|  |  |
| --- | --- |
|  |  |
| **Rådspromemoria** |
|  |  |
| 2013-05-23 |  |
|  |  |

|  |
| --- |
| **Försvarsdepartementet** |
|  |
| Enheten för samordning av samhällets krisberedskap (SSK) |
|  |
| Gemensamberett med: SB/EU, Ju/Po, Ju/Å, Ju/L4, JuL5, S/SF, UD/SP, Fi/BA, Fi/FMA, N/ITP, Rep/TKI |
|  |
|  |
|  |
|  |

Rådets möte (Transport, Telekommunikation och energi) den 6 juni 2013

Dagordningspunkt 4

Rubrik: **Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union (First reading)**

Interinstitutional file 2013/0027 (COD)

-    *progress report*

*- orientation debate*

Dokument: KOM(2013) 48 slutlig - Förslag till Europaparlamentets och Rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen och SWD(2013) 32 final - Commission Staff Working Document Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union

Tidigare dokument: Fakta-PM Fö-dep 2012/13:FPM68

Tidigare behandlad vid samråd med EU-nämnden: Nej.

Bakgrund

Kommissionen överlämnade den 7 februari 2013 direktivförslag om åt­gärder för att säkerställa en hög gemensam nivå av nät- och informa­tionssäkerhet i hela unionen (NIS-direktivet). Direktivförslaget presenterades i samband med att kommissionen och Europeiska utrikestjänsten (EEAS) presente­rade en europeisk strategi för cybersäkerhet – En öppen, säker och trygg cyberrymd. Förslaget till NIS-direktiv är en viktig del i den övergripande cybersäkerhetsstrategin.

Den 10 april 2013 skickade Riksdagen ett motiverat yttrande till Euro­paparlamentet, Rådet och kommissionen (2012/13:FöU11) av vilket framgår att Riksdagen instämmer i den bedömning som gjorts i den Fakta PM som tagits fram av Regeringskansliet. Riksdagen anser att åtgärder av det slag som föreslås i förslaget till direktiv om åt­gärder för att säkerställa en hög gemensam nivå av nät- och informations­säkerhet i unionen bör vara varje medlemsstats eget ansvar i enlighet med subsidiaritetsprincipen. Riksdagen har funnit att kom­missionens förslag i KOM(2013) 48 strider mot subsidiaritetsprincipen.

Kommissionens förslag till direktiv presenterades för medlemsstaterna vid möte med arbetsgruppen för telekom den 28 februari och den 11 april hade gruppen ett första möte där MS hade möjlighet att lämna inledande kommentarer till förslaget. Flera MS, däribland SE, har skickat in skriftliga kommentarer och frågor på förslaget och framför allt på den konsekvensutredning som hör till förslaget och däri framfört frågor och kommentarer kring bl.a. subsidiaritets- och proportionalitetsprincipen. Det irländska ordförandeskapet har inför TTE den 6 juni sammanställt en lägesrapport över arbetet och tagit fram frågor till vägledning för den diskussion man avser hålla kring förslaget på rådsmötet.

Rättslig grund och beslutsförfarande

Europeiska unionen har befogenhet att besluta om åtgärder i syfte att upprätta den inre marknaden eller säkerställa dess funktion i enlighet med tillämpliga bestämmelser i fördragen (artikel 26 i fördraget om Europeiska unionens funktionssätt — EUF-fördraget). Enligt artikel

114 i EUF-fördraget kan EU "besluta om åtgärder för tillnärmning av sådana bestämmelser i lagar och andra författningar i medlemsstaterna som syftar till att upprätta den inre marknaden och få den att fungera".

