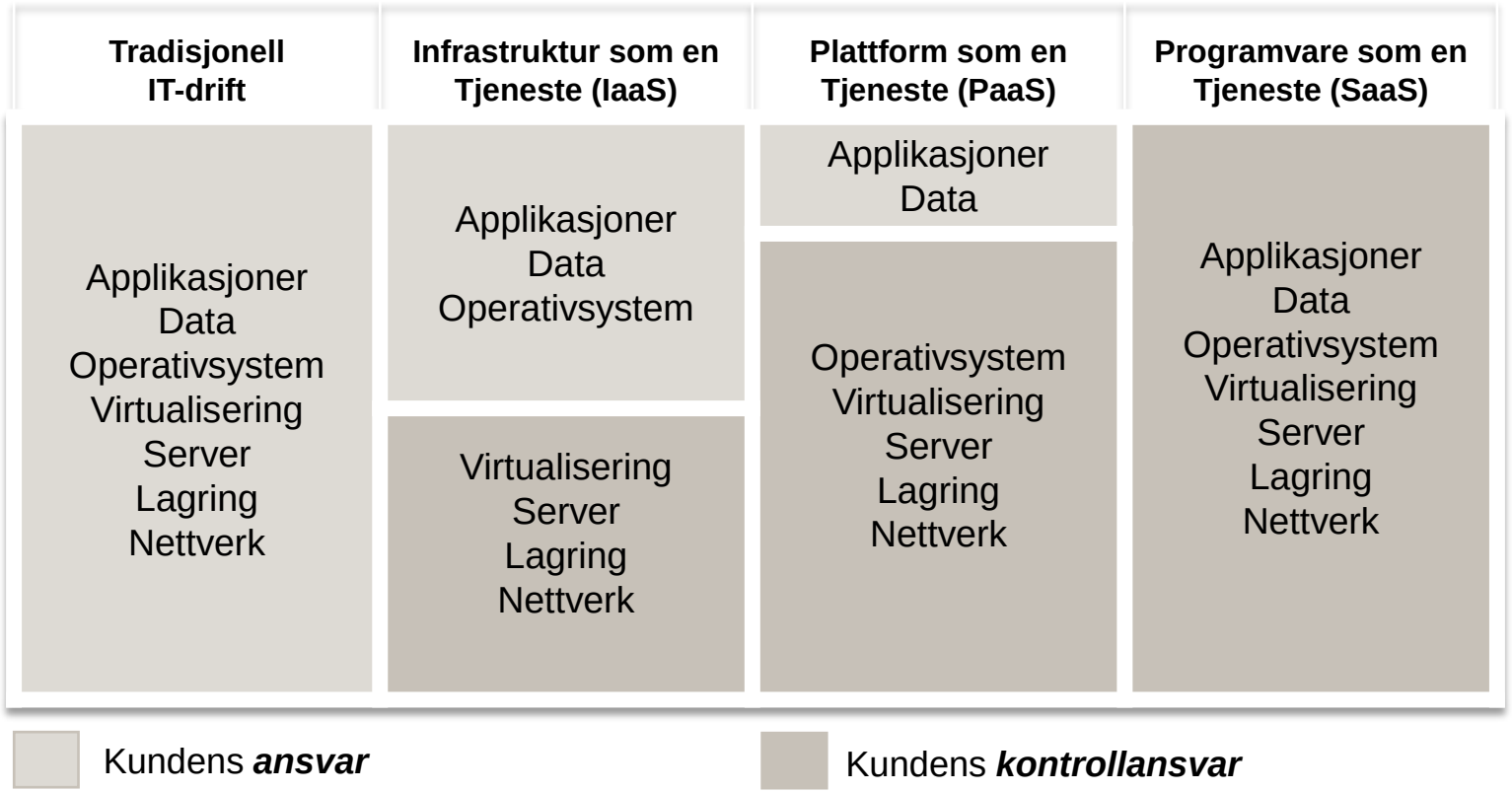
- Å sette ut en eller flere funksjoner/tjenester til andre leverandører – *underleverandører*.
- Man får så tilgang til *et sett med IT-ressurser:*
  - Lett tilgjengelig overalt
  - Blir levert og priset etter behov
  - Rask anskaffelse og tilgjengelighet
  - Betaler kun for ressursene man bruker
  - *Vet du hvor «skyen» befinner seg?*



Ulike modeller for tjenesteleveranser



Men: Hvem har ansvar for *sikkerhet*?



Er tjenesteutsetting lurt?

