

UiO : Institutt for informatikk

Å skape trygge digitale tjenester krever innsats.

IN1020 – Introduksjon til datateknologi

23.09.2026

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: Å skape trygge digitale tjenester krever innsats

Ressurser:

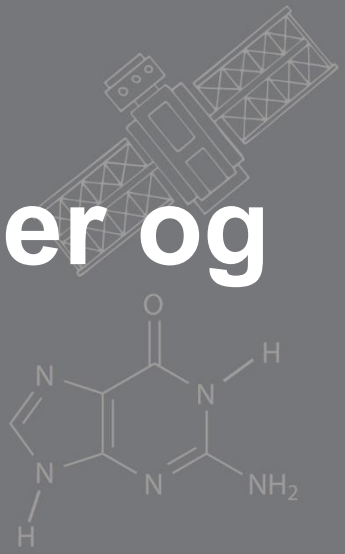
- Forelesning 23.09.26
- Ukeoppgaver og pensumlitteratur
  - Jøsang: Kap. 11: s.271-273,
    17.4, 18.4, 19: s.451-466

Nøkkelord:

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

Lovpålagte rammer og krav





Innebygd personvern (GDPR 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

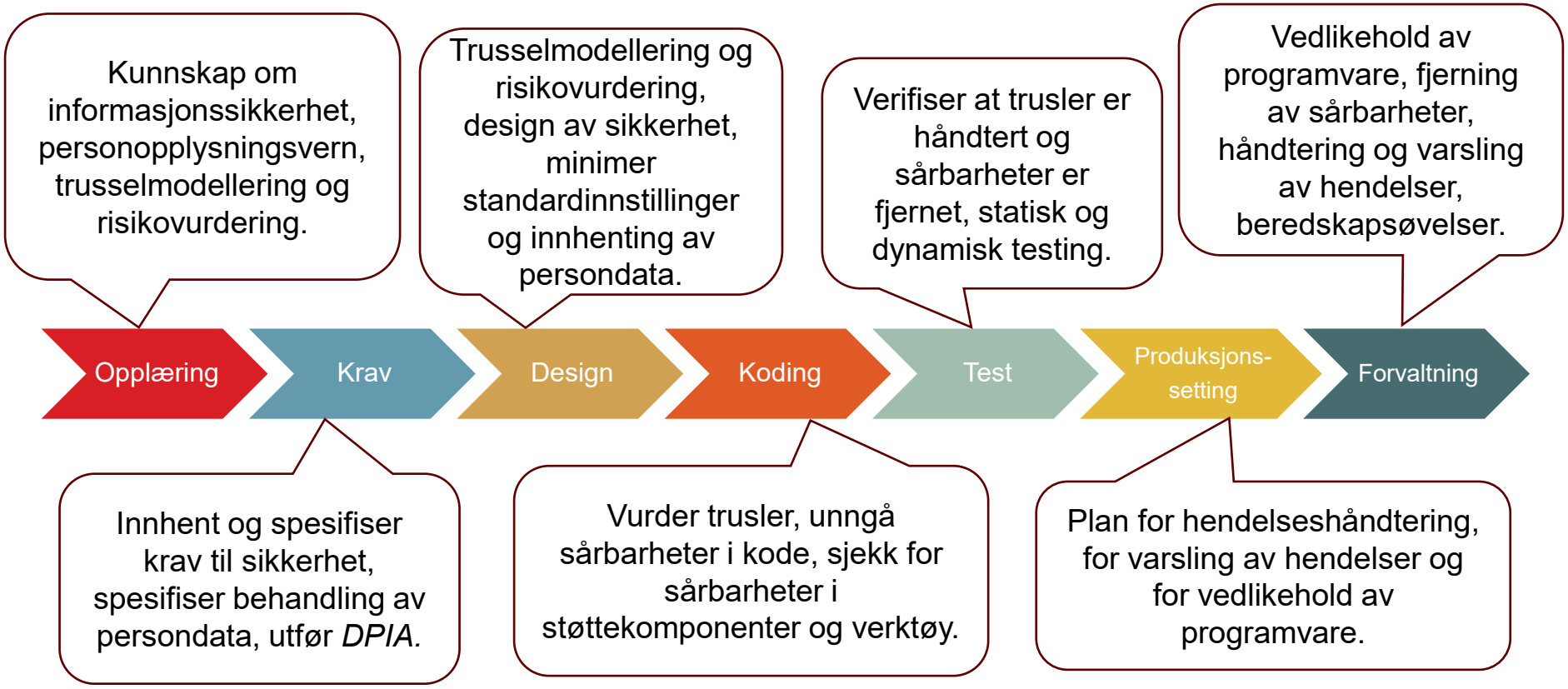
Sikkerhet ved behandlingen (GDPR artikkel 32)

