FAGFORBUNDET

14 MAR 2016

Justis- og beredskapsdepartementet
Postboks 8005 Dep.

0030 OSLO

Deres ref.	Vår ref / Saksbehandler	Dato:
	16/842-2 U01 &13 Marit Wahlstedt / tlf. 23 06 46 52	11.02.2016

HØRING - DIGITAL SÅRBARHET - SIKKERT SAMFUNN - NOU 2015:13

Fagforbundets mener at problemstillingene som reises i høringen Digital sårbarhet – sikkert samfunn er svært viktige. Digitaliseringsutviklingen er tett knyttet til utviklingen av arbeidslivet, og Fagforbundet er opptatt av at hensynet både til enkeltmennesker og samfunnet ivaretas.

Utredningen «Digital sårbarhet – Sikkert samfunn» er omfangsrik og mangeartet, og reflekterer med det hvor samfunnsgjennomgripende problemstillingene som reises er.

Utvalget peker både samlet og sektorvis på sårbarhetsproblematikk som bør tas fatt i. Fagforbundet har valgt å kommentere utredningen på en del av områdene, først og fremst på områder der forbundet har kompetanse gjennom at det organiserer aktuelle yrkesgrupper.

Fagforbundet vil i det vesentlige slutte seg til de viktigste anbefalingene fra utvalget, som er uttrykt i ni strekpunkter i utredningens innledende sammendrag. Noen av disse punktene ønsker vi å kommentere.

Utvalget nevner innledningsvis at Norge regnes som et av de mest digitaliserte landene i verden, og at denne situasjonen gjør at det ofte mangler tydelige eksempler fra andre land å se hen til i arbeidet med å redusere sårbarhet. I den sammenhengen ønsker Fagforbundet å understreke betydningen av at arbeidstakere i alle sektorer og fagområder er godt representert i arbeidet med å utvikle og implementere alle former for digitale verktøy. Også i arbeidet med å vurdere og redusere risiko og sårbarhet, vil erfaring og kunnskap hos de som arbeider med verktøyene til daglig kunne spille en avgjørende rolle. Utvalget er inne på dette, blant annet i kapittel 17.7.1, der det vises til at helsefaglig personell, med bakgrunn i at disse best kjenner sine egne arbeidsprosesser, må være med på å sette premissene for sikkerhetstiltak, for å sikre at tiltakene forankres godt nok i virksomhetene.

I kapittel 17.5.5 om «Særskilte personvernutfordringer», komme utvalget inn på helsesektorens etter hvert svært omfattende registrering av sensitive personopplysninger i form av helseopplysninger, og den mangelfulle styring av tilgangskontroll til disse opplysningene, som har vært påtalt av Datatilsynet og Riksrevisjonen. Fagforbundet er enig i at logging av oppslag i registre og journaler ikke kan veie opp for manglende styring av tilgangskontroll. Samhandlingsreformen vil føre til at stadig flere som arbeider i helsesektoren får tilgang til

pasientopplysninger, noe som vil øke risikoen for at sensitive opplysninger kommer på avveie. Fagforbundet mener at arbeidet med å etablere forsvarlig tilgangskontroll må komme i gang så snart som mulig, og at regjeringen må utarbeidet en plan med tiltak og finansiering som gir denne prosessen det nødvendige politiske løft.

En av utvalgets viktigste anbefalinger er å «sikre balansen mellom personvern og et sikrere samfunn gjennom utredninger og offentlig debatt». Fagforbundet er enig i dette, og vil vektlegge betydningen av at politiske beslutninger på dette området forankres i bred og åpen demokratisk debatt og et generelt godt kunnskapsnivå, både om teknologiens muligheter og de menneskerettslige aspekter av personvernet. Etter Fagforbundets mening preges dagens digitale virkelighet av alt for stor kunnskapsmessig avstand mellom den vanlige samfunnsborger og sentrale beslutningstagere. En bredt anlagt offentlig debatt vil bidra til å redusere denne avstanden.

Fagforbundet er videre enig med utvalget i at kritikaliteten av Telenors kjerneinfrastruktur bør reduseres gjennom at minst en annen aktør bygger opp et kjernenett som på alle sentrale parametre kan måle seg med Telenors. Sårbarheten i Telenors nett ble senest illustrert gjennom hendelsen fredag 19. februar 2016, da om lag en million abonnenter tilknyttet Telenors nett var uten forbindelse i flere timer – også til nødnumrene - etter en feil som var oppstått i Norge, men utløst av trafikk fra utlandet. Fagforbundet mener det må utredes i hvilken grad det teknisk kan legges til rette for konkurrerende aktører med egen infrastruktur å samvirke i under alvorlige hendelser, kriser eller kriselignende situasjoner, og hvordan plikt til et slikt samvirke eventuelt kan hjemles i konsesjonsvilkår eller på andre måter.

