Post- og teletilsynet
Norwegian Post and Telecommunications Authority

Forsvarsdepartementet
Postboks 8126 Dep.
0032 OSLO

FORSVARSDEPARTEMENTET
SAKNR.: 10 / 00794 - 20
28 JUN 2010
ARKBET: 206
KASSERES 5 ÅR
KASSERES 30 ÅR
BEVARES

Vår ref.: 1002616-2 - 450
Vår dato: 25.6.2010

Deres ref.: 2010/00794-1/FD I 5/OFD
Deres dato: 30.3.2010

Saksbehandler: Håkon Styri

www.npt.no

Høring - forslag til strategi for cybersikkerhet

Post- og teletilsynet (PT) viser til brev fra Forsvarsdepartementet datert 30.03.2010 hvor det bes om kommentar til høringsnotatet *Forslag til strategi for cybersikkerhet* og innspill til økonomiske og administrative konsekvenser innen eget ansvarsområde som ikke har kommet til uttrykk i vedlegg til høringsnotatet.

Sikkerhet og beredskap er et viktig område innenfor PTs eget myndighetsområde, og det er følgelig av stor betydning at strategier og tiltak på dette området er samordnet og representerer en helhetlig sikkerhetstenkning. For PT vil foreliggende utkast til strategi, hvis vedtatt, inngå som en del av de rammebetingelser som gjelder for PTs ansvarsområde.

En helhetlig IKT-sikkerhet må omfatte de eksisterende fast- og mobilnett i tillegg til Internett. Det kan virke som høringsnotatet legger vel stor vekt på Internett og IP-baserte nettverk, men det er etter PTs vurdering alt for tidlig å framskrive den teknologiske utviklingen i så stor grad at en strategi ikke omfatter teknologien i dagens fast- og mobilnett.

Forslaget introduserer ny terminologi med ordet cybersikkerhet, som får en kortfattet definisjon på høringsnotatets side 5: «*Begrepet cybersikkerhet representerer i denne strategien en videreutvikling av informasjonssikkerhetsbegrepet, og gjenspeiler samfunnets stadig økende avhengighet av IKT-systemer bundet sammen i cyberspace.*» Slik PT har forstått begrepet er dette en mangelfull beskrivelse som ikke sier noe om forholdet til andre innarbeidede begreper. Begrepet sier heller ikke noe om hvilke egenskaper eller utfordringer denne videreutviklingen av informasjonssikkerhetsbegrepet skal omfatte.

I PTs eget arbeid med sikkerhet og beredskap forholder vi oss til begrepet IKT-sikkerhet. Dette begrepet er i overensstemmelse med språkbruken i høringsnotatet for øvrig, hvor begreper som IKT-system, IKT-trussel, IKT-hendelse og IKT-risikobilde er brukt. PT anbefaler at det avklares hvorvidt begrepet cybersikkerhet skal defineres som en avgrenset del av fagområdet IKT-sikkerhet, eller om det er andre forhold som skal kjennetegne skillet mellom disse to begrepene.

Høringsnotatet vektlegger intenderte (villede) uønskede hendelser, jf høringsnotatet side 5: «*Fokuset i denne strategien er å motvirke uønskede villede handlinger, men strategien vil også langt på vei bidra til å redusere og håndtere konsekvenser av mer tilfeldige påkjenninger som naturskade (lynnedslag, jordskjelv, flom, etc.), teknisk og menneskelig svikt eller uhell.*» PT vil anføre at tilfeldige eller naturskapte uønskede hendelser kan ha like store konsekvenser som

Besøksadresse | Office address
Nygård 1 Lillesand
Postadresse | Postal address
Postboks 93, 4791 Lillesand
+47 22 82 46 00
firmapost@npt.no
Fax: +47 22 82 46 40
Org.nr: NO 974 446871

intenderte uønskede hendelser. PT forutsetter at en helhetlig strategi bør ha som målsetning å etablere, på grunnlag av (estimerte) kostnader og forventet virkning, et balansert sett med tiltak mot både intenderte uønskede hendelser, og naturskapte eller tilfeldige uønskede hendelser.

Høringsnotatet klassifiserer tiltak som *defensive* eller *offensive*, jf første avsnitt side 4, fjerde avsnitt side 13 og tiltak 20. Høringsnotatet gir ingen definisjon eller forklaring på hva som ligger i disse begrepene. I forbindelse med sikkerhetsarbeid betegner PT og ekomsektoren tiltak som forebyggende, sannsynlighetsreduserende eller konsekvensreduserende. For å komme fram til en helhetlig strategi er det etter PTs vurdering ønskelig å samordne begrepsbruken og innarbeide eller vise til klare definisjoner av sentrale begrep.