- 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 og personvern



OWASP Top 10:2025

https://top10.owasp.org/2025/

1. **A01 Brudd på tilgangskontroll:** Brukere kan få tilgang til eller endre data og funksjoner utenfor sine tildelte rettigheter. Kategorien omfatter også *Server-Side Request Forgery*, SSRF.
2. **A02 Feilkonfigurering av sikkerhet:** Systemer er feil konfigurert, for eksempel ved bruk av standardpassord eller manglende *security headers*.
3. **A03 Feil i SW-leveransekjede:** Kategori som dekker risiko knyttet til byggeverkøy, pipeline, containere og avhengigheter.
4. **A04 Kryptografiske feil:** Sensitive data, som passord eller finansielle opplysninger, mangler tilstrekkelig kryptering.
5. **A05 Injeksjon:** Upålitelig inndata behandles av applikasjonen som kode eller kommandoer.
6. **A06 Usikker utforming:** Svakheter som skyldes manglende eller utilstrekkelig sikkerhetsplanlegging fra starten av.
7. **A07 Autentiseringsfeil:** Svake innloggingsmekanismer, problemer med sesjonshåndtering eller manglende flerfaktorautentisering.
8. **A08 Feil knyttet til programvare- eller dataintegritet:** Oppdateringer av kode eller infrastruktur mangler kontroll av integritet for å avdekke manipulering.
9. **A09 Feil i sikkerhetslogging og varsling:** Mangler i overvåking eller logging som forsinker oppdagelsen av sikkerhetsbrudd.
10. **A10 Feilhåndtering ved ekstraordinære tilstander:** Kategori som retter søkelyset mot mangelfull feilhåndtering og sikkerhetshull ved systemunntak.

Eksamensoppgave

Personopplysningsvern

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

Hvilken gruppe har Personopplysningsloven størst konsekvens for?

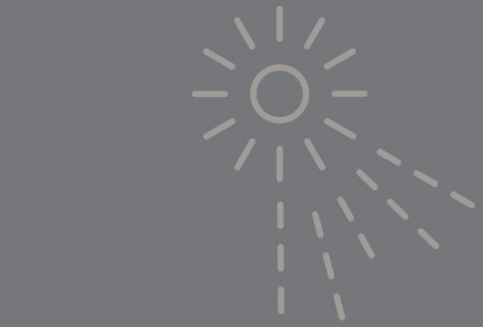
Velg ett alternativ.

- ○ Enkeltpersoner (de registrerte)
- ○ Virksomheter
- ○ Kriminelle

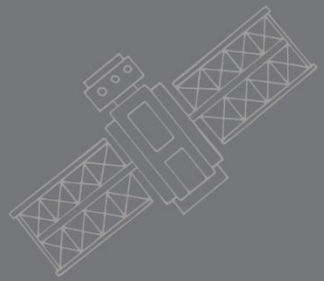
Hva med annen type informasjon?