Det er rapportert at oppkall til nødnumre ikke var mulig under hendelsen 19. februar fra telefoner med Telenor SIM-kort, og at brukerne måtte ta ut SIM-kortet og restarte telefonen for å komme fram. Det er svært uheldig at muligheten til å nå nødnumre faller vekk for et så stort antall brukere samtidig, og det bør vurderes om det er nødvendig å stille krav til telefonprodusenter og nettverksleverandører om teknologiske løsninger som i sterkere gard sikrer tilgangen til nødnumre under lignende framtidige hendelser.

Fagforbundet er enig i utvalgets vurderinger av spørsmålet om regulering av kryptografi.

Fagforbundets øvrige kommentarer er knyttet spesielt til kapittel 5, kapittel 11, kapittel 17 og kapittel 19.

Kapittel 5 Sikring av IKT og digital informasjon

Formålet med Arkivloven er å sikre arkiv som har omfattende kulturell eller forskningsmessig dokumentasjon eller som inneholder rettslig eller viktig forvaltningsmessig dokumentasjon blir tatt vare på og gjort tilgjengelige for ettertiden. Arkivloven omfatter alle typer offentlige arkiv (med noen unntak jf Arkivloven § 5) samt visse typer privatarkiv, jf Arkivloven § 13. Arkivmaterialet er et autentisk vitnesbyrd fra tiden det ble skapt. Det er dermed en gjengivelse av en hendelse, som man kan stole på som primærkilde. Arkivmaterialet bevares i sin originale stand og kan tolkes ut i fra sitt innhold, form og kontekst. Arkivets autentisitet er en forutsetning for at man kan stole på informasjonen som finnes i dokumentasjonen.

Et arkiv har som hensikt å bevare dokumentasjon for ettertiden i en form som gjør at de kan fungere som støtte for samfunnet og kan brukes som bevis. I høringsnotatet står det klart: «Integritet innebærer at informasjon er til å stole på, og at systemer og tjenester fungerer slik

det er tenkt. Informasjonen skal være korrekt og gyldig. Bare de som har lov til å endre informasjonen, får endret den. Relatert til integritet har vi autentisitet, som handler om å sikre opphavet til informasjonen, for eksempel bekrefte identiteten til en sendt melding. Nært relatert har vi også ikke-fornekting (non-repudiation), som handler om at en digital handling ikke skal kunne benektes i etterkant.»

Tilliten til at informasjonen er autentisk og fullstendig er viktig om vi skal kunne regne dokumentene som bevis på handlinger som er utført. Tillitt til arkivets autentisitet er viktig å bevare også i forbindelse med avlevering og uttrekk. Dette må skje etter arkivfaglige prinsipper og retningslinjer, ellers kan rettsikkerheten for hver av oss bli vesentlig svekket. I forskriften om Offentlege arkiv §§ 2-13 og 2-14 stilles det krav til system for å lagre saksdokumentene elektronisk som også sikrer at bevaringsverdig materiale kan avleveres til arkivdepot. Autentitetsgivende funksjoner, bevaring- og kassasjonsfunksjoner, uttrekksfunksjoner og kontekstgivende metadata må være tilstede i systemet for å ta vare på arkivdokumenter. Det er viktig å holde oversikt over dokumentbestanden og gjøre bevaringsvurderinger ut i fra faglige prinsipper (jf «Riksarkivarens forskrift» til Arkivlova). Ikke minst er dette viktig på grunn av den økte informasjonsmengden.

Fagforbundet mener at sårbarhet i denne sammenheng kan være:

- Manglende tilgang til saksbehandlingssystemer ved strømbrudd pga terrorangrep, uvær eller lignende.
    - Systemet vil ikke fungere.
- Manglende eller mangelfull tilgangspolitikk til tilgangsbegrensede opplysninger eller gradert informasjon i systemet.
- Feil konvertering slik at dokumenter ikke lenger er tilgjengelige i systemet.
- Databaser/fagsystemer som ikke er søkbare.
    - Systemene vil fungere, men informasjon er ikke tilgjengelig.
- At det ikke blir foretatt uttrekk av elektroniske sak/arkivsystem (i offentlige arkiv) for avlevering for deponering/langtidsbevaring til arkivdepot
- At fagsystemer ikke blir bevart.
    - Systemene vil fungere selv om uttrekk for avlevering til en depotinstitusjon ikke blir foretatt, men det er her snakk om at vi står i fare for å miste et helt elektroniske arkiv som det ikke blir foretatt uttrekk av.
- I forskriften om offentlege arkiv §2-6 står det at et offentlig organ skal ha en eller flere journaler for registrering av dokumenter i de sakene organet oppretter. Det kan her være snakk om dokumenter underlagt Offentleglova og Personopplysningsloven. Journalene blir offentliggjort på internett. Manglende kvalitetssikring av journalene kan føre til at taushetsbelagte opplysninger blir

offentliggjort, for eksempel personopplysninger

- Systemene vil fungere selv om journalene ikke blir kvalitetssikret, men taushetsbelagte opplysninger kan bli offentliggjort.

