Til Stortingets justiskomité

13.02.2023

Teknas innspill til Meld. St. 9 (2022–2023) Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet. Så åpent som mulig, så sikkert som nødvendig.

Kompetanse

Behovet for IKT-sikkerhetskompetanse har økt i takt med den økende digitaliseringen. Justis- og beredskapsdepartementet utarbeidet i 2019 en nasjonal strategi for digital sikkerhetskompetanse[1]. Vi viser til Riksrevisjonens nylig fremlagt rapport[2] hvor det påpekes at regjeringen ikke har fulgt opp sine egne strategier knyttet til samfunnssikkerhet, noe Tekna har påpekt gjentatte ganger gjennom de siste tre årene.

Regjeringen skriver i sin egen strategi følgende*:*

Det enkelte departement har et overordnet ansvar for digital sikkerhet innenfor sin sektor. I dette inngår også et ansvar for å tilrettelegge for at man i egen sektor/egen virksomhet har adekvat kompetanse.

Nasjonal strategi for digital sikkerhetskompetanse retter seg både mot myndigheter og offentlige og private virksomheter.

Tekna mener departementene har et klart overordna ansvar *for digital sikkerhet innenfor sin sektor* og ansvar for å kartlegge kompetansebehov. Basert på denne kartleggingen vil det være mulig og nødvendig for universiteter og høyskoler å vurdere dimensjonering av studieplasser, enten som etter- og videreutdanning, som gradsprogrammer eller doktorgradsprogrammer.

Tekna mener det ikke kan være universiteter og høyskolers oppgave alene å kartlegge arbeidslivets behov for IT-sikkerhetskompetanse slik regjeringen initierer. Tekna mener regjeringen har et ansvar for at sivil sektor utfordres til å avdekke eget kompetansebehov og at dette rapporteres til de utdanningsleverandørene som er best egnet til å gi eller utvikle kompetansetilbud.

[1] https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf

[2] https://www.riksrevisjonen.no/globalassets/rapporter/NO-2022-2023/myndighetenes-samordning-av-arbeidet-med-digital-sikkerhet-i-sivil-sektor.pdf

Justis- og beredskapsdepartementet har også anbefalt at alle departementer, i samsvar med sikkerhetsloven, kartlegger hvilke lederstillinger i underliggende virksomheter som krever sikkerhetsklarering og sikkerhetsfaglig kompetanse. Resultatet skal nå foreligge.

Tekna mener Stortinget må be regjeringen sikre at virksomheter innen samfunnskritiske områder melder inn kompetansebehovene til utdanningsinstitusjonene i tråd med regjeringens strategi.

Tekna erfarer at det er en stor utfordring å skaffe tilstrekkelig med vitenskapelig ansatte i UH-sektoren til å løse kompetansegapet innen IT og særlig IT-sikkerhet.

Tekna ber Stortinget sikre at det følger friske midler og rekrutteringstiltak for å ansette flere undervisere hvis Stortinget vedtar å øke antallet studieplasser.

Rekruttering av doktorgradskandidater som kan sikkerhetsklareres er en utfordring innenfor ulike teknologiområder allerede i dag. De siste ti årene har godt over 60 prosent av dem som avlegger doktorgrad innenfor teknologi ved et norsk lærested utenlandsk statsborgerskap. Andelen med utenlandsk statsborgerskap som søker rekrutteringsstillinger innen matematikk, naturvitenskap og teknologi var nær 90 prosent i perioden 2016-2018. Dette er en utvikling som må tas på alvor.

Tekna ber Stortinget be regjeringen sette i gang tiltak for å øke rekrutteringen av vitenskapelig ansatte blant norske kandidater til forsknings- og undervisningsstillinger i MNT-fagene.

Regjeringen foreslår å videreføre øremerkede midler til nærings-ph.d.- og offentlig sektor-ph.d.-ordningene i Forskningsrådet rettet mot digital sikkerhet og kryptologi.

Tekna mener det ikke er tilstrekkelig å videreføre øremerkede midler, disse må økes og det må settes i gang et større arbeid med å utvikle konkrete tiltak for å øke rekrutteringen.

Tekna foreslår å øke andelen offentlig finansiering av nærings-PhD og offentlig PhD innen sektorovergripende samfunnskritiske områder som digital sikkerhet.

