IKT-sikkerhetsutvalget

NOU 2018: 14 IKT-sikkerhet i alle ledd

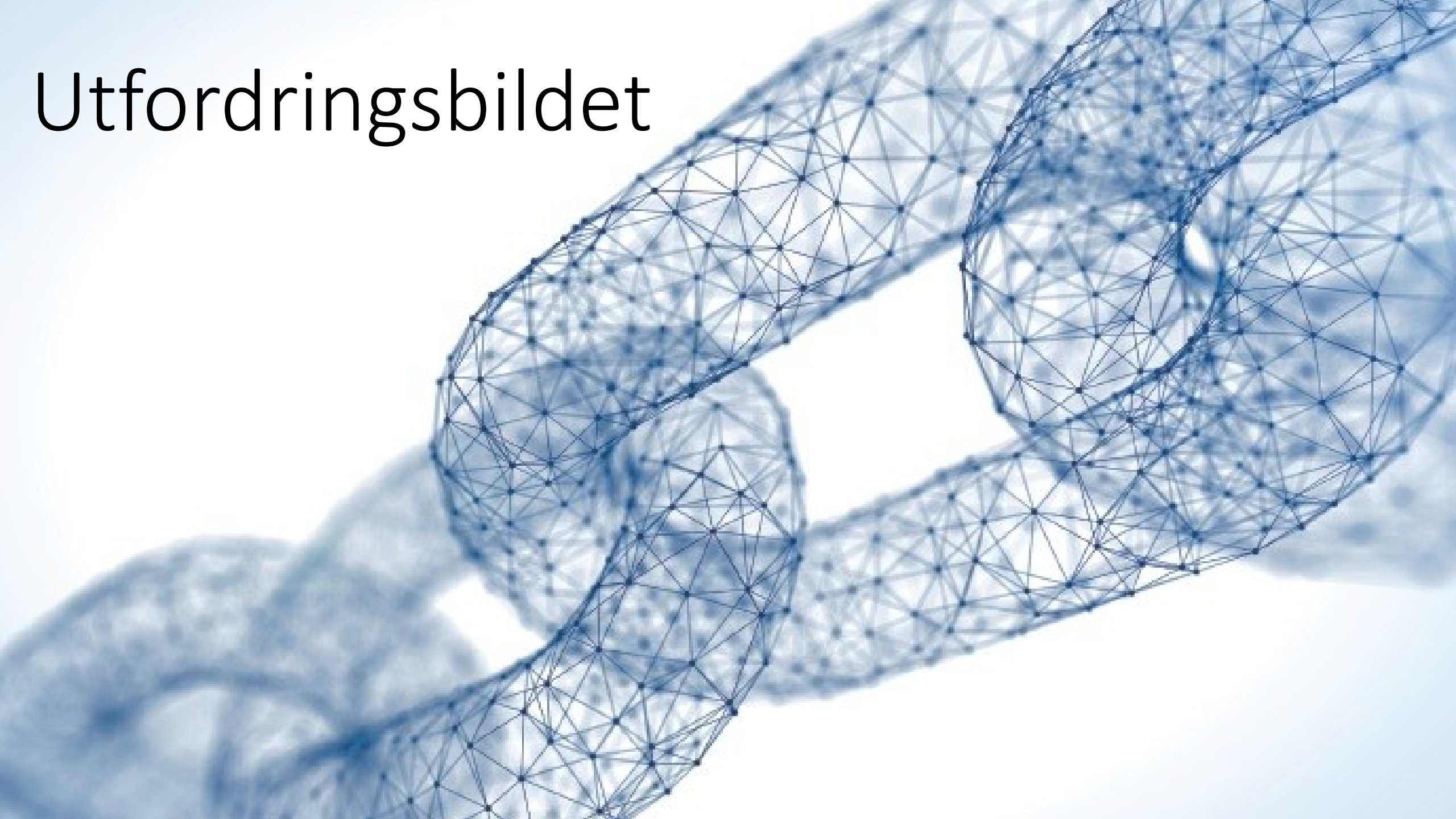
Mandat

- Er dagens regulering hensiktsmessig for å oppnå forsvarlig nasjonal IKT-sikkerhet?
- Har vi en hensiktsmessig fordeling og organisering av tverrsektorielt ansvar på etatsnivå innen nasjonal IKT-sikkerhet?
- Hvilke regulatoriske og organisatoriske grep bør gjøres for å styrke nasjonal IKT-sikkerhet?