Uavhengig av begrepsbruken, forutsetter PT at enhver bruk av "offensive aktørfokuserte tiltak", jf høringsnotatet siste avsnitt side 6, er harmonisert med tilbydere hvis nett slike tiltak benytter. Dette for blant annet å sikre at slike tiltak ikke bryter med den regulering tilbyderne er underlagt. I den grad slike tiltak skulle forekomme, forutsetter PT at dette avklares med PT som sektortilsyn.

Høringsnotatet framholder på side 4 at: «*Små forstyrrelser i nettverkene kan få store konsekvenser.*» PT kan slutte seg til dette utsagnet, men etterlyser en diskusjon om risikoakseptkriterier i strategien, det vil si hvor store forstyrrelser og utfall i IKT-systemer og -infrastruktur kan bli før de er uakseptable for samfunnet. Kostnadene for tiltak vil øke med graden av robusthet. Kostnader som tilbydere av offentlige elektroniske kommunikasjonsnett og -tjenester får som følge av krav eller pålegg om sikkerhetstiltak må betales av brukeren, og i visse tilfeller må merkostnader dekkes over statsbudsjettet, jf ekomloven § 2-10. Som sektormyndighet er det PT som bør sette minstekrav til sikkerhet hos tilbydere av offentlige elektroniske kommunikasjonstjenester og -nett. Brukere med behov for en særskilt høy tjenestekvalitet må også betale ekstra kostnader for dette.

Høringsnotatets innledning beskriver internasjonale tilnærminger til IKT-sikkerhet, jf side 7. I omtalen av EU nevnes EPCIP-direktivet (2008/114/EF) og meddelelse fra EU-kommisjonen COM (2009) 149. PT viser til at en vesentlig del av meddelelse COM (2009) 149 er en handlingsplan med konkrete tiltak for å gjennomføre EPCIP-programmet i forhold til IKT-sektoren. Et annet viktig dokument er en studie om *Availability and Robustness of Electronic Communications Infrastructures*, ARECI-rapporten, som EU-kommisjonen publiserte i 2007. Deler av denne rapporten er tatt inn i EPCIP-arbeidet, og ut over dette arbeides det videre med enkelte av rapportens forslag til tiltak.

PT vil også påpeke at EUs direktiver for ekomsektoren i tillegg inneholder regulering som er relevant for IKT-sikkerhet. Rammedirektivet har i direktiv 2009/140/EF fått et nytt kapittel IIIa om sikkerhet og integritet i nett og tjenester. Dette medfører at kravene til pålitelig og sikker formidling av informasjon over elektroniske kommunikasjonsnett skjerpes. I forbindelse med høringsnotatets forslag 4 og 14 vil PT viser til at de nye bestemmelsene pålegger tilbydere varslingsplikt overfor myndighet ved sikkerhetsbrudd, og om nødvendig skal også myndigheter i andre land, samt ENISA varsles.

Kommentarer til de enkelte tiltak.

PT har valgt å kommentere kun de tiltak som er særlig relevante.

Tiltak 1 Kartlegge og verdivurdere kritiske IKT-systemer i alle sektorer (side 14)

PT er i sitt tildelingsbrev fra Samferdselsdepartementet blant annet pålagt å identifisere risikofaktorer i ekomnett og -tjenester. PT gjennomfører regelmessige informasjonsinnsamlinger for å frambringe oppdaterte oversikter over infrastrukturen til de viktigste tilbydere av offentlige elektroniske kommunikasjonsnett og vurderer i den sammenheng deres risiki og iverksatte sikkerhetstiltak. Ekomloven § 2-10 supplerer videre sikkerhetsloven (lov 20. mars 1998 nr. 10), jf Ot.prp.nr.58 (2002-2003). PT vil understreke at ekomsektoren, som andre sektorer, må forholde seg til sektorspesifikke krav. PT er positive til at flere sektorer samordner sine vurderinger for å få

et bedre grunnlag for en verdivurdering av IKT-infrastrukturen. Samferdselsdepartementet har gjennomført en samlet risikovurdering for egen sektor i prosjektene SAMROS og KRISIS., PT har stor hatt nytte av resultatene fra dette arbeidet. PT vil likevel påpeke viktigheten av at ikke mengden av detaljopplysninger blir for stor. Innen ekomsektoren kan informasjon om hvilke brukere som har samfunnskritisk funksjon, jf ekomforskriften § 8-1, være nyttig for den enkelte tjenestetilbyder, men en samlet liste over slike enkeltbrukere vil ha begrenset verdi for PT i kartleggingen av kritisk ekominfrastruktur.