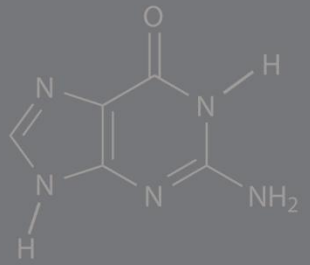
Foreløpig få lovpålagte krav til informasjonssikkerhet generelt. Noe finner man dog i lovverk rettet mot spesifikke bransjer/forvaltningsorganer:

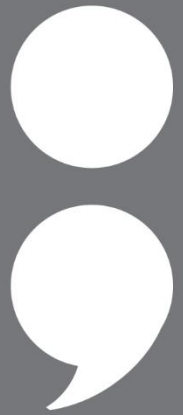
- Sikkerhetsloven (nasjonal sikkerhet)
- Digitalsikkerhetsloven - sikre grunnleggende krav til digital sikkerhet i virksomheter md særlig betydning i sammfunnet.
- Forskrift om IT-standarder i offentlig forvaltning
- eForvaltningsforskriften (elektronisk kommunikasjon i forvaltningsorganer)
- Lov om elektronisk kommunikasjon (ekomloven)
- Også flere EU (EØS)-direktiver under arbeid.











Sikkerhetsstyring

- Systematisk datasikkerhet



UiO : Institutt for informatikk

Dagens trusselbilde

Kilde: Risiko 2026, https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2026

Bakteppe:

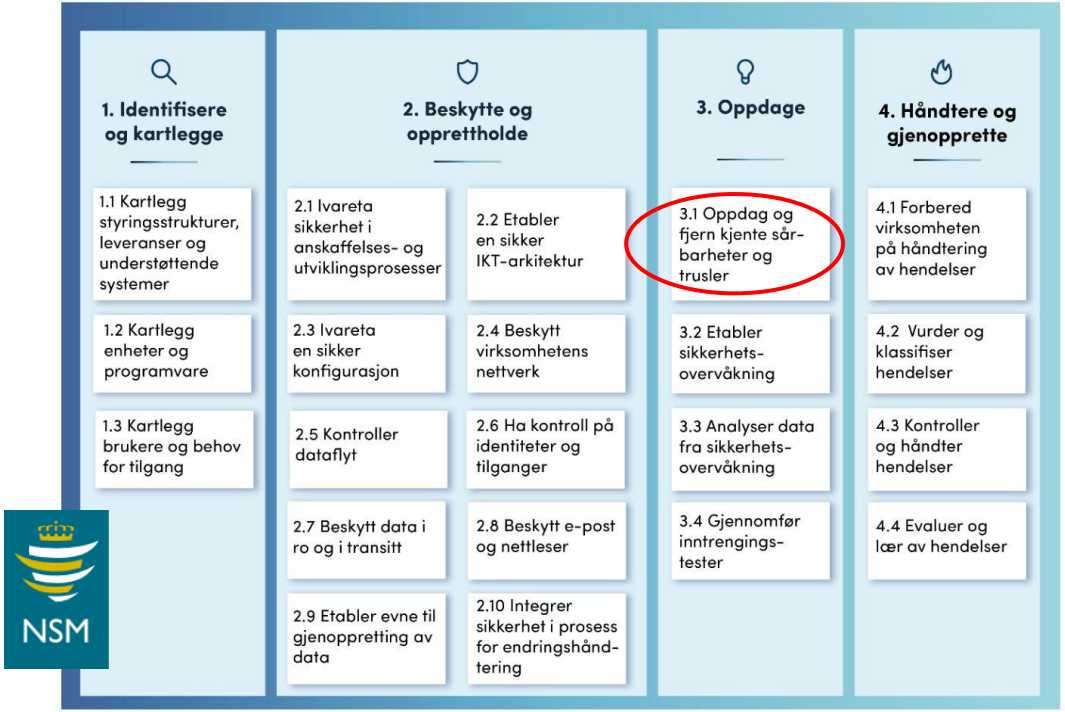
- Stormaktsrivalisering
- Forholdet USA - Europa er i endring
- Krig og konflikt rammer flere kontinenter
- Norges rolle som forsvarsleverandør til Ukraina
- Kinesisk kontroll i verdikjeder
- Rask teknologisk utvikling (bl.a. KI)
- Konsentrasjonsrisiko

Trender:

- Innsidevirksomhet
- Sosial manipulasjon med bruk av KI som støtteverktøy
- Løsepengeangrep og «dobbel utpressing»
- Tjenestenektangrep
- Angrep rammer bredt, på tvers av sektorer

Behov for systematikk og rammeverk

- Rammeverk for informasjonssikring:
  - Svært mange ulike rammeverk
  - NSMs grunnprinsipper for informasjonssikkerhet er tilpasset norske forhold.



