Regeringskansliet
Faktapromemoria 2020/21:FPM71

Direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen

2020/21:FPM71

Justitiedepartementet

2021-01-20

Dokumentbeteckning

COM (2020) 823
Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen

Sammanfattning

Den 6 juli 2016 antogs direktivet om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet). Den 16 december 2020 presenterade kommissionen det nu aktuella förslaget som ska ersätta NIS-direktivet. Förslaget utgör en del i ett paket av åtgärder som syftar till att ytterligare förbättra resiliensen både i den digitala och fysiska infrastrukturen hos den offentliga och privata sektorn, behöriga myndigheter och unionen i dess helhet. Det aktuella förslaget utökar bl.a. tillämpningsområdet till fler sektorer.

Målet är att öka cyberresiliensen hos både privata och offentliga aktörer verksamma inom relevanta sektorer inom EU, minska fragmenteringen på den inre marknaden i sektorer som redan omfattas av NIS-direktivet samt förbättra den gemensamma medvetenheten och förmågan kopplat till cyberresiliensen. Kommissionen vill minska fragmenteringen och öka harmoniseringen genom effektivare samarbete mellan behöriga myndigheter från respektive medlemsstat, genom utvidgning av sektorer som ska omfattas samt genom sanktioner som kan användas för effektiv verkställighet.

Regeringen välkomnar översynen av NIS-direktivet i syfte att ytterligare förstärka resiliensen inom cyberområdet, både på nationell och på EU-nivå. Regeringen noterar dock att förslagen i direktivet är omfattande och långtgående och berör många olika sektorer i samhället varför förslaget

måste analyseras mer i detalj. Regeringen anser vidare att det är viktigt att medlemsstaternas ansvar för att skydda nationell säkerhet säkerställs.

1 Förslaget

1.1 Ärendets bakgrund

Europaparlamentet och Europeiska rådet antog den 6 juli 2016 Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet). I Sverige har direktivet genomförts genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174) som trädde i kraft den 1 augusti 2018. NIS-direktivet var den första EU-omfattande rättsakten om cybersäkerhet.

I enlighet med artikel 23 i NIS-direktivet ska kommissionen regelbundet se över hur direktivet fungerar och rapportera till Europaparlamentet och rådet. Som en del i denna process inleddes en konsultation under juli 2020 i syfte att utvärdera NIS-direktivet. Den 16 december 2020 presenterade kommissionen det nu aktuella förslaget till nytt direktiv som ska ersätta NIS-direktivet (EU 2016/1148).

Förslaget utgör en del i ett paket av åtgärder som syftar till att ytterligare förbättra resiliensen både i den digitala och fysiska infrastrukturen hos den offentliga och privata sektorn, behöriga myndigheter och unionen i dess helhet. I paketet ingår även en ny cybersäkerhetsstrategi, EU:s strategi för cybersäkerhet för ett digitalt decennium (The EU’s Cybersecurity Strategy for the Digital Decade) och Förslag till Europaparlamentets och rådets direktiv om resiliens inom kritiska enheter (KOM (2020) 829). Detta är i linje med kommissionens prioriteringar att skapa ett Europa rustat för den digitala tidsåldern (Europe fit for the digital age) som ska se till att den digitala omställningen fungerar för både enskilda och företag.

1.2 Förslagets innehåll

Syftet med det nya förslaget är att uppdatera den befintliga rättsliga ramen för vilka åtgärder som kan vidtas för att motverka det ökade cybersäkerhetshotet.

Målet är att öka cyberresiliensen hos både privata och offentliga aktörer verksamma inom relevanta sektorer inom EU, minska fragmenteringen på den inre marknaden i sektorer som redan omfattas av NIS-direktivet samt förbättra den gemensamma medvetenheten och förmågan. Utvärderingen av NIS-direktivet har påvisat att cyberresiliensen hos företagen är låg, att medlemsstaternas och sektorernas resiliens är inkonsekvent samt att det finns

en avsaknad av gemensam krishantering. Kommissionen vill minska fragmenteringen och öka harmoniseringen bl.a. genom effektivare samarbete mellan behöriga myndigheter från respektive medlemsstat, genom utvidgning av sektorer som ska omfattas av cybersäkerhetskrav samt genom sanktioner som kan användas för effektiv verkställighet.

Det aktuella förslaget utökar tillämpningsområdet till fler sektorer, utifrån deras betydelse för den ekonomiska och samhälleliga verksamheten samt utifrån deras storlek. Samtliga stora och medelstora verksamheter som verkar eller tillhandahåller tjänster inom relevanta sektorer omfattas av direktivet medan små företag och mikroföretag undantas. Förslaget lämnar dock utrymme för medlemsstater att inkludera även mindre verksamheter om de bedöms ha en nyckelroll inom relevanta sektorer.

