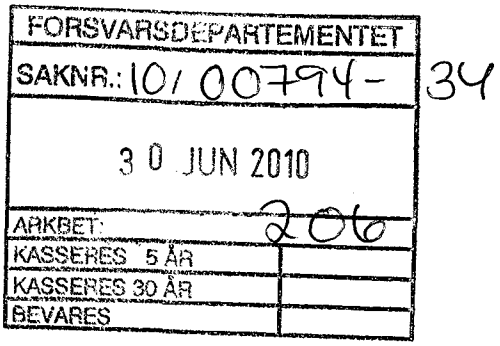
FNO
Finansnæringens
Fellesorganisasjon

Forsvarsdepartementet
Postboks 8126 Dep
0032 Oslo



Dato: 24.06.2010

Vår ref.: 10-320-EV
Deres ref.: 2010/00794-1/FD I5/OFD

Høringsuttalelse – Forslag til strategi for cybersikkerhet

Takk for anledningen til å kommentere det foreliggende utkast til strategi for cybersikkerhet. FNOs høringsuttalelse er utarbeidet i samråd med Bankenes Standardiseringskontor (BSK).

FNO har ikke noe forutgående kjennskap til begrepet "cybersikkerhet" og selv om vi har lest det foreliggende forslaget grundig er vi fortsatt usikre på hva begrepet er ment å dekke. En overordnet kommentar, som utdypes i vedlagt dokument, er derfor at det bør arbeides mer med å klargjøre formålet med strategien.

Som storbruker av IKT har finansnæringen interesse i effektiv og samordnet innsats for å forebygge og om nødvendig håndtere så vel angrep som uhell og ulykker som kan ramme samfunnskritisk IKT-basert infrastruktur. Vi har inntrykk av (men er ikke sikre på) at det foreliggende utkast til strategi har som et av sine formål å legge til rette for en slik samordnet innsats.

Finansnæringen utsettes fra tid til annen av omfattende IKT-basert svindel og kriminalitet, herunder ulike typer malwarebaserte angrep. Vi registrerer at det foreliggende utkast til strategi legger stor vekt på effektiv forebygging, håndtering og etterforskning av slike angrep og håper at deler at denne innsats kan komme finansnæringen til nytte.

Finansinstitusjoner enkeltvis og finansnæringen samlet har allerede mange tiltak og koordinerende aktiviteter når det gjelder sikkerhet. Finansnæringen er derfor opptatt av å sikre at eventuelle nye samordningstiltak blir et konstruktivt og ressurseffektivt supplement til eksisterende analyse-, sikrings- og beredskaps arbeid.

Våre kommentarer for øvrig fremgår av vedlagte dokument.

Med vennlig hilsen

Tor Johan Bjerkedal
Direktør

Eline Vedel
Assisterende direktør

Kopi til:
Bankenes Standardiseringskontor
Finanstilsynet
Norges Bank

NOTAT

FNO
Finansnæringens
Fellesorganisasjon

Dato:15.juni 2010 (Vår ref: 10-320/EV)

VEDLEGG TIL HØRINGSUTTALELSE VEDRØRENDE STRATEGI FOR CYBERSIKKERHET

1. Bakgrunn

Finansnæringen har opplagt interesse av effektiv og samordnet innsats for å forebygge og om nødvendig håndtere så vel angrep som uhell og ulykker som kan ramme samfunnskritisk infrastruktur. Vi har inntrykk av (men er ikke helt sikre på) at det foreliggende utkast til strategi har som et av sine formål å legge til rette for en slik samordnet innsats.

Finansnæringen utsettes fra tid til annen av omfattende IKT-basert svindel og kriminalitet, herunder ulike typer malwarebaserte angrep. Vi registrerer at det foreliggende utkast til strategi legger stor vekt på effektiv forebygging, håndtering og etterforskning av slike angrep og håper at deler at denne innsats kan komme finansnæringen til nytte.

Finansinstitusjoner enkeltvis og finansnæringen samlet har allerede mange tiltak og koordinerende aktiviteter når det gjelder sikkerhet. I tillegg til næringsintern virksomhet, i regi av den enkelte finansinstitusjon, hos Bankenes Standardiseringskontor (BSK) og i Bankenes Sikkerhetsråd (utvalg i FNO) omfatter eksisterende virksomhet rapportering til og tilsyn fra finansmyndighetene: Finanstilsynet og Norges Bank samt deltakelse i Beredskapsutvalget for Finansiell infrastruktur (BFI). Finansnæringen er dessuten representert i Næringslivets Sikkerhetsråd (NSR), og bidrar til arbeider som skjer i regi av NORSIS. Finansnæringen er derfor opptatt av å sikre at eventuelle nye samordningstiltak blir et konstruktivt og ressurseffektivt supplement til eksisterende sikringsarbeid.