Digital motstandskraft i kommunesektoren

Regjeringen vil bidra til forebygging av uønskede digitale hendelser i kommunesektoren og vil utpeke et sektorvis responsmiljø som kan dekke kommunenes behov. Hovedutfordringen er, slik Tekna ser det, mangel på adekvat kompetanse i de fleste av våre kommuner. Vi viser til vår egen undersøkelse om kompetansebehov i kommunesektoren, hvor IT-kompetanse er den absolutte største utfordringen. Et sektorvis responsmiljø vil kunne være et godt tiltak, men hovedutfordringen ligger, slik vi ser det, i mangel på kompetanse og flukten fra kommunesektoren og over i privat næringsliv.

Tekna ber Stortinget be regjeringen komme tilbake med konkrete tiltak for å bidra til bedre rekruttering av IT-sikkerhets-kompetanse og tiltak for kompetanseheving for å møte behovet for avansert IT-sikkerhets-kompetanse i kommunene.

Nasjonal kontroll over verdier og virksomheter

I meldingen heter det at det er et mål at norske myndigheter skal ha mulighet til å fange opp, vurdere og eventuelt gripe inn i økonomisk aktivitet som kan true nasjonal sikkerhet. Samtidig er det viktig at Norges folkerettslige forpliktelser ivaretas og at det ikke legges unødvendige eller uforholdsmessige byrder på næringslivet eller begrensinger på handelen med andre land. Dette er utfordrende siden håndtering av sikkerhetstruende økonomisk aktivitet treffer i skjæringspunktet mellom sikkerhetsinteresser og næringslivs-, utenrikspolitiske og handelspolitiske hensyn. De ulike departementene jobber derfor tett sammen for å vurdere de ulike hensynene opp mot hverandre. Regjeringen foreslår å vurdere hvordan man på en hensiktsmessig måte kan få bedre oversikt over virksomheter og verdier som ikke dekkes av sikkerhetsloven, men som likevel kan ha betydning for nasjonal sikkerhet.

I arbeidet med utpeking av objekter og infrastruktur som skal ligge inn under sikkerhetslovens virkeområde, har sektordepartementene ansvaret for å gjøre gode risiko- og sårbarhetsanalyser (ROS-analyser) som grunnlag for utpekingsarbeidet. I denne vurderingen vil det avdekkes hvilke virksomheter som ligger i grenselandet. Tekna viser til Riksrevisjonens rapport hvor det fremgår at dette arbeide er sterkt forsinket.

Tekna mener Stortinget må be regjeringen sette tidsfrist for ROS-analysene i sektordepartementene for å få oversikt over virksomheter av betydning for nasjonal sikkerhet. Tekna er overrasket og bekymret over at det åpenbart ikke foreligger en slik oversikt i dag.

Nasjonal skytjeneste

Stadig flere virksomheter velger allmenne skytjenester for å imøtekomme behovet for nye og forbedrede IT-løsninger. For flere statlige virksomheter er det imidlertid en utfordring at det ikke finnes tilgang på funksjonelle og kostnadseffektive skytjenester med tilstrekkelig grad av nasjonal kontroll. Det kan føre til økt risiko dersom man likevel velger slike løsninger. Alternativet er at virksomhetene må velge lokale løsninger, noe som kan føre til høyere kostnader og begrenset tilgang til nye teknologiske verktøy. Problemet forventes å øke i tiden som kommer.

De funksjonene samfunnet er mest avhengig av bør leveres fra datasentre i Norge. Offentlig sektor i Norge benytter seg av IKT-tjenester som er lokalisert og driftet utenfor Norge. Så lenge disse sentrene er utenfor Norge vil det være utfordringer knyttet til sikkerheten og dermed vanskelig å bruke slike sentre til samfunnskritiske funksjoner eller skjermingsverdig informasjon. Dersom datasenternæringen skal fortsette å vokse i Norge, så er det viktig at formålstjenlige reguleringer og gode rammevilkår kommer på plass.

Tekna mener Stortinget må be regjeringen legge til rette for at flere norskeide datasentre leverer skytjenester i Norge. Det vil kunne bidra til å bygge opp en sentral verdikjede rundt datasentrene i Norge, og samtidig redusere sårbarheten med bruken av internasjonale skytjenester.