I det aktuella förslaget delas de aktörer som omfattas upp i särskilt samhällsviktiga (essential) och samhällsviktiga (important) enheter. De enheter som klassas som särskilt samhällsviktiga verkar inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälsa- och sjukvård, digital infrastruktur, dricksvatten, avloppsvatten, offentlig förvaltning och rymd medan samhällsviktiga enheter återfinns inom sektorerna post- och kurirtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion och distribution av mat, tillverkning och leverantörer av digitala tjänster. De olika typerna av enheter omfattas av samma riskhanterings- och incidentrapporteringskrav men det finns inte samma krav på tillsyn när det gäller samhällsviktiga enheter som när det gäller särskilt samhällsviktiga enheter.

Förslaget skärper vidare säkerhetskraven genom att tillhandahålla en lista med minimikrav för åtgärder som ska tillämpas för att särskilt samhällsviktiga och samhällsviktiga enheter ska kunna hantera riskerna kopplat till säkerheten i respektive enhets nätverks- och informationssystem. Listan omfattar bl.a. incident- och krishantering, utvärdering av riskhanteringsåtgärder för cybersäkerheten och användning av kryptering. Vidare ska säkerheten i leveranskedjan för särskilt samhällsviktiga och samhällsviktiga enheter hanteras och stärkas.

Kommissionen vill införa strängare tillsynsåtgärder för behöriga myndigheter och strängare tillämpningskrav för att harmonisera sanktionssystemen i medlemsstaterna. Vidare föreslås krav på att införa administrativa sanktionsavgifter vid överträdelser av direktivet och att dessa ska kunna uppgå till vissa angivna maximibelopp.

Samarbetet mellan medlemsstater förstärks ytterligare i detta förslag genom inrättandet av olika forum för både strategiskt och operativt informationsutbyte. I syfte att stödja samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på EU-nivå ska ett europeiskt nätverk, EU Cyber Crisis Liaison Organisation Network (EU-CyCLONe) inrättas. Kommissionen vill därtill införa ett system för inbördes utvärderingar (peer-reviews) i syfte att utvärdera medlemsstaternas effektivitet kopplat till

verkställigheten och genomförandet av cybersäkerhetskraven och rapporteringskraven för relevanta sektorer i direktivet. Utvärderingarna ska genomföras av tekniska experter från medlemsstaterna, som ska utses av Enisa och kommissionen.

I förslaget fastställs vidare en struktur för vidarehantering av sårbarheter i nätverks- och informationssystemen hos särskilt samhällsviktiga och samhällsviktiga enheter.

Medlemsstaterna ska därtill säkerställa att samtliga enheter meddelar nationella behöriga myndigheter eller CSIRT (Computer Security Incident Response Team) om eventuella cybersäkerhetsincidenter med betydande inverkan på den tjänst de tillhandhåller. Genom förslaget införs mer precisa rapporteringskrav samt att rapporteringen till behöriga myndigheter ska ske inom vissa bestämda tidsramar. I direktivet föreslås en tvåstegsrapportering för att hitta en balans mellan å ena sidan rapportering för att förhindra vidarespridning av en pågående incident, å andra sidan rapportering i ett senare skede för att dra lärdomar och förstärka resiliensen utifrån enskilda händelser. En pågående incident ska rapporteras inom 24 timmar och kompletteras med en slutlig rapport inom en månad. Vidare ska medlemsstaterna säkerställa samarbete och utbyte av information mellan vissa nationella behöriga myndigheter.

1.3 Gällande svenska regler och förslagets effekt på dessa

Förslaget, i dess nuvarande utformning, kommer att påverka svensk lagstiftning. Det gäller framförallt lagen om informationssäkerhet för samhällsviktiga och digitala tjänster men även andra regelverk, exempelvis säkerhetsskyddslagstiftningen och lagen (2003:389) om elektronisk kommunikation. Det är dock svårt att i nuläget förutse hur det föreslagna direktivet kommer att påverka svenska regler.

1.4 Budgetära konsekvenser / Konsekvensanalys

Av kommissionens analys framgår bl.a. att förslaget förväntas ge betydande fördelar då ökad cyberresiliens kan komma att bidra till stora besparingar för både företag och samhälle. Ett genomförande av direktivet kan dock också komma att innebära ökade kostnader för både företag och medlemsstater.

De budgetära konsekvenserna utifrån detta förslag har ännu inte hunnit analyseras.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Nätverk och informationssystem spelar en allt viktigare roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och den inre marknadens funktion. Regeringen välkomnar översynen av NIS-direktivet i syfte att ytterligare förstärka resiliensen inom cyberområdet, både på nationell och på EU-nivå.

Regeringen noterar dock att förslagen i direktivet är omfattande och långtgående och berör många olika sektorer i samhället. Vad gäller de konkreta förslagen som anges, som exempelvis den omfattande utökningen av sektorer och indelningen i särskilt samhällsviktiga och samhällsviktiga enheter, ett system för inbördes utvärdering, mer stringenta tillsynsåtgärder, införandet av höga sanktionsavgifter och skärpta säkerhetskrav, måste dessa analyseras mer i detalj. Förslagen behöver bevakas och närmare analyseras inför de kommande förhandlingarna. I det aktuella förslaget tas det vidare alltför lite hänsyn till de olika förutsättningarna som finns i medlemsstater och organisationer i form av bl.a. affärs- och säkerhetsstrukturer och reglering. Regeringen anser att målsättningar kring cybersäkerhet bör vara högt ställda samt att en grundläggande inriktning bör vara att medlemsstaterna ska arbeta utifrån sina förutsättningar och ha möjligheter till inflytande.

