

# Cybersikkerhet for laboratorier

De «nye» truslene og hvordan forbereder og bygger  
vi motstandsdyktige organisasjoner?

**Aleksander Lygren Toppe**

Senioringeniør, Risiko og Security

IFE Cybersikkerhetssenter i Halden



# IFEs Cybersikkerhetscenter

- Etablert cybersikkerhetscenter i mai 2019.
- Kombinere IFEs forskning og utvikling på tvers av kompetanse områder fra **risikostyring, sikkerhet (logisk/fysisk), prosesseteknikk og menneskelige faktorer**.
- Forskning på **cyber-motstandsdyktighet** i organisasjoner og samfunn.
- Tilby fasiliteter og kompetanse for å undersøke **cybersikkerhetstrusler** mot IT og operasjonelle teknologier (OT), og å evaluere beskyttelsesmekanismer.
- Gi et **realistisk miljø** for å **studere** hvordan **mennesker, prosesser og teknologi** samhandler og sammen kan gi helhetlige løsninger for å **håndtere cyberangrep effektivt**.
- Tilbyr en rekke **industrielle enklaver** ved hjelp av **Hardware-in-the-Loop (HiL)** og simulering.



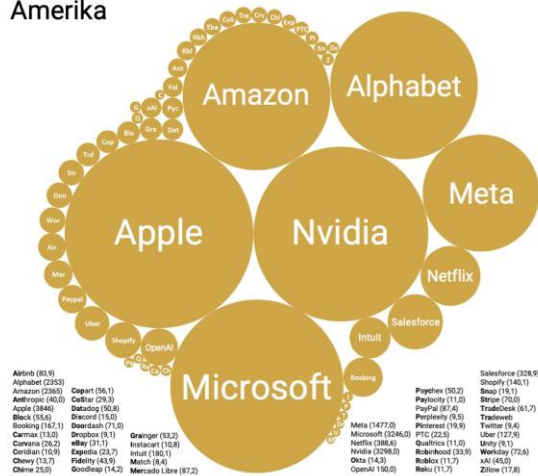
Foto: IFE



# Geopolittikk, innovasjon, data og digitale grenser

## Top-100 Plattformen der Welt

### Amerika

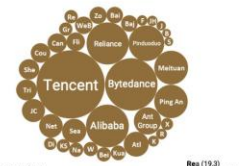


Quelle: Holger Schmidt / Hamidreza Hosseini, 2025

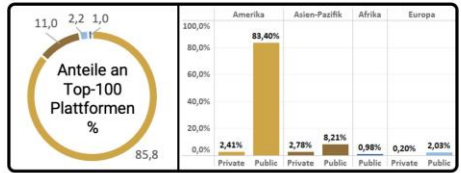
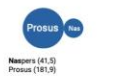
### Europa



### Asien-Pazifik



### Afrika



Börsenwert / Bewertung jüngste bekannte Finanzierung  
Gesamtwert 22,67 Billionen Dollar  
Einzelwerte (in Milliarden Dollar)  
Stand 20. Dezember 2024



Digitaliserings- og forvaltningsdepartementet

Handlingsplan

## Nasjonal sikkerhetsplan for digital infrastruktur

Elektronisk kommunikasjon i fred, krise og krig



[1] ECODynamics <https://www.netzoekonom.de/plattform-oekonomie/>

[2] EU: Mario Dragi rapport [https://commission.europa.eu/topics/eu-competitiveness/draghi-report\\_en](https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en)

[3] <https://www.digi.no/artikler/folger-noye-med-pa-dansk-microsoft-utfasing-ser-om-vi-kan-tenke-lik-i-norge/559422>

[4] Fremtidens digitale Norge [https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/no/pdfs/nasjonal-digitaliseringsstrategi\\_ny.pdf](https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/no/pdfs/nasjonal-digitaliseringsstrategi_ny.pdf)

[5] IT-leveranser er blitt et maktmiddel for Donald Trump | Digi.no

[6] Microsoft Gave FBI BitLocker Encryption Keys, Exposing Privacy Flaw

# Digital suverenitet – hvorfor er det viktig?

- Digital suverenitet er et begrep som beskriver et lands eller en virksomhets evne til å eie, kontrollere og beskytte sin digitale infrastruktur og data. [1]

Det handler om:

## – Eierskap

- Å ha kontroll over data, applikasjoner og infrastruktur – både fysisk og juridisk.
- F.eks. sørge for lagring av informasjonsverdier (data) i Norge eller EØS-land.

## – Sikkerhet og personvern

- Å sikre at sensitive opplysninger ikke blir utsatt for utenlandsk overvåking eller uautorisert tilgang [3].

## – Digital selvstendighet og råderett over egne data

- Å redusere avhengighet av utenlandske leverandører som kan pålegge egne lover og betingelser.
- "access to electronic communications, such as emails and social media posts, stored on servers and in data centers in foreign countries"[4]

## – Bevissthet rundt leverandør-lockin

- Valg av alternativer og åpenkildekode, ISO-standardiserte løsninger, og ha klare exit-strategier.

[1] Digital Suverenitet [https://www.nupi.no/content/pdf\\_preview/24942/file/NUPI\\_Policy\\_Brief\\_2\\_2022\\_deCarvalho.pdf](https://www.nupi.no/content/pdf_preview/24942/file/NUPI_Policy_Brief_2_2022_deCarvalho.pdf)

