# Rikstrygdeverket

Nærings- og handelsdepartementet
Postboks 8014 Dep.
0030 OSLO

Trygdeetaten

29 NOV. 2002

| | | | |
|---|---|---|---|
| Vår dato: | | Saksbehandler: | Herbjørn Andresen |
| Vår ref: | 2002/13313 | Direktenummer: | 22 92 70 73 |
| Deres dato: | 21.10.2002 | Telefaks: | 22 92 72 19 |
| Deres ref: | 2001/5605 KDB | | |

## Høring vedrørende grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet

Rikstrygdeverket deler initiativtakernes syn om at det er behov for en overordnet nasjonal strategi for informasjonssikkerhet. Utfordringene med å opprettholde en fullstendig og oppdatert oversikt over alle relevante regelverk og føringer innen informasjonssikkerhet er kjente problemstillinger også i vår etat.

Etter Rikstrygdeverkets syn bør spørsmål om organisering og eierskap til strategien være avklart og tydeliggjort *før* nasjonal strategi for informasjonssikkerhet utarbeides i første ordinære versjon. I forbindelse med styringsgruppens mandat (s. 9 i grunnlagsdokumentet) henvises til angitt fremdriftsplan for å utarbeide strategien. Det hadde vært ønskelig om det var opplyst nærmere om viktige milepæler, slik at vi så bildet på når noe skal foreligge. Kommentarer og forslag i dette høringsbrevet står i rekkefølge etter hvor viktige vi for tiden anser de ulike momentene å være for Rikstrygdeverkets virksomhet.

**1) Organisering av overordnete myndighetsorganer og/eller koordinerende organer**
Grunnlagsdokumentet demonstrerer godt hvor mange forskjellige myndighetsorganer en stor statlig etat må forholde seg til innen området informasjonssikkerhet. Summen av forslag til tiltak ser dessverre ikke ut til å redusere denne kompleksiteten. Eksempler på dette i de foreslåtte tiltakene er at Nærings- og handelsdepartementet skal "...fungere som pådriver overfor fagdepartementene og tilføre merverdi til deres aktiviteter innen IT-sikkerhet i sektoren", mens Arbeids- og administrasjonsdepartementet "har en særskilt rolle i oppfølgingen av tiltak av tverrsektoriell natur innen IT-sikkerhet i statlig sektor". I tillegg vil Justisdepartementet få en utvidet myndighet i forhold til samfunnskritiske systemer (noe uklart om dette inkluderer Trygdeetatens systemer, se punkt 2 nedenfor). Rikstrygdeverket er bekymret for at disse formuleringene uttrykker uavklarte roller på området, og at effekten for statlige virksomheter i verste fall bli omfattende rapportering og oppfølging av de samme sikkerhetstiltakene overfor flere overordnede myndigheter.

Det fremtidige strategidokumentet bør ha som en uttalt målsetning at organiseringen på nasjonalt nivå skal være oversiktelig og enkel å forholde seg til for den enkelte virksomhet.

*Adresse:* Rikstrygdeverket 0241 Oslo
*Besøksadresse:* Drammensveien 60
*Telefon:* 22 92 70 00 *Telefaks:* 22 92 70 70
*E-post:* rtv@trygdeetaten.no *Internett:* www.trygdeetaten.no
*Bankgiro:* 8200.01.04651 *Postgiro:* 0807 5083506 *Innbet. driftsregnskap:* 8276.01.00958 *Foretaksnr.:* NO 974 760 924 MVA

Det bør kanskje også tas med en målsetning om at den nasjonale strategien skal motvirke tendensen til at nye behov for sikkerhetstiltak genererer nye myndighets- eller samordningsorganer.

Rikstrygdeverket ser med en viss skepsis på forslaget om å "vurdere et permanent koordineringsråd for IT-sikkerhet som skal bestå av departementer og tilsynsmyndigheter som har en rolle på området". Dersom et slikt koordineringsråd skal kunne tjene til å redusere kompleksiteten, bør de imidlertid ha klart definerte og avgrensete oppgaver. Eksempler på slike oppgaver kan være å gi innspill til ulike organer som har en rolle innen informasjonssikkerhet, og å gi veiledning om bruk av metoder for risikovurdering eller oppbygging av internkontrollsystemer som dekker flere relevante regelverk innen informasjonssikkerhet. Et permanent koordineringsråd for IT-sikkerhet kan eventuelt også inneha en funksjon som "mottakssentral" for ulike typer innrapportering av sikkerhetsbrudd som ikke direkte berører rikets sikkerhet, med ansvar for å melde alvorlige brudd videre til rette ansvarlige myndighet.