Regeringen kommer i förhandlingarna verka för att harmonisering på området är ändamålsenlig och att direktivet beaktar nationella regelverk och nationella förutsättningar i form av bl.a. affärs- och säkerhetsstrukturer.

Regeringen anser vidare att det är viktigt att medlemsstaternas ansvar för att skydda nationell säkerhet säkerställs. Direktivet ska inte hindra att medlemsstaterna vidtar de åtgärder som de anser nödvändiga för att skydda den nationella säkerheten.

Det är också av vikt att kommissionen beaktar förslag, strategier och initiativ i syfte att skapa synergier och undvika dubbelarbete och överlappning. Det är av stor betydelse att det tydliggörs hur de olika nätverken som föreslås inom ramen för paketet, som detta förslag är en del av, ska förhålla sig till varandra och till Enisas arbete på området.

Enligt förslaget ska åtgärderna vara genomförda i nationell lagstiftning inom 18 månader från det att beslut om direktivet har fattats. Detta är för kort tid

för att genomföra ett så omfattande direktiv. Ytterligare tid kommer att behövas.

Det är viktigt att Sverige verkar konstruktivt för att medel används så effektivt som möjligt på de utgifter som ingår i uppgörelsen om EU:s långtidsbudget 2021–2027. Tillkommande uppgifter ska som huvudregel finansieras genom omprioritering av medel inom området eller från andra områden. Riksdagen har vid Sveriges EU-inträde beslutat om principer om neutralitet för statens budget vilket innebär att när ett beslut på EU-nivå föranleder en ökning av den svenska EU-avgiften ska ökningen finansieras genom en utgiftsminskning på det utgiftsområde till vilket EU-åtgärden kan hänföras.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter är ännu inte kända.

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

Som rättslig grund har kommissionen angett artikel 114 i Fördraget om europeiska unionens funktionssätt (EUF).

Beslut fattas enligt ordinarie lagstiftningsförfarande, dvs. Europaparlamentet och rådet fattar beslut gemensamt.

3.2 Subsidiaritets- och proportionalitetsprincipen

Enligt kommissionen blir de gränsöverskridande utmaningarna och riskerna allt fler. Cyberresiliensen kan inte uppnås på ett effektivt sätt inom unionen genom att enskilda medlemsstater agerar på egen hand, varför subsidiaritetsprincipen är tillämplig. Enligt kommissionen finns det möjlighet att på EU-nivå förbättra och underlätta för effektivare och bättre samordnad politik för att uppnå ökad harmonisering.

Regeringen delar i huvudsak denna bedömning.

Enligt kommissionen är förslaget förenligt med proportionalitetsprincipen då det inte går utöver vad som är nödvändigt för att uppnå målen för ett cybersäkert EU. Förslaget utgår från redan existerande praxis och kommissionen menar att samordnade krav för att uppnå ökad skyddsnivå står i proportion till de ökade riskerna. Vidare menar kommissionen att kostnaderna för att säkerställa det systematiska säkerhetsarbetet mellan medlemsstaterna är liten i jämförelse med de ekonomiska- och samhällsförluster som en cybersäkerhetsincident skulle kunna leda till.

Regeringen anser att förslaget är långtgående och att genomförandet av förslaget skulle innebära ökade kostnader för såväl medlemsstater som för unionen. Det är centralt att förslaget står i proportion till behovet och att det medför ett tydligt mervärde.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Förslaget kommer troligen börja förhandlas i rådet under våren 2021. Någon närmare tidsplan har ännu inte presenterats.

4.2 Fackuttryck/termer

Resiliens: förmågan att förhindra, motstå och återhämta sig från en störning eller ett avbrott i verksamheten.

Incident: en händelse som innebär en oönskad och oplanerad störning eller ett avbrott i verksamhet som kan påverka säkerheten och enhetens förmåga att bedriva sin verksamhet.

Infrastruktur: en tillgång, ett system eller en del därav, som är nödvändigt för att leverera en samhällsviktig tjänst.

Samhällsviktig enhet: nödvändig enhet för att upprätthålla livsviktiga och nödvändiga samhälleliga funktioner eller ekonomiska verksamheter.

Risk: potentiell förlust eller störning orsakad av en cybersäkerhetsincident.

Riskhanteringsåtgärder: åtgärder för att identifiera eventuella risker för incidenter i syfte att förhindra, upptäcka och hantera incidenter och mildra deras påverkan. Säkerheten för nätverks- och informationssystem bör omfatta säkerheten för lagrad, överförd och bearbetad data.

Riskbedömning: en metod för att bestämma riskens art och omfattning genom att analysera potentiella hot och risker och utvärdera befintliga sårbarheter som kan störa eller orsaka avbrott i den kritiska enhetens verksamhet.