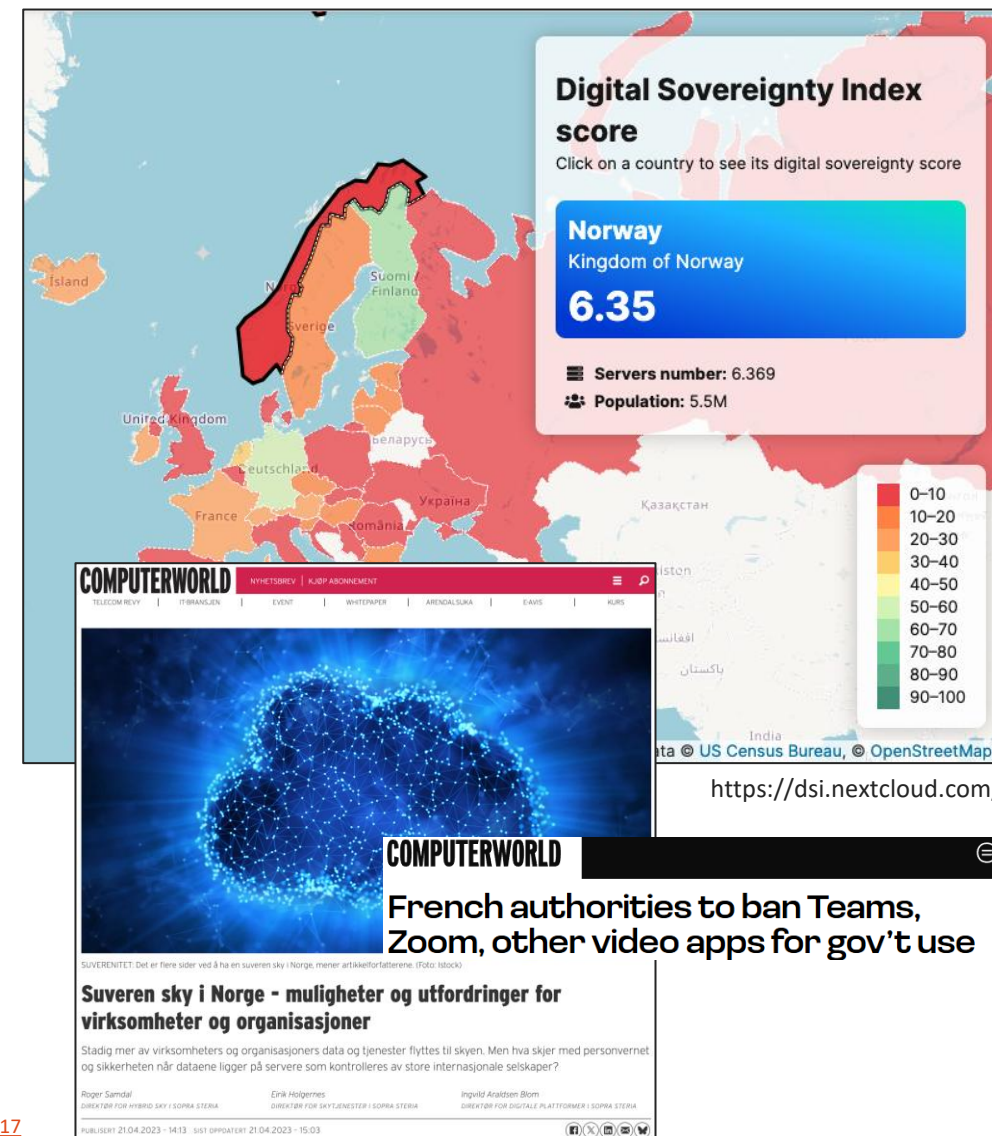
[2] Nasjonal sky <https://www.cw.no/debatt-sopra-steria/suveren-sky-i-norge-muligheter-og-utfordringer-for-virksomheter-og-organisasjoner/2128717>

[3] Nasjonal kontroll av IKT tjenester <https://nsm.no/getfile.php/1313327-1696336231/NSM/Filer/Dokumenter/Rapporter/Nasjonal%20kontroll%20av%20IKT-tjenester.pdf>

[4] CLOUD Act <https://www.congress.gov/crs-product/R45173>

[5] French authorities to ban Teams, Zoom, other video apps for gov't use – Computerworld

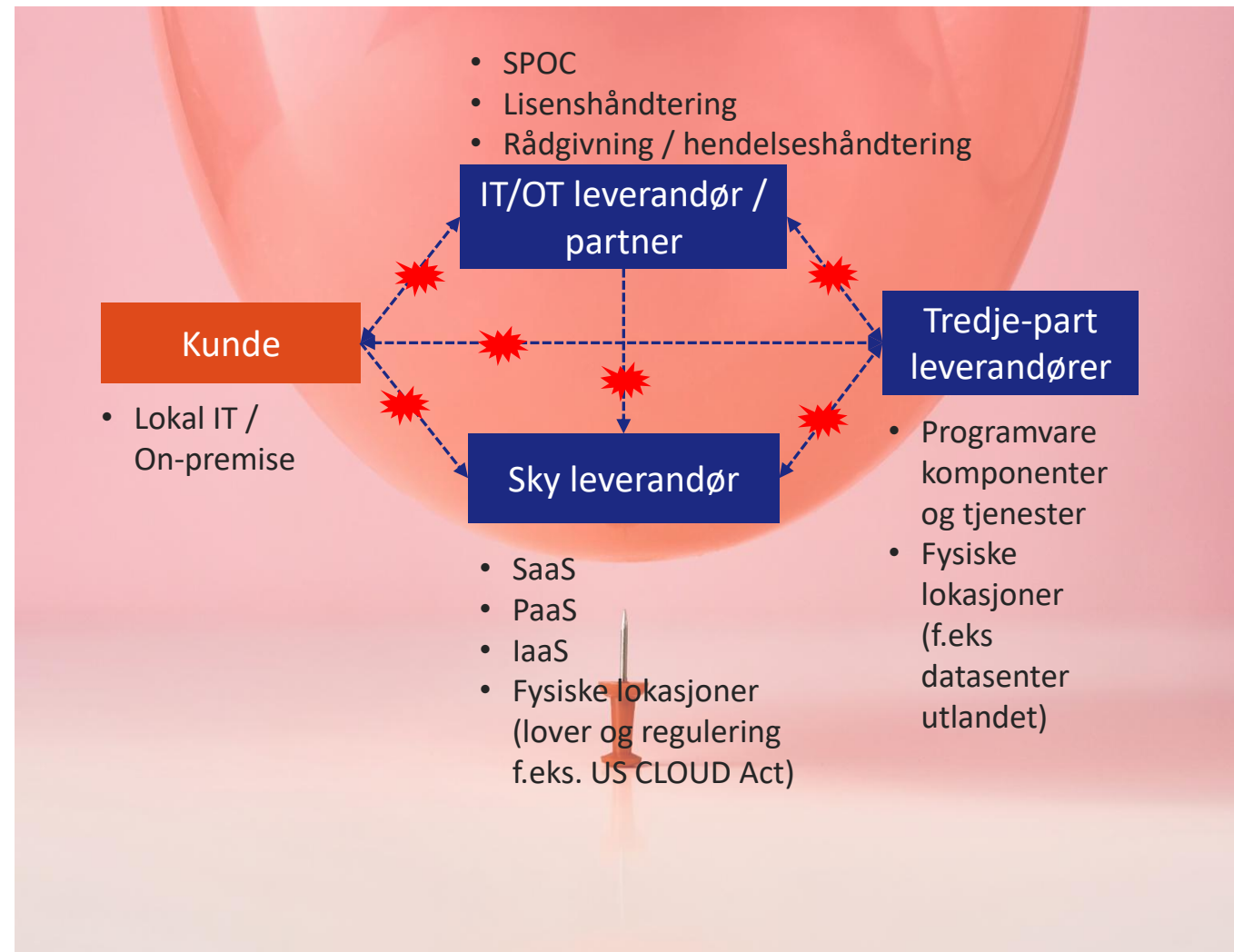
# 4



## Uoversiktelig og utfordrende?

Noen sentrale faktorer vi må ta hensyn til <sup>[1]</sup>:

- IT systemer **endrer seg over tid**.
- Når verdier endres, endres også risiko – justere Verdi
- Sårbarheter endres ved at:
  - nye **sårbarheter gjøres kjent...**
  - ny **teknologi** innføres...
  - nye **angrepsmåter** introduseres...
- Trusler endres:
  - trussellandskapet er i **kontinuerlig endring**
  - påvirkes av **ytre faktorer** som virksomheten **ikke** kan kontrollere eller gjøre noe med.



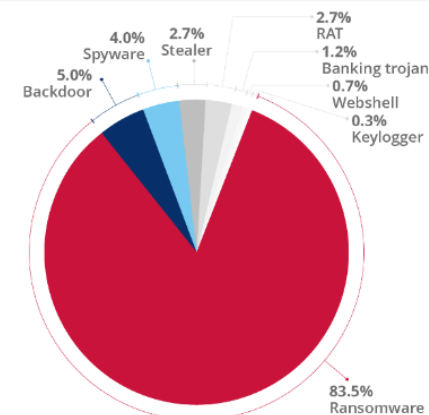
[1] <https://nsm.no/getfile.php/136603-1625054089/NSM/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf>

# De «nye» truslene og fokuset på kritisk infrastruktur

- **ENISA Threat Landscape 2025** (1. oktober) [1]
- Trusler mot kritisk infrastruktur konsekvenser **tilgjengelighet** og **integritet**
- Ransomware-as-a-service (RaaS) – **LockBit 5.0** (september 2025) [7]
  - Ny versjon - inneholder mer avansert maskerings- og anti-analyseteknikker.
  - Økt angrepsflate med krypteringsteknikker og funksjoner som fungerer på tvers av plattformer: **Linux, Windows og VmWare ESXi**.
- **Digitale angrep via leverandører** er den vanligste angrepsveien inn i digital infrastruktur. Kompromittering av leverandørkjeder [8].
- IoT Vulnerabilities
- Phishing Attacks – Avansert og sofistikert – bruk av K.I.
- Data Breaches

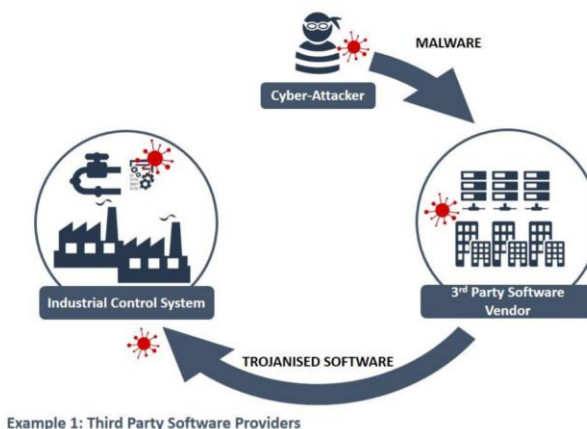


Fig. 3 - Distribution of identified malicious codes.  
Source: ENISA dataset



TLP: CLEAR

# 6



[1] ENISA Threat Landscape 2025 [https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025\\_0.pdf](https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf)

[2] <https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2026>

[3] <https://www.nsr-org.no/uploads/documents/Publikasjoner/Telenor-Digital-sikkerhet-2023.pdf>

[4] <https://www.skyradar.com/blog/eurocontrols-website-attack-and-ongoing-cybersecurity-implications#>

[5] <https://slashnext.com/blog/xanthorox-ai-the-next-generation-of-malicious-ai-threats-emerges/>

[6] <https://wormgpt.net/>

[7] <https://sosransomware.com/en/lockbit-en/lockbit-5-0-back-with-enhanced-cross-platform-capabilities/>

[8] KraftCERT 2025 <https://www.kraftcert.no/filer/KraftCERT-Trusselvurdering2025.pdf>

# Trusler og sårbarheter mot vann-systemer og laboratorier?

## Vannforsyning

- “...hovedmål for angrep som forstyrrer vannforsyningen og forringer vannkvaliteten – inkludert å hindre vannbehandling, ødelegge pumper og ventiler, og tilføre farlige kjemikalienivåer.” [1]
- [Vannkrise kan lamme næringslivet – Næringslivets Sikkerhetsråd](#)

## Laboratoriesystemer – målinger, analyse, systemintegrasjon

- Lab LIMS
  - Bruk av leverandører og tredjepartselskaper. Skytjenester – I Norge eller utlandet?
- Utstyr med særegne krav som kan påvirke security
- Operational security compliance for IT infrastructure.
- Forstå **kompetansegapet** i OT-miljø og cybersikkerhet, samt IT-miljøet og de faktiske kravene OT-systemer har (tilgjengelighet, sanntid, endringsmuligheter)[1]



[1] <https://www.idexcurrents.com/en/latest/cybersecurity-in-water-labs-and-utilities-requires-constant-vigilance/>

[2] Kripos temarapport: “Trusselen mot OT-avhengige virksomheter” 2025.

