Regeringskansliet
Faktapromemoria 2012/13:FPM68

NIS-direktivet

Försvarsdepartementet

2013-03-06

Dokumentbeteckning

KOM (2013) 48
Förslag till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen

Sammanfattning

Direktivet ålägger alla medlemsstater att se till att de har en miniminivå av nationell kapacitet genom att inrätta nationella myndigheter för nät- och informationssäkerhet, inrätta incidenthanteringsorganisationer (CERT) och anta nationella strategier för nät- och informationssäkerhet samt nationella samarbetsplaner för nät- och informationssäkerhet.

Behöriga nationella myndigheterna ska samarbeta inom ett nätverk. Genom detta nätverk ska medlemsstaterna utbyta information och samarbeta på grundval av den europeiska planen för samarbete inom detta område för att bekämpa nät- och informationssäkerhetshot och nät- och informationssäkerhetsincidenter.

Företag inom specifika 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 ska 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.

Regeringen anser att flera av de föreslagna åtgärderna på ett effektivt sätt kan bidra till ökad säkerhet på europeisk och nationell nivå. Regeringen anser dock att förslagen i direktivet är för omfattande, långtgående och oproportionerligt kostsamma i förhållande till vad som kan förväntas uppnås. Förslagen rör dessutom flera sektorer och nivåer i samhället. En grundläggande inriktning bör vara att genomförandet av förslagen i direktivet

görs utifrån de förutsättningar som finns i respektive medlemsstat. Att genomföra åtgärderna bör inte vara tvingande.

1 Förslaget

1.1 Ärendets bakgrund

EU-kommissionen inledde 2011 arbetet med att det ska finnas en EU-strategi för internetsäkerhet. Sverige har under 2012 aktivt verkat för att bredda strategin och att den tar sin utgångspunkt i och även ska omfatta mänskliga rättigheter, dvs. mer än nät- och informationssäkerhet i teknisk mening. Strategin som nu presenterats som ”Cybersecurity Strategy of the European Union” har fått ett bredare omfång med mänskliga rättigheter som viktig utgångspunkt. Informationssäkerhet, it-relaterad brottslighet och it-relaterade utrikes- säkerhets- och försvarspolitiskafrågor är substansmässigt viktiga delar av strategin.

En ”Friends of the Presidency Group (FoP) on cyber” har inrättats genom beslut i Coreper. Syftet är att öka medlemsstaternas insyn, föbättra det horisontella arbetet och stärka samordningen såväl internt som externt avseende ”cyberfrågor” i vid mening. Gruppen ska utgöra ett strategiskt verktyg för unionens övergripande politiska mål på området.

Kommissionen överlämnade den 7 februari 2013 direktivförslag om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen. 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 direktiv om nät- och informationssäkerhet är en viktig del i den övergripande cybersäkerhetsstrategin.

1.2 Förslagets innehåll

Huvuddelarna i kommissionens förslag:

För det första ålägger direktivet alla medlemsstater att säkerställa att de har en miniminivå av nationell kapacitet genom att inrätta nationella myndigheter för nät- och informationssäkerhet (NCA, National Competent Authority), inrätta incidenthanteringsorganisationer (CERT, Computer Emergency Response Team) och anta nationella strategier för nät- och informationssäkerhet samt nationella samarbetsplaner för nät- och informationssäkerhet.

För det andra ska de behöriga nationella myndigheterna samarbeta inom ett nätverk som tillåter säker och effektiv samordning, inbegripet ett samordnat informationsutbyte, samt upptäckt av angrepp och insatser på EU-nivå. Genom detta nätverk ska medlemsstaterna utbyta information och samarbeta för att bekämpa nät- och informationssäkerhetshot och nät- och

informationssäkerhetsincidenter på grundval av den europeiska planen för samarbete inom detta område.

För det tredje syftar förslaget till att utifrån ramdirektivets modell för elektronisk kommunikation säkerställa att en riskhanteringskultur utvecklas och att information utbyts mellan privat och offentlig sektor. Företag inom specifika kritiska sektorer och den offentliga förvaltningen dvs. myndigheter, kommuner och landsting 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 företag som avses är marknadsoperatörer dvs. leverantörer av informationssamhällestjänster som möjliggör tillhandahållandet av andra informationssamhällestjänster samt operatörer av kritisk infrastruktur som är nödvändig för upprätthållandet av viktig ekonomisk och samhällelig verksamhet inom områdena energi-, transport-, bank-, börs- samt hälso- och sjukvårdsverksamhet. De kommer att vara skyldiga att underrätta de behöriga myndigheterna i respektive medlemsstat 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.

