# Regeringskansliet
# Faktapromemoria 2010/11:FPM100

# Meddelande om skydd av kritisk informationsinfrastruktur

Näringsdepartementet

2011-05-04

## Dokumentbeteckning

KOM(2011) 163 slutlig
Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén om skydd av kritisk infrastruktur "Resultat och kommande åtgärder: vägen mot global it-säkerhet"

## Sammanfattning

Detta nya meddelande från 2011 beskriver de resultat som uppnåtts sedan handlingsplanen för skydd av kritisk informationsinfrastruktur antogs 2009. Det beskriver vilka åtgärder som nu planeras för varje område, på både europeisk och internationell nivå. Meddelandet inriktar sig också på den globala dimensionen av problemen och vikten av att öka samarbetet mellan medlemsstaterna och den privata sektorn på nationell, europeisk och internationell nivå, med tanke på det ömsesidiga beroendet på global nivå.

Regeringen ser generellt sett positivt på att kommissionen arbetar aktivt med frågorna och välkomnar denna uppföljning av den tidigare satta handlingsplanen. Sverige har dock kring vissa frågor en annan syn än kommissionen om hur arbetet kan och bör bedrivas eller var fokus skall ligga.

## 1 Förslaget

### 1.1 Ärendets bakgrund

Den 30 mars 2009 antog kommissionen ett meddelande om skydd av kritisk informationsinfrastruktur – ”Skydd mot storskaliga IT-attacker och avbrott: förbättrad beredskap, säkerhet och motståndskraft i Europa” som innehåller en plan (handlingsplan för skydd av kritisk informationsinfrastruktur) för att

stärka viktig IKT-infrastrukturs säkerhet och motståndskraft. Syftet var att främja och stödja utvecklingen av en hög nivå vad gäller beredskap, säkerhet och motståndskraft på både nationell och europeisk nivå. Strategin fick brett stöd av rådet 2009.

Handlingsplanen för skydd av kritisk informationsinfrastruktur (nedan kallad handlingsplanen) bygger på följande fem åtgärdsområden: Beredskap och förebyggande åtgärder, upptäckt och insatser, begränsning av verkningar och återställning, internationellt samarbete och kriterier för europeisk kritisk infrastruktur för sektorn för informations- och kommunikationsteknik. I planen beskrivs vad kommissionen, medlemsstaterna och/eller industrin, med stöd av Europeiska byrån för nät- och informationssäkerhet (Enisa), ska göra inom varje område.

Detta nya meddelande från 2011 beskriver de resultat som uppnåtts sedan handlingsplanen för skydd av kritisk informationsinfrastruktur antogs 2009.

## 1.2 Förslagets innehåll

Detta meddelande beskriver de resultat som uppnåtts sedan handlingsplanen för skydd av kritisk informationsinfrastruktur antogs 2009. Det beskriver vilka åtgärder som nu planeras för varje område, på både europeisk och internationell nivå. Meddelandet inriktar sig också på den globala dimensionen av problemen och vikten av att öka samarbetet mellan medlemsstaterna och den privata sektorn på nationell, europeisk och internationell nivå, med tanke på det ömsesidiga beroendet på global nivå.

**Kommissionen anser att:**

- Det är särskilt viktigt att insatserna ingår i en global samordningsstrategi och att de därför förs ut till den internationella arenan, med alla berörda intressenter, och når andra regioner, länder och organisationer som ägnar sig åt liknande frågor. Man bör också bygga upp partnerskap för att ta fram gemensamma strategier och därmed relaterad verksamhet och för att undvika att insatserna överlappar varandra.
- Vi måste främja en global riskhanteringskultur. Tyngdpunkten bör ligga på att främja samordnade åtgärder för att förhindra, upptäcka, mildra och bemöta alla typer av avbrott, oavsett om de är skapade av människor eller naturliga, liksom att lagligen beivra relaterade it-brott. Häri ingår att vidta riktade åtgärder mot säkerhetshot och datorbaserade brott.