Kapittel 11 Elektronisk kommunikasjon
Nødnett
Som utredningen også peker på, er de nasjonale nødnettene basert på de eksisterende infrastrukturene for telekommunikasjon. Videre er det pekt på store usikkerhetsfaktorer på området, manglende kartlegging og forhold knyttet til blant annet strømbrudd. Nødmeldingssentralene som opererer disse nettene er helt avhengig av nettet fungerer. Det er her snakk om forhold knyttet til livreddende tjenester. Det er høyst kritikkverdig at man ikke har sett på hvilke muligheter man har, og foretatt de nødvendige kartlegginger som trengs for å ha et alternativt opplegg.

Den sterke sentraliseringen som har funnet og vil finne sted gjennom samlokalisering og reduksjon av nødmeldingssentraler har ytterligere forsterket risikomomentet. Nødetatene har ved flere tilfeller de siste årene hatt hendelser som har satt varsling og kommunikasjon ut av spill. Nødetatene har opplevd problem der publikum ikke har kunnet varsle om nødsituasjoner. Nødmeldingssentralene har heller ikke kunnet varsle ut sine ressurser og de har ikke kunnet kommunisere under aksjon.

Under ekstremværet Tor 29. januar 2016 opplevde nødetatene at over 40 basestasjoner i nødnettet ramlet ut. Hele 95 stasjoner gikk på reservestrøm, og flere av basestasjonene var ute av drift i flere dager. Dette er en situasjon vi ikke kan leve med siden nødetatene ikke har nødsystemer. Det som gjorde at en ble berget i dette tilfellet var at mobilnettet denne gang stort sett ikke hadde nedetid.

Sårbarheten i Nødnettet får størst konsekvenser i distriktene siden en her har lite infrastruktur for nettet. I de områdene som er tettest befolket er det en overdekning av basestasjoner slik at det fungerer her selv om noen faller ut. I distriktene vil nedetid kunne få den konsekvens at alt samband i området faller ut.

Kapittel 17 Helse- og omsorg
Helse- og omsorgsektoren er komplekst organisert og har derfor en stor digital sårbarhet knyttet til taushetsplikt, dokumentasjonsplikt og informasjonsplikt. Det fordrer at bruk av IKT må sikres på alle nivå med tanke på sårbarhet både ved strømbrudd, dataløsninger og andre uforutsette hendelser. Det fordrer også at de ansatte har nødvendig opplæring i bruk av IKT-løsninger. Fagforbundet er enig med utvalget i at det er behov for en beredskap for at sentrale helse- og omsorgstjenester kan opprettholdes uavhengig av IKT.

Fagforbundet er enig med utvalget i at det er behov for sterkere nasjonal styring fra Helse- og omsorgsdepartementets side og stiller oss like undrende som utvalget gjør til at HOD ikke allerede har tatt grep.

Fagforbundet mener at internkontrollforskriften for helse- og omsorgstjenestene er et viktig verktøy for å sikre gode løsninger ved bruk av IKT. Fagforbundet vil vise til vårt høringssvar til «Forskrift om styringssystem i helse – og omsorgssektoren», som ble sendt HOD 01.02.16.

For øvrig viser vi til utvalgets anbefaling i pkt. 17.7. Vurderinger og tiltak om at de ansatte som kjenner arbeidsprosessene tas med på å sette premissene for sikkerhetstiltak.

Kapittel 19 Kompetanse
Utvalget innleder kapitlet med: «For å kunne delta i en stadig mer digital hverdag er det en forutsetning å ha grunnleggende kunnskap om bruk av IKT.» Utvalget sier videre at dette også gjelder hvordan man forholder seg til digitale trusler og sårbarheter. Det er behov for å styrke befolkningens grunnleggende kompetanse om bruk av IKT og bevissthet og dømmekraft i forhold til digital sikkerhet. Men det er også behov for å øke den mer spesialiserte kompetansen om bruk av IKT.

Fagforbundet mener utvikling av grunnleggende kunnskap om bruk av IKT starter allerede i barnehagen. I barnehagen tas digitale verktøy i bruk i stadig større grad og er en naturlig del av barnehagens hverdag. For å kunne sikre god IKT-kompetanse i befolkningen må det legges vekt på dette i barnehagen. Dette er viktig for å gi alle et best mulig utgangspunkt for videre læring og bevisst IKT-bruk.

