FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Forsvarsdepartementet
Pb 8126 Dep
0032 OSLO

01.07.2010

SAKSBEHANDLER:	VÅR REFERANSE:	DERES REFERANSE:
Stig Ulstein	10/7002	
DIR.TLF:	ARKIVKODE:	
22 93 99 66	008	

Høring - om Nasjonal strategi for cybersikkerhet

Det vises til høringsnotat om forslag til strategi for Cybersikkerhet 08. april 2010 med vedlagt dokument Nasjonal strategi for Cybersikkerhet og korrespondanse med Annette Tjaberg ang. utsettelse for Finanstilsynets bidrag i høringen. Finanstilsynet vil først angi noen mer generelle kommentarer og deretter gi kommentarer til aktuelle enkeltavsnitt.

Generelle kommentarer

Det området strategien skal gjelde for bør klart avgrenses. Begrepet Cyberspace er noenlunde definert, men kan i sin ytterste tolkning omfatte all databehandling; kommunikasjonsnett, maskiner, systemer og data. Det kan derfor være hensiktsmessig å definere nærmere hvordan begrepet skal forstås i sammenheng med strategien. Også begrepet Cybersikkerhet bør defineres nærmere.

En viktig del av trusselbildet knyttet til bruk av åpne nett kan avgrenses til bruk av internett som begrep. Det vil likevel være nødvendig å definere dette inn i ulike kategorier som internett service provider (ISP), teleleverandør, innholdsleverandør, kunder av slike tjenester og brukere. Bruk av begrepet infrastruktur krever også en nærmere klargjøring, f. eks. om det er felles infrastruktur, infrastruktur knyttet til en bestemt sektor eller enkeltforetak. Tilnærmingsmåte og tiltak kan være helt ulike og det bør derfor presiseres hva det til enhver tid dreier seg om.

Det hadde antagelig vært mest hensiktsmessig å ta utgangspunkt i gjeldende Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007 – 2010 og at høringsnotatet i større grad la opp til operasjonalisering av tiltaksområder som er omhandlet der og som det er aktuelt for NSM å realisere (nærmere om dette i våre kommentarer til kapittel 1.2).

Kommentarer til sammendrag

Finanstilsynet mener det er viktig å hensynta hva som er gjort av tiltak i de enkelte sektorer når tiltak på tvers av sektorene skal etableres. Dette kan bidra til å sikre en mest mulig koordinert og optimal gjennomføring.

Det er etablert en rekke bilaterale samarbeidsopplegg mellom ulike sektormyndigheter. Finanstilsynet har for sin del etablert et formelt samarbeid med Nasjonal Sikkerhetsmyndighet (NSM) som også omfatter NorCERT. Samarbeidet bidrar til å sikre at nødvendig informasjon om eventuelle angrep på internett og som kan påvirke den finansielle infrastrukturen også tilfaller Finanstilsynet. Likeledes har Finanstilsynet også bilaterale samarbeidsopplegg med Norges Bank, Datatilsynet, Post & teletilsynet og andre relevante instanser som kan berøre vårt tilsynsområde. Vi

antar at dette også kan gjelde andre sektormyndigheter. En av begrunnelsene for opprettelsen av Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS) var nettopp få til en felles møteplass for utveksling av informasjon, oppfølging av tiltaksområder og aktuelle sektorovergripende tiltak.

Det vises i høringsnotatet til behov både for overordnet og billateralt samarbeid, noe vi er enig i. Finanstilsynet har erfart at koordinering og samarbeid krever en proaktiv deling av informasjon og et langsiktig samarbeid mellom aktuelle sektorer for å kunne oppnå resultater. Hensikten med å peke på dette er at denne typen samarbeid oppnås gjennom klar rollefordeling og konkrete samordningsbehov.

Ellers bemerkes at finanssektoren er omfattende med mange aktører som ivaretar kritiske samfunnsfunksjoner. Derfor har Norges Bank i samarbeid med Finansdepartementet og Finanstilsynet etablert Beredskapsutvalget for finansiell infrastruktur (BFI) i 2000. BFI skal koordinere tiltak for å forebygge og å løse krisesituasjoner og andre situasjoner som kan resultere i store forstyrrelser i den finansielle infrastruktur og forestå nødvendig koordinering av beredskapssaker mellom aktørene.