**Kommissionen föreslår i detta syfte följande aktiviteter och ståndpunkter:**

- **Främja principerna för ett motståndskraftigt och stabilt Internet.** Det bör utarbetas internationella principer för ett motståndskraftigt och stabilt Internet tillsammans med andra länder, internationella organisationer och i tillämpliga fall med globala organisationer i den privata sektorn. Detta bör ske med hjälp av existerande forum och processer, så som de som avser förvaltning av Internet. Principerna ska fungera som ett verktyg för alla intressenter för att utforma åtgärder för ett motståndskraftigt och stabilt Internet. De internationella principerna skulle kunna grundas på de europeiska principerna och riktlinjerna.
- **Skapa strategiska internationella partnerskap.** De strategiska partnerskapen bör basera sig på pågående insatser på kritiska områden, så som förvaltning av it-incidenter, inbegripet övningar och samarbete mellan organisationer för incidenthantering. Det är av största vikt att den del av den privata sektorn som verkar på global nivå är engagerad. EU och Förenta staternas gemensamma arbetsgrupp för it-säkerhet och it-brottslighet, som inrättades vid toppmötet mellan EU och Förenta staterna i november 2010, är ett viktigt steg i den riktningen. Arbetsgruppen kommer att inrikta sig på förvaltning av it-incidenter, offentlig-privata partnerskap, åtgärder för att öka medvetenheten och it-brottslighet. Den kan också överväga möjligheterna att vidga samarbetet till andra regioner eller länder, i synnerhet genom att diskutera liknande problem i syfte att skapa gemensamma strategier och verksamheter, och se till att insatserna inte överlappar varandra. Man bör också eftersträva ytterligare samarbete och samordning i internationella forum, i synnerhet i G8. På den europeiska sidan är de centrala faktorerna för att lyckas god samordning mellan alla EU-institutioner, berörda byråer (i synnerhet Enisa och Europol) och medlemsstaterna.
- **Skapa förtroende för moln**. Det är nödvändigt att stärka diskussionerna om hur man bäst förvaltar ny teknik med globala effekter, så som datormoln. Diskussionerna bör under alla omständigheter omfatta, men inte begränsas till, lämplig förvaltningsram för skyddet av personuppgifter. Förtroende är av avgörande betydelse för att till fullo kunna ta del av den nya teknikens fördelar.

Kommissionen anser att eftersom säkerhet är ett ansvar som delas av alla måste alla medlemsstater se till att deras nationella åtgärder och insatser kollektivt bidrar till en samordnad europeisk strategi för att förhindra, upptäcka, mildra och bemöta alla typer av it-avbrott och attacker.

**Kommissionen anser därför att medlemsstaterna därför måste åta sig:**

- **Öka EU:s beredskap genom att inrätta ett nät av väl fungerande nationella/statliga organisationer för incidenthantering senast 2012.** EU-institutionerna ska likaledes inrätta en egen organisation för incidenthantering senast 2012. Alla dessa insatser bör grunda sig på den grundläggande kapacitet och de grundläggande tjänster och politiska rekommendationer som Enisa formulerat. Enisa kommer även fortsättningsvis att stödja dessa initiativ. Insatsen kommer också att främja utvecklingen av ett EU-system för informationsutbyte och varningar (Eisas) för allmänheten senast 2013.
- **Införa en EU-omfattande beredskapsplan för it-incidenter senast 2012 och regelbundna EU-omfattande it-övningar.** It-övningar utgör en viktig del i en samordnad strategi för beredskapsplanering och återställning i samband med it-incidenter, både på nationell och europeisk nivå. Framtida EU-omfattande it-övningar bör baseras på en europeisk beredskapsplan för it-incidenter som bygger på och är sammanlänkad med nationella beredskapsplaner. En sådan plan bör ange grundläggande mekanismer och förfaranden för meddelande mellan medlemsstaterna och sist, men inte minst, utgöra ett stöd i samband med fastställandet av framtida EU-omfattande övningars omfattning och organisation. Enisa vill tillsammans med medlemsstaterna senast 2012 utarbeta en sådan europeisk beredskapsplan för it-incidenter. Inom samma tidsperiod bör alla medlemsstater utarbeta nationella beredskapsplaner och regelbundna övningar för insatser och återställning.
- **Verka för samordnade europeiska insatser i internationella forum och diskussioner om ökad säkerhet och motståndskraft för Internet.** Medlemsstaterna bör samarbeta sinsemellan och med kommissionen för att främja utarbetandet av en strategi baserad på principer och normer för frågan om Internets globala stabilitet och motståndskraft. Syftet bör vara att främja beredskap och förebyggande åtgärder på alla nivåer och av alla intressenter, och således uppnå balans i den tendens som finns idag att fokusera diskussionerna på militära och/eller nationella säkerhetsaspekter.

## 1.3 Gällande svenska regler och förslagets effekt på dessa

Såväl direktiv 2008/114/EG som CIIP-meddelandet berör ett stort antal frågor som omfattas av medlemsstaters nationella kompetens samt den privata sektorns kompetens. Ett antal aspekter av meddelandet berör nationell säkerhet.