Høringsnotatet refererer også til arbeidet med prioritetsordninger: «*Post og teletilsynet (PT) på sin side arbeider med prioriteringsordninger knyttet til elektroniske informasjonssystemer.*» PT antar at det er arbeidet med innføring av trafikkprioritet i mobilnettene det siktes til, og vil anføre at det arbeides med en forskrift om prioritet i mobilnett som trolig vil bli sendt på høring i løpet av 2010.

Tiltak 2 Målrettet satsning på forskning og utvikling (side 15)

PT er positiv til en økt satsing på FoU innen sikkerhetsområdet, og vil understreke at i tillegg til engasjement fra offentlig sektor er det er viktig at tjenestetilbydere også bør med i dette arbeidet. Strategien bør utvides til å vurdere virkemidler for å sikre at disse aktørene fra privat sektor også inkluderes.

Tiltak 5 Etablere partnerskap mellom offentlige myndigheter og private aktører (side 15)

NorCERT er et viktig tiltak for IKT-sikkerhet, men PT vil gjerne oppfordre til at samarbeidet mellom NorCERT og andre offentlige aktører, i det minste, blir likeverdig med det samarbeidet NorCERT har med NorCERT-partnere fra privat sektor.

PT har regelmessig møter med de private aktørene innen egen sektor, og har i den sammenheng også forum innenfor fagområdet sikkerhet. Som tilsynsmyndighet er det imidlertid ikke nødvendigvis slik at partnerskap er en hensiktsmessig samarbeidsform. Det kan derfor være hensiktsmessig om ordlyden i tiltak 5 tilpasses flere samarbeidsformer enn partnerskap.

Tiltak 6 Stille felles krav til kritiske IKT-systemer (side 16)

PT vil anføre at det i dette tiltaket ikke kommer klart fram om det er felles krav for kritiske IKT-systemer i offentlig sektor som foreslås eller om det er nasjonale krav som også skal omfatte privat sektor. Dersom kravene også skal gjelde privat sektor er det viktig at felles krav utvikles i nært samarbeid med de enkelte sektormyndigheter og avgrenses slik at en på en effektiv måte kan forholde seg til sektorspesifikke krav og behov.

PT er i 2010 gjennom tildelingsbrevet fra Samferdselsdepartementet pålagt å utarbeide et forslag om innføring av regelverk for klassifisering av ekominfrastruktur. PT arbeider med en forskrift som formodentlig vil grense opp mot objektsikkerhetsforskriften, og etter planen vil klassifiseringsforskriften sendes ut på høring i annet halvår 2010.

Tiltak 7 Styrke tilsyn med IKT-sikkerhet (side 16)

PT har i dag tilsyn med tilbydere i ekomsektoren som omfatter både merkantile og tekniske forhold. PT ser nytteverdien av å koordinere tilsynsaktiviteter med enkelte andre sektorer, men vurderer det slik at antall tilsynsmyndigheter som deltar må være begrenset for at tilsynsarbeid skal bli effektivt og ha mulighet til å fokusere på særlig viktige spørsmål.

Tiltak 8 Utvikle og implementere sikre og robuste kommunikasjonsløsninger for krisehåndtering (side 17)

PT vil anføre at de kommunikasjonsløsninger som i dag benyttes i krisesituasjoner bruker offentlige elektroniske kommunikasjonsnett, enten som tjenester eller i form av leid kommunikasjonskapasitet. PT vil understreke viktigheten av at offentlige etater, private

virksomheter og organisasjoner gjennomfører egne risiko- og sårbarhetsvurderinger for å avdekke sine behov for elektronisk kommunikasjon i krisesituasjoner. Å bygge opp en egen infrastruktur for krisekommunikasjon som er mer robust enn dagens offentlige ekomnett kan, etter vår mening, bli meget kostbart både i anskaffelse og drift. Dette kommer ikke klart frem av høringsnotatets vedlegg. PT gir imidlertid sin tilslutning til at kommunikasjonsbehovet for krisehåndtering bør utredes, og vil legge til at det er viktig at en slik utredning også omfatter kommunikasjonsbehovet for arbeidet med å gjenopprette normaltilstand. Uten en slik utredning er det vanskelig å anslå kostnadene forbundet med å utvikle og implementere sikre og robuste kommunikasjonsløsninger for krisehåndtering.

