Juss kan faktisk også være det

Harald Omdal
Adm dir. IDA, 1967

UNIVERSITETET I OSLO

IT-sikkerhet

Isak Falch Alsos
IT-juridisk rådgiver
IT-avdelingen

UNIVERSITETET I OSLO

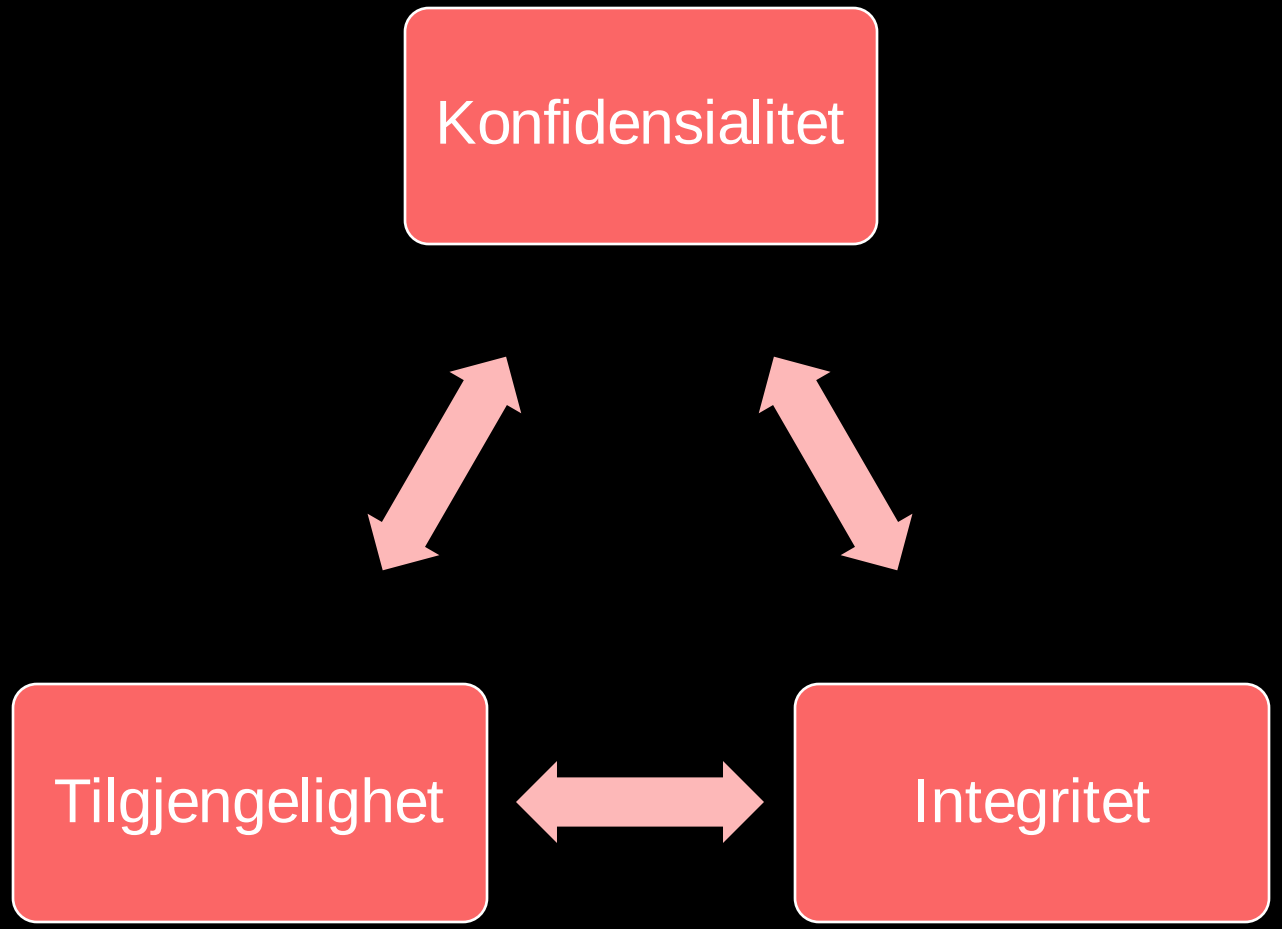
IT-sikkerhetsregulering

Hvilke lovkrav gjelder, og hva betyr disse for deg?