Kommentarer til kapittel 1.2 Forholdet til Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007 – 2010

Finanstilsynet mener det er viktig at myndighetene viderefører arbeidet med nasjonale retningslinjer for å styrke informasjonssikkerheten og at dette arbeidet videreføres uavhengig av arbeid med en Cybersikkerhetsstrategi. Den foreslåtte strategien for Cybersikkerhet kan i denne sammenheng inngå som operasjonalisering av deler av den nasjonale strategien. De Nasjonale retningslinjene må nødvendigvis gi mer overordnede og helhetlige føringer enn en mer konkret operasjonalisering innen en sektor eller på bestemte områder som også kan være sektorovergripende. Det er derfor etter Finanstilsynets mening ikke hensiktsmessig å illustrere Cyberskkerhetsstrategien ved å plassere denne visuelt inn i toppen av en pyramide for de nasjonale retningslinjene, slik dette er gjort i høringsnotatet. De foreslåtte tiltakene i høringsnotatet overlapper i tekst en rekke av de områder som allerede er beskrevet i de Nasjonale retningslinjene.

Kommentarer til kapittel 1.3 Internasjonale tilnærminger til cybersikkerhet

I avsnittet om EU savnes henvisning til sluttrapport fra European Security Research & Innovation Forum (ESRIF) som kom i desember 2009. Denne rapporten omhandler forslag til EUs satsning på hele sikkerhetsområdet (også IKT) når det gjelder forskning, utvikling og andre tiltak i perioden frem mot 2030.

Kommentarer til 2.1 *Etablere en felles situasjonsoversikt og forståelse*

Kommentarer nedenfor er begrenset til kun der vi har kommentarer til angitte tiltak og følger nummereringen fra høringsnotatet:

1. Kartlegge og verdivurdere kritiske IKT-systemer i alle sektorer

Finanstilsynet slutter seg til at det er viktig å sikre tilstrekkelig informasjon om dette på myndighetsnivå, men arbeidet må ta utgangspunkt i sektoransvaret. Utveksling av relevant informasjon på tvers av sektorer må skje gjennom et bilateralt samarbeid, eventuelt gjennom KIS.
Det bemerkes at Finanstilsynet i 2008/2009 gjennomførte et større kartleggingsprosjekt for den IKT-tekniske og logiske infrastrukturen innenfor finansnæringen.

2. Målrettet satsning på forskning og utvikling
Dette er angitt som et viktig tiltaksområde i gjeldende Nasjonale retningslinjer for å styrke

informasjonssikkerheten 2007 – 2010, kapittel 3.8. Etter Finanstilsynets vurdering bør tiltaket i foreliggende høringsnotat tilpasses innenfor rammene av de nasjonale retningslinjene.

4. Styrke internasjonalt samarbeid om cybersikkerhet

Finanstilsynet støtter dette. Det bemerkes at Finanstilsynet i de senere år har vært med på å etablere en nordisk, europeisk og global møteplass innenfor finanssektorens IKT-tilsynsområde som vi har stor nytte av. I dette samarbeidet utveksler landene seg i mellom informasjon om alvorlige hendelser som oppstår.

5. Etablere partnerskap mellom offentlige myndigheter og private aktører

En videreføring av NorCERT og VDI i regi av NSM ser Finanstilsynet på som viktig. For øvrig er Finanstilsynets erfaring at reguleringer som gjelder for finanssektoren blir fulgt opp mht etterlevelse gjennom tilsyn og andre direkte oppfølgingstiltak.

Kommentarer til 2.2 Bygge og opprettholde robuste og sikre IKT-systemer

6. Stille felles krav til kritiske systemer

Dette tema er omhandlet i de Nasjonale retningslinjer for å styrke informasjonssikkerheten og det foreligger også flere andre dokumenter som omhandler dette. Eksempler er NOU 2006:6 Når sikkerheten er viktigst, Rapport fra arbeidet i BAS 5 som gir veiledning for å identifisere hva som kan være samfunnskritisk, Rapport i regi av KIS, Klassifisering av informasjon og informasjonssystemer er utarbeidet.).

7. Styrke tilsyn med IKT-sikkerhet

Det foregår et bilateralt samarbeid på dette området allerede i dag. Det er hensiktsmessig at dette videreutvikles, både for å sikre deling av kompetanse og for utveksling av informasjon om tilsynsmetoder.

