UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi
10.11.2022 - Systematisk datasikkerhet

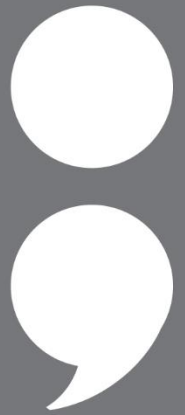
Kristin Skar
kritisk@ifi.uio.no

«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/

Lovpålagte krav til personopplysningsvern



UiO : Institutt for informatikk

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)

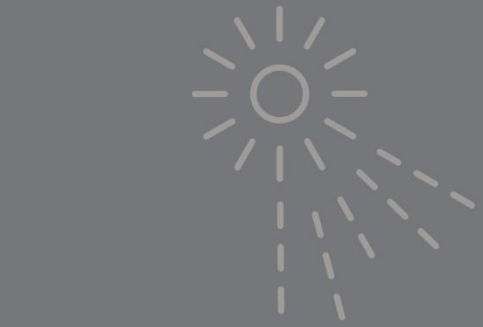
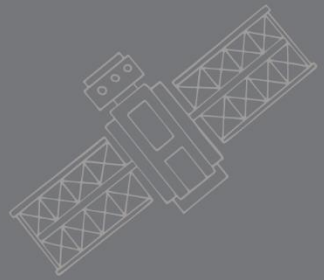
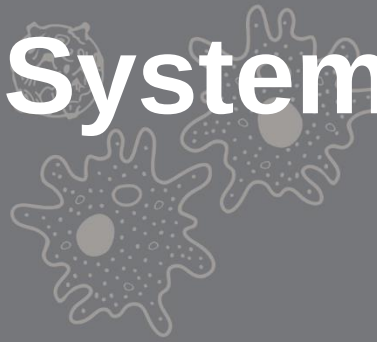
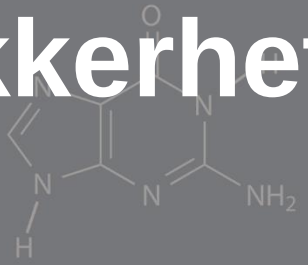
- Ivareta informasjonssikkerhet gjennom hele behandlingsperioden:

«… 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,

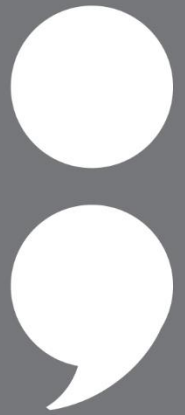
a) pseudonymisering og kryptering av personopplysninger
b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,
c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk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

Innebygd informasjonssikkerhet

- 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.