Isak Falch Alsos
IT-juridisk rådgiver
IT-avdelingen

Hva er informasjonssikkerhet?

Hva er informasjonssikkerhet?



Beskyttelse av informasjons**verdier**

mot interne og eksterne **trusler**

ved hjelp av risikobaserte **tiltak**

Noen utgangspunkt

- Overlappende begreper
  - Datasikkerhet, cybersikkerhet, informasjonssikkerhet eller digital sikkerhet
- Mange typer sikkerhet
  - **Fysisk sikkerhet**: fysiske verdier
  - **Personellsikkerhet**: sikkerhetsrisikoen personer kan utgjøre
  - **Samfunnssikkerhet**: opprettholde kritisk infrastruktur for samfunnet så en kan beskytte liv og helse
  - **Statssikkerhet**: sikre at staten fortsatt eksisterer, har territoriell integritet og politisk handlingsfrihet
  - **Nasjonal sikkerhet**: statssikkerhet med elementer av samfunnssikkerhet
- **Sikkerhet** er ikke det samme som **trygghet** eller **beredskap**

Hvorfor i h****** skal en jurist fortelle oss om informasjonssikkerhet?

Det finnes noen lovkrav...

Illustrasjon: The Malware Museum

Cyberoperasjoner kan skade kritisk infrastruktur

Statlig etterretnings-virksomhet

Profesjonalisering av angrep

NSM

Risiko 2024

Nasjonal sikkerhet – et felles ansvar

METODENE

Fremmede staters etterretnings-tjenester bruker en rekke ulike metoder mot mål i Norge. I denne delen skisserer vi hvordan enkelt-personer og virksomheter kan bli utsatt for følgende fenomen og virkemidler:

- Cyberoperasjoner
- Rekruttering av menneskelige kilder
- Etterretning ved bruk av sivile fartøy
- Påvirkningsoperasjoner
- Sabotasje
- Fordekte anskaffelsesforsøk
- Sikkerhetstruende økonomiske virkemidler
- Transnasjonal undertrykkelse

Trusselen i cyberdomenet er dynamisk og i stadig utvikling

Sikkerheten i cyberdomenet må styrkes

Cyberoperasjoner har blitt hverdagskost for både offentlige og private virksomheter. Derfor må virksomhetene gjøre det de kan for å forhindre, avdekke og håndtere sikkerhetstruende hendelser.