I Sverige regleras ansvaret för skydd av kritisk informationsinfrastruktur liksom skydd av all annan infrastruktur av ansvarsprincipen. Enligt ansvarsprincipen är alla svenska myndigheter ansvariga för att ha en tillräcklig informationssäkerhet inom sin verksamhet. Det finns med andra ord inte någon enskild myndighet med ansvar för dessa frågor. Vissa svenska myndigheter har ett mer utpekat ansvar för frågor som rör informationssäkerhet. I det formella uppdraget kan det ingå tillsynsansvar, det vill säga utövande av kontroll över en verksamhet, samt föreskriftsrätt på området. De myndigheter med ett särskilt formellt ansvar för informationssäkerhet i Sverige är:

- Datainspektionen
- Försvarsmakten
- Försvarets materielverk
- Försvarets radioanstalt
- Myndigheten för samhällsskydd och beredskap
- Post- och telestyrelsen
- Rikspolisstyrelsen

Förutom dessa finns ytterligare myndigheter vars verksamheter har betydelse för informationssäkerhet.

## 1.4 Budgetära konsekvenser / Konsekvensanalys

Meddelandet innehåller i sig själv inga lagstiftningsförslag men innehåller ett antal uppmaningar som kan få budgetära konsekvenser om medlemsstater efterkommer dem. Någon närmare konsekvensanalys finns inte i meddelandet.

# 2 Ståndpunkter

## 2.1 Preliminär svensk ståndpunkt

Regeringen ser generellt sett positivt på att kommissionen arbetar aktivt med frågorna och välkomnar denna uppföljning av den tidigare satta handlingsplanen. Sverige har dock kring vissa frågor en annan syn än

kommissionen om hur arbetet kan och bör bedrivas eller var fokus skall ligga.

Nedan följer en genomgång av svenska detaljståndpunkter kring CIIP. Handlingslinjen i förhandlingarna kring rådsslutsatser om meddelandet består i att påverka slutsatserna i den riktning som följer av dessa ståndpunkter.

Regeringen anser att det är angeläget med en sammanhållen europeisk inriktning i frågor om skydd av kritisk informationsinfrastruktur (CIIP). EU-samarbetets roll bör enligt regeringen i första hand fokusera på att stödja samordning av medlemsstaters aktiviteter, sprida bästa praxis samt stödja de medlemsstater som ligger efter i utvecklingen.

Regeringen anser att många frågor som rör CIIP omfattas av medlemsstaters nationella kompetens och nationella säkerhetsintressen. Medlemsstaters nationella säkerhet och skyddet av deras informationsinfrastruktur är inte en fråga för EU-nivån som sådan, utan tillhör i första hand medlemsstaternas kompetens.

Regeringen anser att EU:s roll måste ses i ett globalt sammanhang mot bakgrund av Internets gränslöshet samt att många multinationella företag är verksamma både inom och utanför EU:s gränser. Hotet mot den digitala informations- och kommunikationsinfrastrukturen ser inte heller några geografiska gränser och dess aktörer arbetar utifrån varierande bevekelsegrunder och ideal.

Regeringen anser att både medlemsstatsnivån och EU-nivån bör fokusera mer på hur informationssäkerhet kan utvecklas på global nivå. Särskild tonvikt bör läggas vid den gradvisa utvecklingen av internationella regelverk som på ett effektivt sätt förebygger och motverkar IT-attacker.

Så kallad kritisk informationsinfrastruktur återfinns i både offentlig och privat sektor i medlemsstaterna. Regeringen anser att varje form av förteckning och inventering av kritisk infrastruktur innebär risker i sig och kan vara kontraproduktiva i förhållande till syftet att höja säkerheten. Regeringen ifrågasätter nyttan av samt möjligheten att särskilt på övernationell nivå försöka sammanställa det slags känsliga information som omnämns i kommissionens meddelande från 2009.

Regeringen noterar att det inom EU på medlemsstats- och unionsnivå pågår omfattande arbeten med ett antal initiativ som tagits under 2009 och 2010. Mot denna bakgrund betonar regeringen vikten av att det tas hänsyn till dessa, och andra, pågående processer för att undvika onödigt dubbelarbete.