Tiltak 9 Videreutvikle beredskapsplaner med tanke på cybersikkerhetstiltak (side 17)

Nasjonale beredskapsplaner for IKT-sikkerhet bør utvikles i tett samarbeid mellom de ulike sektormyndighetene. PT er i tildelingsbrevet fra Samferdselsdepartementet pålagt å avhjelpe identifiserte risikofaktorer hos aktuelle tilbydere gjennom pålegg eller avtaler om utbedring. Når PT inngår slike avtaler med tilbydere omfatter disse også krav til beredskapsplaner. I disse avtalene med tilbydere kan PT også innarbeide krav som er relevante for det nasjonale beredskapssystemet (NBS).

Tiltak 10 Behov for regulatorisk forankring av cybersikkerhet (side 10)

Dagens regulering av ekomsektoren omfatter krav til IKT-sikkerhet. PT vil også vise til de over nevnte endringer i EU-direktiver som er relevante i den pågående revisjon av ekomlov og -forskrift. Når det gjelder behovet for en helhetlig gjennomgang av eksisterende regelverk, er det allerede gjennomført en slik gjennomgang av KIS. PT vurderer det som hensiktsmessig at en først identifiserer hvilke nye tiltak som er nødvendige, før en utreder den regulatoriske forankringen.

Tiltak 11 Styrke tiltak for bevisstgjøring, utdanning og holdningsskapende arbeid (side 18)

PT deltar i holdningsskapende arbeid innen IKT-sikkerhet gjennom tiltak som nettvett.no og Nasjonal sikkerhetsdag, og gjennom tilsynsarbeid og faglig dialog med tilbydere. PT deltar gjerne i arbeid for å utvikle slike samarbeid videre, men vil påpeke at den nasjonale strategien for cybersikkerhet gjerne kunne vært litt mer konkret med hensyn til hvordan disse tiltakene skal styrkes ut over det arbeidet som allerede pågår.

Tiltak 12 Arrangere og delta i øvelser (sektorvise, nasjonale og internasjonale) (side 18)

PT deltar i og arrangerer øvelser innen egen sektor. PT har siden 2008 også samarbeidet med NVE om sektorovergripende regionale øvelser som over en periode skal gjennomføres i alle fylker. I EU-kommisjonens meddelelse COM (2009) 149 er et av tiltakene i handlingsplanen å gjennomføre en paneuropeisk øvelse i løpet av 2010. En flernasjonal øvelse EuroCyberEx under fransk ledelse planlegges for 2011. Det er etter PTs vurdering ikke et behov for flere øvelser, men snarere et behov for bedre samordning av øvelser og et samarbeid for å heve kvaliteten på de øvelser som gjennomføres.

Tiltak 13 Styrke samfunnets evne til å oppdage trusler og sårbarheter (side 19)

PT har ikke tilstrekkelig kjennskap til dagens VDI for å uttale seg om behovet for og nytten av at dette systemet utvides. PT vil likevel anføre at det kan være nyttig med en bedre utveksling av informasjon om uønskede hendelser for å bidra til at en raskest mulig kan få en god oversikt over situasjonen, samt både faktiske og mulige konsekvenser av hendelsen. Til første setning av tiltak 13 som gir uttrykk for at tiltaket forutsetter økende grad av registrering og analyse av datakommunikasjon, har PT samme kommentar som for tiltak 17 under.

Tiltak 14 Legge til rette for innrapportering av hendelser

PT har etablert rutiner for innrapportering av hendelser av en viss alvorlighetsgrad fra de viktigste tilbydere av ekomtjenester. Dagens ordning er frivillig, men PT viser til omtalen av endringene i EUs rammedirektiv for ekom over hvor det innføres en varslingsplikt. En bedre samordning med NorCERT av hendelsesrapporteringen er ønskelig. PT følger EU-prosjektet MIMER som utvikler et GIS-basert system for varsling av hendelser. I siste setning av tiltak 14 omtales videreapportering til sentralt nivå. PT er usikker på hva som menes med begrepet «*sentralt nivå*» i denne sammenheng. PT foreslår at det opprettes et sektorovergripende koordineringsutvalg som regelmessig møtes for å sammenstille hendelsesrapporter som har hatt sektorovergripende konsekvenser, og som på grunnlag av dette kan utrede behovet for koordinering av hendelsesrapporter.

Tiltak 15 Etablere sektorvise CSIRT-miljøer i samfunnsviktige sektorer og i de største enkeltvirksomheter (side 19)

PT vil framheve viktigheten av rask varsling og informasjonsdeling mellom sektorene, som beskrevet i første avsnitt av dette tiltaket.