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

Kjente sårbarheter?

Abonner og følg med på varslinger:

- Varsler fra NSM: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/
- Varsler fra CVE: https://www.cve.org/
- NIST NVD: https://nvd.nist.gov/
- European union vulnerability database: https://euvd.enisa.europa.eu/

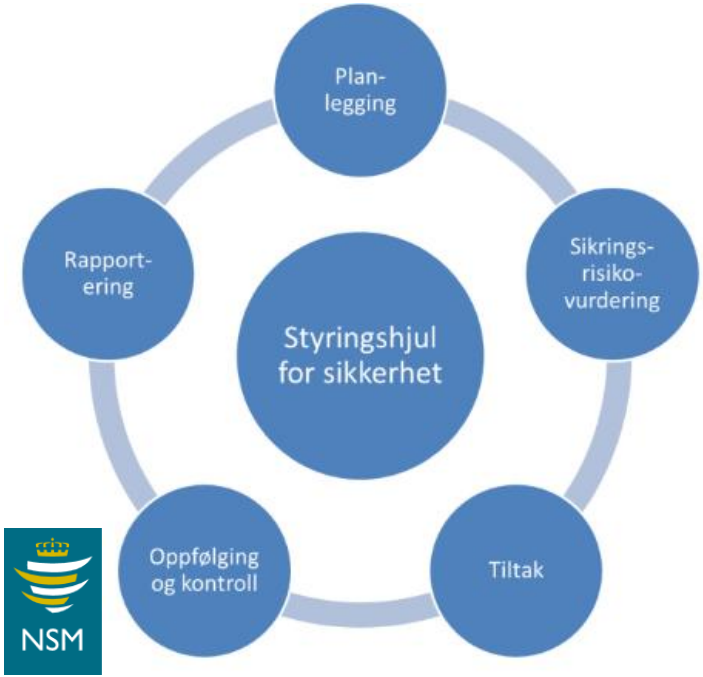
Håndtere lange leveransekjeder:

- Må ha system for oversikt over avhengigheter: SBOM

Behov for systematisk styring

*«**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

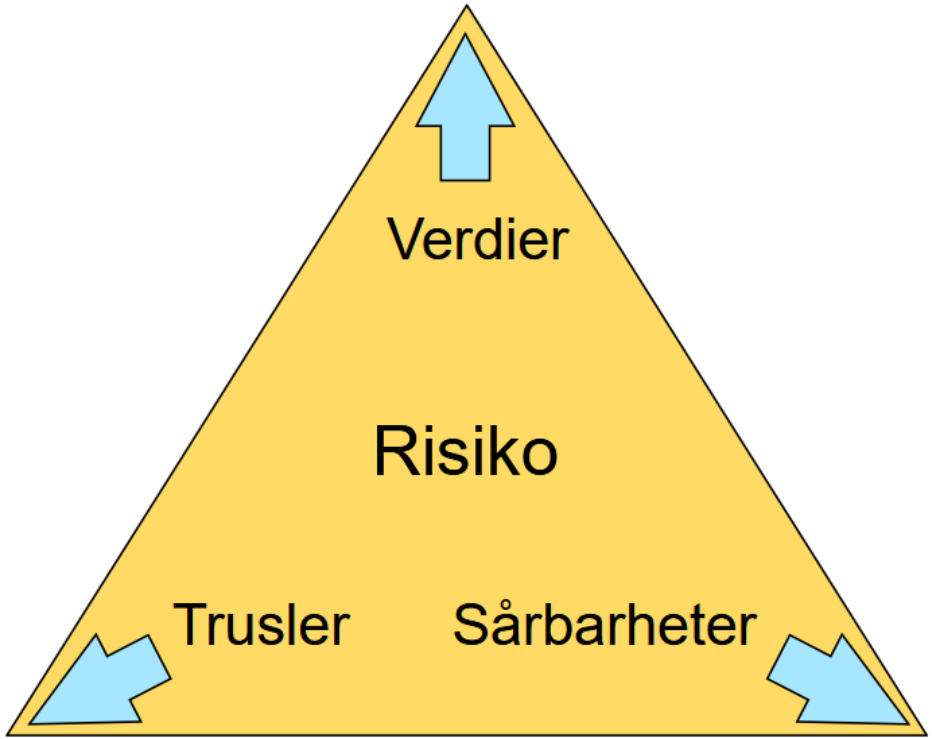


Å identifisere trusler og risiko

Ønsker oss:

- **Tidlig innsats:** Forebygge og håndtere sikkerhetsproblemer tidlig
- **Bedre forståelse:** Gjøre gode risikovurderinger
- **Tiltak som fungerer:** Effektiv sikkerhetstesting

Risiko



Trusselmodellering

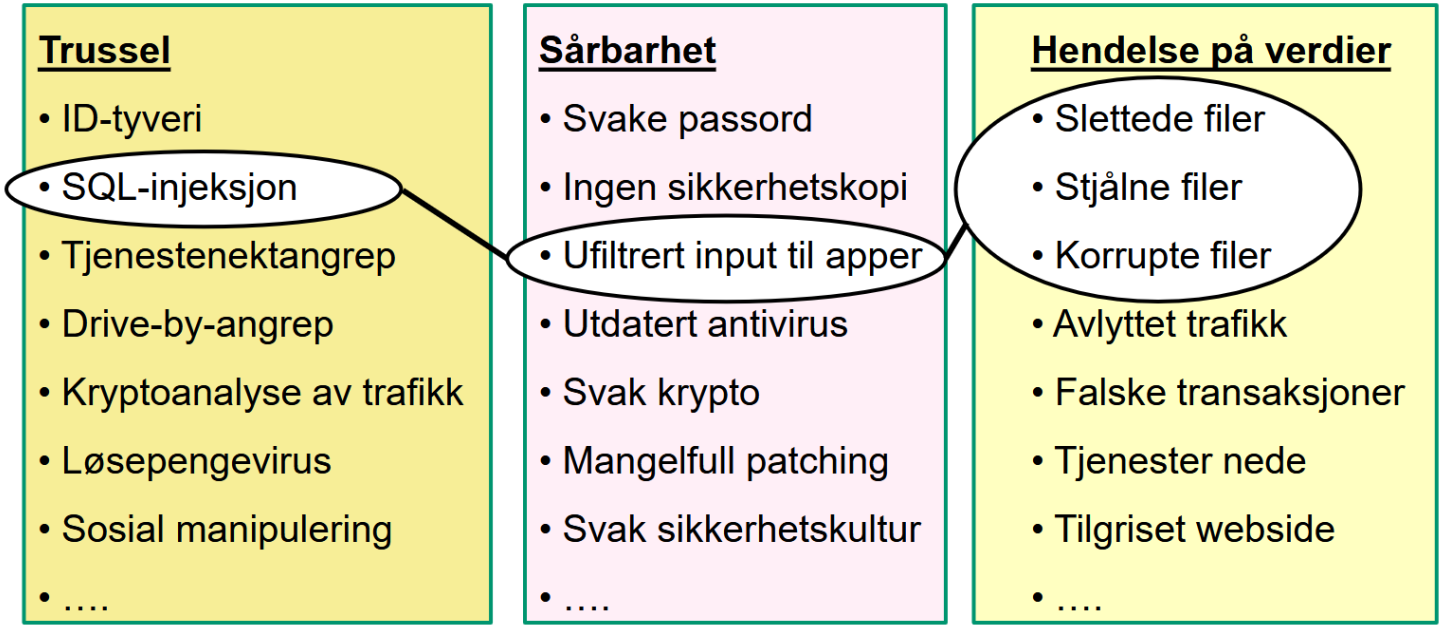
Trusselmodellering består i å identifisere og beskrive relevante angreps-scenarier. Ulike innfallsvinkler:

- Fokus på **trusler og trusselaktør**
  - Identifisere trusselaktørens mål, hvordan går de fram for å oppnå dem, hva er angrepsvektor og angrepsflate.
- Fokus på **sårbarheter**
  - «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».

