Samlenotat til Folketingets Europaudvalg og Folketingets Udvalg for Teknologi og Udvikling

Samlenotat for it- og telepunkter på rådsmøde (transport, telekommunikation og energi) den 11. juni 2009

---

9. Kommissionens meddelelse til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om beskyttelse af kritisk informationsinfrastruktur: Beskyttelse mod storstilede cyberangreb og sammenbrud: øget beredskab, sikkerhed og robusthed
KOM(2009) 149 endelig
Udveksling af synspunkter

27. maj 2009

IT- og Telestyrelsen
Holsteinsgade 63
2100 København Ø
Telefon 3545 0000
Telefax 3545 0010
E-post itst@itst.dk
Netsted www.itst.dk
CVR-nr. 2676 9388

Kommissionens meddelelse til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om beskyttelse af kritisk informationsinfrastruktur: Beskyttelse mod storstilede cyberangreb og sammenbrud: øget beredskab, sikkerhed og robusthed

KOM(2009) 149 endelig

Udveksling af synspunkter

Optrykt på baggrund af grundnotat oversendt den 5. maj 2009. Ændringer er markeret i marginen.

1. Resumé

Kommissionens meddelelse "Beskyttelse mod storstilede cyberangreb og sammenbrud: øget beredskab, sikkerhed og robusthed" bygger videre på EU's ambition om at styrke sikkerheden i og tilliden til informationssamfundet. Kommissionen fremhæver i meddelelsen særligt strategien for et sikkert informationssamfund fra 2006[1]. Kommissionen anfører, at det ser ud til, at de berørte parter ikke i tilstrækkelig grad har taget strategien til sig og gjort en indsats for at føre den ud i livet.

I meddelelsen lægger Kommissionen vægt på forebyggelse, beredskab og bevidstgørelse og opstiller en plan over øjeblikkelige tiltag, der skal styrke sikkerheden og robustheden i kritisk informationsinfrastruktur.

Det bliver anført, at samfundets afhængighed af kritisk informationsinfrastruktur og informationsinfrastrukturens sammenhæng på tværs af grænserne og med anden infrastruktur samt dens sårbarhed og truslerne mod den gør, at det som første skridt i et forsvar mod svigt og angreb er nødvendigt at drøfte spørgsmålet om sikkerhed og robusthed ud fra et systemisk perspektiv.

2. Baggrund

Nogle IKT-systemer, -net og -tjenester spiller en helt afgørende rolle i den europæiske økonomi og det europæiske samfund som grundlag for levering af uundværlige varer og tjenesteydelser. Disse systemer benævnes kritisk informationsinfrastruktur, eftersom det vil have alvorlige følger for samfundets kritiske funktioner, hvis de bryder sammen eller bliver ødelagt.

Meddelelsen bygger videre på EU's politik for at styrke sikkerheden i og tilliden til informationssamfundet. I 2005 fremhævede Kommissionen det akutte behov for en koordineret indsats for at opbygge tillid til elektroniske kommunikationsnet og

[1] KOM(2006) 251: En strategi for et sikkert informationssamfund – "Dialog, partnerskab og myndiggørelse"

tjenester. Til dette formål blev der i 2006 vedtaget en strategi for et sikkert informationssamfund, KOM(2006) 251: En strategi for et sikkert informationssamfund – "Dialog, partnerskab og myndiggørelse"

Meddelelsen dannede grundlag for drøftelserne på ministerkonference om beskyttelse af kritisk informationsinfrastruktur, der blev afholdt i Estland den 27. - 28. april 2009.

Meddelelsen forventes drøftet på det kommende rådsmøde (it og telekommunikation) den 12. juni 2009.

3. Hjemmelsgrundlag

Da der er tale om en meddelelse fra Kommissionen, er spørgsmålet om hjemmelsgrundlag ikke relevant.

4. Nærhedsprincippet

Spørgsmålet om nærhedsprincippet er ikke relevant.

5. Formål og indhold

Kommissionens meddelelse om beskyttelse af kritisk informationsinfrastruktur lægger vægt på forebyggelse, beredskab og bevidstgørelse og opstiller en plan over øjeblikkelige tiltag, der skal styrke sikkerheden og robustheden i kritisk informationsinfrastruktur.

Aktiviteterne, der skitseres i Kommissionens meddelelse, vil blive gennemført som led i og parallelt med det europæiske program for kritisk infrastruktur (EPCIP), hvori to af nøgleelementerne er direktivet om indkredsning og udpegning af europæisk kritisk infrastruktur, der peger på IKT-sektoren som et højt prioriteret område for fremtidige tiltag, og informationsudvekslingsnetværket CIWIN.