Tilbydere av tjenester og nett i ekomsektoren er avhengige av fungerende operasjonssentre. I noen virksomheter er dette operasjonssenteret tjenesteutsatt (outsourcet) til underleverandører, og noen tilbydere har satt ut så vel utbygging, vedlikehold og drift av nett til underleverandør. Andre tilbydere har samlet drift av tjenester og nett for flere land i et felles operasjonssenter. For enkelte tilbydere er CSIRT-funksjonen en del av operasjonssenteret, men noen tilbydere har etablert egen enhet for slike oppgaver.

For sektormyndigheter som ikke eier egen infrastruktur, bør det utredes nærmere hvilken nytte det har å opprette en CSIRT for sektoren og hvordan slike CSIRTer eventuelt bør organisere. En CSIRT for ekomsektoren vil etter PTs vurdering representere en betydelig andel av det ansvarsområdet NorCERT dekker i dag. Å opprette en CSIRT for ekomsektoren vil kreve investering i utstyr og programvare, og driften vil kreve flere årsverk. I forhold til høringsnotatets vedlegg om økonomiske og administrative konsekvenser vil PT anføre at det er nødvendig å utrede delingen av ansvar mellom NorCERT og et CSIRT for ekomsektoren før det er mulig å legge fram et realistisk kostnadsoverslag. PT fremlegger derfor ikke noe kostnadsoverslag på dette punkt.

PT vil understreke viktigheten av at en struktur med sektorvise CSIRTer ikke må gå på bekostning av effektiv informasjonsutveksling og rask håndtering av hendelser. PT vil derfor anbefale at dette tiltaket utredes særskilt og med deltagelse fra alle relevante sektorer.

Tiltak 17 Sikre mulighet til nødvendig lagring av data ved hendelser med tanke på å muliggjøre effektiv etterforskning (side 20)

Beskrivelsen av dette tiltaket er såpass kortfattet at PT vil be om at det utdypes og utredes bedre. Det er særlig viktig at det kommer klart fram hvilke utfordringer dette tiltaket skal adressere som går ut over det som vil følge av en eventuell implementering av datalagringsdirektivet.

Tiltak 19 Avdekke og identifisere trusler og trusselaktører (side 21)

Siste setning i første avsnitt av dette tiltaket har ordlyden: «*Bekjempelse av nye og komplekse trusler bør ikke bare innrettes defensivt, men etter behov også som kilde til kunnskap om trusselaktørens oppfatninger og prioriteringer.*» PT viser til den innledende diskusjon om begrepene defensiv og offensiv, og er i forbindelse med siterte setning usikker på hvilken bruk av "offensive" metoder som er tenkt brukt for å avdekke trusselaktørers oppfatninger og prioriteringer. PT ber om at det kommer klarere fram i hvilken grad infrastrukturen til tilbydere av offentlige elektroniske kommunikasjonsnett og -tjenester kan bli involvert i det som beskrives som "offensive" metoder. Videre bør mulige konsekvenser av slik eventuell bruk analyseres.

Tiltak 20 Offensive kapasiteter (side 21)

PT har samme anførsel til dette tiltaket som for tiltak 19, og ber om at det avklares bedre hva begrepet offensive tiltak omfatter og at det i forhold til private aktører, og særlig tilbydere av offentlige elektroniske kommunikasjonsnett og -tjenester, beskrives hvilken rolle disse aktørene er tiltenkt og i hvilken grad offensive tiltak vil benytte disse aktørenes infrastruktur og tekniske installasjoner. Som for tiltak 19, bør mulige konsekvenser av slik bruk analyseres.

PT vil understreke betydningen av at tilbydere hvis nett blir benyttet til "offensive aktørfokuserte tiltak" blir informert om slike tiltak. Som nevnt over er dette viktig for å sikre overholdelse av rammebetingelser, men dette er også viktig for at tilbyderne skal kunne hensynta dette i eget planverk og for å kunne tilrettelegge egen drift i situasjoner hvor det er aktuelt at slike tiltak benyttes.

Vedlegg A: Eksisterende roller, ansvar og myndighet nasjonalt

I tredje avsnitt, siste setning omtales tjenestetilbydere. I denne forbindelse vil PT nevne at tjenestetilbydere i 1999 opprettet bransjeforeningen ITAKT (Internett- og Telebransjens Anti-Kriminalitets Tiltak) for å bekjempe svindel og misbruk av tjenester og infrastruktur i forbindelse med virksomheten til norske internett- og teleoperatører.

Med hilsen

Willy Jensen
direktør

Aslaug Hagestad Nag
avdelingsdirektør

Kopi til: Samferdselsdepartementet