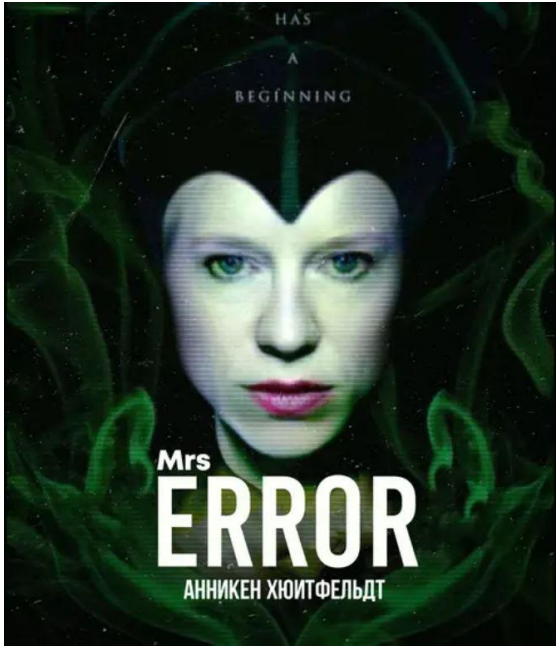
Systematisk datasikkerhet



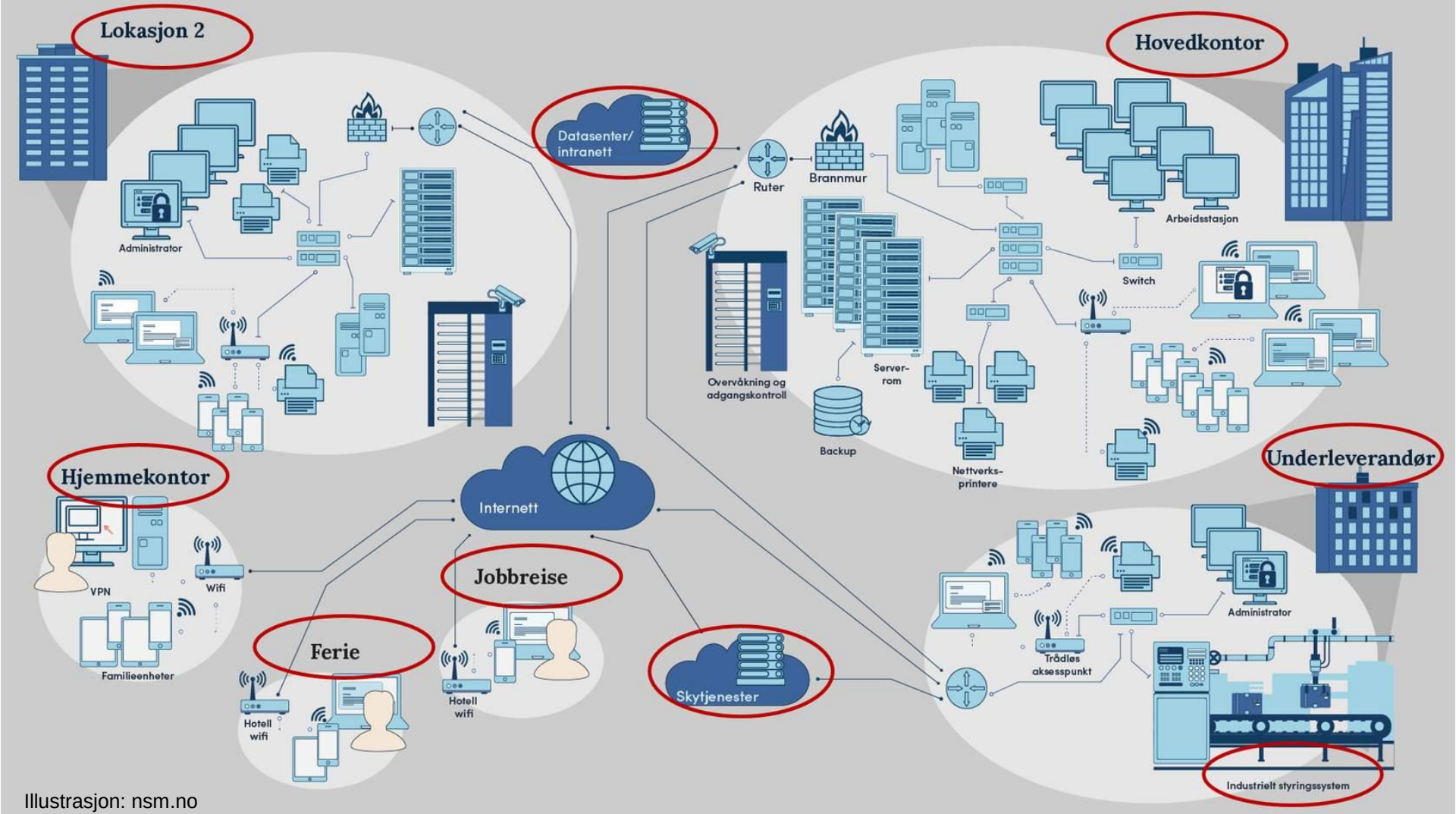
UiO : Institutt for informatikk

Dagens trusselbilde

- Trusselbilde:
  - Fra global pandemi til krig i Europa
  - Stadig mer komplekse systemer og teknologier
  - Stadig mer komplekse digitale verdikjeder
- Hva:
  - Tjenestenektangrep
  - Digital svindel og utpressing
- Hvordan:
  - Programvare-sårbarheter:
    - Egen programvare
    - Leverandørkjeder: Microsoft Exchange, Atlassian Confluence Apache Log4j, Kaseya VSA, SolarWinds6
  - Phishing



Kilde: Nasjonalt digitalt trusselbilde 2022 (NSM, oktober 2022)