CIIP-handlingsplanen innehåller ett stort antal åtgärder som riktar sig till medlemsstater. Några av dessa åtgärder, t.ex. utvecklingen av nationella och statliga Computer Emergency Response Teams (CERT:ar), skulle enligt regeringen mening vara till stort stöd för mindre utvecklade medlemsstater. Sverige anser att CERT-samarbete måste bygga på personligt förtroende, ömsesidig nytta och respekt för den känsliga grunden för samarbetet. Därför bör detta samarbete inte framtvingas genom order och/eller lagstiftning.

Regeringen anser att övningar är ett viktigt redskap för att utveckla och stärka samhällets förmåga att hantera IT-relaterade störningar. Informationssäkerhet kräver samverkan såväl nationellt som internationellt. Regeringen och andra länder bedriver redan omfattande övningsverksamhet. Regeringen anser det angeläget att den övningsverksamhet som stöds av kommissionens, t.ex. Cyber Europe, är gemensamt samordnad mellan medlemsstater och kommissionens för att maximera nyttan av dem. Genom gemensam samordning och planering av övningar kan dessutom onödigt och kostsamt dubbelarbete undvikas.

Sverige vill ta bort fokus på övervägda och/eller sofistikerade attacker. Det är mer relevant och kostnadseffektivt att fokusera på att finna modeller som beaktar alla incidenter, i synnerhet de med högre sannolikheter, till exempel strömavbrott och störningar på grund av väder-, markgrävningar, uppdatering av programvara, att man skär av kablar, växande teknisk komplexitet (IPv6 migration, molntjänsteanvändning) och så vidare. Aktiviteter för att ta itu med övervägda och/eller sofistikerade attacker skulle bli en naturlig del av denna "allriskmodell".

## 2.2 Medlemsstaternas ståndpunkter

Sannolikt stödjer flertalet medlemsstater kommissionens initiativ på en övergripande nivå. Medlemsstaternas åsikter går dock troligen isär vad gäller de mer specifika frågorna t.ex. om informationsutbyte. Medlemsstaternas förmåga att fullt ut kunna delta i arbetet samt den egna nationella utvecklingen inom informationssäkerhetsområdet ligger sinsemellan på olika nivåer inom EU. Generellt sett kan Sverige räknas till den grupp medlemsstater som har mest utvecklade förmågor på detta område.

Ett flertal generaldirektorat i kommissionen berörs: DG INFSO, DG HOME m.fl. DG INFSO tillsammans med europeiska byrån för nät- och informationssäkerhet (ENISA) är starkt drivande i att identifiera europeisk kritisk informationsinfrastruktur inom IKT-sektorerna inför översynen av direktiv 2008/114/EG om europeisk kritisk infrastruktur som förutses 2012.

## 2.4 Remissinstansernas ståndpunkter

Meddelandet är ej remissbehandlat.

# 3 Förslagets förutsättningar

## 3.1 Rättslig grund och beslutsförfarande

Ej aktuellt då det rör sig om ett meddelande. Det ungerska ordförandeskapet siktar på rådsslutsatser om meddelandet vid TTE-rådet den 27 maj 2011. Dessa antas med enhällighet.

## 3.2 Subsidiaritets- och proportionalitetsprincipen

CIIP-meddelandena berör ett antal frågor som omfattas av medlemsstaternas nationella kompetens samt den privata sektorns kompetens. Ett antal aspekter av meddelandet berör nationell säkerhet. Meddelandet innehåller dock ingen lagstiftning av tvingande natur varför subsidiaritetsprincipen inte är direkt relevant i sammanhanget. Kommissionens åtgärder kan sägas vara proportionella eftersom de endast kan utmynna i rekommendationer till medlemsstaterna om hur vi kan eller bör agera på olika områden. Detta är ett ganska svagt styrmedel om man jämför med viken av att skydda kritisk informationsinfrastruktur.

# 4 Övrigt

## 4.1 Fortsatt behandling av ärendet

Det ungerska ordförandeskapet siktar på rådsslutsatser om meddelandet vid TTE-rådet den 27 maj 2011.

## 4.2 Fackuttryck/termer

EU Europeiska unionen

| | |
|---|---|
| CIIP | Critical Information Infrastructure Protection / Skydd av Kritisk Inforamtionsinfrastruktur |
| TTE | Tele, transport och energi |
| DG HOME | Directorate-General for Home Affairs |
| DG INFSO | Directorate-General Information Society and Media |
| ENISA | Europeiska byrån för nät- och informationssäkerhet |
| IKT | Informations- och kommuikationsteknik |
| CERT | Computer Emergency Response Team |