Risikoidentifisering

Å identifisere en risiko betyr å finne en relevant kombinasjon av en trussel, sårbarhet(er) og hendelse(r) som kan skade verdier.



Risikoanalyse

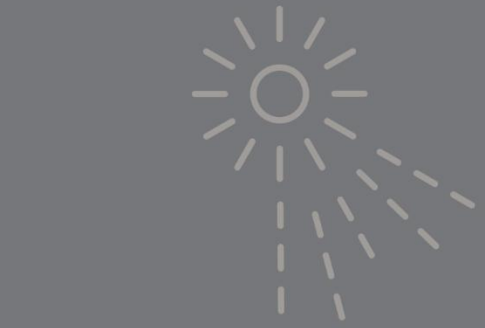
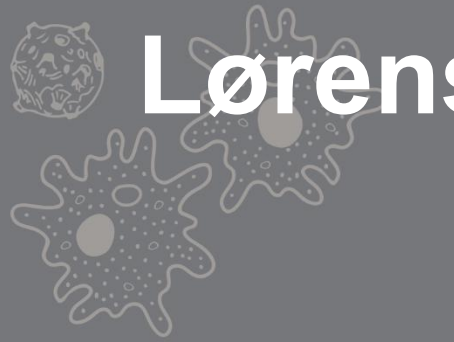
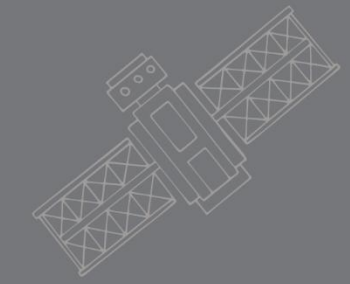
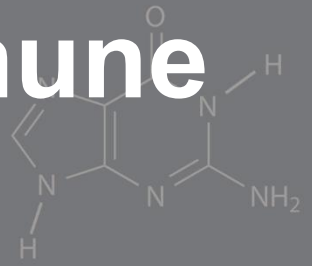
- Risiko involverer *konsekvens* (f.eks. målt i kroner og øre).
- Praktisk risikoanalyse vurderer vanligvis to faktorer for å bestemme nivået på hver risiko
  - Sannsynlighet (snarhet/frekvens) av hver type hendelse
  - Konsekvens for verdier som følge av hver type hendelse
- Hvor skal innsatsen legges?
  - Usannsynlig hendelse som medfører store tap?
  - Sannsynlige hendelser som har lavere kostnad?

Nr.	Risikoelement	Sårbarhet / svakhet	Eksisterende beskyttelses tiltak	Eksisterende kontrolltiltak	K I T	Sannsynlighet	Konsekvens	Risikonivå
5	Uvedkommende får tilgang pga. passord på avveie.	Usikker oppbevaring av passord, passord som brukes på flere systemer. Lite komplekse passord.				1	4	4
6	Data kommer på avveie pga. utro tjener blant driftspersonell	Dårlig opplæring/sjekk av driftspersonell. Konsulenter med for mye tilgang, for mange med systemtilgang.				1	4	4
7	Data eksponeres for mye pga. for mange med systemtilganger	Lite granulerte system/drift tilganger				2	2	4
8	Data kommer på avveie pga. ekstern tilgang for leverandør eller konsulent	Tilganger er gitt til eksterne for oppsett, drift eller feilsøking. Ikke tilstrekkelig sikring og kontroll med hva som utføres av arbeid.	Benytte FUDO for fjerntilgang			2	3	6
9	Passord lagres i løsningen	Benytter ikke felles innloggingsmekanismer som AD, FEIDE, Weblogin el.l.						0
10	Systemet blir ødelagt pga. hendelse i datarom (brann, vann osv.)	System plassert i ett serverrom. Dårlig sikring av serverrrom.				1	4	4
11	Systemet kan ikke gjenopprettes etter feil / krasj	Manglende backup av systemet. Ikke testet backup.				2	4	8
12	Data kommer på avveie via backup eller gammel kopi.	Manglende kontroll av lagringstid på backup. Ikke rutiner for destruksjon av data når systemet legges ned eller oppgraderes.				1	4	4

Risikovurdering og risikohåndtering – hvem gjør hva?