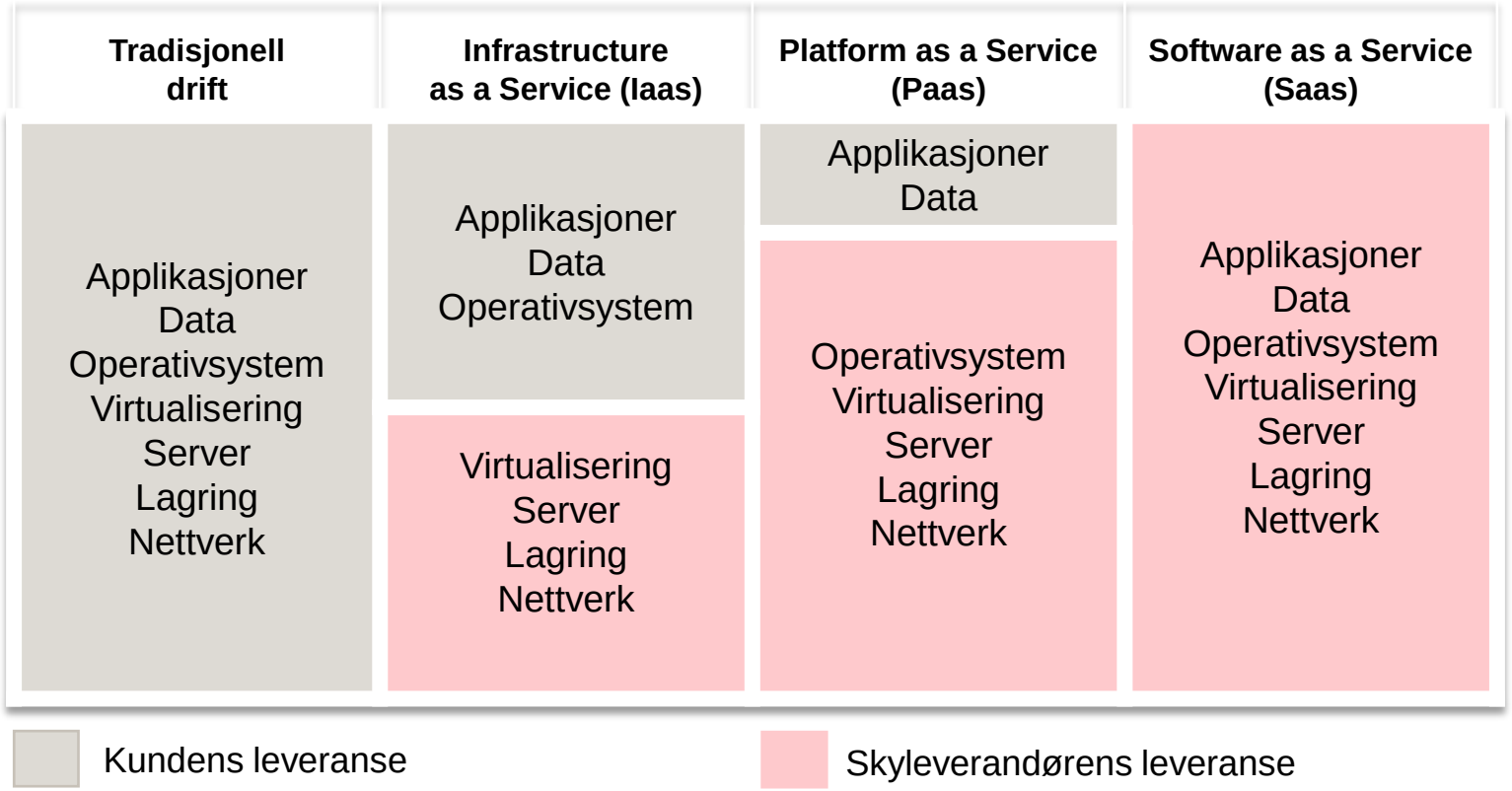
Illustrasjon: nsm.no


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

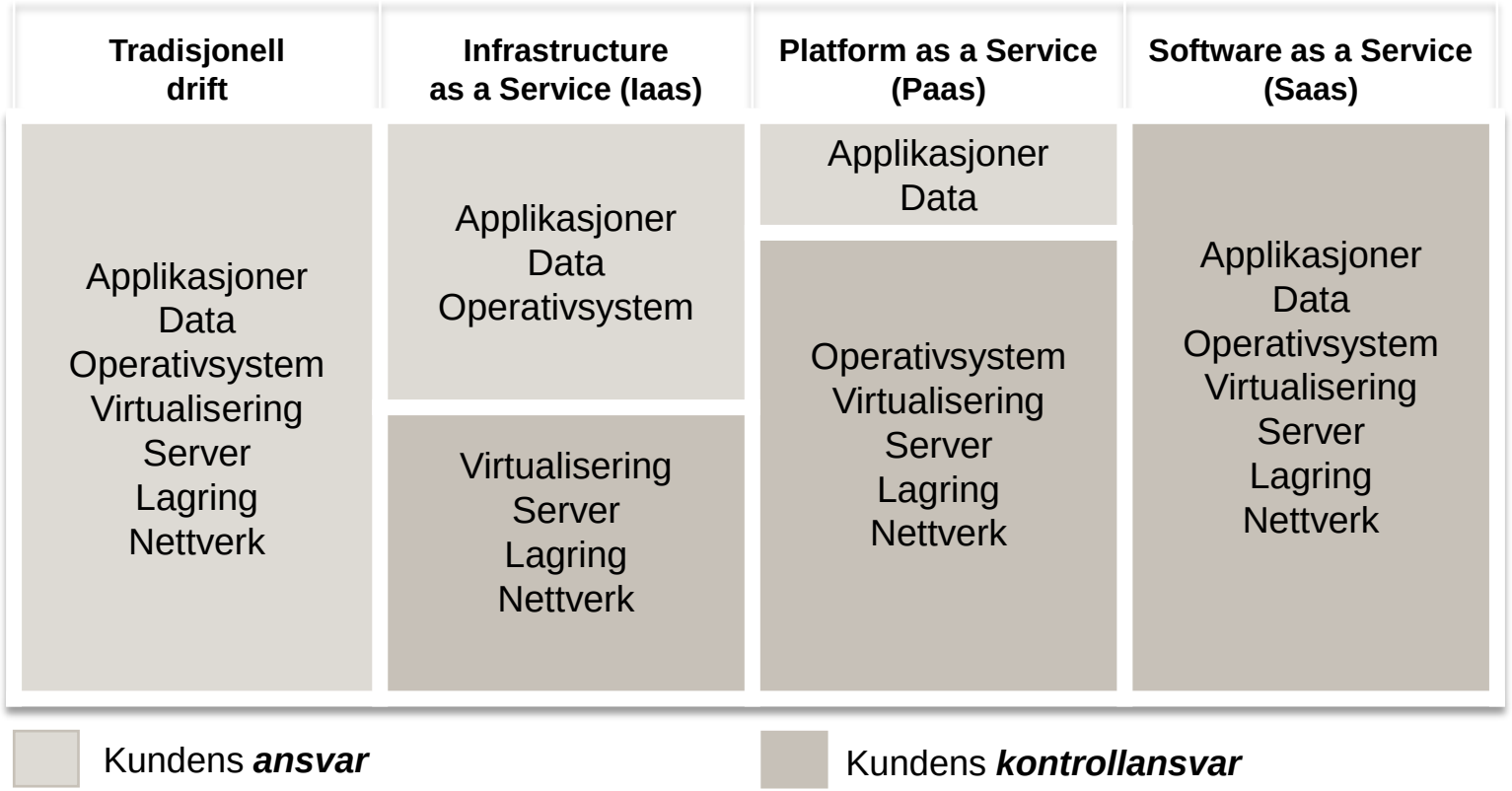
Tjenesteutsetting

- Tjenesteutsetting innebærer å sette ut en eller flere funksjoner/tjenester til andre leverandører – *underleverandører*.
- *Skytjenester som modell* innebærer å få tilgang til *et sett med dataressurser:*
  - 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 et smart trekk?