En överklagandemöjlighet ska införas i frågan om beslut som fattas med anledning av de skyldigheter som framgår av direktivet. Medlemsstaterna är enligt förslaget även skyldiga att införa sanktionsmöjligheter som kan användas vid bristande efterföljnad av de nationella bestämmelser som införts för att genomföra direktivet.

1.3 Gällande svenska regler och förslagets effekt på dessa

Idag finns ingen svensk lagstiftning som reglerar informationsutbyte samt upptäckt av angrepp och insatser på EU-nivå avseende it-incidenter. Detta sker idag på frivillig basis. I säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633) finns bl.a. bestämmelser om informationssäkerhet till skydd för rikets säkerhet. Säkerhetsskyddslagstiftningen är för närvarande under översyn och utredningen ska redovisa sitt resultat i april 2014 (Utredningen om säkerhetsskyddslagen, Ju 2011:14). Det är svårt att i nuläget förutse hur regleringen om säkerhetsskydd kan komma att påverkas av det nu föreslagna direktivet. Även i förordningen (2006:942) om krisberedskap och höjd beredskap regleras informationssäkerhet till viss del. Denna reglering kan komma att beröras av direktivet.

Det är inte möjligt att nu göra en komplett i av vilka bestämmelser som idag finns avseende alla som träffas av den reglering som här föreslås. En sådan inventering förutsätter ett omfattande utredningsarbete, Utgångspunkten är att det ser lite olika ut i respektive sektor och att inga eller få har idag krav på sig att rapportera it-incidenter (det finns krav för teleoperatörer enligt LEK att rapportera incidenter). Det kan även noteras att nya åtaganden för den kommunala sektorn innebär en inskränkning av den kommunala självstyrelsen och kan utlösa den kommunala finansieringsprincipen.

Kravet att utse en myndighet avseende nät- och informationssäkerhet kan, beroende på utformning, komma att påverka gällande svenska regler och organisationen av myndigheter. Även förslaget om att inrätta incidenthanteringsfunktioner kan komma att påverka gällande svenska regler.

Överlag innebär direktivet skyldigheter i fråga om många åtgärder som idag sker på frivillig basis. Det kan inte uteslutas att delar av detta kan behöva regleras för att Sverige ska kunna genomföra direktivet på ett korrekt sätt. Då direktivet innebär skyldigheter för såväl kommuner, landsting som företag och inkluderar sanktioner och överklagandemöjligheter krävs lagstiftning för genomförande av förslaget.

1.4 Budgetära konsekvenser / Konsekvensanalys

Kommissionens redovisning av de budgetära konsekvenserna:

Samarbete och informationsutbyte mellan medlemsstaterna bör stödjas genom en säker infrastruktur. Förslaget kommer endast att påverka EU:s budget om medlemsstaterna väljer att gemensamt anpassa en befintlig infrastruktur (t.ex. STESTA (Secure Trans European Services for Telematics between Administrations)) och ge kommissionen i uppdrag att genomföra detta i enlighet med den fleråriga budgetramen 2014–2020. Engångskostnaden uppskattas till 1 250 000 euro, som skulle belasta EU-budgeten, budgetpost 09.03.02 (Samtrafikförmåga och interoperabilitet mellan nationella offentliga onlinetjänster samt tillgång till sådana nät — kapitel 09.03, Fonden för ett sammanlänkat Europa — telenät) under förutsättning att tillräckliga medel finns tillgängliga inom fonden för ett sammanlänkat Europa. Alternativt kan medlemsstaterna antingen dela på engångskostnaden för att anpassa en befintlig infrastruktur eller besluta att inrätta en ny infrastruktur och ta kostnaderna, som uppskattas uppgå till omkring 10 miljoner euro per år.