*Svensk ståndpunkt*

Sverige välkomnar förslaget och flera av de föreslagna åtgärderna kan på ett effektivt sätt bidra till ökad säkerhet på europeisk och nationell nivå. Förslagen i direktivet dock är för omfattande, långtgående och opro­portionerligt kostsamma i förhållande till vad som kan förväntas uppnås. En grundläggande inriktning bör vara att genomförandet av förslagen i direktivet görs utifrån de förutsättningar som finns i respektive med­lemsstat och att genomföra åtgärderna bör inte vara tvingande. Däremot anser Regeringen att det är viktigt att höja miniminivån på säkerheten inom EU. Detta kan med fördel göras t.ex. genom koordinering, utbildning och utbyte av goda exempel snarare än tvingande lagstiftning. Som förslaget är formulerat just nu strider det också mot subsidiaritetsprincipen. Det bör tydliggöras att den nationella kompetenta myndigheten (National competent authority) kan bestå av fler aktörer eller myndigheter. Förslaget rörande incidentrapportering bör begränsas när det gäller incidenter med antagonistiskt ursprung och att ansvarsfördelning i förhållande till brottsutredande myndigheter tydliggörs. Även incidenter som rör rikets säkerhet, bl.a. försvarsrelaterade incidenter och kvalificerade brottsliga angrepp, bör undantas från rapporteringsskyldigheten. Det är viktigt att kommissionens förslag och åtgärder inte inverkar på respektive medlemsstats nationella säkerhet och att det fortsatta arbetet också beaktar de förhandlingar som pågår mellan medlemsstater t.ex. förslaget till dataskyddsförordning.

Europaparlamentets inställning

Ej kända

*Förslaget*

Förslaget till direktiv ålägger alla medlemsstater att

1. se till att de har en miniminivå av nationell kapacitet genom att inrätta nationella myndigheter för nät- och informationssäkerhet, inrätta incidenthanteringsorganisationer (Computer Emergency Response Teams (CERT)) och anta nationella strategier för nät- och informationssäkerhet och nationella samarbetsplaner för nät- och informationssäkerhet,
2. de nationella myndigheterna samarbetar inom ett nätverk som tillåter säker och effektiv samordning, inbegripet ett samordnat informationsutbyte samt upptäckt och insatser på EU-nivå, och
3. utifrån ramdirektivet för elektronisk kommunikations modell säkerställa att en riskhanteringskultur utvecklas och att information utbyts mellan privat och offentlig sektor. Företag inom kritiska sektorer och offentliga förvaltningar kommer att åläggas att bedöma de risker som de står inför och vidta ändamålsenliga åtgärder som står i proportion till hoten för att garantera nät- och informationssäkerheten. De kommer att vara skyldiga att underrätta de behöriga myndigheterna om alla incidenter som utgör ett hot mot deras nät- och informationssystem och som på ett allvarligt sätt påverkar kontinuiteten för kritiska tjänster och tillhandahållandet av varor.

*Gällande svenska regler och förslagets effekter på dessa*

Offentlighets- och sekretesslagens (2009:400) regler om sekretess kan komma att behöva justeras mot bakgrund av förslaget att dela viss information till samarbetsnätverket.

Ekonomiska konsekvenser

Förslagen i direktivet är omfattande, långtgående och kan bli opro­portionerligt kostsamma i förhållande till vad som kan förväntas uppnås. Som exempel kan nämnas att för enskilda och myndigheter som ska rapportera incidenter beräknas kostnaden för en incidentrapport till den aktuella myndigheten uppgå till 125 €, vilket kan vara lågt räknat. Utredningskostnaden för en incidentrapport som behöver undersökas närmare beräknas uppgå till 25 000 € per utredning. Kommissionen räknar med att cirka 170 till 340 utredningar kan behöva genomföras per år vilket motsvarar mellan 4,25 och 8,5 miljoner € per år för de myndigheter som ska utreda incidenterna. Vartannat år ska en övning genomföras som beräknas kosta mellan 50 000 och 60 000 € per medlemsstat. Därtill kommer kostnaderna för att upprätta en nationell NIS-strategi och en samarbetsplan.

För samtliga utgiftsökningar på statens budget som följer av ett beslut på EU-nivå finns ett finansieringsansvar. Den ökade utgiften ska finansieras genom en utgiftsminskning på det område till vilket EU-åtgärden kan hänföras.