Innsidevirksomhet

Kritisk infrastruktur og verdier må sikres

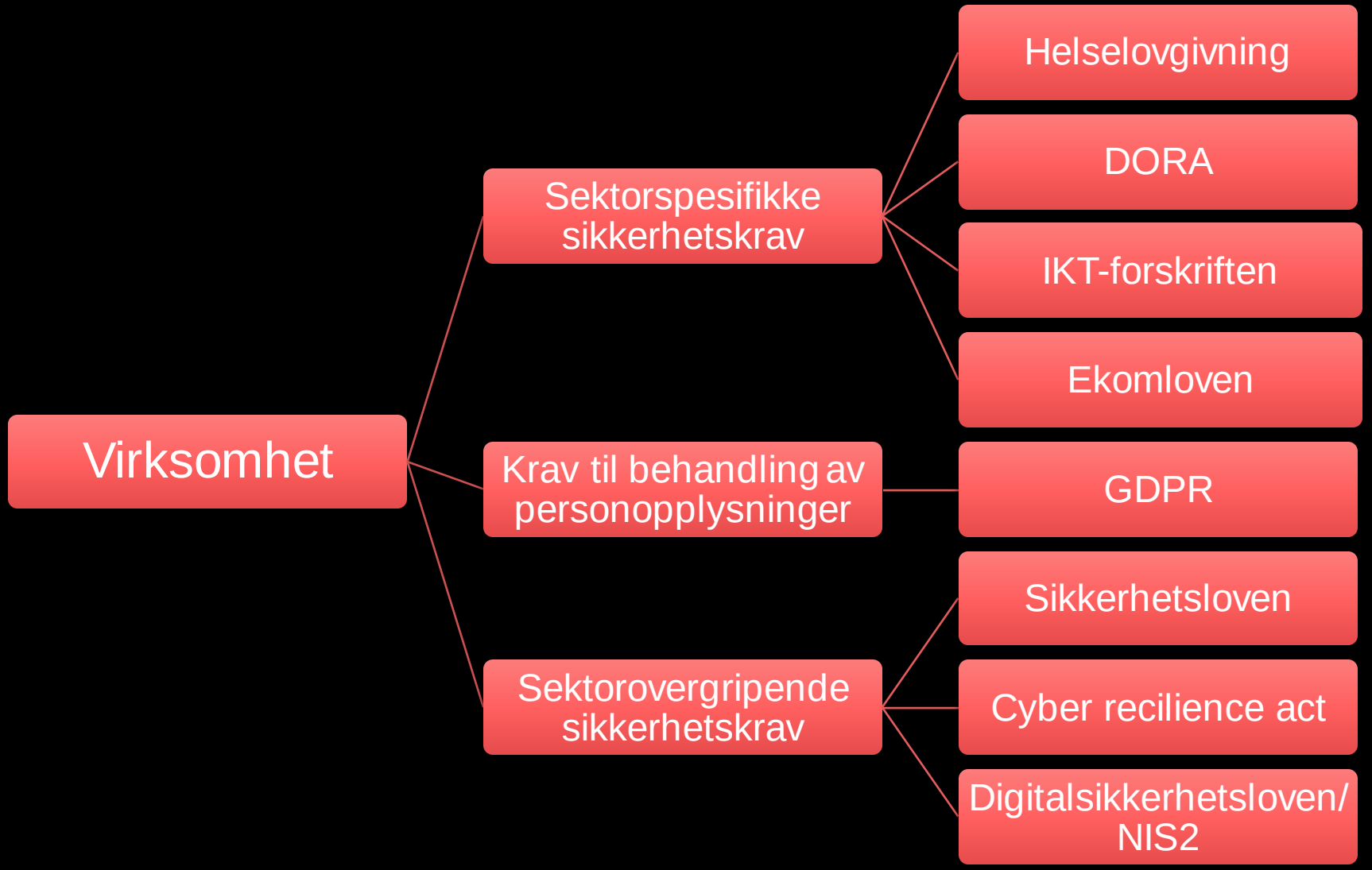
Nye sårbarheter vokser frem

Ifølge PST utgjør Russland den største etterretnings-trusselen mot Norge i 2024, mens trusselen fra Kina vurderes som betydelig og skjerpet. Den kinesiske

Det finnes ingen felles «cybersikkerhetsregulering»