Utvalgets vurderinger og tiltak
19.8.1. Etablere en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet
Fagforbundet støtter utvalgets forslag om å etablere en overordnet nasjonal kompetansestrategi om IKT-sikkerhet. Dette er nødvendig for å se ulike forhold rundt dette i sammenheng, for å kunne målrette kompetansehevingstiltak, kompetanseutvikling, forskning, og for å dekke hele spekteret fra grunnleggende kompetanse til spesialisert IKT-sikkerhetskompetanse.

19.8.2 Prioriteringer i en overordnet strategi
Oppvekst- og utdanningssektoren
I hele oppvekst- og utdanningssektoren er IKT-sikkerhet og personvernrelaterte problemstillinger svært sentrale. I tillegg er det denne sektoren som skal ta ansvar for å sikre samfunnets behov for både grunnleggende og spesialisert kompetanse om bruk av IKT og IKT-sikkerhet. Økt bruk av IKT fordrer større årvåkenhet og systemer som reduserer sårbarheten i hele samfunnet så mye som mulig. I mange sektorer vil det da kreves høyere kompetanse enn i dag, og det må være ansatte i offentlig og privat sektor som har IKT-sikkerhet som sitt hovedarbeidsområde.

I barnehage- og skolesektoren oppbevares mye personopplysninger, dokumentasjon av barn og unge og deres utvikling, bakgrunn, opplysninger om eventuelle spesialfaglige tiltak med eksterne, skoleresultater, kartlegginger osv. Barnehage- og skoleeiere, ledere i barnehager og skoler må alle ha en viss kompetanse i IKT-bruk, IKT-sikkerhet og digital sårbarhet. IKT-bruk og IKT-sikkerhet må bli del av lederutdanningene innen barnehage og skole. I tillegg må personalet ha kompetanse om det samme siden det er de som også skal tilrettelegge for den framtidig økte kompetanse på dette området i samfunnet.

Fagforbundet er bekymret over at Datatilsynet under tilsyn har avdekket at barnehageeiere i liten grad kjenner til personopplysningsloven og plikten de har til å sikre at opplysninger om barn behandles lovlig og sikkert[1]. Norske barn kartlegges både i barnehage og på skole. Noen ganger er dokumentasjon viktig i tilrettelegging av tiltak for å hjelpe barn tilstrekkelig, men

[1] https://www.personvernbloggen.no/2016/02/16/onsker-vi-okt-lagring-av-opplysninger-om-barnehagebarn/

både mengden informasjon, hva som er kartlagt og måten opplysningene behandles og lagres på, er viktig. I denne sammenhengen er både utstyret som benyttes, kartleggingsverktøyet og informasjonssystemene, samt kunnskapen til foreldre, ansatte og eierne avgjørende.

Fagforbundet støtter utvalgets vurdering om at dette temaet må inn i læreplaner i grunnopplæringa. Dette er Utdanningsdirektoratets ansvar og kan tas på en slik måte at temaene og fordypningsgraden tilpasses de ulike fagene og de ulike delene av læreplanverket. På denne måten kan også opplæring i teknisk bruk av IKT og programmering komme inn der det passer. Når det gjelder yrkesfaglig videregående opplæring er det viktig at de faglige rådene for fagopplæringa involveres i dette. De kan vurdere dette faglig og se det i sammenheng med arbeidslivets behov for kompetanse, for eksempel slik utvalget peker på innen elektrofagene.

19.4.3, 19.4.4 og 19.5 Forskning og høyere utdanning
Fagforbundet støtter også utvalgets forslag om tiltak på forskningsområdet og innen høyere utdanning. Målet er å heve det generelle kompetansenivået i befolkningen innen IKT-bruk og IKT-sikkerhet, men ambisjonen må være også å ha spesialisert kompetanse i IKT i bachelorutdanningene og økt kapasitet på masterutdanning med spesialisering innen IKT-sikkerhet. Dette er minst like viktig når det gjelder deltidsutdanninger som retter seg spesielt mot deltakere i arbeidslivet.

Digi-utvalget har påpekt at behovet for forståelse for teknologi også gjelder jurister, økonomer, leger og sykepleiere. Dette støtter Fagforbundet. Samtidig mener Fagforbundet at det vil være hensiktsmessig å forbedre læringsplanen for ledelsesrettede utdanninger. Dette er fordi den digitale utviklingen vil kreve at organisasjoner og ansatte må inneha en helhetlig forståelse for teknologi og de muligheter, begrensninger og risikoer som ligger i digitalisering.

Med hilsen
FAGFORBUNDET

Marit Wahlstedt
konstituert avdelingsleder SKA

Vedlegg:
Kopi: