

## Innspill til Stortingets behandling av Meld. St. 5 (2020-2021) – Samfunnssikkerhet i en usikker verden

*Tekna – Teknisk naturvitenskapelig forening er den største masterforeningen i Norge, og den største fagforeningen i Akademikerne med over 87 000 medlemmer. Våre medlemmer har mastergrad eller mer fra tekniske og naturvitenskapelige fagområder.*

Tekna vil trekke frem tre områder Stortinget særskilt bør drøfte i behandlingen av meldingen.

### **Helseområdet og samfunnssikkerhet**

Helseområdet er en del av nasjonal kritisk infrastruktur. Også helsetjenesten baserer sine tjenester på digitale løsninger. Enorm mengde informasjon må til enhver tid være korrekt og tilgjengelig.

God, effektiv og sikker pasientbehandling er svært viktig og et kritisk område, noe siste året har vist oss til gangs. Utfall, hacking, manipulering og informasjon på avveie, er en løpende trussel. Tekna mener man ikke har vært god nok til å se disse utfordringene innen helseområdet, og har påpekt et stort behov for kompetanse, sterkere styring og tettere oppfølging fra justisdepartementet når man nå er offensive i å utvikle E-helseområdet. Tekna mener det er stort rom for tydeligere føringer og krav om sikkerhet i helsesektoren.

Tekna viser til Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer<sup>1</sup>.

I tre av de fire helseregionene fikk gruppen gjennom angrepssimuleringen høy grad av kontroll over viktige IKT-systemer, og derigjennom tilganger som kunne utnyttes til å volde stor skade. Med de tilganger som ble oppnådd i disse tre helseregionenes systemer kunne en reell angriper blant annet ha:

- stjålet store mengder sensitive helse- og personopplysninger
- slettet eller utilgjengeliggjort opplysninger som er nødvendige for pasientbehandlingen
- stoppet og utilgjengeliggjort systemer og utstyr som er kritisk for driften av sykehusene
- manipulert opplysninger om pasientene

Dette er svært alvorlig.

---

<sup>1</sup> <https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/undersokelse-av-helseforetakenes-forebygging-av-angrep-mot-sine-ikt-systemer.pdf>

Tekna viser også til lovforslaget regjeringen i fjor høst la frem for Stortinget om en ny E-helselov<sup>2</sup>. Tekna mente lovproposisjonen sviktet i å behandle sikkerhet og sårbarhet knyttet til utvikling og bruk av IKT-systemer og digitale løsninger. Det ser ut til å være en gjennomgangstone at man ikke jobber aktivt med IT-sikkerhet innen helse før det avdekkes grove feil og mangler, en blir utsatt for angrep eller man opplever at data er på avveie.

**Tekna mener Stortinget må understreke at IT-sikkerhet må ivaretas på en mer systematisk måte og få langt høyere prioritet enn det vi ser i dag innen helsesektoren.**

## Avansert IT-sikkerhetskompetanse

Tekna er bekymret over rekrutteringen til studier som sikrer avansert teknologisk og realfaglig kompetanse. Det er en betydelig overrepresentasjon av utenlandske kandidater innen matematikk, naturvitenskap og teknologi i våre doktorgradsprogrammer. Samfunnssikkerhetsområdet rekrutterer i stor grad fra disse fagområdene. Det er urovekkende at man ikke har klart å få opp rekrutteringen av norske kandidater. Det svekker vår evne til å håndtere IT-sikkerhet nasjonalt, det svekker våre fagmiljøer og det svekker vårt tilbud i universiteter og høyskoler.

Tekna registrerer at man i meldingen viser til en større digital kompetansesatsing, men har behov for å nyansere dette bildet.

Justis- og beredskapsdepartementet utarbeidet i 2019 en nasjonal strategi for kompetanse innenfor digital sikkerhet<sup>3</sup>.

I meldingen henvises det til at *om lag 800 mill. kroner er adressert til å styrke digital sikkerhetskompetanse, blant annet innenfor utdanning og forskning* (sit.). Tekna har på forespørsel til departementet blitt orientert om at dette dreier seg om absolutt alt som er gjort på utdanningsområdet.

Departementet svar viser oss at det kun er en liten del av denne satsningen som er rettet mot IT-sikkerhet – i beløpet ligger så godt som all satsning på forskning og rekrutteringsstillinger, som ikke er direkte koblet mot IT-sikkerhet.

Tekna mener det er en sterk overdrivelse å si at man har satset tungt på IT-sikkerhetskompetanse. Tekna viser i den sammenheng til NIFU-rapport om det kompetansegapet vi har på området<sup>4</sup>.

