NITO NORGES STØRSTE ORGANISASJON FOR INGENIØRER OG TEKNOLOGER

Justis- og beredskapsdepartementet

15. mars 2016

Vår ref. 487549 Deres ref.

Høringssvar NOU 2015:13 Digital sårbarhet – sikkert samfunn

NITO - Norges Ingeniør- og Teknologorganisasjon er Norges største organisasjon for ingeniører og teknologer med over 80 000 medlemmer. Vi organiserer ingeniører og teknologer i alle sektorer, herunder ca 10 000 innen IKT.

NITO mener det positivt at Regjeringen har nedsatt et digitalt sårbarhetsutvalg. Norge er langt fremme på bruk av IKT, og tillit til digitale tjenester er en forutsetning for videre digitalisering av Norge. Datakriminalitet påfører samfunnet enorme kostander hvert år, og reduksjon i digital sårbarhet er derfor viktig for så vel rikets sikkerhet, innbyggernes sikkerhet, personvern og verdiskapingen/innovasjon.

Kunnskap og rekruttering innen digital sårbarhet
Rapporten konkluderer med mangel på kompetanse om digital sårbarhet på alle nivåer. Dette er ikke overraskende, da Norge generelt mangler personer med IKT-kompetanse. Skal vi fortsette å være i verdenstoppen på digitalisering må IKT-kompetanse og kunnskap om digitalisering styrkes. NITO støtter derfor hovedforslaget om en nasjonal kompetansestrategi for IKT-sikkerhet. Denne burde ses i sammenheng med en opptrapping av studieplasser innen IKT generelt.

Utvalget viser til en underdekning av kandidater med generell IKT-kompetanse og av kandidater med spesifikk IKT-sikkerhetskompetanse. Flere studiesteder har ikke IKT-sikkerhet i sin undervisning. Personer med generell IKT-kompetanse bør ha grunnleggende kunnskaper om IKT-sikkerhet. Ved et digitalt angrep kan ordinært driftspersonell i verste fall gjøre situasjonen verre, fordi de ikke forstår konsekvensene av sine handlinger sett fra angriperens ståsted. NITO støtter innføring av krav til IKT-sikkerhet i alle IKT-bachelorgrader. Kapasiteten på mastergrader innen IKT-sikkerhet må også styrkes.

I tillegg til flere studieplasser har NITO lenge vært opptatt av at det må satses mye mer på reduksjon i frafall. Gjennomstrømning på ingeniørstudiet totalt er 65 % etter fem år. Satsing på gjennomstrømning innebærer at utdanningene har midler til infrastruktur og tilføres flere lærerkrefter.

Utvalget ser ut til å legge lite vekt på å løfte kompetansen blant de som allerede jobber med IKT. Læring på arbeidsplassen vil bli enda viktigere framover, og arbeidsgiver og arbeidstaker har et felles ansvar for kursing og videreutdanning. NITO mener ledere i offentlige virksomheter må gå foran ved å legge til rette for slik kompetanseheving. I tillegg bør Regjeringen innføre kompetanseFUNN etter modell fra skatteFUNN. Det vil si at mens skatteFUNN er en modell for skattefradrag på forskning, så kan kompetanseFUNN bli en modell for skattefradrag på satsing på ansattes kompetanse. Dette vil også kunne bli en del av nasjonal kompetansestrategi for IKT-sikkerhet.

NITO mener barn og unges kompetanse i realfag og teknologi må styrkes i grunnskolens ungdomstrinn og i videregående skole, og støtter utvalgets forslag til tiltak. Ikke minst må barn og unge forstå konsekvensene av de digitale sporene de etterlater seg, og at data om dem lett kan bli tilgjengelige for andre. Det er behov for å styrke lærerutdanningen og kursing av lærere i teknologifag. Valgfag i koding bør etter prøveperioden utvides til

alle skoler. Det må tilstrebes en undervisningsform som inspirerer elevene, med både en praktisk og teoretisk tilnærming til fagene. Eksempler på slik undervisning er Teknologi og Design (barne- og ungdomstrinn), Teknologi i praksis (ungdomstrinn) og Teknologi og forskningslære (videregående skole).

Organisering av det offentlige for en bedre IKT-sikkerhet

Når den fjerde industrielle revolusjon treffer oss handler det i stor grad også om nye forretningsmodeller, og at samfunnet organiseres på nye måter. Her er det helt avgjørende at organiseringen av IKT-sikkerhet i offentlig sektor følger utviklingen. Ikke minst er dette viktig for å skape riktig balanse mellom sikkerhet og innovasjon. Regjeringen må sørge for at IKT-sikkerhetsnivået får det tilstrekkelige løftet uten at det unødig bidrar til å bremse for nødvendig innovasjon.