Medlemmer

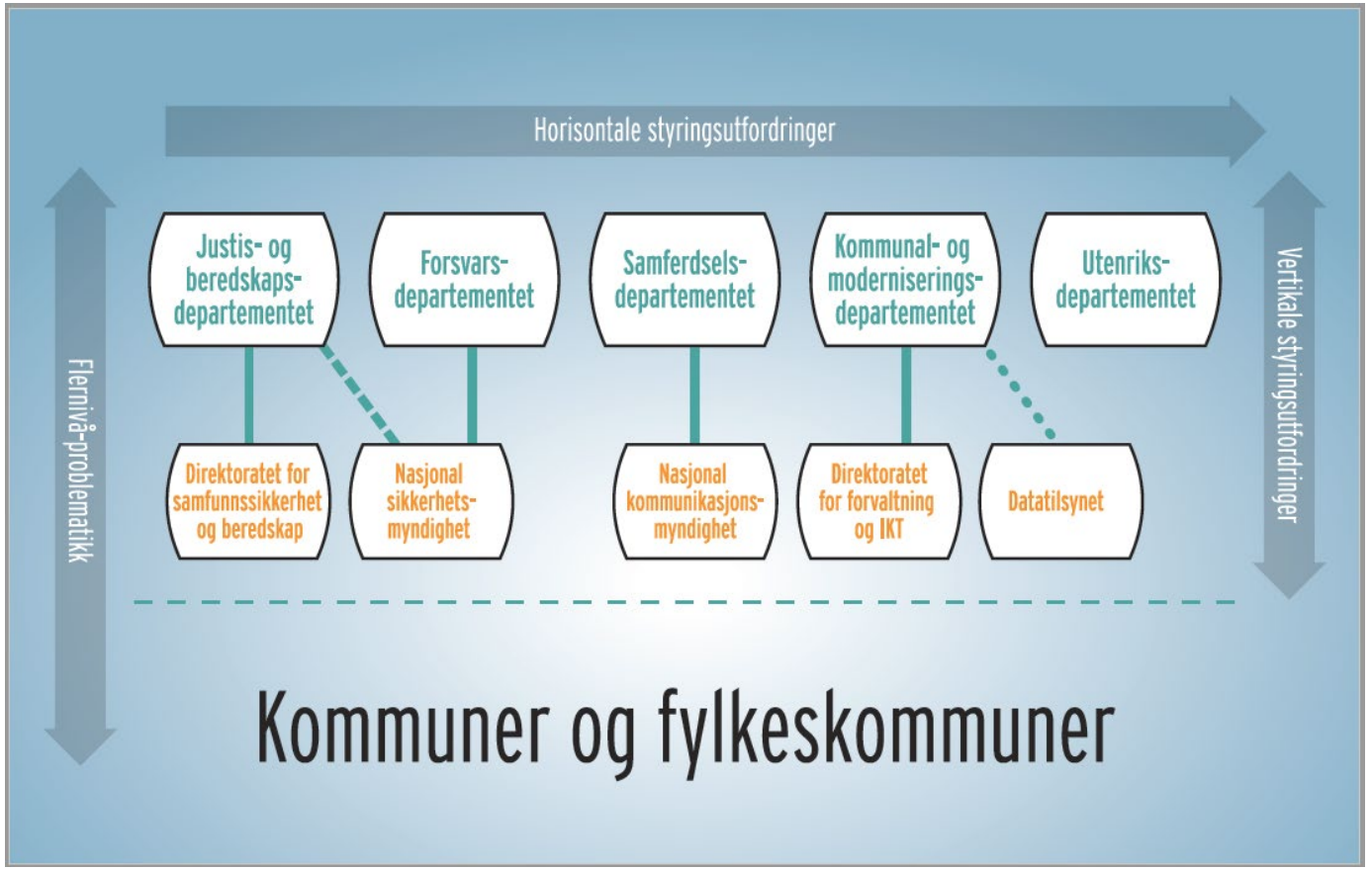
- Hans Christian Holte (leder), Therese Steen, Terje Wold, Lee A. Bygrave, Marie Moe, Torgeir A. Waterhouse, Lillian Røstad, Håkon Grimstad