- 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

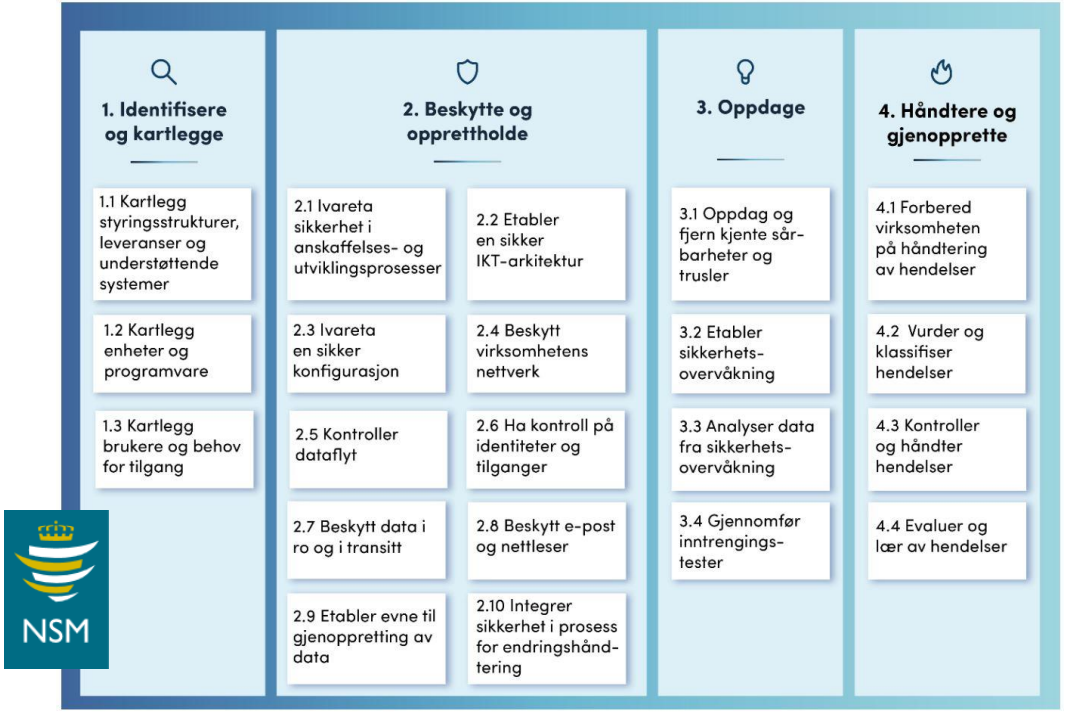
Datatilsynet har vedteke å gje Ålesund kommune eit overtredelsesgebyr på 50 000 kronar for deira bruk av treningsappen Strava.

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.

Behov for systematisering

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

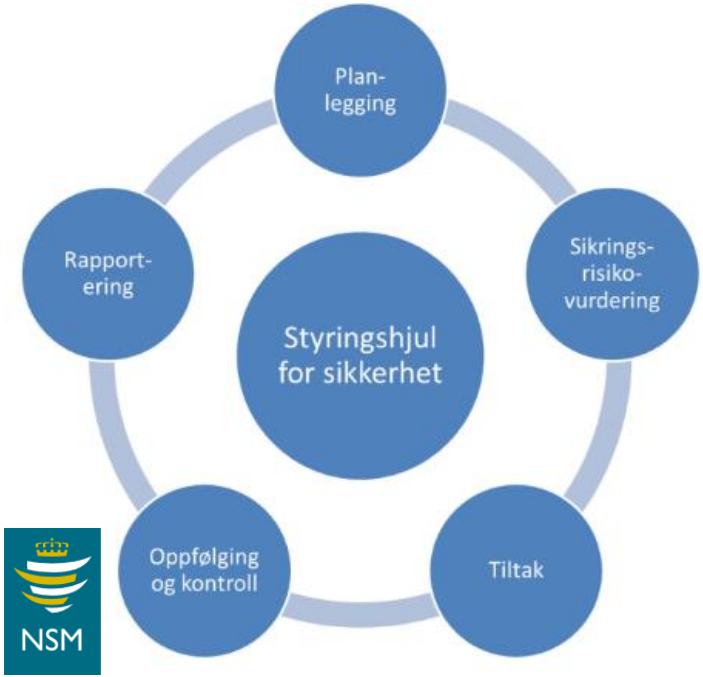


https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/

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



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

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.

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

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.

Nok en historie fra virkeligheten

Forbrukerrådets testet GPS-klokker beregnet på barn:

Alvorlige sikkerhetsbrister
Fremmede kan med enkle grep ta kontroll over klokkene for å spore, avlytte og kommunisere med barnet. Det er også mulig for uvedkommende å spore hvor barnet beveger seg eller gi inntrykk av at barnet er et annet sted. Data sendes og oppbevares også ukryptert.

