Grundnotat til Folketingets Europaudvalg og Folketingets Udvalg for Videnskab og Teknologi

Kommissionens meddelelse til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om beskyttelse af kritisk informationsinfrastruktur "Resultater og næste skridt: vejen til global internetsikkerhed"

– KOM (2011) 163

27. april 2011

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

Resumé

Meddelelsen indeholder en gennemgang af de tiltag, der er gennemført siden Kommissionens meddelelse KOM(2009) 149, som skitserede en handlingsplan for europæisk kritisk informationsinfrastrukturbeskyttelse. Den nye meddelelse peger på nødvendigheden af et øget internationalt samarbejde på området.

Det forventes, at punktet vil blive sat på dagsordenen for rådsmødet (transport, telekommunikation og energi) den 27. maj 2011 med henblik på vedtagelse af rådskonklusioner.

1. Baggrund

Rådet vedtog ved rådsmødet den 18. december 2009 en rådsresolution på baggrund af kommissionsmeddelelse af 30. marts 2009 om "Beskyttelse mod storstilede cyberangreb og sammenbrud: Øget beredskab, sikkerhed og robusthed"[1] (CIIP).

Den 19. maj 2010 offentliggjorde Kommissionen sin meddelelse om "En digital dagsorden for Europa"[2], i hvilken der blandt andet blev lagt vægt på, at der opbygges en fælles forståelse for tillid og sikkerhed som grundlæggende forudsætninger for en almen udbredelse af IKT og dermed for at nå Europa 2020-strategiens mål om intelligent vækst.[3] Sammen med en række andre initiativer fra Kommissionen understreger det et ønske om på at skabe digitale rammer, der gør det muligt for alle europæere at udnytte deres økonomiske og sociale potentiale fuldt ud.

Denne nye meddelelse er en status over de resultater, der er opnået siden CIIP-handlingsplanen blev iværksat i 2009.

[1] KOM(2009) 149

[2] KOM(2010) 245

[3] KOM(2010) 2020

Punktet forventes sat på dagsordenen for det kommende rådsmøde (transport, telekommunikation og energi) den 27. maj 2011 med henblik på vedtagelse af rådskonklusioner.

2. Formål og indhold

De risikoanalyser, der foretages både af private og offentlige interessenter, viser en stadig udvikling i risikobilledet hen mod mere teknologisk sofistikerede angreb i takt med, at samfundene bliver mere og mere afhængige af IKT. Truslerne mod it-systemer kan opdeles i tre kategorier:

- Udnyttelse med henblik på at opnå økonomiske og/eller politiske fordele, herunder spionage og identitetstyveri.
- Forstyrrelse af informationssystemer, som kendes fra angreb på informationssystemer med den følge, at de ikke har været i stand til at fungere normalt. Et eksempel herpå er de angreb, der fandt sted mod Estland i 2007 og senere mod Georgien i 2008.
- Ødelæggelse af fysiske systemer, hvilket endnu ikke har fundet sted, men som ikke kan udelukkes i fremtiden i takt med, at kritiske systemer forbindes til internettet. I Iran har den såkaldte Stuxnet-orm været i stand til at trænge ind i et beskyttet uran-oparbejdningsanlæg. I takt med at flere og flere for samfundets funktion livsvigtige systemer bliver forbundet til internettet, herunder el- og vandforsyning, vil det ikke kunne udelukkes, at et sådant angreb vil finde sted i de kommende år.

Disse trusler er ikke specifikke for EU, og kan ikke løses af EU alene. Det er derfor nødvendigt at opnå en global forståelse for de risici, samfundene står over for.

Kommissionen gennemgår i meddelelsen de forskellige tiltag, som blev defineret i CIIP-handlingsplanen fra 2009:

Beredskab og forebyggelse

I regi af Kommissionen og med støtte fra Det europæiske agentur for net- og informationssikkerhed (ENISA) er der blevet oprettet Det europæiske forum for informationsudveksling mellem medlemsstaterne (EFMS). Formålet er at udvikle en fælles forståelse for sikring af internettet.

Som middel til at styrke samarbejdet mellem den europæiske offentlige sektor og den private sektor er oprettet Det europæiske offentlig-private partnerskab for en robust infrastruktur (EP3R) og som med hjælp fra ENISA skal udbygges til at fungere som en platform for internationalt samarbejde.

Desuden fortsættes arbejdet med at hjælpe de medlemsstater, der endnu ikke har etableret nationale/statslige CERT'er, således at alle medlemsstater vil have en national CERT med udgangen af 2012.

Opdagelse og reaktion
ENISA vil samarbejde med CERT'erne med henblik på at belyse mulighederne for, at CERT'erne kan danne grundlaget for det Europæiske forum for informationsudvekslings- og varslingssystem (EISAS), som er planlagt til at blive etableret i 2013.

Afhjælpning og genopretning
ENISA vil fortsætte med at hjælpe medlemsstaterne med at udarbejde nationale katastrofeplaner og beredskabsøvelser for IKT.

Den første fælleseuropæiske beredskabsøvelse på området blev afholdt 4. november 2010. ENISA stod for planlægningen. Arbejdet er begyndt med henblik på den næste øvelse, som er planlagt til 2012. ENISA har arbejdet på at styrke samarbejde mellem nationale/statslige CERT'er.

Internationalt samarbejde
Et udvidet samarbejde er påbegyndt med især USA. Som et første skridt i et internationalt samarbejde har EU og USA nedsat en "EU-US Working Group on Cyber-security and Cyber-crime" i november 2010. Samarbejdet forventes udstrakt til andre regioner med henblik på at fremme et robust og stabilt internet på globalt plan. I 2012/13 er det planlagt at gennemføre en stor international øvelse i samarbejde med USA og deltagelse af et større antal medlemsstater.