https://www.deviantart.com/vi3x/art/One-Ring-v3-53651274

Ulike varianter sikkerhetsregulering



Informasjonssikkerhet grunnprinsipper

Standarder

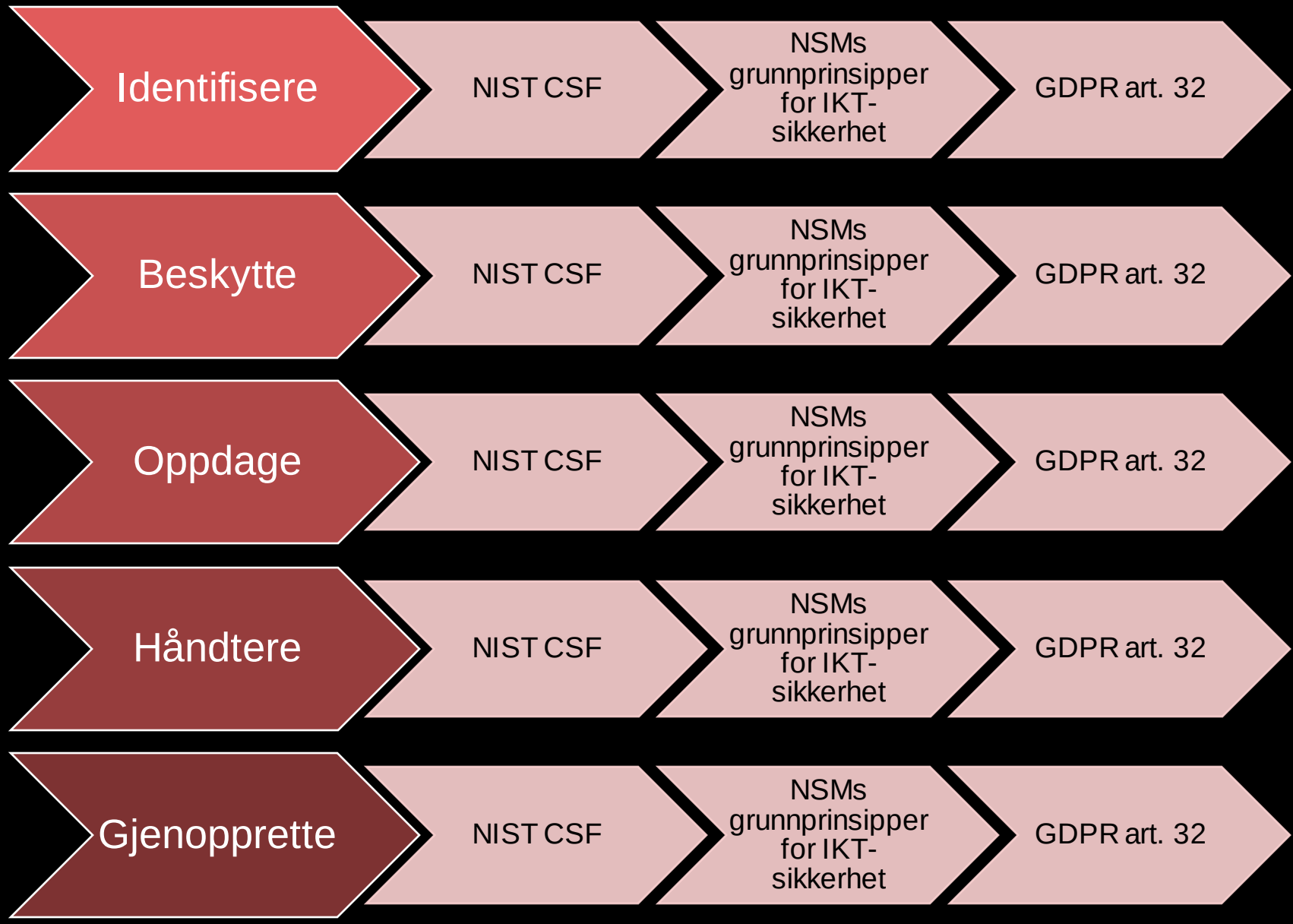
- NIST Cyber Security Framework (CSF)
- CIS Controls
- ISF Standard of Good Practice for Information Security (SOGP)

- NSMs standard for IKT-sikkerhet
- Normen

ISO-standarder

- **ISO 27001**: Informasjonssikkerhetsstyring
- **ISO 27002**: Implementering av sikkerhetstiltak
- **ISO 27017**: Sikkerhetstiltak for leverandører og brukere av skytjenester
- **ISO 27018**: Personopplysninger i offentlige skyer
- **ISO 22301**: Kontinuitetsledelse

NIST CFS


Identifisere
NIST CSF
NSMs grunnprinsipper for IKT-sikkerhet
GDPR art. 32
Beskytte
NIST CSF
NSMs grunnprinsipper for IKT-sikkerhet
GDPR art. 32
Oppdage
NIST CSF
NSMs grunnprinsipper for IKT-sikkerhet
GDPR art. 32
Håndtere
NIST CSF
NSMs grunnprinsipper for IKT-sikkerhet
GDPR art. 32
Gjenopprette
NIST CSF
NSMs grunnprinsipper for IKT-sikkerhet
GDPR art. 32