NITOs medlemmer uttrykker frustrasjon over små kompetansemiljø og manglende koordinering av ansvaret innen IKT-sikkerhet i offentlig sektor. Det er for lav utnyttelse av de gode kompetansemiljøene som finnes, samtidig som andre miljøer mangel nødvendig kompetanse. Nasjonal sikkerhetsmyndighet er i denne sammenheng et sentralt direktorat med omfattende IKT-sikkerhetskompetanse og med et sektorovergripende mandat, men uten tilstrekkelig myndighet til å følge opp mandatet. Vår erfaring er at fragmenterte miljøer og svake sektorovergripende virkemidler har som konsekvens at ingen blir målt på fremdrift og leveranse for helheten, noe som igjen får konsekvenser for Norges samlede IKT-sikkerhet.

NITO er derfor enig med utvalget i at organiseringen av IKT-sikkerhet har et tydelig behov for flere sektorovergripende virkemidler. I dag har Justisdepartementets samordningsansvar for IKT-sikkerheten og skal sikre et «koordinert og helhetlig arbeid på tvers av sektorgrenser». Forsvarsdepartementet har ansvar for forebyggende IKT-sikkerhet i forsvarssektoren. Det enkelte fagdepartement som har det overordnede ansvaret for å ivareta sikkerheten i sektorens IKT-infrastruktur, og for å drive forebyggende IKT-sikkerhetsarbeid. I tillegg har en rekke myndighetsaktører et særlig ansvar for oppfølging av ulike sider ved IKT-sikkerheten knyttet til forebygging, avdekking, håndtering og etterforskning.

NITO støtter utvalgets forslagene til sektorovergripende tiltak som omhandler etablering av en minstestandard for beskyttelse av kritisk infrastruktur, tiltak for et felles tverrdepartementalt kunnskapsgrunnlag for virkemiddelbruk, og etablering av strategisk arena for offentlig privat samarbeid. Når det gjelder digitale angrep er det uten tvil også behov for et helhetlig rammeverk for digital hendelseshåndtering som beskriver relevante myndighetsaktørers roller og ansvar.

NITO er imidlertid i tvil om dette er tilstrekkelig, og mener det burde utredes hvordan IKT-sikkerhetsansvaret kan styrkes med sektorovergripende ansvar på departementalt nivå. F.eks. gjennom et fast interdepartementalt utvalg med ansvar for koordinering av IKT-sikkerhet. En slik utredning bør ses i sammenheng med Stortingets egen utredning av organisering av IKT-ansvaret i offentlig sektor.

Tilsynene er sentrale forebyggende aktører ved at de kan føre tilsyn med sårbarhetsreduserende tiltak i den enkelte sektor. Gjennomgangen av de enkelte tilsynene viser at mange har for lav IKT-sikkerheteskompetanse og/eller lav kapasitet til å gjennomføre tilsyn.[1] Samtidig møter de mange av de samme utfordringene og et tettere samarbeid gjennom en fellesarena for tilsynsarbeid på IKT-sikkerhetsområdet slik utvalget foreslår synes nødvendig.

I dag blir tilsynenes sikkerhetsarbeidet fragmentert, og virksomhetene som har flere sektorer i sin portefølje blir spesielt rammet. Tilsynene møter svært ulike krav, og har i ulik grad nødvendig hjemmel til å utøve IKT-sikkerhetsrettet aktivitet. Det vil være mye enklere for den enkelte virksomhet å forholde seg til ett sektorovergripende regelverk for IKT-sikkerhet. Mange hendelser går på tvers av sektorer. NITO mener at det er behov for samordning av regelverk som omtaler IKT-sikkerhet.

[1] Herunder Norges Vassdrag- og Energidirektorat, Petroleumstilsynet, Mattilsynet og tilsynsmyndighetene innen transport.

En samordning av regelverk bør og legge til rette for et teknologisk rammeverk for IKT-sikkerhet. Det vil si at de som vil utvikle og innovere på IKT-siden (f. eks. innovasjon innen helsesektoren) må forholde seg til minstekrav for sikker håndtering av informasjon (knyttet til personvern og samfunnssikkerhet) og i form av minstekrav til innebygd sikkerhetsnivå. Et slikt rammeverk vil kunne gi samfunnet den nødvendige grad av tillit til nye løsninger som kommer gjennom innovasjon, samtidig som det blir forutsigbart og sannsynligvis enklere å drive med innovasjon.

Tilsynene kan i dag bli utfordret fordi regelverkene ikke klarer å følge den tekniske utviklingen. Regelverket må tilpasses det faktum at teknologien endrer seg raskt. NITO mener det må satses kraftig på funksjonsbaserte regelverk som retter seg mot mål og resultater i motsetning til tekniske spesifikasjoner.