<https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2216.pdf>

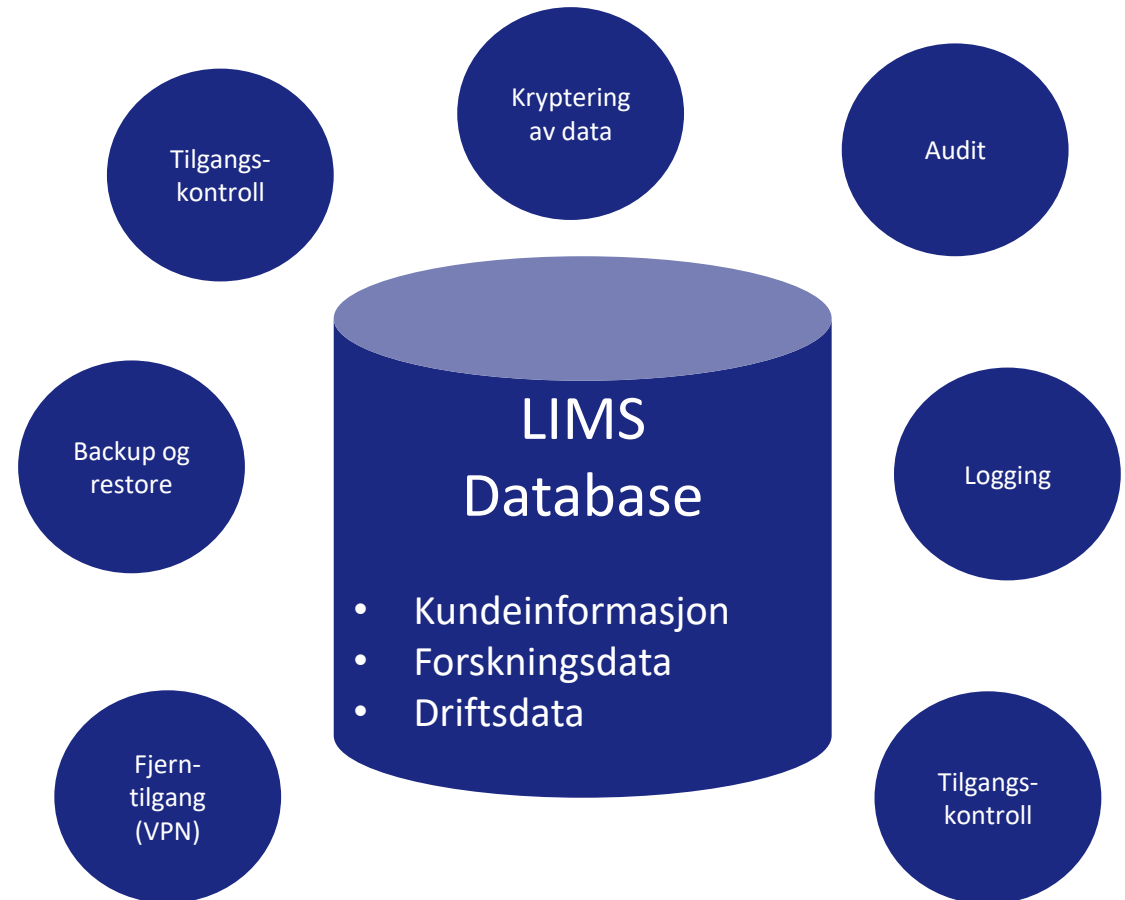
<https://www.lablynx.com/wp-content/uploads/2022/10/Article-Guide-to-Lab-Security-with-a-Laboratory-Information-Management-System.pdf>

<https://www.flickr.com/photos/worldbank/7157007243>

[https://en.wikipedia.org/wiki/Water\\_testing#/media/File:Broken\\_Bow\\_Water\\_Treatment\\_Facility\\_water\\_testing.jpg](https://en.wikipedia.org/wiki/Water_testing#/media/File:Broken_Bow_Water_Treatment_Facility_water_testing.jpg)

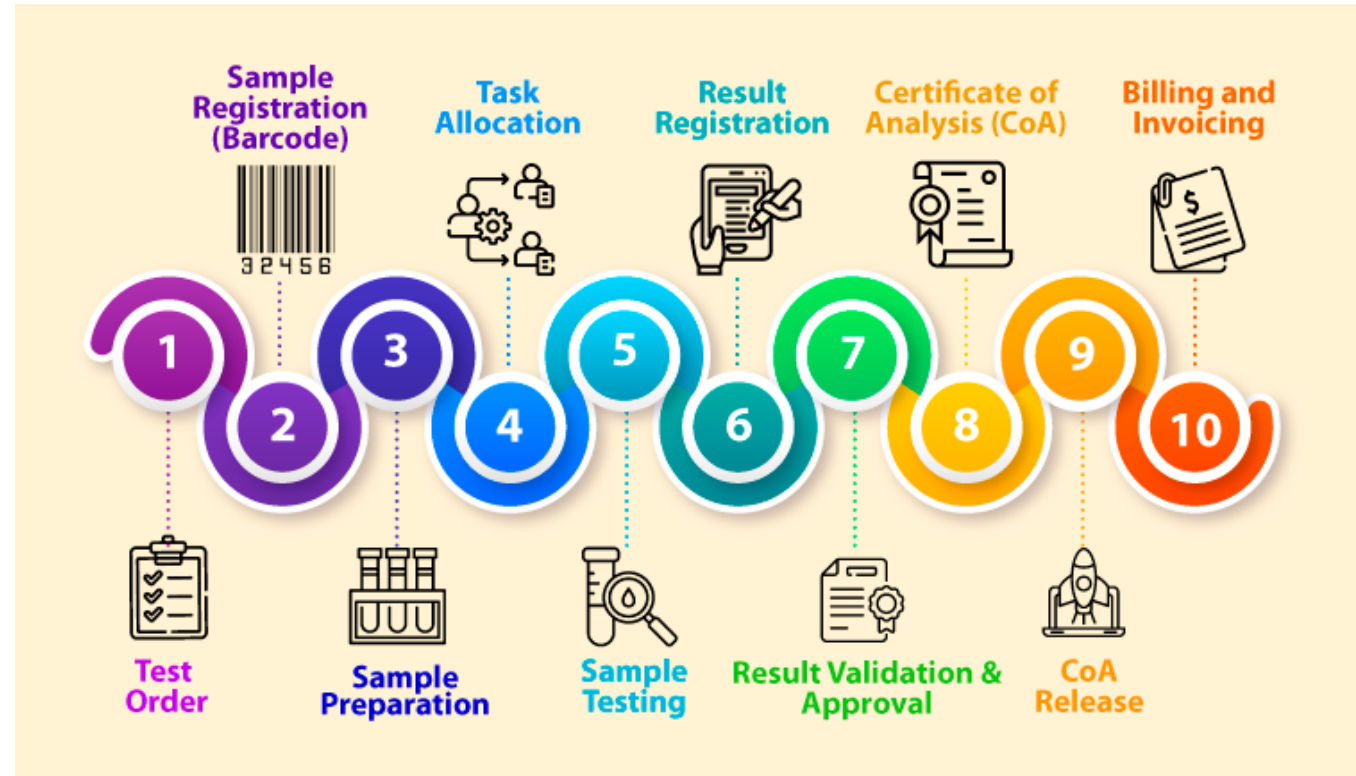
# Laboratory Information Management System (LIMS)