- Utfordringer:
  - Uvedkommende kunne enkelt få tilgang til andre brukeres opplysninger.
  - Fremmede kunne med enkle grep ta kontroll over klokkene.
  - Personopplysninger ble sendt ukryptert.

- Tydelig mange på kunnskap og bevissthet.

Risikovurdering og tusselmodellering

- Behov:
  - Tidlig håndtering av sikkerhetsproblemer
  - Gjøre bedre risikovurderinger
  - Mer effektiv sikkerhetstesting

- Trusselmodellering består i å identifisere, analysere og beskrive relevante angreps-scenarier:
  - Utfordringen er å identifisere relevante trusler
  - Tenk: Hva kan skje? Hvordan kan våre verdier skades? Hvem kunne være interessert i å skade oss?

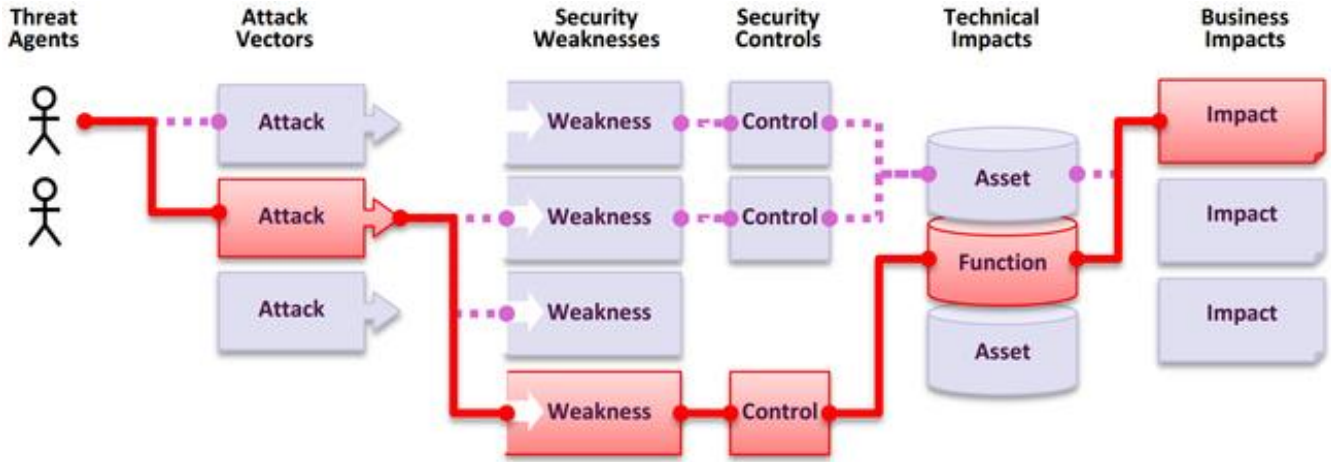
Trusselmodellering

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: 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?

Risikoanalyse

Hvilke **to hovedelementer** er sentrale når det skal gjennomføres en risikoanalyse av et IT-system?
Velg to alternativer:

- [ ] Sannsynlighet for en hendelse
- [ ] Mulige rootkit
- [ ] Konsekvens av en hendelse
- [ ] Verdibasert trusselidentifikasjon
- [ ] Angrepsvektor som benyttes

Refleksjoner til slutt

- Brukervennlighet versus sikkerhet
- Fremmedgjør vi datasikkerhet?
- Håndtering av sikring og hendelser: Åpenhet versus lukkethet
- Hvordan etablere god sikkerhetskultur i organisasjoner og samfunn?
- Neste krav: Universell utforming (UU) og *tilgjengelighetserklæring*

Dagens læringsmål

- Kjenne til hovedprinsipper i EUs personvernforordning gjennomgått på forelesning.
- Forstå sammenhengen mellom personvernregelverk og krav til informasjonssikkerhet.
- Kjenne til sikkerhetsutfordringer knyttet til tjenesteutsetting.
- Vite hva *skadevare* er, kjenne ulike typer skadevare og hva som kjennetegner dem.
- Forstå viktigheten av at datasikkerhet er 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 nytten 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/

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