Kommissionen finder, at der er behov for en europæisk indsats, der kan give de nationale politikker og programmer merværdi ved at skabe øget bevidsthed om og en fælles forståelse af udfordringerne og sætte gang i vedtagelsen af fælles politiske mål og indsatsområder, styrke samarbejdet mellem medlemsstaterne og integrere de nationale politikker i et mere europæisk og verdensomspændende perspektiv.

En stærk europæisk varslings- og reaktionsevne forudsætter velfungerende landsdækkende/statslige it-beredskabsenheder (CERT – Computer Emergency Response Team). Desuden skal de indgå i et effektivt samarbejde og i informationsudveksling på tværs af grænserne, eventuelt via eksisterende organisationer som European Governmental CERT's Group.

Kommissionen konstaterer i meddelelsen, at der er begrænset europæisk varslings- og reaktionsevne til imødegåelse af truslerne mod IKT-infrastrukturen. Processerne og fremgangsmåderne for overvågning og rapportering af sikkerhedshændelser på

nettene varierer betydeligt fra medlemsstat til medlemsstat. Nogle medlemsstater har ingen it-beredskabsenheder, som er ansvarlig for overvågningen.

Meddelelsen foreslår på den baggrund en handlingsplan, der indeholder følgende mål:

Beredskab og Forebyggelse
Minimumstandarder for landsdækkende/statslige it-beredskabsenheder (CERT) skal være fastlagt ved udgangen af 2010. Der skal være oprettet velfungerende landsdækkende/statslige CERT-enheder i alle medlemsstater ved udgangen af 2011.

Der skal foreligge en køreplan for et europæisk offentlig-privat partnerskab for en robust infrastruktur ved udgangen af 2009. Partnerskabet skal være etableret midt i 2010. De første resultater af partnerskabet skal foreligge i slutningen af 2010.

Der skal etableres et europæisk forum, hvor medlemsstaterne kan udveksle information og god strategisk praksis vedrørende sikkerheden og robustheden i kritisk informationsinfrastruktur ved udgangen af 2009. Forummets første resultater skal foreligge i slutningen af 2010.

Opdagelse og reaktion
Kommissionen støtter udviklingen og indførelsen af et europæisk informationsudvekslings- og varslingssystem (EISAS), der når ud til borgerne og de små og mellemstore virksomheder. Køreplanen for et europæisk informationsudvekslings- og varslingssystem skal foreligge i slutningen af 2010.

Afhjælpning og genopretning
Kommissionen opfordrer medlemsstaterne til at udforme nationale katastrofeplaner og afholde jævnlige øvelser i håndtering af omfattende netsikkerhedshændelser. Der skal være gennemført mindst én national katastrofeøvelse i hver medlemsstat inden udgangen af 2010.

Kommissionen vil yde økonomisk støtte til tilrettelæggelse af fælleseuropæiske øvelser i håndtering af hændelser, der truer internettets sikkerhed: Den første fælleseuropæiske øvelse skal være tilrettelagt og gennemført inden udgangen af 2010. Der skal være fælleseuropæisk deltagelse i internationale øvelser inden udgangen af 2010.

Kommissionen opfordrer medlemsstaternes til at styrke samarbejdet mellem de landsdækkende/statslige CERT-enheder. Derfor skal antallet af nationale instanser, der deltager i European Governmental CERTs Group være fordoblet inden udgangen af 2010.

Internationalt samarbejde
Kommissionen vil sætte gang i en europadækkende debat med deltagelse af alle relevante offentlige og private parter med det formål at fastlægge EU's vigtigste mål for langsigtet robusthed og stabilitet. EU's vigtigste mål vedrørende kritiske internetkomponenter og -spørgsmål skal ligge fast inden udgangen af 2010.

Kommissionen vil samarbejde med medlemsstaterne om at opstille retningslinjer for internettets robusthed og stabilitet. Der skal foreligge en europæisk køreplan for opstilling af principper og retningslinjer for et robust og stabilt internet inden udgangen af 2009. Der skal være enighed om et første udkast til et sådant sæt principper og retningslinjer inden udgangen af 2010.

Kommissionen vil samarbejde med medlemsstaterne om at opstille en køreplan for at fremme de europæiske principper og retningslinjer på verdensplan. Der skal opstilles en køreplan for det internationale samarbejde om principper og retningslinjer for robusthed og stabilitet i starten af 2010. Det første udkast til internationalt anerkendte principper og retningslinjer skal drøftes med tredjelande og i relevante fora, herunder et dialogforum for internetforvaltning (Internet Governance Forum) i slutningen af 2010.