Utfordringsbildet



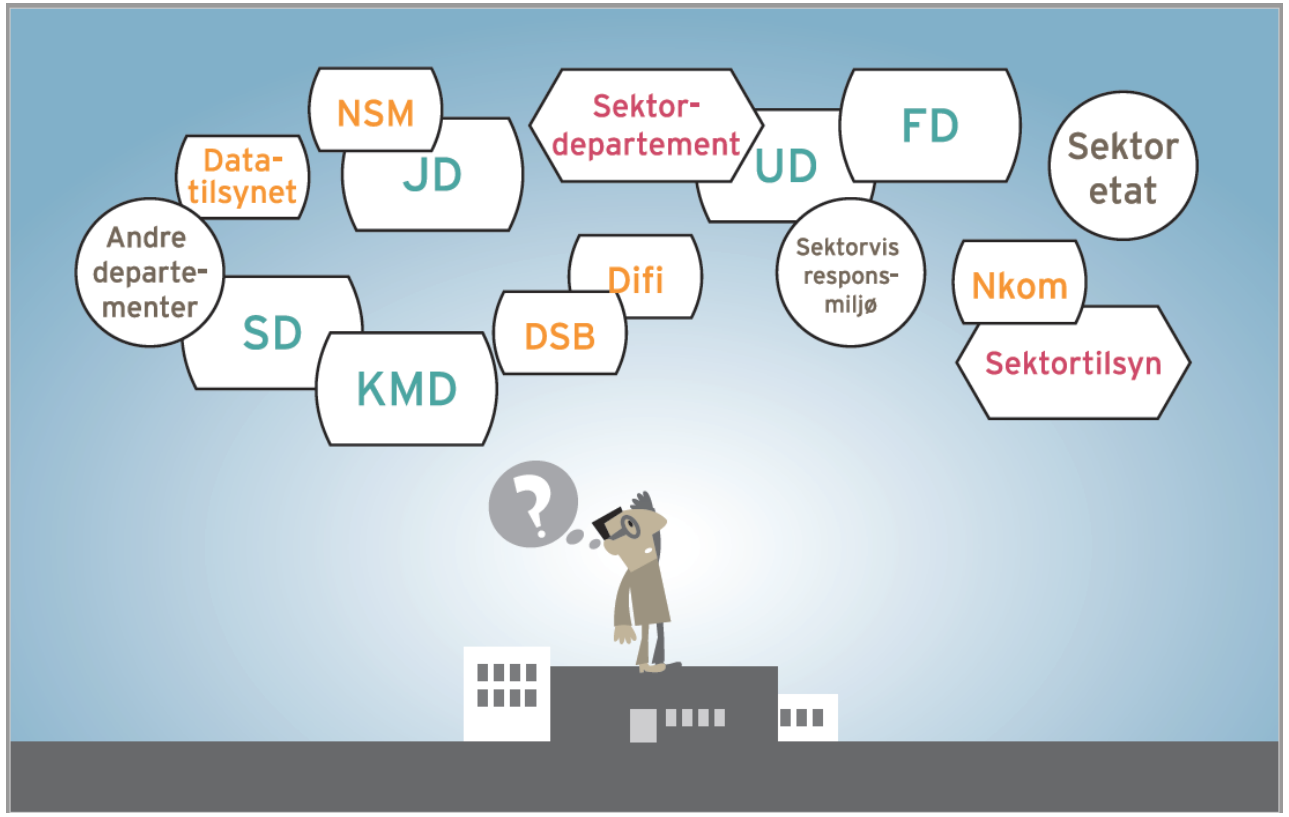
Styrings- og samordningsutfordringer

- Horisontale styringsutfordringer mellom departementene og mellom direktoratene
- Vertikal styringsutfordring mellom departementene og direktoratene
- Flernivå-problematikk mellom stat og kommune
- Begrensede styringsmuligheter overfor private virksomheter