Regeringens preliminära bedömning är att förslaget kan komma att orsaka betydande extra kostnader, även utöver de som redovisas av EU-kommissionen, jfr ovan, om det skulle genomföras i sin helhet. En preliminär bedömning pekar på kostnader främst för:

- Artikel 9 rörande infrastrukturen för informationsutbyte. Om den infrastruktur som föreslås ska kunna hantera information med klassningen ”confidential” kan ej existerande infrastruktur som SGSI (Swedish Government Secure Intranet) och STESTA användas utan en helt ny infrastruktur behöver byggas med högre säkerhet och därmed högre kostnader.
- Artikel 14 och 15 berör krav på säkerhet, incidentrapportering och tillsyn av public administrations och market operators. Ökande krav på säkerhet samt utökad incidentrapportering

kommer att innebära en kostnadsökning för berörda parter, inklusive NCA och sektorsmyndigheter.

Regeringen anser att de åtgärder som föreslås i direktivet inte ska medföra några extra kostnader.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen anser att flera av de föreslagna åtgärderna på ett effektivt sätt kan bidra till ökad säkerhet på europeisk och nationell nivå. Regeringen anser dock att förslagen i direktivet är för omfattande, långtgående och oproportionerligt kostsamma i förhållande till vad som kan förväntas uppnås. Förslagen rör dessutom flera sektorer och nivåer i samhället.

Den största utmaningen är dock att tydliggöra vad respektive medlemsstat ska göra i relation till EU och andra medlemsstater. De flesta av direktivets förslag bör kunna genomföras i Sverige utan att förändra nuvarande struktur där dessa frågor hanteras, dvs. myndigheternas oberoende ställning och krishanteringssystemets utgångspunkter formulerade i ansvars- närhets- och likhetsprincipen. Inom offentlig sektor finns de flesta av de mekanismer som efterfrågas i direktivförslaget redan på plats, bl.a. kravet på att statliga myndigheter ska arbeta i enlighet med en ISO-standard (Ledningssystem för informationssäkerhet) för sitt informationssäkerhetsarbete. Om de föreslagna åtgärderna blir obligatoriska för medlemsstaterna utgör de en inskränkning av den kommunala självstyrelsen och kan utlösa den kommunala finansieringsprincipen. Det kvarstår dock en hel del arbete inom kommuner, landsting och den privata sektorn.

Att genomföra åtgärderna bör inte vara tvingande. En grundläggande inriktning bör vara att medlemsstater arbetar utifrån sina respektive förutsättningar på området. Direktivet anger dessutom att åtgärderna ska vara genomförda inom 1-1½ år från att beslut om direktivet fattats vilket är en orimlig kort tidsfrist. Den är inte möjlig att hålla.

I förslaget till direktiv påtalas också att många incidenter utgör brottsliga handlingar. Utredning av sådana brottsliga incidenter kräver ofta tillgång till information om elektronisk kommunikation, s.k. ”trafikdata” från operatörer och/eller de som tillhandahåller elektroniska kommunikationstjänster samt abonnemangsuppgifter. Det är oklart i förslaget hur denna typ av incidenter ska hanteras och hur det relaterar till brottsutredning och Cybercrime-konventionen samt EU:s direktiv om lagring av information om elektronisk kommunikation (”Trafikdatadirektivet”, där det bl.a. finns krav på skydd av uppgifter). Offentliggörande av sårbarheter kan även leda till ytterligare skada.

Regeringen anser att begränsningar i rapporteringsskyldigheten när det gäller incidenter med antagonistiskt ursprung och ansvarsfördelning i förhållande

till brottsutredande myndigheter måste tydliggöras. Incidenter som rör rikets säkerhet, bl.a. försvarsrelaterade incidenter måste generellt undantas från rapporteringsskyldigheten. Nu finns inget sådant undantag inskrivet i direktivet. De möjligheter som direktivet innebär för medlemsstaterna är att inte lämna viss information är mycket vaga och otillräckliga. Dessutom föreslås kommissionen få långtgående delegerade befogenheter.

Både övningar och faktiska incidenter på europeisk nivå har tydligt visat att incidenthantering inte bedrivs på det sätt som kommissionen anger. Dessutom visar erfarenheter att det land som drabbas allvarligast vid en it-incident i de flesta fall måste rikta all fokus och samtliga resurser mot att hantera incidenten. Den koordinerande rollen gentemot andra medlemsstater respektive andra länder tas ofta av en medlemsstat som också drabbats men inte i lika stor omfattning. Etablerade samverkanskanaler mellan olika länders CERT-organisationer och motsvarande används. Att som i direktivet föreslå att samtliga deltagande NCA, oavsett om de har drabbats eller inte, tillsammans ska komma överens om en koordinerad åtgärd ligger långt ifrån hur den här typen av incidenter kan och bör hanteras. Dessutom är tidsaspekten av mycket stor betydelse vid incidenthantering något som inte berörs i direktivet.