GDPR art. 32

Kommer til anvendelse når vi **behandler personopplysninger**

- Risikobasert tilnærming
- Egnede tekniske og organisatoriske tiltak
- Sikkerhetsnivå som er egnet med hensyn til risikoen
  - Pseudonymisering og kryptering av personopplysninger
  - Sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet
  - Gjenopprette tilgjengeligheten og tilgangen
  - Regelmessig testing, analysering og vurdering
- Godkjente handlingsnormer

Fremtidens lovgivning

Digitalsikkerhetsloven

- Vedtatt i desember 2023, men ikke i kraft
- Gjennomfører bla.a. NIS1-direktivet
- Formål:
  - Styrke digital sikkerhet for virksomheter med særlig betydning for samfunnet
  - Ansvarliggjøre ledelse
  - Risko og tiltak
  - Forbedre og ivareta tverrsektoriell, nasjonal situasjonsforståelse ved hendelser
  - Samarbeid og informasjonsdeling på tvers av sektorer og på tvers av land

Digitalsikkerhetsloven

Gjelder for tilbydere av **viktige samfunnstjenester**:

- Energi
- Transport
- Helse
- Vannforsyning
- Bank
- Finansmarkedinfrastruktur
- Digital infrastruktur

Digitalsikkerhetsloven

Hovedforpliktelser

Grunnleggende sikkerhet

- Gjennomføre risikovurderinger
- Risikobaserte tiltak
- Forebygge, avdekke og redusere konsekvens av hendelser

Varslingsplikt

- Ved store hendelser
- Virker betydelig på tjenesteleveransen
- Uten unødig opphold

Digitalsikkerhetsloven

Virkemidler for håndhevelse av loven

- Pålegg om retting
- Tvangsmulkt
- Overtredelsesgebyr

Men vent litt...

Gjelder for tilbydere av **viktige samfunnstjenester**:

- Energi
- Transport
- Helse
- Vannforsyning
- Bank
- Finansmarkedinfrastruktur
- Digital infrastruktur

NIS1-direktivet

NIS2-direktivet

Virkeområde – hvem er omfattet av NIS2?

Vesentlige sektorer:

- energi
- transport
- bank
- finansmarkedsinfrastrukturer
- helse
- drikkevann
- avløpsvann
- digital infrastruktur
  - elektronisk kommunikasjon, datasentertjenester, skytjenester, tillitstjenester, samtrafikkpunkter etc.
- IKT-tjenester
- offentlig forvaltning (sentral og regional)
- romvirksomhet