Digitaliseringen av samfunnet utfordrer oppgaveløsning, ansvar og roller

- Samfunnssikkerhet og statssikkerhet overlapper – krevende grenseflater mellom NSM og DSB
- Rådgivning og veiledning fremstår fragmentert og lite koordinert
- Koordinering og informasjonsdeling ved uønskede digitale hendelser er krevende
- Tilsyn med IKT-sikkerhet oppleves som mangelfull og lite koordinert



Mangelfull regulering av IKT-sikkerhet

- Regelverket adresserer sikring av informasjon, konfidensialitet
- IKT-sikkerhet er ulikt regulert i sektorene
- Lite hensiktsmessig regulering av IKT-sikkerhet i offentlig forvaltning
- Begrensninger i sikkerhetsloven

Manglende insentiver for å investere i IKT-sikkerhet

- For lite kunnskap, forståelse eller kjennskap til digitale trusler til å iverksette hensiktsmessige tiltak
- IKT-sikkerhet koster penger
- Potensiell målkonflikt mellom digitalisering og effektivitet og IKT-sikkerhet

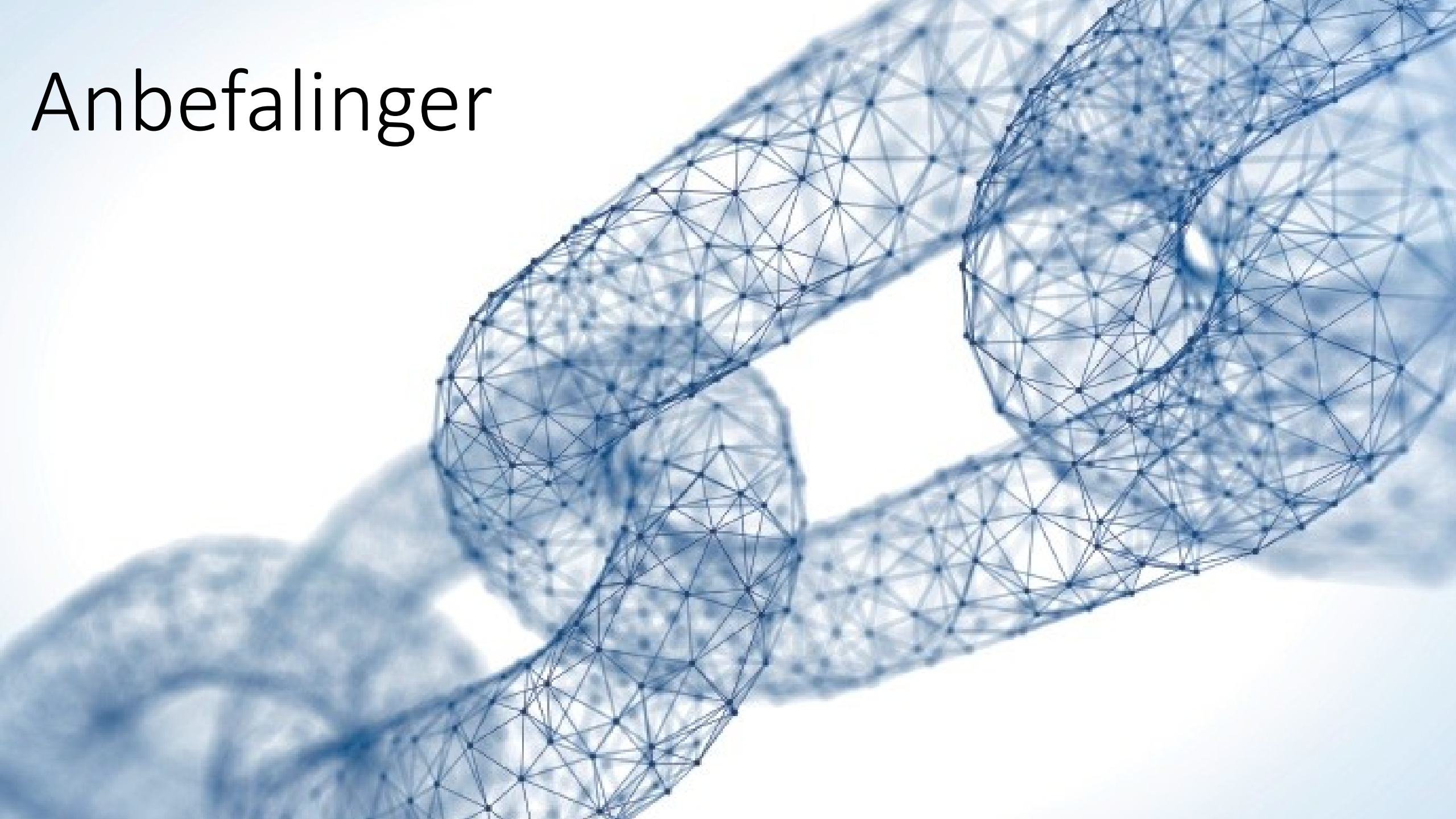
Anskaffelser og digitale sårbarheter

- Gjeldene lover og forskrifter regulerer IKT-sikkerhet ved anskaffelser i varierende grad
- IKT-sikkerhet er ikke godt nok vektlagt i anskaffelsesregelverket og i statens standardavtaler

Utfordringer med IKT-sikkerhet i tilkoblede produkter og tjenester

- Dagens regelverk gir få insentiver for å produsere og selge tilkoblede produkter og tjenester med tilstrekkelig IKT-sikkerhet
- Uklart hvem som har myndighetsansvar for IKT-sikkerhet i tilkoblede produkter og tjenester
- Vanskelig å vite til hvem og hvordan man skal varsle om alvorlige IKT-sikkerhetshull i tilkoblede produkter og tjenester