Ledelse, eiere, brukere og fageksperter må samarbeide:

- Eiere av verdier må hjelpe til med å
  - lage oversikt over verdier, og spesifisere sikkerhetsmålsettinger (KIT+P),
  - vurdere konsekvens av brudd på sikkerhetsmål.
- Brukere og sikkerhetseksperter må hjelpe til med å
  - identifisere trusler og sårbarheter,
  - vurdere sannsynligheter.
- Risikoeksperter må veilede risikoanalyseprosessen
  - Sikkerhetseksperter må gi råd om sikkerhetstiltak.
  - Ledelsen må gjennomgå risikostyringsprosessen og godkjenne budsjett for foreslåtte sikkerhetstiltak.

Lørenskog kommune

UiO : Institutt for informatikk

Utsatt for datainnbrudd våren 2026

«Tirsdag 7. april gjennomførte en ansatt et vanlig internettsøk. I søkeresultatene lå en nettside som fremsto som legitim, og den ansatte klikket seg inn og lastet ned en fil derfra. Filen inneholdt skadevare, som ga kriminelle hackere tilgang til den ansattes PC.»

Lørenskog kommune

Resultat:

- Nedetid for kommunens IT-tjenester
- Virksomhetskritiske opplysninger på avveie
- Sensitive personopplysninger på avveie

Angrepsvektor



7. april:

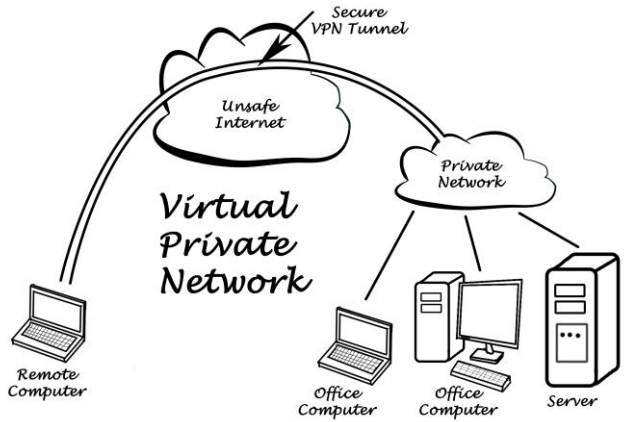
- SEO-forgiftning (SEO poisoning, også kalt search poisoning).
- Brukeren lastet ned en .zip-arkiv, inneholdt fila ‘FULL DOCUMENT .js’
- Bruker dobbeltklikket på fila for å åpne den.
- Startet *Javascript*, som lastet ned og kjører *Powershell-script* fra nett, som igjen etablerte en *«command&control» (C2) server*. Server ble rigget for *persistens.*

10. april og 22. april:

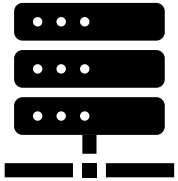
- To nye script ble lastet ned og kjørt, etablerte to nye «command&control» (C2) servere, også rigget for *persistens.*

Eskalering

Kompromittert maskin er en laptop med VPN inn til kommunens nett, og angriper kommer seg dermed fra klient til innsiden av kommunens LAN.



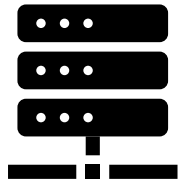
Angrepsvektor forts.