9. Videreutvikle beredskapsplaner med tanke på cybersikkerhetstiltak

Finanstilsynet er positiv til tiltak som etableres for å kunne videreutvikle beredskapsplaner knyttet til cybersikkerhet. Etter Finanstilsynets vurdering bør et eventuelt tverrsektorielt kompetansesenter innen cybersikkerhet etableres i offentlig regi. Med basis i en samlet oversikt over regelverk og tiltak innenfor den enkelte sektor og etablerte samarbeidsarenaer, kan det allerede nå igangsettes aktiviteter for å kunne videreutvikle beredskapsplaner med tanke på cybersikkerhet.

Kommentarer til kapittel 2.3 Bevisstgjøre, opplyse og påvirke

12. Arrangere og delta i øvelser (sektorvise, nasjonale og internasjonale)

Finanstilsynet er enig i at øvelse innenfor beredskapsområdet er viktig og at organisering og initiativ bør komme fra det organ som har sektoransvar. Der hvor det igangsettes øvelser som omhandler flere sektorer bør det organ som har fått det sektorovergripende ansvaret være organisator (f. eks. slik som den siste nasjonale øvelsen IKT-08 i regi av DSB).

Kommentarer til kapittel 2.4 Styrke evnen til å oppdage, varsle og håndtere IKT-hendelser

Dette er et område som allerede er omhandlet i Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007 – 2010, kapittel 3.5 .Utvikling av en strategi for cybersikkerhet bør tilpasses innenfor disse rammer.

13. Styrke samfunnets evne til å oppdage trusler og sårbarheter

Etter det vi forstår innebærer tiltaket mer omfattende overvåking av IKT-basert aktivitet. 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

Finanstilsynet støtter dette tiltaket. Finanstilsynet etablerte i november 2007 en ordning for hendelsesrapportering, hvor bl.a. nettkriminalitet inngår som rapporteringsgrunnlag. Hensikten med å etablere hendelsesrapportering for finanssektoren var å følge opp alvorlige hendelser som oppstår i foretakene og som grunnlag for risikovurderinger. Det har så langt vært meget gode erfaringer med opplegget.

15. Etablere sektorvise CSIRT-miljøer i samfunnsviktige sektorer og i de største enkeltvirksomheter

Finanstilsynet vil ikke utelukke at forslaget kan være formålstjenlig, men forutsetter at et slikt miljø etableres i de organisasjoner som har det sektorvise ansvaret.

Kommentarer til kapittel 2.5 Etterforske og bekjempe IKT-hendelser

Finanstilsynet er enig i tilnærmingen til dette alvorlige problemområdet. Prioriteten bør være at det først og fremst er etablert hensiktsmessige tiltak i det enkelte foretak/institusjon, dernest innenfor aktuelle sektor. I hvilken grad det også skal etableres sektorovergripende opplegg bør drøftes når behovet er klarlagt. Selv om det er politiet som skal forestå etterforskningen, kan sektormyndigheter kunne bidra til politiets etterforskning. For øvrig vil sektormyndigheten ha behov for å sikre seg mest mulig korrekt informasjon om en hendelse, både for å håndtere denne, begrense skadene og etablere preventive tiltak.

19. Avdekke og identifisere trusler og trusselaktører

Finanstilsynet slutter seg til forslaget. Innenfor finanssektoren er foretakene pålagt å utarbeide årlige ROS-analyser av egen IKT-virksomhet.

22. Etablere et nasjonalt cybersenter

Finanstilsynet er positiv til tiltak som etableres for å bedre kunnskapen rundt sikkerhet av informasjonssystemer. Etter Finanstilsynets vurdering bør et eventuelt tverrsektorielt kompetansesenter innen cybersikkerhet etableres i offentlig regi. Med basis i en samlet oversikt over sektorielt regelverk og tiltak og allerede etablerte samarbeidsarenaer, kan det allerede nå igangsettes aktiviteter nødvendige for å bedre håndteringen av cybersikkerhet.

For Finanstilsynet

Anne Merethe Bellamy
direktør for regnskaps og revisjonstilsyn

Frank Robert Berg
seksjonssjef

FINANSTILSYNET
REVIERSTREDET 3
POSTBOKS 1187 SENTRUM
0107 OSLO

TELEFON: 22 93 98 00
TELEFAKS: 22 63 02 26

post@finanstilsynet.no
www.finanstilsynet.no