- Fordeler:
  - Reduserte driftskostnader: kompetanse, infrastruktur
  - Besparelser i form av betaling for faktisk bruk
  - Lokasjonsuavhengig tilgang
  - Sannsynligvis god informasjonssikring



- MEN:

  Dersom en virksomhet ønsker å benytte skytjenester til behandling av personopplysninger, er virksomheten juridisk ansvarlig for at personopplysningene prosesseres og lagres i samsvar med personvernregelverket.

  ➡ Databehandleravtale (artikkel 28)

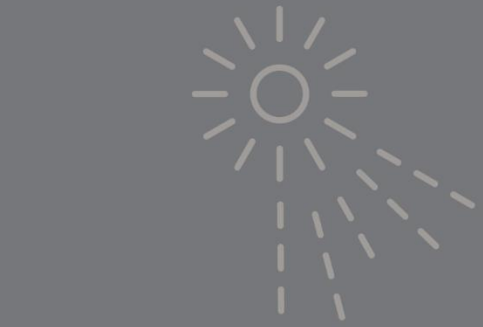
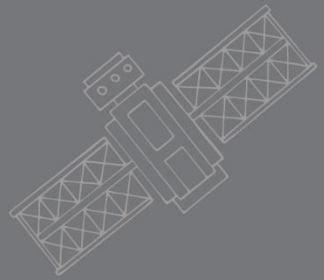
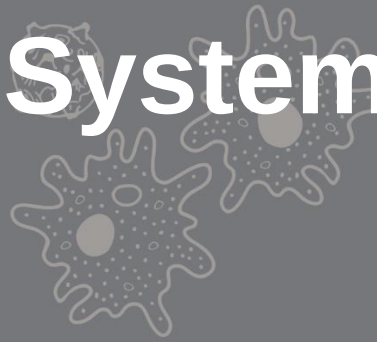
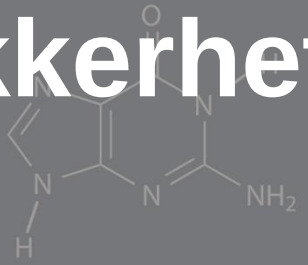
Gebyr til Ålesund kommune for bruk av Strava

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

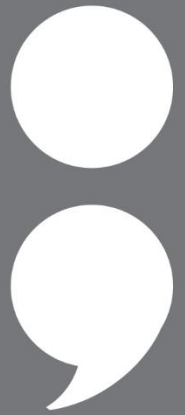


Elevane måtte bruke treningsapp i gym, no får kommunen bot

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.

Systematisk 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 styret i en virksomhet.

En historie fra virkeligheten

NotPetya: – Skrinla oppgradering av IT-sikkerheten hos Mærsk fordi det ikke ga lederne økt bonus

Planer om sikkerhetstiltak som kunne ha begrenset utpressingsvaren NotPetya, som kostet Mærsk minst 1,9 milliarder danske kroner, ble skrinlagt blant annet på grunn av manglende bonusfordeler til de ansvarlige sjefene.



Milliardtap

Tapene blir nå tallfestet til et sted mellom 250 og 300 millioner dollar, tilsvarende mellom 2,0 og 2,5 milliarder kroner – som følge av virusangrepene i juni og juli.

Men på sikt er det lønnsomt

Beskytte ressurser = skape verdi:

- ✓ Forebygge og redusere (økonomiske) tap
- ✓ Skape robusthet og sikre kontinuitet (håndtere hendelser og katastrofer)
- ✓ Tillitt (fra kunder, forretningspartnere, investorer, ansatte)
- ✓ Rykte, merkevare
- ✓ Konkurransefortrinn
- ✓ Øker selskapets verdi

Behov for systematisering

- Rammeverk for informasjonssikring:
  - Svært mange ulike rammeverk
  - Tilpasset norske forhold: NSMs grunnprinsipper for informasjonssikkerhet
- 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-2-0/

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:

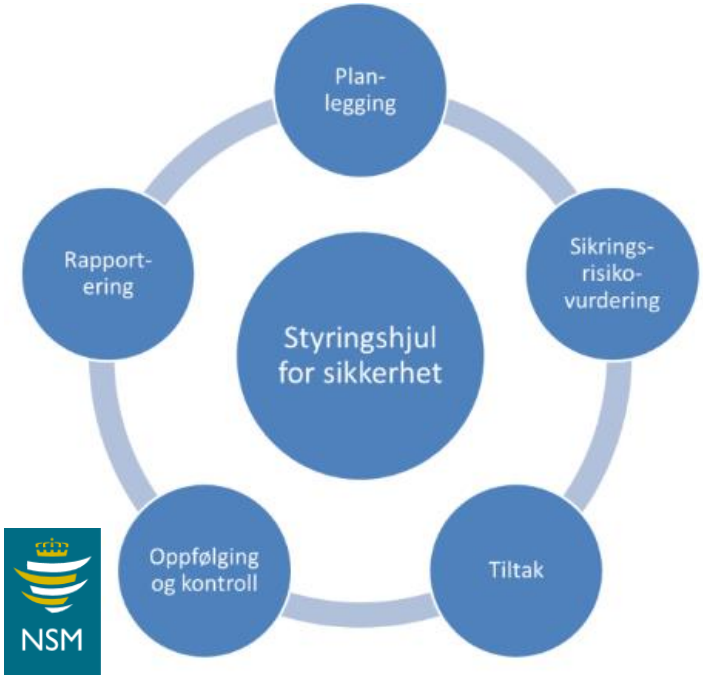


- For den interesserte: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/programvareutvikling-med-innebygd-personvern/opplaring/

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:
  - Tidlig håndtering av sikkerhetsproblemer
  - 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 kunne være interessert i å skade oss?

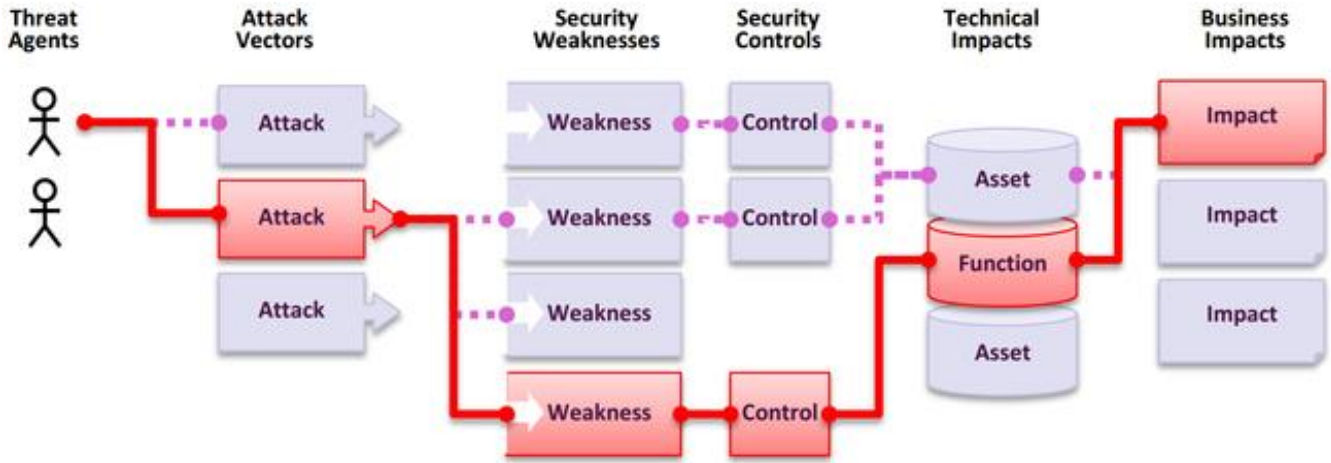
Trusselmodellering

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?

Eksempel: Illustrasjon av trusselbilde



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?

Administrative sikkerhetstiltak

Hvorfor går det galt?

- Sikkerhet nedprioriteres
- Ingen lang fagtradisjon
- Komplekse systemer
- Evig kappløp
- Lite åpenhet om feil

Hvilke tiltak kan gjøres?

- Internkontroll / LSIS
- Policyer / Standarder
- Prosedyrer og praksis
- Bevissthetstrening
- Sikkerhetsøvelser
- Håndtere hendelser

Dagens læringsmål

- 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.

- **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.stat.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

- OWASP: https://owasp.org/
- NSM Digital sikkerhet og cybersikkerhetssenter: https://nsm.no/fagomrader/digital-sikkerhet/
- Nasjonale Cyber Security Centre:
  - UK: https://www.ncsc.gov.uk/
  - Norge: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/
- NIST: https://www.nist.gov/ og NIST NVD: https://nvd.nist.gov/
- CVE-database: https://cve.mitre.org/
- Biblioteksressurser, Oria via Universitetsbiblioteket: https://www.ub.uio.no/

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)
  - IN5130: Uangripelige IT-systemer (høst)
  - IN5280: Security by Design (vår)
  - 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 internet (høst)

Takk for i dag!

mn.uio.no/ifi