Sikkerhet ved bruk av skytjenester

Regjeringen har oppe til vurdering en endring av lov om offentlige arkiv for å tillate lagring av arkiver fra offentlige virksomheter i skyløsninger med servere i utlandet. Det vil også foretas en gjennomgang av regnskapsloven. Skytjenester har selvsagt mange fordeler herunder rimelige og fleksible IT-løsninger, effektivisering av driften, økt tilgang og enkel skalerbarhet. Ved offshoring av data til utlandet vil imidlertid tjenesteleverandøren befinne seg under en annen jurisdiksjon enn Norge. NITO mener norske data må lagres i henhold til norsk lovgivning også i utlandet.

NITO er opptatt av de sikkerhetspolitiske konsekvensene ved bruk av skytjenester. Det finnes gode eksempler på norske virksomheter som har hatt ønske om å ha datasentre i land med ustabil sikkerhetspolitisk situasjon. Ukraina er et aktuelt eksempel på dette. Norges politiske uavhengighet blir utfordret dersom vi er prisgitt et annet lands forvaltning av sensitive eller samfunnskritiske data.

Et godt lovverk og gode avtaler løser mye, men det vil ikke ha mye å si dersom vertslandet ignorer avtalene. Det er en risiko for at offentlige registre eller elektronisk styring av vital infrastruktur som blir utflagget til et datasenter i et annet land kan bli brukt mot Norge. F.eks. gjennom utpressing eller andre former for obstruksjon.

Mange offentlige etater anbefalt å lagre data i Norge for eksempel forsvar, politi og helsevesen. Det er likevel knyttet usikkerhet til kravene for lagring. Utvalget deler inn data i tre kategorier: (1) informasjon som kun bør lagres i Norge, (2) informasjon som kan lagres i utlandet, men som må flyttes tilbake Norge ved særlige behov og (3) informasjon som kan lagres i utlandet uten vilkår. NITO mener at alle offentlige registre som lagrer sensitive eller samfunnskritiske data må lagre data på servere i Norge, og at registrene må driftes av norske selskap, og altså må høre innunder kategori 1. NITO støtter en felles utredning av tilsynspraksis for data lagret i skytjenester.

Utvalget påpeker at mange virksomheter ikke vil ha nødvendig teknisk eller juridisk kompetanse, og det kan være praktisk vanskelig å gjennomføre en risikovurdering. Offentlige virksomheter må ha tilgang til både kompetanse og klare retningslinjer ved bruk av skytjenester. En av fem virksomheter vet ikke i hvilket land deres data blir lagret ifølge Mørketallsundersøkelsen 2014. Kun 2 av 5 av virksomhetene i offentlig sektor har avsatt interne ressurser til oppfølging av tjenesteleverandør. Mørketallsundersøkelsen påpeker at underleverandører blir benyttet for å nå frem til data hos offentlige aktører. NITO mener rådgivningsmiljøene i Datatilsynet og Difi må styrkes slik at det blir enklere å ta beslutninger om dataplassering for kommuner og andre virksomheter i offentlig sektor. Videre må det utvikles et samarbeid med Nasjonal Sikkerhetsmyndighet slik at man tar hensyn både til personvern og sikkerhetspolitiske aspekterr ved bruk av skytjenester i utlandet.

Utvalget påpeker at sikkerhetskompetanse hos leverandører av skytjenester er svært uensartet. NITO mener det bør opprettes et felles minimumskrav for tilbydere av skytjenester til offentlig sektor med standarder for bl.

a. grensesnitt og sikkerhetsnivå. Dette skal sørge for at det opprettholdes et gitt sikkerhetsmessig nivå. Det skal samtidig gjøre det enklere for det offentlige å bytte leverandør.

Tredjepartskontroll kan være en løsning for kvalitetssikring av skytjenester, noe som blant annet Datatilsynet har godtatt tidligere. Slike kontroller må imidlertid påse at tjenesten er i forhold til norsk lov, i tillegg til at den holder en gitt standard. Det vil være nødvendig med en felles utredning av dette slik både Lysneutvalget og en interdepartemental gruppe som ser på skytjenester anbefaler.

NITO for øvrig vil fremheve, som utvalget gjør, at utstrakt bruk av utkontraktering kan bidra til å svekke den nasjonale evnen til utvikling og oppfølging på sentrale kompetanseområder. Selv om utkontraktering kan være innenfor akseptabel risiko for den enkelte virksomhet kan det få store konsekvenser for samlet risiko dersom mange virksomheter flytter sin IKT-virksomhet ut av landet.

Med vennlig hilsen

Trond Markussen
President

Steinar Sørlie
Generalsekretær