- Prosesser og prosedyrer SOPer og rolle som Quality Assurance (QA), Qualified Person (QP)
- Behov for validerte systemer?
- LIMS systemer basert på moderne teknologi komponenter [1]:
  - Sky basert arkitekturer (mikro-tjenester)
  - API først integrasjonskapabiliteter
  - Muliggjør “sanntids” dataanalyse
  - KI-drevet automatisering (for repetitive oppgaver, data validering, mm)
  - Sikkerhetsrammeverk på bedriftsnivå (IAM, IdP)
- Brukeradministrasjon av tillatelser og grupper
- Backup og restore av data (immutable backup)
- Kryptering av data
- Logging og trussel deteksjon



# IFEs laboratorier og krav til sikkerhet

- Tydelige roller og ansvar (Seperation of duties)
- Data integritet
- Tilgangskontroll med audit log for sporbarhet i hele livssyklusen
- Data håndtering og krav til sikkerhet
  - Lagring og kryptering (at-rest/in-transit)
- Kunderportaler (data port for analyse)
- Fysisk sikkerhet og adgangskontroll
- Integrasjon mot eksterne datakilder / instrumenter
- Krav til validering (akkrederte laboratorier) for analyse prosesser.
- Systemrevisjon med hensyn på security, beste praksis
  - Ofte kjente sårbarheter som må håndteres via tiltak. Nettverksisolering, forsvarlig sikkerhetsnivå



Kilde: CloudLIMS

# Hva og hvem er kritisk infrastruktur?

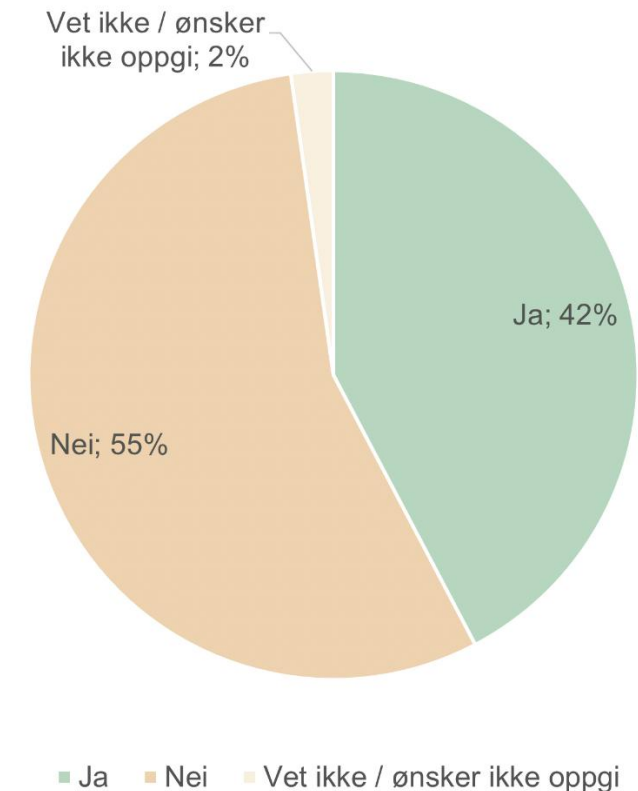
# 10



- Digitalsikkerhetsloven (NIS2)  
«Gruppe A: Loven gjelder for en del offentlige og private tilbydere av samfunnsviktige tjenester innenfor områdene energi, transport, helse, vannforsyning, bank og finansmarkedsinfrastruktur og digital infrastruktur. Loven gjelder ikke bare tradisjonelle IT-systemer, men omfatter også operasjonell teknologi.»
- «Kriterier:
  - a) Dere leverer en tjeneste som er viktig for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter.
  - b) Dere er avhengige av ett eller flere nettverks- og informasjonssystemer for å levere tjenesten.
  - c) Leveransen av tjenesten kan bli betydelig forstyrret av en hendelse.»
- Laboratorier? Kanskje ikke direkte under digitalsikkerhetsloven, men kan fort være kritisk infrastruktur? – Hvem bruker tjenestene deres? Avklar forventninger med de berørte.
  - Kontrollforordningen artikkel 100[2]
- Næringslivet sikkerhetsråd – Mørketallsundersøkelsen 2024 [1]
  - Vesentlig andre leverer indirekte eller direkte samfunnskritiske tjenester

42 prosent av virksomhetene opplever at de leverer samfunnskritiske tjenester. Dette spørsmålet er stilt for første gang i 2024.

Figur 7. Leverer din virksomhet, slik du ser det, samfunnskritiske tjenester? base n = 2500



[1] Mørketallsundersøkelsen 2024 [https://www.nsr-org.no/uploads/documents/Publikasjoner/Mcrketalls-2024\\_med\\_erfaringer\\_2.pdf](https://www.nsr-org.no/uploads/documents/Publikasjoner/Mcrketalls-2024_med_erfaringer_2.pdf)

[2] [https://lovdata.no/dokument/SF/forskrift/2020-03-03-704/ARTIKKEL\\_100#ARTIKKEL\\_100](https://lovdata.no/dokument/SF/forskrift/2020-03-03-704/ARTIKKEL_100#ARTIKKEL_100)

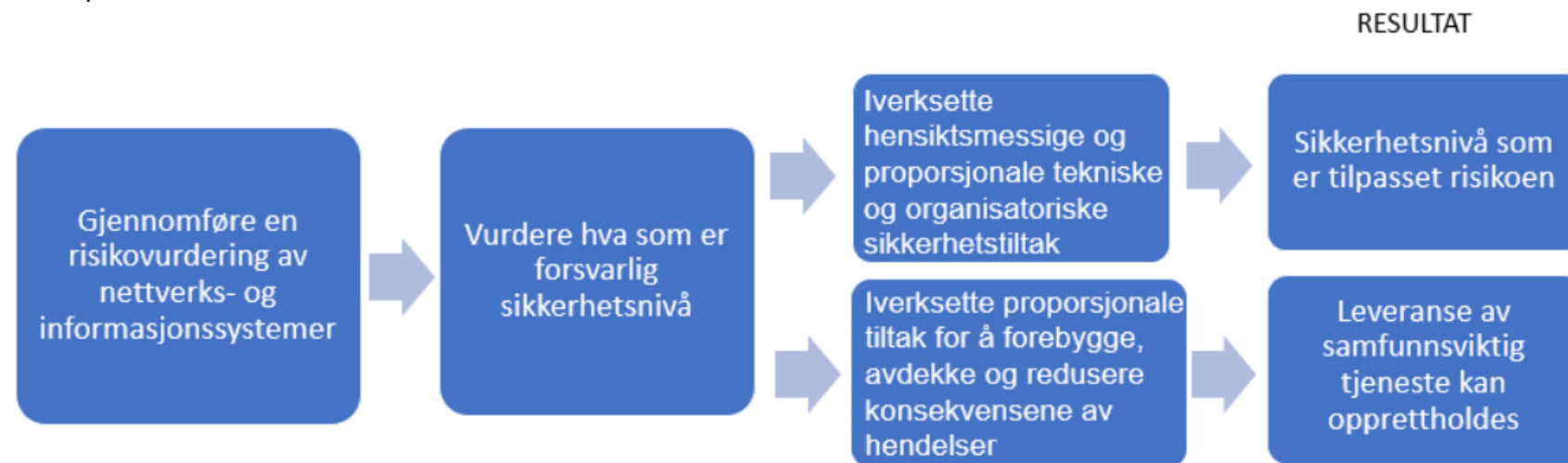
# Sikkerhetsarkitektur og digitalsikkerhetsloven