Det må plasseres et entydig organisatorisk ansvar for og eierskap til den nasjonale strategien for informasjonssikkerhet. Det er likevel viktig å unngå en skjev fokusering på avgrensete områder. Den enkelte virksomhet har behov for å vite hvilke regler og føringer som gjelder i medhold av ulike regelverk, og hvilke tiltak som er påkrevd i forhold til ulike typer trusler og eventuelt ulike sider ved virksomheten.

**2) Begrepet "samfunnskritiske systemer" i forhold til Trygdeetaten**

Skillet mellom samfunnskritisk og virksomhetskritisk er en sentral premiss i mange av forslagene til tiltak i grunnlagsdokumentet. Trygdeetatens oppgaver og IT-systemer er ikke tatt med i oversikten over det som anses som samfunnskritiske systemer. Vi ser et behov for å presisere nærmere kriteriene for hva som er samfunnskritisk. Begrepet defineres slik at et informasjonssystem "...er samfunnskritisk hvis samfunnets funksjonsevne i stor grad påvirkes av at systemet eller infrastrukturen ikke fungerer". Senere i dokumentet defineres *samfunnssikkerhet*, som "den evne samfunnet som sådan har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger".

Folketrygdlovens § 25-16, som bygger på Lov om Sosial og Helsemessig beredskap, pålegger Rikstrygdeverket en planplikt for beredskap. Blant annet heter det at "Rikstrygdeverket skal påse at avtaler med leverandører av varer og tjenester inneholder krav til leveringsdyktighet og informasjonssikkerhet ved kriser i freds- og krigstid". § 25-17 pålegger å prioritere stønader til livsopphold (utbetalinger i henhold til enkelte bestemte kapitler i loven) foran annen virksomhet ved eventuelle krisesituasjoner. Dette er bestemmelser som indikerer at lovgiver antakelig har betraktet disse ytelsene som en del av "borgernes grunnleggende behov". Det er likevel ikke uten videre klart om manglende tilgjengelighet til Trygdeetatens systemer innebærer at "samfunnets funksjonsevne i stor grad påvirkes" i den betydning som ligger til grunn for det utvidede ansvarsområdet som Justisdepartementet skal ha for samfunnskritiske systemer i henhold til forslaget.

Rikstrygdeverkets syn er at deler av etatens systemer, nærmere bestemt de rutinene som inngår i utbetaling av stønad til livsopphold, bør betraktes som samfunnskritiske. Vi har imidlertid også en viss bekymring for at et nytt regime for rapportering, felles tiltaksplaner og oppfølging av samfunnskritiske systemer kan innebære et krevende merarbeid for etaten. Våre eksisterende tiltaksplaner for informasjonssikkerhet er preget av at trygdeetaten

behandler store mengder personopplysninger, som tildels er av sensitiv karakter. Derfor er personopplysningsloven med tilhørende forskrift og føringer fra Datatilsynet vårt primære regelregime innen informasjonssikkerhet. Det går ikke tydelig frem av grunnlagsdokumentet hva forslagene til samordnings- og oppfølgingsoppgaver for Justisdepartementet vil innebære for den enkelte virksomhet som er eier av samfunnskritiske systemer. Vi går i utgangspunktet ut fra at det ikke vil medføre faktiske endringer eller omprioriteringer i Rikstrygdeverkets eksisterende tiltaksplaner.

Den nasjonale strategien bør angi klarere kriterier for hva som er samfunnskritiske systemer. Det bør også fremgå hvilke forpliktelser, og eventuelle fordeler eller ulemper, som følger med det å være eier av samfunnskritiske systemer.