Sverige ställer sig positiv till de åtgärder som stärker den personliga integriteten.

2.2 Medlemsstaternas ståndpunkter

Inga välutvecklade ståndpunkter är kända. Underhandskontakter ger dock vid handen att det åtminstone finns en handfull länder med liknande ståndpunkter som regeringens.

2.3 Institutionernas ståndpunkter

Institutionernas ståndpunkter är inte kända.

2.4 Remissinstansernas ståndpunkter

Förslaget har inte varit föremål för remiss.

3 Förslagets förutsättningar

3.1 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".

EU-lagstiftarna har redan konstaterat att det är nödvändigt att harmonisera nät- och informationssäkerhetsbestämmelserna för att säkerställa den inre marknadens utveckling. Ett exempel är förordning 460/2004/EG om inrättandet av Enisa (Europeiska Nät- och informationssäkerhets myndighet), som grundas på artikel 114 i EUF-fördraget.

De skillnader som beror på medlemsstaternas olika nationell kapacitet, politik och skyddsnivå när det gäller nät- och informationssäkerhet skapar hinder på den inre marknaden och gör det motiverat att vidta EU-åtgärder.

3.2 Subsidiaritets- och proportionalitetsprincipen

Subsidiaritet

Subsidiaritetsprincipen regleras i artikel 5 i fördraget om Europeiska unionen. Enligt denna ska unionen, på de områden där den inte har exklusiv befogenhet, vidta en åtgärd endast om och i den mån som målen för den planerade åtgärden inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och därför, på grund av den planerade åtgärdens omfattning eller verkningar, bättre kan uppnås på unionsnivå.

Enligt Lissabonfördraget ska alla nationella parlament få del av utkasten till lagstiftningsakter för att bedöma initiativens förenlighet med subsidiaritetsprincipen. I enlighet med 10 kap. 6 § riksdagsordningen ska riksdagen pröva om lagstiftningsakten strider mot subsidiaritetsprincipen.

EU-kommissionen menar att europeiska åtgärder inom nät- och informationssäkerheten kan motiveras enligt subsidiaritetsprincipen enligt följande.

Kommissionen anser att frånvaro av åtgärder på EU-nivå, på grund av nät- och informationssäkerhetens gränsöverskridande natur, skulle leda till en situation där varje medlemsstat agerar på egen hand och inte tar hänsyn till att näten och informationssystemen i EU är helt beroende av varandra. En lämplig nivå av samordning mellan medlemsstaterna skulle säkerställa att nät- och informationssäkerhetsriskerna hanteras på rätt sätt i det gränsöverskridande sammanhang där de uppstår. Olika lagstiftning om nät- och informationssäkerhet utgör ett hinder för företag som vill bedriva verksamhet i flera länder och står i vägen för globala stordriftsfördelar. Kommissionen anser vidare att skyldigheterna på EU-nivå krävs också för att säkra samma konkurrensvillkor.

Regeringen anser att det som ovan anförs kan utgöra skäl för reglering men det finns inget som motiverar varför detta måste genomföras på EU-nivå. Det finns gott om exempel på företag inom berörda sektorer som är verksamma i flera EU-länder trots skillnader i lagstiftning etc.

Kommissionen anser att ett tillvägagångssätt baserat på frivillighet hittills endast har mynnat ut i samarbete inom den minoritet av medlemsstaterna som har en hög skyddskapacitet. För att man ska kunna involvera samtliga medlemsstater måste det säkerställas att alla har en kapacitet som uppnår den nödvändiga miniminivån.

Regeringen menar att ovanstående uttalande har låg relevans för huruvida lagstiftningsåtgärder måste ske på EU-nivå. Det är inte låg kapacitetsnivå som är huvudorsaken till bristande informationsutbyte mellan medlemsstaterna. Det är snarare en fråga om förtroende baserat på andra parametrar som är en nyckelfaktor vilket inte bör lagstiftas om. Däremot anser Regeringen att det är viktigt att höja miniminivån på säkerheten inom EU. Detta kan med fördel göras genom koordinering, utbildning och utbyte av goda exempel snarare än tvingande lagstiftning.