2. Innretning av strategien som helhet

En hovedutfordring med det foreliggende forslag til strategi er at formålet/målsettingene ikke er klart formulert. Det sies en del om årsaker til at "cybersikkerhet" er aktualisert, men gis ingen klar definisjon av hva ordet faktisk dekker. Det samme gjelder "kritiske IKT-systemer". Videre opplyses det at "vi ikke har tilstrekkelig situasjonsoversikt og forståelse", men foreslås likevel en rekke tiltak for å forbedre situasjonen.

FNO mener at det bør arbeides mer med å klargjøre formålet med innsatsen før det eventuelt nedlegges samfunnsmessige investeringer i etablering av nye enheter, rutiner mv. En slik klargjøring bør bl.a. omfatte:

a. Hva er det en ønsker å sikre? Deler av det foreliggende strategidokument viser at forsvar av Norge og norske interesser samt overvåking og etterforskning står sentralt. Dessuten nevnes en rekke sektorer (inkludert finansiell sektor), men det forklares ikke hvorfor eller på hvilken måte aktivitet i disse sektorer har betydning for "cybersikkerhet"? Dekker "sikkerhet" i denne sammenheng bare det en i sikkerhetsfaglig sammenheng kaller "security", dvs. beskyttelse mot angrep, eller dekker det også det en kaller "safety", dvs. beskyttelse mot uhell, ulykker mv.?

b. På hvilke områder er tilgjengelighet (opprettholdelse av drift) kritisk? På hvilke områder er integritet (at det ikke oppstår feil) spesielt viktig? Og på hvilke områder er konfidensialitet (at informasjon ikke kommer på avveier) avgjørende?

c. Er det riktig å fokusere bare på "kritiske IKT-systemer"? Burde en kanskje også /heller fokusere på samfunnskritisk IKT-basert infrastruktur? (for eksempel strømnettet, telenettet og betalingssystemene). Kan tiltakene vedrørende "cybersikkerhet" forventes å bidra til en konkretisering av pålegg i "Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften)" kapitel 8: Sikkerhet og beredskap?

d. Skal strategien avgrenses til IKT-hendelser, eller skal den også dekke hendelser der bruk av IKT er medvirkende til skadene? For eksempel en rekke former for ID-tyveri og spionasje

Med mulig unntak av detaljer i punkt b) mener FNO at de nevnte avklaringer både kan og bør gjennomføres før det gjennomføres en detaljert kartlegging av kritiske IKT-systemer mv. FNO mener i det hele tatt at en bør være varsom med å iverksette de foreslåtte tiltak før formålet er nærmere avklart. Se for øvrig kommentarer til enkelttiltak under.

3. Kommentarer til de enkelte hovedmål og forslag til tiltak

Kommentarene følger forslaget til strategi fra Nasjonal sikkerhetsmyndighet (NSM).

3.1 Etablere en felles situasjonsoversikt og forståelse

Som ledd i nærmere avklaring av formålet kan det være behov for dialog med interessenter i ulike samfunnssektorer, herunder bl.a. myndighetstilsyn. Gjennom en slik dialog bør en kartlegge hvilke formål sikkerhetsarbeidet i bestemte sektorer har og på hvilke områder ulike sektorer har spesielt stort behov for en samordning på tvers av sektorer. Direkte dialog med privat sektor kan bl.a. skje gjennom Næringslivets Sikkerhetsråd (NSR) der både FNO og NSM er representert.

1. Kartlegge og verdivurdere kritiske IKT-systemer i alle sektorer
Den skisserte kartlegging i forslaget til strategi virker svært omfattende, og vil, etter vår vurdering, ikke nødvendigvis gi en bedre og mer felles situasjonsoversikt og forståelse. For å sikre at tiltaket blir nyttig vil vi anbefale at en:

1) Endrer fokus fra IKT-systemer til IKT-baserte infrastrukturer (som hver for seg kan omfatte en rekke IKT-systemer). Noen IKT-baserte infrastrukturer som vi antar kan oppfattes som samfunnskritiske er strømnettet, telefonnettet, internett, ID-porten og utvalgte betalingssystemer.

2) Innledningsvis vurderer å fokusere spesielt på IKT-systemer/-infrastrukturer der høy grad av tilgjengelighet vurderes som samfunnskritisk. Integritet og konfidensialitet er også viktig, men å kartlegge ut fra alle tre perspektiver samtidig er neppe hensiktsmessig.