- Det er ingen styrt tilnærming til hvordan man skal behandle og offentliggjøre digitale sårbarheter

Anbefalinger



Overordnede prinsipper til grunn for utvalgets anbefalinger

- Arbeidet med IKT-sikkerhet må ha en risikobasert tilnærming som innebærer at vesentlig risiko på IKT-sikkerhetsområdet prioriteres
- IKT-sikkerhet må balanseres opp mot brukervennlighet, økonomi og grunnleggende menneskerettigheter. En slik balanse vil innebære at et visst nivå av risiko må aksepteres for å oppnå økonomiske og sosiale mål
- Arbeidet med IKT-sikkerhet krever fleksibilitet i reguleringen og organiseringen slik at man kan tilpasse seg nye trusler, sårbarheter, teknologier og forretningsmodeller

Utvalgets anbefalinger

- Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning
- Krav om IKT-sikkerhet ved anskaffelser
- Etablere et nasjonalt IKT-sikkerhetssenter
- Tydelig regulering og ansvar for tilkoblede produkter og tjenester
- Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet

Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning

- Den nye loven skal gjennomføre NIS-direktivet i norsk rett
- Den nye loven skal gjelde for samfunnskritiske virksomheter, offentlig forvaltning og virksomheter som omfattes av NIS-direktivet
- Den nye loven skal stille krav om forsvarlig IKT-sikkerhet. Kravene bør konkretiseres i forskrift og veiledning
- Den nye loven skal stille krav om varsling av uønskede digitale hendelser.
- Det skal føres tilsyn med etterlevelsen av den nye loven
- Justis- og beredskapsdepartementet må sørge for koordinert veiledning til loven, herunder vurdere en sertifiseringsordning
- Fremtidige regelverk må harmoniseres med kravene i den nye loven