13. april – 8. mai:

- Forsøk på *kerberoasting*, men mislykkes
  Bruker (på vegne av angriper) ber om «ticket» til servicebruker, ticket er kryptert med passordet til servicebrukeren som nøkkel. Laster ned ticketen og forsøker knekke kryptering vha *brute-force*.
- Forsøker utnytte *ESC1-sårbarhet*, og lykkes
  Bruker (på vegne av angriper) ber om sertifikat for admin, og får dette. Bruker gis samme rettigheter som admin har…
- Hacker beveger seg vertikalt til kommunens *SCCM-server*, installerer skadevare som spres videre til andre servere inkludert *domenekontroller*.
- Hackere henter ut 1,8 TB data (1,3 millioner filer).

Når oppdages angrepet?



8. mai:

- Angriper starter kryptering av IT-systemer

9. mai:

- Angrepet oppdages når ansatte ikke får tilgang til systemene.
- Umiddelbart tiltak: Alle kommunens nettverk og systemer stenges ned.
- Kommunen setter krisestab.
- Kommunen varsler politi, Datatilsynet og Nasjonal sikkerhetsmyndighet (NSM).

6. juli:

- Hackere publiserte oversikt over filområder de har hatt tilgang til og hentet ned.

Konsekvens for kommunen

Lørenskog kommune

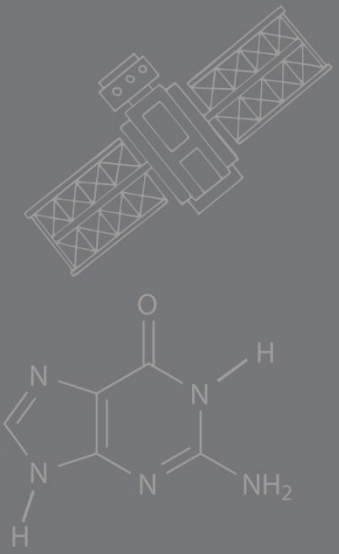
Kostnader og ressursbruk

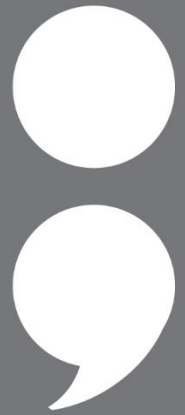
- **Direkte anslag:** Beregnet til 25 millioner kroner.
- **Ressursbruk:**
  - Store personell- og IT-ressurser bundet opp til feilretting.
  - Etablering av innsynssenter
- **Konsulentbruk:** Utgifter til ekstern granskning og sikring (blant annet Deloitte)
- **Overtredelsesgebyr fra Datatilsynet?**

https://www.lorenskog.kommune.no/it-hendelse/
https://www.lorenskog.kommune.no/it-hendelse/uavhengig-gjennomgang-etter-dataangrepet/rapporten-fra-deloitte/

Administrativ datasikkerhet







UiO : Institutt for informatikk

God informasjonssikkerhet koster

Budsjett og ressurser til:

- ✓ Kompetanse og bevissthet
- ✓ Styring og kontroll
- ✓ Drift og vedlikehold
- ✓ 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.

Datatilsynet

«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/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2022/overtredelsesgebyr-til-ostre-toten-kommune/

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 omdømme, merkevare

Informasjonssikkerhet er et viktig bidrag til konkurransefortrinn og å øke selskapets verdi.

Administrative sikkerhetstiltak

Hvorfor går det galt?

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

Hvilke tiltak kan gjøres?

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

Læringsmål for økten

- Forstå sammenhengen mellom personvernregelverk og krav til informasjonssikkerhet.
- 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, risikovurdering og risikoanalyse innebærer, samt nytteverdien av gjennomføring.
- Vite hva et administrative sikkerhetstiltak er, og kjenne tiltakene nevnt i undervisningen.

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

Nyttig lesestoff og ressurser

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-og-personvern-som-standard/
- Lov om behandling av personopplysninger: https://lovdata.no/dokument/NL/lov/2018-06-15-38
- Publikasjoner fra Nasjonal sikkerhetsmyndighet: https://www.nsm.no/publikasjoner/

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/
- 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)
  - 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

