Tekna – Teknisk-naturvitenskapelig forening
Etatsforeningen i forsvaret

Vår dato
2009-12-18

Vår referanse
2009/TEKNA-FORSVARET/GM/005

Vår saksbehandler
Gunnar Mortensen
Tlf +47 99 20 81 10
gumortensen@mil.no

Tidligere dato
2009-11-10

Tidligere referanse
2009/00484-45/FD I 4/FRI

Til
Akademikerne

Kopi til
KOL

Internt

Intern kopi til

Høringssvar – utkast til instruks om sikkerhetstjeneste i Forsvaret

Bakgrunn

Akademikerne viser til høringsutkastet til ny instruks om sikkerhetstjeneste i Forsvaret. Akademikerne har vurdert instruksen, og i dette dokumentet følger våre merknader og kommentarer.
Akademikerne har bedt om innsyn i nødvendige underlagsdokumenter, men FD har ikke besvart alle våre henvendelser. Spesielt ville S-gruppens rapport av 25. februar dette år vært viktig for denne høringsuttalelsen, denne har vi ikke mottatt.

Drøfting

Akademikerne ser viktigheten av FOST som organisasjonen som ivaretar forsvarssjefens ansvar for sikkerhetstjenesten i Forsvaret. Dette innebærer at FOST må ha de nødvendige kapasiteter og myndighet for å sikre at dette ansvaret ivaretas. FOST skal beskytte forsvarets operasjoner og operative evne mot sikkerhetstruende hendelser.

FOSTs virkeområder

I henhold til gjeldende direktiv for sikkerhetstjenesten punkt 7.10 og 7.11, kan Forsvarets sikkerhetstjeneste iverksette undersøkelser av militære nettverk i forbindelse med sikkerhetstruende hendelser. Dette inkluderer bruk av data fra blant annet sensorer, brannmurer og systemlogger. Hensikten med denne virksomheten er å beskytte Forsvarets kritiske infrastruktur mot dataangrep og etterretning. Videre skal Forsvarets sikkerhetstjeneste lede oppdrag der kartlegging av omstendighetene rundt sikkerhetstruende hendelser og annet uhjemlet bruk av forsvarets informasjonssystemer har forekommet.

FOST har ansvaret for forebyggende sikkerhetstjeneste, nettverksforsvar, emisjonssikkerhet, personellklarering, militær kontraetterretning samt vakt og sikring i Forsvaret. Akademikerne mener at dette er oppgaver som naturlig inngår i et komplett sikkerhetsansvar, med de synergier som finnes mellom disse oppgavene. Forsvar av datanettverk er nå en integrert del av den totale militære virksomheten.
Forsvaret baserer seg mer enn noen gang på informasjonssystemer i sin operative virksomhet. En viktig oppgave for en militær sikkerhetstjeneste, er å sikre forsvarets kritiske systemer mot angrep og kompromittering. Informasjonssikkerhet og nettverksforsvar (CND) har vokst fram som avgjørende faktorer for å kunne sikre forsvarets systemer og personell i Norge og i utlandet.

Behov for begrepsavklaring

Akademikerne har merket seg en del begrepsforvirring i sakens anledning. De ulike aktørene som har kommet med utspill i denne saken har lagt ulik betydning i en del nøkkeluttrykk. Akademikerne tror det kan være veldig hensiktsmessig at det blir enighet om en rekke entydige begrepsdefinisjoner. Dette vil være fordelaktig i denne saken, og framover. Spesielt har vi merket oss ulik bruk av uttrykk som: CND, monitoring, overvåkning, monitorering og dataanalyse. Særlig har det vært problematisk at det ikke har vært klart skille mellom analyse av metadata og full innholdsanalyse. Som et eksempel kan nevnes innlegget til assisterende departementsråd av 4.9.09 hvor han gjør han det klart at FOST hverken skal kunne utføre monitoring, TSU eller overvåkning av trafikkinnhold i sitt arbeid for å ivareta sikkerhet. Akademikerne er kjent med at faglige anbefalinger tilsier at FOST tvert i mot bør ha ansvar for monitoring og TSU for å kunne ivareta det helhetlige sikkerhetsansvaret for Forsvaret.

I følge NATOs JP 3-13 er CND handlinger utført via datanettverk for å beskytte, monitorere, analysere, detektere og reagere på nettverksangrep, penetrasjoner, forstyrrelser eller andre uautoriserte handlinger som vil kunne kompromittere eller ødelegger militære informasjonssystemer og nettverk.

Gjeldende og tidligere høringsutkast

Akademikerne har merket seg en betydelig forskjell mellom gjeldende høringsutkast, og høringsutkastet datert 5.juni i år. Myndighets- og virkeområdet til FOST er innskrenket på flere viktige områder. Det er uklart for Akademikerne hva grunnlaget for disse endringene er. I høringsutkastet datert 5. juni har FOST klart ansvar for CND (computer network defence) og TSU.

I forsvarsministerens svar til høyres stortingsgruppe datert 17. juni 2009 sier forsvarsministeren at årsakene til utarbeidelse av ny instruks og økt tilsynsaktivitet med FOST er basert på bekymringsmeldingen fra NSM. Fredag 11.12.2009 konkluderte KRIPOS med at intet straffbart forhold var funnet på bakgrunn av anmeldelsen. Anmeldelsen kom på bakgrunn av bekymringsmeldingen fra NSM.

Akademikerne har merket seg uttalelser i mediene omkring EOS utvalgets vurdering av FOST. Denne rapporten er nylig avgradert, og synes å ha hovedvekt på tre enkelthendelser. FOST har tidligere meldt ønske om tydeligere rammer og grenser for tjenesten. Akademikerne synes det er fornuftig å foreta en gjennomgang av dette. Derimot er det en vesentlig forskjell mellom ytterligere detaljering av oppgaver og rammer for tjenesten, og det å fjerne sentral operativ virksomhet fra FOST. Grunnlaget for de omfattende endringene i instruksen, synes ikke å være grunngitt tilstrekkelig i de grunnlagsdokumentene som akademikerne har tilgang til.

Sammenslåing av drift og sikkerhetsmessig overvåkning

I utkastet til instruks er det foreslått å flytte en stor del av FOSTs kjernevirksomhet til driftsorganisasjonen. Akademikerne er av den oppfatning at sikkerhetsmessig overvåkning og sikkerhetstiltak ikke bør utføres av samme organisasjon som er tillagt driftsoppgavene.
Dette er en uheldig sammenblanding av funksjoner i forhold til faktisk evne til å detektere trusler og vurdere utbedringstiltak.
Vurderingen om sikkerhetstiltak og endringer i systemsikkerhet bør fristilles fra eierskap til systemenes daglige drift. Begrepet driftsorganisasjonen er heller ikke entydig. Drift avtaktiske systemer skjer for eksempel i forsvarsgrenene.

I det tilfelle at driftsorganisasjonen skulle overta CND ansvaret, vil en rekke problematiske situasjoner kunne oppstå. CND som er en militær sikkerhetsdisiplin, forutsetter militær

kompetanse og ledelse. CND er en del av den operative virksomheten til Forsvaret og omfatter forsvarssystemer innenlands, og systemer deployert i internasjonale operasjoner. Vurderinger som må gjøres omkring sikkerhetstruende hendelser vil ofte kreve militær kompetanse og operativ forståelse. Det kan eksempelvis være nødvendig å vurdere hvorvidt man skal ta ned et kompromittert, kritisk system som har direkte innvirkning på operasjoner, og liv og helse for forsvarets ansatte. Dette kan være kartsystemer, taktiske applikasjoner, kommunikasjonsenheter o.l.

Akademikerne mener at ansvaret for oppetid, robusthet og tilgjengelighet for forsvarets systemer naturlig hører hjemme i driftsorganisasjonen.

FOST har som nevnt i innledningen ansvaret for forebyggende sikkerhet, og gjennomgående sikkerhet for Forsvarets operasjoner.
Akademikerne vurderer det slik at en fragmentering av oppgaveporteføljen til FOST vil ha negative konsekvenser i forhold til disse oppgavene.

Konsekvensvurdering

Det bør foreligge en konsekvensvurdering i forkant av iverksettelse av instruksen, da endringene kan medføre store konsekvenser for FOST og driftsorganisasjonen. Oppgavene som per dags dato er tillagt FOST stiller spesielle krav til utstyr, organisasjon og, det mest sentrale, høyt utdannet og godt trent personell innenfor informasjonssikkerhet. CND oppgavene, er nært er knyttet opp mot militær virksomhet, og har med hensikt vært lagt til en militær avdeling.

Akademikerne er bekymret for at Forsvarets forsvarsevne innenfor IKT svekkes betydelig om man foretar disse instruksendringene uten en korrekt prosess med konsekvensvurderinger. Akademikerne etterlyser en konsekvensutredning i forhold til instruksendringene, og ringvirkningene disse vil ha i de ulike organisasjonene i Forsvaret.

Under § 5 i utkast til ny instruks, gis det føringer om at innkjøp og utplassering av sensorer skal forelegges for FD. Dette vil virke kompliserende og forsinkende på FOSTs arbeid. Dette er arbeid som må gjøres raskt etter et sikkerhetsbehov er oppstått, og er således tidskritisk. Utplassering av sensorer er en del av oppdraget gitt sjef FOST, og grunnlaget for den foreslåtte endringen er uklart.

I utkast til ny instruks § 3 kreves det at enhver militær sjef skal rapportere direkte til NSM, og ikke til virksomhetsleder. Dette bryter med § 2.1 i 'forskrift om sikkerhetsadministrasjon': Virksomhetsleder har overordnet ansvar for den forebyggende sikkerhetstjeneste i innen sitt ansvars- og myndighetsområde, herunder underlagte virksomheter. Denne delen av instruksen kan antyde at man ønsker å omgå forsvarssjefens som virksomhetsleder i rapporteringslinjen.

Akademikerne merker seg den skisserte økningen av tilsynsvirksomheten ved FOST.
Som alle andre lignende tjenester, bør det være tilsyn for å kvalitetssikre arbeidet som gjøres. Det bør derimot gjøres en vurdering på hyppigheten av denne tilsynsvirksomheten. I dag har både EOS-utvalget og NSM tilsyn med FOST, FD har signalisert økt tilsynsaktivitet, i tillegg kan Forsvarets ledelse kontrollere egen virksomhet. Akademikerne stiller spørsmål ved om disse organene ikke gjør en god nok jobb og har tillit, ettersom det er flere som ønsker å inspisere FOST? I tillegg bør inspeksjonsvirksomheten koordineres mellom de ulike aktørene. Akademikerne etterlyser grunnlaget for eventuell økning av denne tilsynsvirksomheten.

Skulle det vise seg at oppgavene fratas medarbeiderne i FOST vil det være en reell fare for kompetanseflukt da personellet ikke vil ha funksjoner relatert til sin utdanning og yrkeserfaring. Dette er kompetanse som er vanskelig å oppdrive for arbeidsgiver, og som det er brukt store ressurser på å videreutvikle. Akademikerne er bekymret for at dette trenings- og

utdanningsløpet må påbegynnes på nytt i ny organisasjon, noe som med stor sannsynlighet vil føre til svekket forsvarsevne innenfor forsvarets IKT systemer over en lengre periode. Forsvarets sikkerhetstjeneste avdekker daglig angrep og rekognosering mot Forsvarets datasystemer. På dette tidspunktet er det uklart for akademikerne om de ansatte ved FOST er tenkt overført til driftsorganisasjonen eller ikke.

Vurdering av faktagrunnlaget

For å foreta så betydelig endring i en avdelings kjernevirksomhet, bør det foreligge et solid faktagrunnlag som tilsier at endringene er nødvendige. Akademikerne kan ikke se å ha mottatt faktagrunnlag som tilsier at de foreslåtte endringene er nødvendige.

Tekna har tidligere poengtert flere mangler ved revisjonsprosessen utført ved FOST av FD 04.09.09. Dette skulle danne faktagrunnlaget for eventuelle instruks- og rutineendringer. Inspeksjonen skulle følge revisjonsstandard ISO 19011:2002. Denne modellen stiller sterke krav til ansvarsmessig uavhengighet og objektivitet. Det er også satt store krav til den reviderte organisasjonens mulighet for presiseringer og tilbakemeldinger i forhold til det innsamlede materialet. Akademikerne er også bekjent med et sett med hypoteser som var utgangspunktet for denne revisjonen. Disse bar preg av å være partiske og unyanserte, og gir dermed et uttrykk for at kravene til denne revisjonen ikke var oppfylt.

Videre vil Akademikerne poengtere at avdelingens navn er en forhandlingssak som må overlates til partene i Forsvaret.

Avslutningsvis vil akademikerne vise til skrivet fra statsadvokat Petter Mandt datert 10. desember, angående konklusjonen av etterforskningen av FOST: ' *Hjemmelsgrunnlaget for FOST sin virksomhet er innhentet og vurdert. Etter en gjennomgang av sakens dokumenter finnes statsadvokaten å henlegge saken i det intet straffbart forhold anses bevist'.*

Akademikerne ser, som nevnt tidligere, at det kan være hensiktsmessig å detaljere FOSTs oppdrag og tjenesterammer ytterligere, men kan ikke se fakta i denne saken som krever endringene som er foreslått i utkastet til ny instruks

Konklusjon

Akademikerne er bekymret for at foreslåtte instruksendring vil føre til svekket forsvarsevne innenfor forsvarets IKT systemer. I tillegg etterlyser Akademikerne konsekvensvurderinger og faktagrunnlag for de omfattende endringene. Akademikerne er bekymret for at det ikke er tilstrekkelig bevissthet omkring CND som en viktig integrert del av den operative militære sikkerhetsvirksomheten. Avslutningsvis innskrenker det gjeldende høringsutkastet forsvarssjefens frihet til å ivareta sitt ansvar som virksomhetsleder i forhold til sikkerhetsloven

På vegne av Akademikerne i Forsvaret

Gunnar Mortensen
Leder Teknas etatsgruppe i Forsvaret