- Sette ned et lovutvalg som skal utrede en lov som stiller krav om IKT-sikkerhet til alle norske virksomheter

Krav om IKT-sikkerhet ved anskaffelser

- Det må stilles krav om IKT-sikkerhet ved alle offentlige anskaffelser. Anskaffelsesregelverket bør endres slik at oppdragsgiveren får en slik plikt
- IKT-sikkerhet må ivaretas bedre i Statens standardavtaler
- Veiledning om IKT-sikkerhet ved anskaffelser må videreutvikles

Etablere et nasjonalt IKT-sikkerhetssenter

- Det må etableres et nasjonalt IKT-sikkerhetssenter for å styrke koordinering og samordning mellom sektorer og mellom offentlig og privat aktører
- Justis- og beredskapsdepartementet må, i samarbeid med Forsvarsdepartementet, sørge for at det gjennomføres en uavhengig behovs- og kostnadsanalyse før et nasjonalt IKT-sikkerhetssenter etableres
  - Behovs- og kostnadsanalysen må baseres på en bred involvering av potensielle interessenter i privat og offentlig sektor
  - Behovs- og kostnadsanalysen må avklare IKT-sikkerhetssenterets myndighetsforankring og kobling til NSM

Følgende oppgaver bør vurderes lagt til IKT-sikkerhetssenteret

- Koordinere myndighetenes råd og veiledning
- Være nasjonalt responsmiljø (NSM NorCERT)
- Være sentralt kontaktpunkt for råd- og veiledning og ved uønskede digitale hendelser
- Tilgjengeliggjøre oppdatert informasjon om trusler og sårbarheter
- Motta rapportering og offentliggjøre informasjon om digitale sårbarheter i IKT-systemer («Coordinated Vulnerability Disclosure»)
- Være pådriver for offentlig-privat samarbeid
- Stimulere til mer forskning, utvikling og innovasjon

Tydelig regulering og ansvar for tilkoblede produkter og tjenester

- Ansvaret for IKT-sikkerhet i tilkoblede produkter og tjenester bør i større grad flyttes fra forbrukeren til produsentene og leverandørene. For å oppnå dette, bør det blant annet stilles krav om innebygd sikkerhet («Security by design») i tilkoblede produkter og tjenester
- Norge må fortsette sitt internasjonale samarbeid på dette området, særlig opp mot regelverksprosesser i EU
- Myndighetene må gi bedre råd og veiledning til importører, forhandlere og norske produsenter av tilkoblede produkter og tjenester. Utarbeidelse av råd og veiledning må gjøres i samarbeid mellom myndighetene og bransjeaktørene
- DSB bør få en tydelig rolle når det gjelder varsling, rapportering, tilbakekalling og håndtering av manglende IKT-sikkerhet i tilkoblede produkter og tjenester

Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet

- Justis- og beredskapsdepartementet må utøve et tydeligere lederskap for nasjonal IKT-sikkerhet
  - Etablering av et nasjonalt IKT-sikkerhetssenter og den nye loven om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning vil styrke departementets evne til å utøve et tydeligere lederskap for nasjonal IKT-sikkerhet
  - Justis- og beredskapsdepartementet og Forsvarsdepartementet må gjennomgå styringsmodellen til NSM for å sikre at IKT-sikkerhet i sivil sektor blir bedre ivaretatt, samtidig som koblingen mellom sivil sektor og forsvarssektoren beholdes
- Justis- og beredskapsdepartementet må tilrettelegge for at tilsyn på IKT-sikkerhetsområdet koordineres bedre, og at tilsyn med teknisk IKT-sikkerhet gis økt oppmerksomhet

Videre prosess

- NOUen sendt på høring 21.12.18
- Endringer i regjeringen og departementsstrukturen kommunisert 22.1
- Nasjonal strategi for digital sikkerhet lansert 30.1
  - Tilak 6 omhandler oppfølging av utvalgets arbeid
  - Tiltak 3 (Nasjonalt Cybersikkerhetssenter) og tiltak 30 (NIS-direktivet) viser også til utvalget