# 11

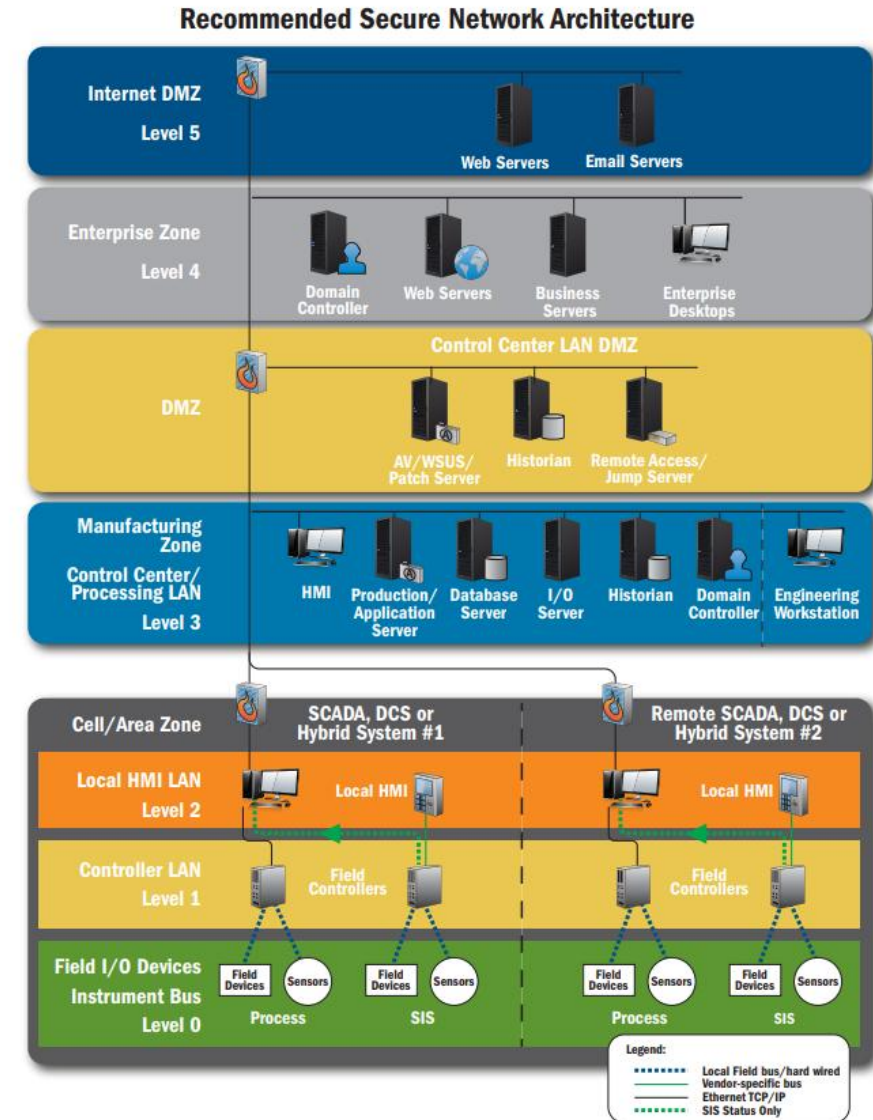
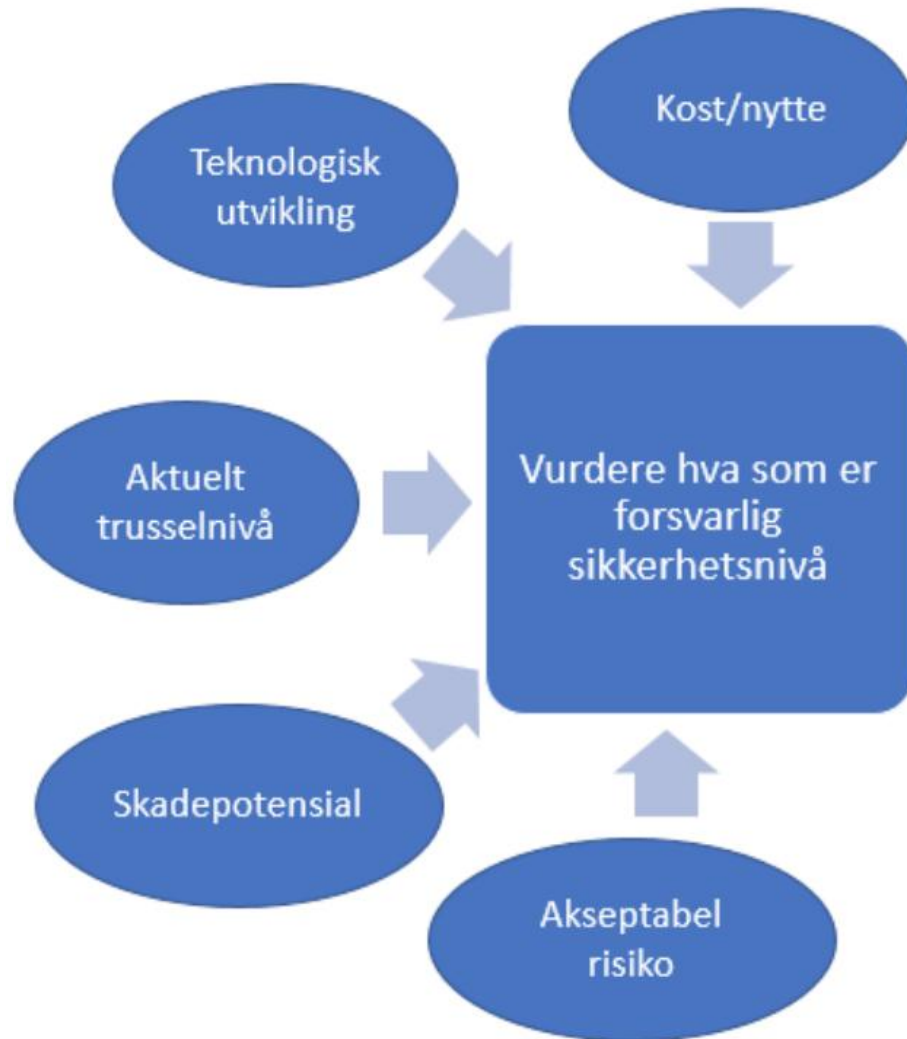