Kommissionen menar att de nät- och informationssäkerhetsåtgärder som vidtas av regeringar måste vara enhetliga och samordnas för att begränsa och minimera konsekvenserna av nät- och informationssäkerhetsincidenter. Inom nätverket kommer de behöriga myndigheterna och kommissionen att samarbeta, genom ett utbyte av bästa praxis och med kontinuerligt deltagande av Enisa, för att främja ett enhetligt genomförande av direktivet i hela EU.

Regeringen menar att ovanstående har låg relevans för huruvida lagstiftningsåtgärder måste ske på EU-nivå. Även här är förtroende en av grundförutsättningarna för samarbete och informationsdelning.

Kommissionen anser att åtgärder på EU-nivå skulle öka effektiviteten i befintliga nationella strategier och underlätta utvecklingen av sådana.

Regeringen anser att det är tveksamt på vilket sätt arbetet med nationella strategier skulle bli effektivare genom lagstiftandeåtgärder på EU-nivå. Dessutom kräver effektiva nät- och informationssäkerhetsåtgärder ofta ett snabbt lokalt agerande snarare än ett EU-centraliserat samordnat agerande.

Regeringens sammanfattande bedömning är att målet med en hög gemensam nivå av nät- och informationssäkerhet i hela unionen inte uppnås med hjälp av tvingande lagstiftning på EU-nivå. Att stärka unionens gemensamma nät- och informationssäkerhet kan snarare uppnås genom icke tvingande åtgärder, samverkan mellan medlemsstaterna och ett aktivt nationellt arbete. . Sådana åtgärder som beskrivs i det nu aktuella förslaget bör vara varje medlemsstats ansvar i enlighet med subsidiaritetsprincipen.

Proportionalitet

Kommissionen anser att de föreslagna åtgärderna är motiverade utifrån proportionalitetsprincipen. De krav som fastställs för medlemsstaterna ligger enligt kommissionen på den miniminivå som krävs för att uppnå adekvat beredskap och möjliggöra ett förtroendefullt samarbete.

Regeringen anser att det redan finns ett förtroendefullt samarbete mellan många medlemsstater. Denna typ av samarbete kräver ett långtgående förtroende, något som inte kan uppnås genom lagstiftning. Enisa genomför dessutom redan idag kunskapshöjande och förtrodeskapande åtgärder för att höja miniminivån avseende nät- och informationssäkerhet inom EU.

Kommissionen menar att kraven på riskhantering gäller endast för kritiska enheter och omfattar åtgärder som står i proportion till riskerna och att rapporteringskraven endast skulle omfatta incidenter med betydande konsekvenser för den egna verksamheten.

Regeringen anser att ”kritisk enheter” definieras väldigt brett i förslaget. De säkerhetsåtgärder och den incidentrapportering som föreslås står inte i proportion till de risker som finns. Det är operatören av den ”kritiska enheten” som har ansvar för sina system och utifrån det kan bedöma risker och kostnader som är relevanta. Det måste som regeringen tidigare konstaterat som en grundförutsättning, alldeles oavsett, finnas ett generellt undantag för frågor som för rikets säkerhet, såsom försvarsrelaterade frågor från rapporteringsskyldigheten.

Kommissionen menar att åtgärderna inte skulle medföra några oproportionerligt stora kostnader, eftersom många av dessa enheter är registeransvariga som redan i enlighet med nuvarande dataskyddsbestämmelser måste se till att personuppgifter skyddas.

Regeringen anser att detta har låg relevans. Kostnaderna ligger inte endast i frågor som rör personuppgiftshanteringen.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Förslaget kommer att hanteras i rådsarbetsgrupen för telekommunikation och informationssamhällets tjänster (H05). I EP kommer frågan behandlas av utskottet för inre marknaden och konsument skydd (IMCO).

4.2 Fackuttryck/termer

CERT: Computer Emergency Response Team

NCA: National Competent Authority

TESTA: secure Trans European Services for Telematics between Administrations

SGSI: Swedish Government Secure Intranet