Kriterier for europæisk kritisk infrastruktur i ikt-sektoren
I EFMS har der været drøftelser med henblik på at identificere europæisk kritisk informationsinfrastruktur for fastnet og mobil kommunikation samt internettet. Kommissionen vil drøfte med medlemsstaterne om sektorspecifikke elementer skal inkluderes i revisionen af direktivet om identifikation og udpegning af europæisk kritisk informationsinfrastruktur (2008/114/EF) i 2012.

Det videre forløb
Det er Kommissionens holdning, at CIIP-handlingsplanen har haft en række positive resultater, ikke mindst anerkendelsen af, at der er behov for en samarbejdsbaseret tilgang til net- og informationssikkerhed, der involverer alle parter.

Kommissionen ser behov for at udvide indsatsen internationalt og udvikle partnerskaber for at få fuldt udbytte af bestræbelserne. Der er behov for at fremme en global kultur, der underbygger risikostyring. Der bør gennemføres målrettede foranstaltninger mod sikkerhedstrusler og it-baseret kriminalitet.

Kommissionen har til hensigt at bidrage til opbygningen af denne globale tilgang således:

- **Fremme principper for et robust og stabilt internet**
  Der bør opstilles internationale principper for et robust og stabilt internet i samarbejde med andre lande, internationale organisationer og eventuelt med globale private organisationer. Dette bør ske gennem eksisterende fora og processer.

- **Opbygning af strategiske internationale partnerskaber**
  Strategiske partnerskaber bør bygge på igangværende bestræbelser på kritiske områder. Involvering af den private sektor, der opererer på et globalt plan, er af afgørende betydning. EU-USA arbejdsgruppen er et vigtigt skridt i denne retning. Yderligere koordinering ville blive videreført i internationale fora, især i G8.

- **Opbygge tillid til "cloud computing"**
  Det er vigtigt at styrke drøftelserne om bedste styringsstrategier for nye teknologier, som har global indvirkning, såsom cloud computing. Tillid er afgørende for at høste det fulde udbytte.

Da sikkerhed er et fælles ansvar for alle, foreslår Kommissionen, at medlemsstaterne bør forpligte sig til:

- **Styrke EU's beredskab ved at etablere et netværk af velfungerende nationale/statslige CERT'er inden 2012**
  EU-institutionerne vil ligeledes etablere deres egen CERT inden 2012.

- **Fastlægge en europæisk beredskabsplan for internet-hændelser inden 2012 samt jævnlige fælleseuropæiske beredskabsøvelser**
  Øvelser er et vigtigt element i en sammenhængende beskyttelsesstrategi både på nationalt og europæisk niveau. ENISA vil samarbejde med medlemsstaterne med henblik på etablering af sammenhængende nationale og europæiske beredskabsplaner i 2012.

- **Tilstræbe en koordineret europæisk indsats i internationale fora og drøftelser om forbedring af internettets sikkerhed og robusthed**
  Medlemsstaterne bør samarbejde med hinanden og med Kommissionen for en fælles holdning til internettets globale stabilitet og robusthed. Målet bør være at styrke forebyggelse og beredskabet på alle niveauer og blandt alle parter, og dermed rette op på den nuværende tendens til at fokusere på militære aspekter og/eller national sikkerhed.

Kommissionens konklusion
Erfaringen viser, at rent nationale eller regionale strategier med hensyn til sikkerhed og robusthed ikke er tilstrækkelige. Det europæiske samarbejde har udviklet sig meget positivt siden 2009. Men Europa bør gå videre i bestræbelserne på at udvikle en sammenhængende og samarbejdsorienteret strategi for hele EU.

Den europæiske indsats er nødt til at blive en del af en globalt koordineret strategi for at blive en succes. Derfor vil Kommissionen fremme udviklingen af en international strategi for internetsikkerhed i alle relevante internationale fora.

3. Europa-Parlamentets udtalelser
Europa-Parlamentet har ikke udtalt sig.

4. Nærhedsprincippet
Da det er en meddelelse, er nærhedsprincippet ikke relevant.

5. Gældende dansk ret
Da meddelelsen ikke er juridisk bindende, får den ikke konsekvenser for dansk ret.

6. Konsekvenser
Meddelelsen har ingen lovgivningsmæssige konsekvenser.

Meddelelsen har ingen statsfinansielle konsekvenser eller administrative konsekvenser.

Meddelelsen skønnes ikke at have væsentlige samfundsøkonomiske konsekvenser, og medfører ingen administrative konsekvenser for erhvervslivet.

7. Høring
Meddelelsen vil blive sendt i høring i EU-specialudvalget for it og telekommunikation.

8. Generelle forventninger til andre landes holdninger
Der har endnu ikke været indholdsmæssige drøftelser blandt medlemsstaterne om meddelelsen.

Da meddelelsen i høj grad er en status over det udførte arbejde siden 2009, og idet Kommissionens fremadrettede strategi ikke indeholder nogen overraskende, nye tiltag, må det forventes, at der bakkes overordnet op om meddelelsen.

9. Regeringens foreløbige generelle holdning

Kommissionens meddelelse vurderes overordnet at være i overensstemmelse med regeringens prioriteringer på området og i overensstemmelse med planlagte eller allerede iværksatte tiltag.

Regeringen stiller sig positivt over for internationalt samarbejde med henblik på beskyttelse af kritisk informationsinfrastruktur, og støtter derfor meddelelsen.

Regeringen har allerede iværksat et samarbejde med andre internationale aktører, der også har igangsat en række initiativer for at dæmme op for ikt-sårbarheder, herunder oprettet en GovCERT og moderniseret teleberedskabet.

10. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt Folketingets Europaudvalg.