- Hva mener vi når vi snakker om **sikkerhetsarkitektur**?
  - Forskjellige roller kan oppfatte dette litt forskjellig da en sikkerhetsarkitektur er en del av den helhetlige **virksomhetsarkitekturen** og spenner sånn sett over de fleste delene av en bedrift. **Organisatorisk** og **teknisk**.
  - Strategisk **helhetlig** tilnærming til sikkerhet.
  - **Livssyklus**håndtering – Inkludert beredskap.
- **Kapabiliteter** for å ivareta tilgjengelighet, integritet, konfidensialitet.
  - Robusthet og resiliens.
- **Kontinuerlig prosess**
  - Mennesker er veldig flinke til å finne løsninger for et problem
  - **Antagelser** er en utfordring. Endringer vil skje.

- **Digitalsikkerhetsloven** (NIS1+deler av NIS2)– et forsvarlig sikkerhetsnivå
- **Fysisk** sikkerhet
- **Personellsikkerhet**
- **Styringssystem**



# Sikkerhetsarkitektur – forsvarlig sikkerhetsnivå?



# Erfaringer fra NSM

# 13



## Erfaringer fra NSMs inntrengingstester i perioden 2020-2022 [1]

- Virksomhetene som er testet er *forsvars- og justissektoren og sentralforvaltning*. Utvidet inntrengingstester i **2024-2025**. [2]
- I hovedsak **Windows-baserte** systemer
- NSM ser **de samme sårbarhetene år etter år**.

### NSM – Fem effektive tiltak mot dataangrep

1. Installer **sikkerhetsoppdateringer** så fort som mulig, og mest mulig automatisk.
2. Ikke tildel **administrator-rettigheter** til sluttbrukere.
3. Ikke tillat bruk av **svake passord**, og bruk **flerfaktoraутentisering** der det er mulig.
4. Fas ut **eldre IKT** produkter
5. Tillat kun **programvare som er godkjent** av virksomheten eller enhetsleverandøren.

- De **ti sårbarhetene** NSM sine testere oftest finner i norske virksomheter er:

#### Passord

1. Svake passord
2. Mulighet for å utføre passordgjettingsangrep
3. Uendrede standardpassord
4. Ubeskyttede passord og andre autentiseringsdata

#### Brukerkontoer

5. Gamle, inaktive administratorkontoer
6. For høye rettigheter på og for bred bruk av administratorkontoer

#### Operativsystemer og programvare

7. Sårbar og utdatert programvare og protokoller
8. Ikke-støttede operativsystemversjoner
9. Mangelfull herding av informasjonssystemet

#### Nettverk

10. Mangelfull nettverkssegmentering og trafikkstyring

[1] Ti sårbarheter i norske IKT-systemer <https://nsm.no/getfile.php/1313387-1700026023/NSM/Filer/Dokumenter/Rapporter/Ti%20s%C3%A5rbarheter%20i%20norske%20IKT-systemer.pdf>