Når det gjelder **forslag til tiltak nr. 2, 3 og 4** har vi ingen særskilte merknader.

5. Etablere partnerskap mellom offentlige myndigheter og private aktører
Her vil FNO gjøre oppmerksom på at finansnæringen allerede, bl.a. på bakgrunn av offentlig regulering og tilsyn, har investert mye i sikring av kritisk IKT-basert infrastruktur og årlig bruker mye ressurser på rapportering, risikoanalyser (egne og Finanstilsynets) samt individuelle og samordnede tiltak for å opprettholde tilstrekkelig sikkerhet. Når det gjelder sikring av samfunnsmessige viktige verdier mener vi for øvrig at å sikre interesse og investeringsvilje fra myndighetene og offentlig sektor bør oppfattes som like viktig som å sikre interesse og investeringsvilje fra privat sektor.

FNO slutter seg til den positive omtalen av NORCERT, og vil i denne sammenheng også fremheve NORSIS.

3.2 Bygge og opprettholde robuste og sikre IKT-systemer

6. Stille felles krav til kritiske systemer + 7. Styrke tilsyn med IKT-sikkerhet
Robuste og sikre IKT-systemer er avgjørende. Når det gjelder (kritiske) IKT-systemer i Finansnæringen mener FNO at det etablerte tilsynsregimet basert på forskriftsregulerte krav og samarbeid/koordinering mellom privat og offentlig sektor bør dekke det behov utredningen viser til.

Vi vil videre vise til at ekomforskriftens kapittel 8 omhandler sikkerhet og beredskap knytet til "samfunnskritiske funksjoner". Etter FNOs vurdering kan det være fornuftig om det videre arbeid med "cybersikkerhet" og oppfølging av ekomforskriftens kapitel 8

koordineres. Bl.a. er det sentralt å få større klarhet i hvordan det bestemmes hva som til enhver tid skal regnes som "samfunnskritiske funksjoner".

Generelle anbefalinger/krav som skal gjelde alle "kritiske IKT-systemer" bør formuleres i samråd med og formidles via etablerte tilsynsorganer, som også må ha ansvaret for å kontrollere at de følges opp. Dersom kravene har direkte konsekvenser for innretning av IKT-systemer i finansnæringen og/eller for omfanget av rapportering, forventer FNO at finansnæringen blir involvert i behovs- og konsekvensvurdering.

8. Utvikle og implementere sikre og robuste kommunikasjonsløsninger for krisehåndtering
FNO vil påpeke at etablering av sikre og robuste kommunikasjonsløsninger kan være et relevant sikkerhetstiltak ikke bare for krisehåndtering, men også mer allment. En rekke uhell og ikke minst angrep kan unngås ved å sørge for at en del kritisk informasjon bare utveksles i spesielt sikrede nett, type ekstranett. Slike nett benyttes bl.a. i datautveksling mellom finansinstitusjoner både nasjonalt og internasjonalt. Vi tillater oss også å minne om at kommunikasjonsløsninger som ikke brukes jevnlig ofte er vanskelige å få til å fungere godt i en krisesituasjon.

9. Videreutvikle beredskapsplaner med tanke på cybersikkerhetstiltak
FNO ser gjerne at relevant offentlig myndighet tar et overordnet ansvar for å utforme, forvalte og ved behov iverksette plan for håndtering av alvorlige hendelser som rammer kritiske IKT-systemer i *flere sektorer*. I det omfang det "bare" er tale om alvorlige hendelser innen en sektor mener vi derimot at ansvaret fortsatt, som hovedregel, kan overlates til relevante myndigheter/organer i denne sektor, som for eksempel Beredskapsutvalget for finansiell infrastruktur (BFI). Dersom det er sektorer der beredskapsplaner/-organisering er mangelfulle forventer vi at dette håndteres særskilt og ikke gjennom generelle krav som "rammer" alle sektorer. Vi viser for øvrig til kommentarer til tiltak nr. 6, 12 og 22.

10. Behov for regulatorisk forankring av cybersikkerhet
Ingen særskilte kommentarer.

3.3 Bevisstgjøre, opplyse og påvirke

11. Styrke tiltak for bevisstgjøring, utdanning og holdningsskapende arbeid
Også her mener FNO det er viktig å ta høyde for at utgangssituasjonen i ulike sektorer kan være nokså ulik. NORSIS utfører allerede en del arbeid på dette område.