**3) Utbredelse av PKI**

Rikstrygdeverket gjennomfører i disse dager et prosjekt vedrørende rammeavtale for PKI-løsning til bruk i elektronisk samhandling innen trygde- og helsesektoren: For å kunne få til elektronisk innsending av sykmeldinger og legeerklæringer er det nødvendig at det finnes en PKI-løsning som ivaretar en sikker kommunikasjon mellom avsender og mottaker. Målet er at kontrakt om rammeavtale skal være signert før julen 2002. Prosjektet ønsker differensierte løsninger som kan gi tilpasningsmuligheter i henhold til den enkelte brukers behov. Den videre målsetningen er at PKI-løsningen etter hvert skal kunne benyttes av alle aktørene i helsenettene, og derved virke som en motor for storskalautbredelse av PKI i helsesektoren. Dette ivaretar kommunikasjonen innen helse- og trygdesektoren, der både offentlige og private aktører deltar i samhandlingen. Ved å utarbeide en felles PKI-løsning for samhandlende aktører kan dette bidra til økt tillit hos befolkningen. Det er sensitive personopplysninger som skal overføres i denne infrastrukturen, og det er viktig for alle involverte parter i samfunnet at det er tillit til sikkerhet og robusthet ved utveksling av denne type informasjon.

Rikstrygdeverket støtter målsetningen om en allment tilgjengelig samfunnsinfrastruktur for elektronisk signatur mv. Det er særlig viktig at sluttbrukere kan forholde seg til relativt likeartede verktøy og rutiner uavhengig av hvilke bedrifter eller offentlige etater de kommuniserer med. Dersom sluttbrukere må investere i ulike typer teknologi avhengig av hvem de skal kommunisere med, vil det bli svært vanskelig å oppnå allmenn tilgjengelighet.

Den omfattende listen av tiltak på samfunnsnivå ser likevel etter vårt syn ikke ut til å være tilstrekkelig for å komme forbi den "vranglåssituasjonen" som ligger i at mange aktører frykter uforholdsmessige investeringskostnader dersom man etablerer løsninger før markedet har oppnådd tilstrekkelig volum (kritisk masse).

Det er uklart hva det er ment å innebære når grunnlagsdokumentet tar til orde for et koordineringsorgan for PKI i offentlig sektor som har "nødvendige fullmakter". Den nasjonale strategien for informasjonssikkerhet bør presisere dette nærmere. Et koordineringsorgan for PKI bør ha som primær oppgave å arbeide for å oppnå at de ordinære sektormyndighetsorganene forplikter seg til og stiller seg bak valg av felles standarder og sikkerhetsnivå.

Vi ser også behov for at et koordineringsorgan kan tilby veiledning og kompetanse knyttet til en helhetlig tilnærming til utgiftssiden av å innføre PKI-løsninger. Etablering av elektronisk samhandling kan kreve store endringer i den enkelte etats interne systemløsninger. (Jf. våre

merknader om dette i høringssvar vedrørende strategi for bruk av elektronisk signatur og elektronisk ID i Norge, avsendt i september i år).

**4) Forslag knyttet til felles klassifiseringskriterier mv.**
Ulike regelregimer innen informasjonssikkerhet har forskjellige måter å klassifisere beskyttelsesbehov på. Vi tolker grunnlagsdokumentet slik at det foreslås å innføre mer enhetlige klassifiseringsmåter, primært med tanke på å etablere ansvarsdelingen mellom ulike overordnede myndigheter.

Utvikling av metodikk for å klassifisere beskyttelsesbehov kan medvirke til økt bevissthet om sårbarhet og robusthet i egne IT-systemer. Mange virksomheter har heterogene IT-systemer med ulike teknologier, disse kan ha ulike sikkerhetsnivåer. Et felles rammeverk for å klassifisere trusler bidra til å synliggjøre eventuell manglende robusthet i egen infrastruktur. Metoder for klassifisering vil kunne bidra til økt fokus på interne rutiner og prosedyrer vedrørende informasjonen, og kompleksiteten i virksomhetens IT-portefølje.

Det påpekes i grunnlagsdokumentet at inndelinger basert på vurdering av risiko og sårbarhet kan synes lite egnet for sortering av ansvar. En inndeling basert på ulike typer informasjon kan sannsynligvis treffe bedre når det gjelder å fastslå hvilke sikkerhetsregelverk de forskjellige systemer og rutiner for informasjonsbehandling hører inn under. Likevel vil ikke klassifisering av informasjonstyper endre det faktum at samme type informasjon i en virksomhet kan sortere under flere forskjellige typer regelverk.