Kommissionen opfordrer de berørte europæiske parter til at overveje, hvordan afhjælpnings- og genopretningsøvelserne rent praktisk kan udvides og gennemføres på verdensplan. Der foreslås en ramme og en køreplan for europæisk engagement og deltagelse i verdensomspændende øvelser i genopretning og afhjælpning ved omfattende internetsikkerhedshændelser inden udgangen af 2010.

Kriterier for europæisk kritisk infrastruktur i ikt-sektoren
Kommissionen vil i samarbejde med medlemsstaterne og alle relevante parter videreføre arbejdet med at opstille sektorspecifikke kriterier for indkredsning af europæisk kritisk infrastruktur i IKT-sektoren i første halvdel af 2010.

Meddelelsens konklusion
Kommissionen konkluderer i meddelelsen, at en sikker og robust kritisk informationsinfrastruktur er det bedste forsvar mod svigt og angreb. Handlingsplanens succes afhænger af, hvor godt den kan bygge videre på og bidrage til aktiviteter i den offentlige og den private sektor, og af medlemsstaternes, EU-institutionernes og de øvrige parters engagement og fulde samarbejde.

Forbedring af sikkerheden og robustheden i IKT-infrastrukturen er et langsigtet mål, og strategien og foranstaltningerne for at nå dette mål må jævnligt tages op til fornyet overvejelse. Som led i den overordnede debat om net- og informationssikkerhedspolitikkens fremtid i EU efter 2012 vil Kommissionen derfor hen imod slutningen af 2010 iværksætte en evaluering af den første fase af foranstaltninger og om nødvendigt foreslå yderligere tiltag.

6. Europa-Parlamentets udtalelser

Europa-Parlamentet har endnu ikke udtalt sig.

7. Gældende dansk ret og forslagets konsekvenser herfor

Området er i dag ikke reguleret af dansk lov.

Meddelelsen får ikke i sig selv konsekvenser for gældende dansk ret. Det kan ikke udelukkes, at området vil blive reguleret, hvis Kommissionen følger meddelelsen op med initiativer, der kræver regulering i Danmark.

8. Forslagets konsekvenser for statsfinanserne, samfundsøkonomien, miljøet eller beskyttelsesniveauet

Meddelelsen har ikke i sig selv konsekvenser for statsfinanserne, samfundsøkonomien, miljøet eller beskyttelsesniveauet.

Afhængigt af, hvorledes man fra dansk side vælger at gennemføre Kommissionens opfordringer, vil det kunne medføre udgifter for staten. Eventuelle økonomiske konsekvenser vil afhænge af, hvordan man vælger at implementere initiativerne. Derudover vil der kunne være tale om udgifter på EU-budgettet afhængigt af de konkrete forslag, som Kommissionen vil fremføre.

9. Høring

Meddelelsen har været i høring i EU-specialudvalget for it og telekommunikation, hvilket ikke gav anledning til bemærkninger.

10. Regeringens foreløbige generelle holdning

Kommissionens meddelelse vurderes at være i tråd med regeringens prioriteringer på området og i overensstemmelse med planlagte eller allerede iværksatte tiltag. Regeringen har i sin politik for beredskabet fra 2005 anført, at forebyggelse prioriteres højt for at mindske samfundets sårbarhed og dermed øge robustheden, især inden for energi-, tele-, it- og transportområdet. Regeringen stiller sig positivt over for beskyttelse af kritisk informationsinfrastruktur, og støtter derfor meddelelsen. Regeringen vil endvidere arbejde for, at tiltag som følge af meddelelsen bliver så omkostningseffektive som muligt, og at de i videst muligt omfang vil bygge på eksisterende nationale og europæiske tiltag, herunder særligt arbejdet der allerede pågår i forbindelse med EPCIP-programmet. Ligeledes ønsker regeringen et tæt samarbejde med andre internationale aktører, der også har igangsat en række initiativer for at dæmme op for sårbarheden ved cyberangreb.

Regeringen imødeser udmøntningen af Kommissionens forslag.

11. Generelle forventninger til andre landes holdninger

Kommissionens meddelelse er blevet drøftet indledningsvist på ministerkonference i Tallinn mellem den 27. og 28. april 2009. Her gav medlemsstaterne udtryk for generel støtte til meddelelsen og dens initiativer.

12. Tidligere forelæggelse for Folketingets Europaudvalg

Meddelelsen har ikke tidligere været forelagt Folketingets Europaudvalg.

Grundnotat til Folketingets Europaudvalg er oversendt den 5. maj 2009.

Notatet er ligeledes fremsendt til Udvalget for Videnskab og Teknologi.