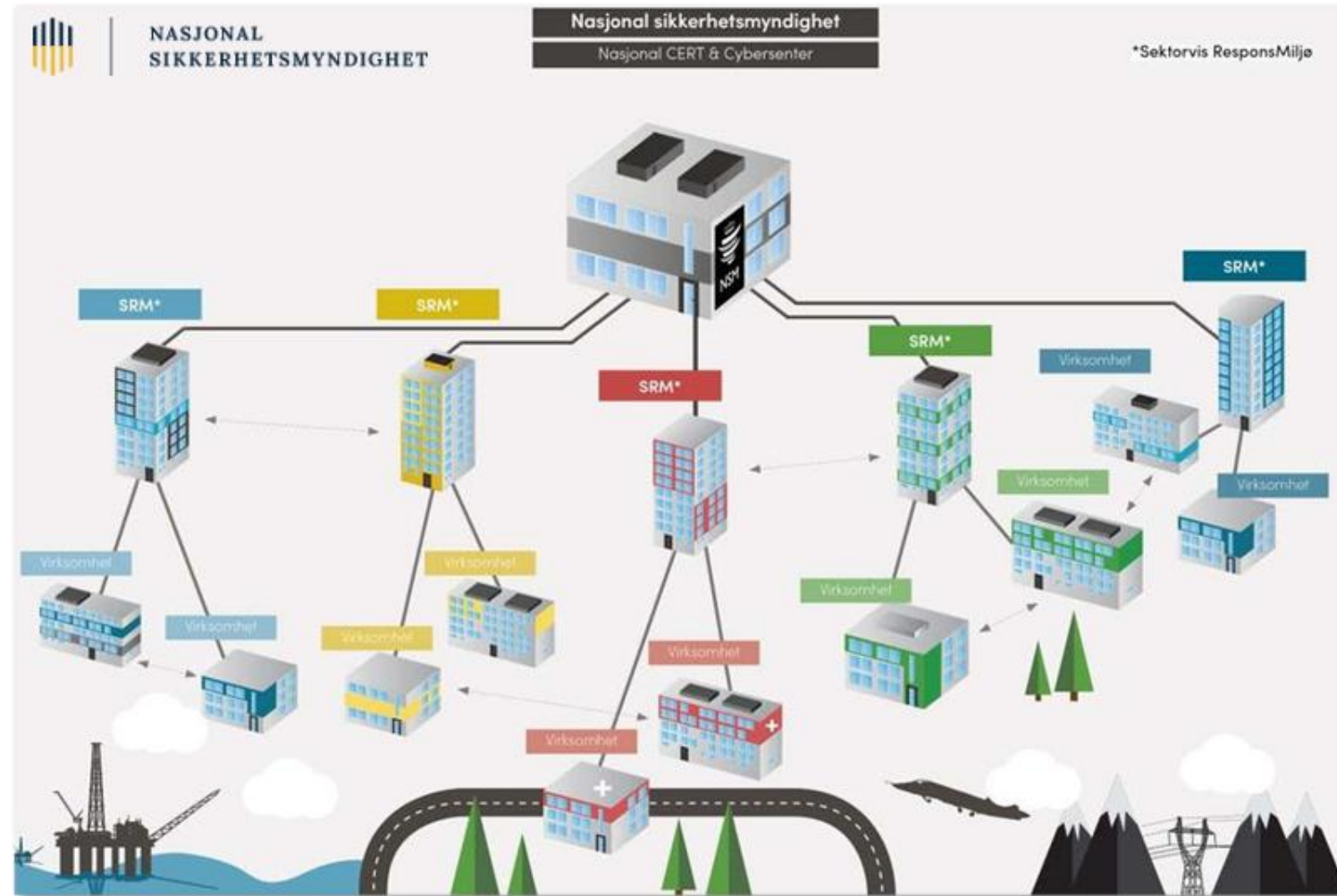
[2] NSM - Risiko 2026

# Nasjonal organiseringen ved digitale angrep

# 14



- Nasjonalt cybersikkerhetssenter (NCSC)
  - Nasjonalt rammeverk for håndtering av digitale angrep og cyberhendelser [1]
- Sektorvise responsmiljøer (SRM)
  - En SRM skal ha kapabiliteter til å **detektere, analysere, varsle, koordinere og håndtere alvorlige digitale hendelser.**
- Virksomhetens ansvar å **ivareta tilstrekkelig digital sikkerhet** og gjennom dette være en del av den nasjonale motstandsdyktigheten [1]
- Nytt **cybersikkerhetssenter (SRM) for næringslivet** etablert 7. august 2025 [2] av **Næringslivetssikkerhetsråd** [3]
  - Bygg- og anleggsbransjen
  - **Industri (med unntak av olje- og gass)**
  - Mat- og drikkeproduksjon (næringsmiddelindustri)
  - Matdistribusjon
  - Sjømatnæringen
  - Reiselivsnæringen
  - Varehandel
  - Konsulent- og rådgiving



[1] <https://nsm.no/getfile.php/1314739-1750852039/NSM/Files/Dokumenter/Nasjonalt%20rammeverk%20for%20h%C3%A5ndtering%20av%20digitale%20angrep%20og%20cyberhendelser.pdf>

[2] <https://www.regjeringen.no/no/aktuelt/etablerer-nytt-cybersikkerhetssenter-for-naringslivet/id3116355/>

[3] <https://www.nsr-org.no/cybersikkerhetssenter>

[4] <https://www.iustiscert.no/tjenester>

## Bruk de ressursene og nettverkene som er tilgjengelig

# 15



NSM

Cybersjekk



Hjelp!  
Vi er underlagt  
Sikkerhetsloven  
- En enkel veileder



<https://www.sikkert.no/>

<https://cybersjekk.no/>

<https://nsm.no/regelverk-og-hjelp/grunnprinsipper/>

<https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker/digitalsikkerhetsloven-og-forskrift>

<https://www.nsr-org.no/>

# Oppsummering - sikkerhet i laboratorier

# 16



- Det handler om å **identifisere, vurdere og implementere sikkerhetstiltak** som dekker hele systems livssyklus – fra design og utvikling til drift og vedlikehold.
- Dette krever at vi:
  - Forstår hvilke komponenter som finnes, deres avhengigheter og hvordan de kommuniserer.
  - Identifiserer svakheter og mulige angrepsvektorer.
  - Implementerer sikkerhet gjennom hele arkitekturen og systemet livsyklus.
  - Opprettholder sikkerheten kontinuerlig ved å gjennomføre og installere sikkerhetsoppdatering, overvåkning og hendelseshåndtering.



## Nemonoor.no – utvalg av tjenester fra IFE



### Risikovurdering, trusselmodellering og vurdering av sikkerhetsarkitektur (IFE)

Styrk din bedrifts forståelse av informasjons- og datasikkerhet!

Gjennom en praktisk tilnærming lærer deltakerne i dette dagskurset hvordan de kan



### Sikker bruk av AI: Risiko, sårbarhet og strategier

Bli med på vårt dagskurs om AI-sikkerhet! Ønsker du å forstå hvordan du kan balansere risiko og nytte ved bruk av AI? Vårt kurs gir deg innsikt og konkrete verktøy for å håndtere AI-relaterte sikkerhetsaspekter i praksis-

[Les mer](#)



### European Data Spaces

Ønsker du å forstå hvordan European Data Spaces kan revolusjonere datadeling og samarbeid? Bli med på vårt spennende heldags kurs om European Data Spaces!

[Les mer](#)



### Forsker for en dag - få hjelp av en erfaren forsker fra IFE for å løse konkrete utfordringer innen AI og digitalisering

Vårt team av erfarne AI-forskere kan hjelpe deg med å løse varierte utfordringer og implementere forbedringer knyttet til AI og digitalisering. Du bestemmer selv antall timer du ønsker å bruke forskeren for.

[Les mer](#)



### Interoperabilitet i Smarte Byer: Standarder og mekanismer for sømløs systemintegrasjon

Oppdag vårt banebrytende hel dags kurs som gir deg nøkkelen til fremtidens smart by teknologi!



### Fra angrep til forsvar: Live demo av hackerverktøy og konkrete tiltak for å beskytte både privatpersoner og bedrifter

Vil du lære hvordan cyberkriminelle faktisk jobber? Bli med på vårt foredrag hvor vi avdekker verktøyene og metodene som brukes for å angripe både bedrifter og privatpersoner.

[Les mer](#)

# 17



# Takk for meg!

Aleksander Lygren Toppe  
Senioringeniør

IFE Cybersecurity Centre

[Aleksander.lygren.toppe@ife.no](mailto:Aleksander.lygren.toppe@ife.no)

Opprinnelig presentør/kollega:

Per Arne Jørgensen

Seniorforsker, Digital Suverenitet

IFE Cybersecurity Centre

[Per.arne.jorgensen@ife.no](mailto:Per.arne.jorgensen@ife.no)