Rikstrygdeverket er noe bekymret for den arbeidsmengden det kan medføre dersom man skal klassifisere alle typer informasjon etter deres forskjellige beskyttelsesbehov. Omfattende klassifisering av informasjon vil også kunne generere merarbeid i form av behov for jevnlig å gjennomgå og eventuelt reklassifisere informasjon. Vi mener derfor at det ikke bør etableres generelle regelverk eller rapporteringsplikter som forplikter de enkelte virksomhetene til å gjennomføre detaljerte klassifiseringer av informasjon.

**5) Reaksjoner på sikkerhetshendelser**
Som et av tiltakene for å styrke sikkerhetskulturen refereres OECDs prinsipp om at alle aktører må "reagere raskt og på en samarbeidsrettet måte" på sikkerhetshendelser. Dette er delvis et spørsmål om hva som skal eskaleres i medhold av de ulike regelverkene (som for eksempel rapport til Datatilsynet om utilsiktet eksponering av sensitive personopplysninger overfor uvedkommende).

Det kan også være aktuelt å vurdere om det bør etableres felles nasjonale anbefalinger om hva som er hensiktsmessige reaksjonsformer i forhold til sikkerhetshendelser i tilfeller som ikke reguleres i de enkelte regelverkene. Visse typer sikkerhetsbrudd vil i enkelte virksomheter kunne utløse personalmessige sanksjoner. I slike tilfeller vil en nasjonal anbefaling også kunne fungere som et tiltak for å unngå at den enkelte virksomhet overreagerer i forhold til sine ansatte. Tjenestemannsorganisasjonene bør tas med på råd ved utvikling av nasjonale anbefalinger om reaksjoner på sikkerhetshendelser.

**6) Om utviklingstrender og nye utfordringer for IT-sikkerhet**
Rikstrygdeverket ønsker å peke på behovet for å arbeide med robusthet og sikkerhet i de enkelte applikasjoner. Dette er strengt tatt en "gammel" utfordring, men elektroniske løsninger rettet mot publikum gjør det stadig mer aktuelt å bygge ut applikasjonssikkerheten side om side med sikring av nettverk og kommunikasjon. I grunnlagsdokumentet ser det ut

til at tiltakene som foreslås for sikring av applikasjoner først og fremst dreier seg om sertifisering av produkter, leverandører og utviklingsmiljøer. Vi ønsker at det i tillegg utvikles kompetanse og gis veiledning om strategier og teknikker for å sikre applikasjoner mot ulike typer trusler. Selv om det etableres gode sertifiseringsordninger vil den enkelte virksomhet uansett i en eller annen form måtte velge mellom ulike måter å sikre applikasjoner på, og være i stand til å vurdere løsningsvalg i forhold til en konkret risikovurdering. Strategien på nasjonalt nivå bør derfor inneholde tiltak for å etablere kompetanse for å veilede den enkelte virksomhet i forhold til å ivareta applikasjonssikkerhet.

**7) Forslaget om å vurdere skikkethet for funksjoner relatert til IT-drift og -sikkerhet**
Det ser ut til at grunnlagsdokumentet foreslår at virksomheter gjennomfører vurderinger av enkeltpersoners skikkethet for å jobbe med IT-sikkerhet. Rikstrygdeverket støtter *ikke* et slikt forslag, dersom dette er ment å gjelde utover de alminnelige vurderinger som gjøres i forbindelse med ansettelser, og utover sikkerhetslovens virkefelt. Utenfor sikkerhetslovens område bør det gjelde et prinsipp om forholdsmessige tiltak. Personkontroller eller vandelsvurderinger og lignende som baseres på å innhente opplysninger utenfra om de som tilsettes i en funksjon kan være mer inngripende enn nødvendig.

**Avsluttende merknader**
Grunnlagsdokumentet er omfattende og interessant, og vi ser positivt på en samordnet nasjonal strategi for informasjonssikkerhet. Vi har avgrenset merknadene til å gjelde de tiltak som kan berøre Rikstrygdeverkets virksomhet direkte. Vår etat er allerede i stor grad på linje med de kravene til tiltak som det foreslås at de enkelte virksomhetene stilles overfor.

Med hilsen
Rikstrygdeverket

Arild Sundberg
Trygdedirektør

Kari Haugstvedt
Avdelingsdirektør

Kopi: Sosialdepartementet