12. Arrangere og delta i øvelser (sektorvise, nasjonale og internasjonale)
FNO er enig i at øvelser er viktige. Vi mener at ansvaret for å planlegge og gjennomføre slike øvelser må ligge hos de organer som har beredskapsansvar. Hovedansvaret for øvelser som omfatter flere sektorer må ligge hos det organ eller den myndighet som har eller får ansvaret for sektorovergripende beredskap (jfr. også merknader til tiltak 9 og 22).

3.4 Styrke evnen til å oppdage, varsle og håndtere IKT-hendelser

13. Styrke samfunnets evne til å oppdage trusler og sårbarheter
Så vidt vi forstår innebærer tiltaket mer omfattende overvåking av IKT-basert aktivitet. FNO mener generelt at ressurser rettet mot å redusere skadevirkninger av angrep i første rekke bør rettes mot forebygging og håndtering av angrep.
Bare der det er godt begrunnet bør personrettet overvåking iverksettes. Sammenstilling av personrelatert informasjon fra ulike kilder bør etter vår vurdering ikke forekomme uten forutgående grundig vurdering av behov og konsekvenser. Et viktig delmål i denne sammenheng må være å opprettholde tillit til samfunnskritisk IKT-basert infrastruktur.

14. Legge til rette for innrapportering av hendelser
Hvilke hendelser som vurderes som kritiske og hvordan de rapporteres og tolkes bør, etter vår vurdering, være bestemt av formålet med og bruken av de ulike IKT-systemer. FNO mener på denne bakgrunn at rapportering av hendelser som gjelder IKT-systemer i finansnæringen fortsatt bør skje til Finanstilsynet. Finanstilsynet og andre sektortilsyn kan bes rapportere videre til sentral sikkerhetsmyndighet, dels gjennom samlede oversikter (for eksempel årlig) og dels spesielt urovekkende/problematiske enkelthendelser.

15. Etablere sektorvise CSIRT-miljøer i samfunnsviktige sektorer og i de største enkeltvirksomheter
Vi oppfatter at det her legges opp til at hver sektor skal etablere eget CSIRT-miljø. FNO vil ikke utelukke at dette kan være formålstjenlig, men ber om at det gjennomføres nærmere kost-/nyttevurdering før det eventuelt treffes vedtak om at Finansnæringen og/eller Finanstilsynet skal etablere et slikt miljø.

3.5 Etterforske og bekjempe IKT-hendelser

16. Styrket kapasitet og kompetanse for håndtering av målrettede dataangrep
FNO er positive til dette tiltak.

17. Sikre mulighet til nødvendig lagring av data ved hendelser med tanke på å muliggjøre effektiv etterforskning
Ingen særskilte merknader.

18. Utrede behov for endringer i det legale grunnlaget for etterforskning
Ingen særskilte merknader.

19. Avdekke og identifisere trusler og trusselaktører
Som nevnt trues kritiske IKT-systemer ikke bare av angrep, men også at uhell, naturkatastrofer mv. Gitt at "cybersikkerhet" skal favne så bredt som innledende formuleringer i utkast til strategi synes å legge opp til bør alle aktuelle trusler tas med i vurderingen.

20. Offensive kapasiteter
Se merknader til tiltak nr. 22. Ellers ingen kommentarer.

3.6 Styrke samordningen av cybersikkerhetsarbeidet.
I kommentarer over har vi basert oss på at "cybersikkerhet" handler både om "safety" og "security" (jfr. overordnede merknader). Når vi leser dette hovedavsnitt får vi imidlertid et inntrykk av at det primære formål er å forebygge, håndtere og etterforske villede angrep? Dette forsterker vår oppfatning av at formålet med innsatsen må avklares nærmere før en strategi fastsettes..

21. Opprette en gruppe for faglig støtte til Justisdepartementet og Forsvarsdepartementet
Ingen kommentarer.

22. Etablere et nasjonalt cybersenter
I strategiforslaget omtales "cybersenter" som en "operativ funksjon rettet inn mot nye og endrede behov knyttet til ivaretakelse av cybersikkerheten".

På denne bakgrunn antar vi at "cybersenter" i alle fall må ha et ansvar for:

- Jevnlige (for eksempel årlige) risikoanalyser, innrettet mot å identifisere trusler og vurdere konsekvenser for på det grunnlag å kunne komme med anbefalinger/råd om forebyggende tiltak og beredskap.

- At det finnes helhetlige og innøvde planer for håndtering og oppfølging av hendelser som krever koordinert innsats fra flere sektorer.

- Myndighet til å iverksette planlagte tiltak og nødvendige øvelser.