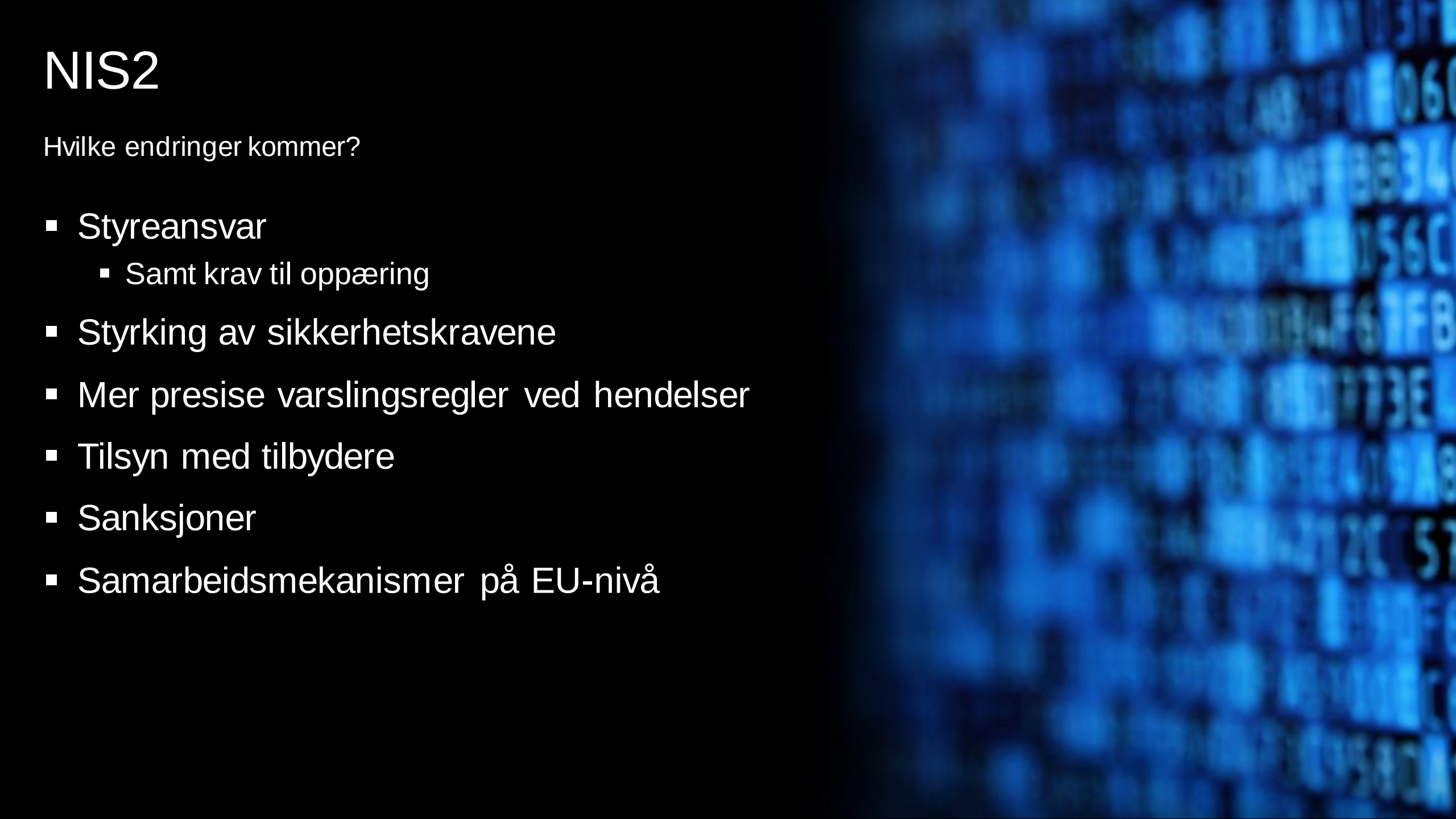
Viktige sektorer:

- post - og kurertjenester
- avfallshåndtering
- produksjon og distribusjon av kjemikalier
- matproduksjon
- produksjon av visse varer (medisinsk utstyr, IKT-utstyr, kjøretøy, elektronikk, maskiner, transportutstyr)
- tilbydere av digitale tjenester
- forskning

NIS2

Hvilke endringer kommer?

- Styreansvar
  - Samt krav til oppæring
- Styrking av sikkerhetskravene
- Mer presise varslingsregler ved hendelser
- Tilsyn med tilbydere
- Sanksjoner
- Samarbeidsmekanismer på EU-nivå



NIS2 – Styrking av sikkerhetskravene

Hva må du vite om de de operative **minimumskravene** til cybersikkerhet?

a. Informasjonssikkerhetspolicy for virksomheten og retningslinjer for risikovurderinger
b. Planer for hendelseshåndtering
c. Planer for driftskontinuitet, inkludert backup og gjenoppretting
d. Sikkerhet i leverandørkjeder
e. Sikkerhet i anskaffelser, utvikling og vedlikehold av informasjonssystemer,
   - deling av informasjon om sårbarheter
f. Vurdere effekten av sikkerhetstiltak
g. Grunnleggende informasjonssikkerhetstiltak og opplæring av personell
h. Tilgangskontroll, personellsikkerhet og assetmanagement
i. Kryptering
j. Multifaktorautentisering og kontinuerlig autentisering, og sikker kommunikasjon

- Risiko, risiko, risiko
- Hold orden i sysakene
- Det er ingen skam å dele sine feil

Kommer disse nye lovkravene til å påvirke oss?

Ja.

Men mageføIelsen sier vi er relativt godt rustet etter godt IT-sikkerhetsarbeid over mange år

Takk for meg!

Isak Falch Alsos
IT-juridisk seniorrådgiver
IT-avdelingen
isakfa@uio.no