**Tekna ber Stortinget be regjeringen om en redegjørelse av hvordan Nasjonal strategi for digital sikkerhetskompetanse er blitt fulgt opp, hvor mange kurs og studieplasser samt forskningsstipendiater som er opprettet på dette særskilte området.**

Tekna viser til den offentlige oppmerksomhet som er reist i senere tid om forskere som utvises, datainnbrudd, spionasje og ubudne gjester på laboratorier ved norske høyskoler og universiteter<sup>5</sup>.

---

<sup>2</sup> <https://www.regjeringen.no/no/dokumenter/prop.-65-l-20192020/id2696053/>

<sup>3</sup> Nasjonal strategi for digital sikkerhetskompetanse.

<sup>4</sup> <https://nifu.brage.unit.no/nifu-xmlui/bitstream/handle/11250/2490041/NIFUrapport2017-32.pdf?sequence=6&isAllowed=y>

<sup>5</sup> <https://www.dn.no/magasinet/dokumentar/politiets-sikkerhetstjeneste/ntnu/tekna/pst-hudfletter-universitetene-fullstendig-blaoyde-og-veldig-veldig-naive/2-1-919171>

Det hevdes at antallet utenlandske forskere og akademikere som havner i norske myndigheters søkelys, har økt kraftig de seneste årene. Det handler både om spionasje og ulovlig kunnskapsoverføring til land Norge ikke har noe sikkerhetssamarbeid med.

Tekna er svært opptatt av at vi skal orientere oss internasjonalt når det gjelder utdanning, men det er også behov for å trekke opp sikkerhetsrutiner og sørge for at de er etterlevbare for de områdene i akademia hvor vi sitter på kritisk informasjon av stor nasjonal betydning. «Overføring av kunnskap» defineres som en klar trussel av norske myndigheter. Fagområder som PST anser har flerbrukspotensial omfatter både elektronikk, informasjonsteknologi, kjemi, biologi, fysikk, matematikk, romfartsteknologi, bygg og anlegg, olje og gass materialteknologi, metallurgi, mekatronikk. Og veterinærstudier.

**Tekna mener Stortinget i meldingen må adressere økt innsats fra regjeringen for å møte de utfordringer vi har knyttet til mangel på avansert nasjonal kompetanse innen disse kritiske fagområder samt utfordringer med internasjonalisering innenfor disipliner og områder overføring av kunnskap defineres som en klar trussel av norske myndigheter.**

## Skytjenester

Tekna viser til pågående arbeid og diskusjoner både nasjonalt og internasjonalt om bruk av skytjenester. I meldingen foreslår regjeringen å etablere en markeds plass for skytjenester hos Digitaliseringsdirektoratet. Markeds plassen skal gjøre det enklere for virksomheter i offentlig sektor å anskaffe sikre, lovlige og kostnadseffektive skytjenester. Dette forslaget oppfatter vi dithen at regjeringen avviser forslag om å etablere en nasjonal skyløsning.

Tekna kan ikke se at markeds plassen er et svar på sikkerheten knyttet til bruk av skytjenester. Den bidrar ikke til å sikre "nasjonal kontroll" over samfunnskritiske funksjoner. De store aktørene som Google, Amazon eller Microsofts vil måtte bli liggende på denne markeds plassen. De har definitivt de beste løsningene og det er få andre aktører som vil kunne konkurrere med disse. Derfor mener vi at markeds plassen kan være nyttig for kunder som skal kjøpe skytjenester, men at den ikke "løser" den større beredskapsproblematikken rundt å bruke skytjenester til å drifte samfunnskritiske tjenester.

Men Tekna mener likevel det er svært krevende å etablere en nasjonal skyløsning som vil fylle funksjonen til en kommersiell nettsky. De store aktørenes skytjenester består ikke bare av datalagring og beregninger, men også av tjenester, f.eks. tilgangsstyring (hvem som skal kunne legge inn og hente ut data), driftsovervåkning og mange andre tjenester (f.eks. for analyse).

Innovasjonstakten innenfor de dominerende skytjenesteplattformene er enorm, og vil aldri kunne matches av en eventuell nasjonal sky. En nasjonal sky er nødt til å ha gode grensesnitt både mot de tre store skyleverandørene, men også mot mer spesialiserte skyløsninger, f.eks. helse, politi etc. Alt dette må kontinuerlig overvåkes, testes og videreutvikles. Det er antakelig ikke mulig for staten å utvikle og drifte en slik tjeneste.

**Tekna mener Stortinget bør adressere utfordringer knyttet til en skylagring og komme tilbake til Stortinget med sak om hvordan man skal håndtere de sikkerhets- og sårbarhetsutfordringer bruk av skytjenester bidrar til.**