Regeringskansliet
Faktapromemoria 2015/16:FPM118

Meddelande om stärkt motståndskraft i nätverk och informationssystem (cyberresiliens)

2015/16:FPM118

Justitiedepartementet

2015-08-19

KOM(2016)410

Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén: Stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch

Sammanfattning

Meddelandet innehåller en presentation av ett antal initiativ och förslag till åtgärder som syftar till att stärka Europas system för cyberresiliens (IT-system, kritisk infrastruktur m.m. ska vara motståndskraftiga och kunna fortsätta leverera önskade tjänster vad som än händer) och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch i Europa.

Initiativen och förslagen presenteras inom ramen för tre huvudområden:

1) ett intensifierat samarbete för att stärka beredskapen och hantera cyberincidenter
2) utmaningar på Europas inre marknad för cybersäkerhet och
3) främjande av industriell kapacitet på cybersäkerhetsområdet

Kommissionens initiativ och förslag har i nuläget ingen påverkan på svensk reglering och meddelandet innehåller inte några konkreta förslag till nya rättsakter. Regeringen ställer sig generellt positiv till fortsatta satsningar på området inom ramen för EU. Regeringen vill dock framhålla vikten av att de åtgärder som meddelandet innehåller inte avleder resurser från det pågående arbetet med NIS-direktivet.

1 Förslaget

1.1 Ärendets bakgrund

Kommissionens meddelande är framtaget på eget initiativ av kommissionen. Meddelandet tar avstamp i olika åtgärder på policyområdet som redan genomförs eller håller på att genomföras inom cybersäkerhetsområdet. Dessa åtgärder är t.ex. beslutet om EU:s Cybersäkerhetsstrategi och EU-direktivet för en hög gemensam nivå av säkerhet i nätverk och informationssystem (NIS-direktivet, se faktapromemoria 2012/13:FPM68). Det är även åtgärder om samt inrättandet av specialiserade organ som står till EU:s förfogande, bl.a. Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), Europeiska it-brottscentrumet vid Europol och organisationen för incidenthantering.

Trots dessa framsteg har EU, enligt kommissionens meddelande, fortfarande otillräckligt skydd mot cyberincidenter, vilket kan undergräva den digitala inre marknaden, det ekonomiska livet och samhällslivet i stort. Mot denna bakgrund undersöker kommissionen hur den föränderliga cybersäkerhetssituationen kan mötas och analyserar vilka ytterligare åtgärder som kan behövas för att öka EU:s cyberresiliens, förmåga att hantera incidenter samt främja en konkurrenskraftig och innovativ cybersäkerhetsbransch i Europa. Kommissionens meddelande kopplar arbetet till EU:s Cybersäkerhetsstrategi och strategin för den digitala inre marknaden (se faktapromemoria 2014/15:FPM35). Meddelandet presenterades den 5 juli 2016.

1.2 Förslagets innehåll

Meddelandet innehåller en presentation av ett antal initiativ och förslag till åtgärder som syftar till att stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch i Europa.

Initiativen och förslagen presenteras inom ramen för tre huvudområden:

1) ett intensifierat samarbete för att stärka beredskapen och hantera cyberincidenter
2) utmaningar på Europas inre marknad för cybersäkerhet och
3) främjande av industriell kapacitet på cybersäkerhetsområdet

1.2.1 Ett intensifierat samarbete för att stärka beredskapen att hantera cyberincidenter

Initiativen och förslagen om ett intensifierat samarbete för att stärka beredskapen och hantera cyberincidenter syftar till att stärka existerande och överenskomna samarbetsmekanismer för att öka EU:s resiliens och beredskap, även gentemot eventuella cybersäkerhetskriser som kan påverka flera medlemsstater samtidigt. Genom NIS-direktivet inrättas ett CSIRT-nätverk för att främja ett effektivt operativt samarbete om specifika

cybersäkerhetsincidenter och ett ökat informationsutbyte om risker. Genom direktivet kommer också en samarbetsgrupp att inrättas för att underlätta det strategiska samarbetet och öka förtroendet mellan medlemsstaterna. Med tanke på cyberhotens art och mångfald uppmuntrar kommissionen medlemsstaterna att utnyttja direktivets samarbetsmekanismer maximalt och öka det gränsöverskridande samarbetet kring beredskap inför storskaliga cyberincidenter. Ett sådant samarbete skulle enligt kommissionen gagnas av en samordnad strategi för hur den typen av storskaliga cyberincidenter kan hanteras, och en sådan strategi skulle kunna vara i form av en konkret plan. Under första halvåret 2017 kommer kommissionen därför att lägga fram en sådan samarbetsplan så att samarbetsgruppen, CSIRT-nätverket och andra berörda intressenter kan ta ställning till den.

Inom samma huvudområde presenterar kommissionen även andra initiativ och förslag för ett ökat samarbete. För att stödja samarbetsmekanismerna inom ramen för NIS-direktivet bör man, enligt Kommissionen, samla informationen i ett ”informationsnav” som gör den lättillgänglig på begäran för samtliga medlemsstater. Informationsnavet skulle vara en central resurs så att EU-institutionerna och medlemsstaterna kan utbyta information på lämpligt sätt. Vidare anser Kommissionen att en reguljär rådgivande högnivågrupp för cybersäkerhet bör inrättas på EU-nivå och bestå av experter och beslutsfattare från näringslivet, den akademiska världen, civilsamhället och andra berörda organisationer. Gruppen kan ge kommissionen tillgång till extern expertis och synpunkter.

Kommissionen hänvisar även till att den kommer att slutföra utvärderingen av Enisa före utgången av 2017. I samband med utvärderingen ska man ta ställning till om Enisas mandat behöver ändras eller utvidgas, med målet att ta fram ett eventuellt förslag så snart som möjligt.

Kommissionen pekar också på behovet av ökade insatser för utbildning och övning på cybersäkerhetsområdet. Som en uppföljning av antagandet av NIS-direktivet och ramen för EU:s politik för it-försvar (antagen av rådet den 18 november 2014 dok. 15585/14), kommer kommissionens avdelningar att samarbeta med medlemsstaterna, Europeiska utrikestjänsten (EEAS), Enisa och andra berörda EU-organ för att inrätta en plattform för utbildning och övning på cybersäkerhetsområdet som kommer att främja synergier mellan civil och militär utbildning.

Slutligen behandlas inom detta huvudområde problematiken kring ömsesidiga och gränsöverskridande säkerhetsberoenden mellan sektorer. En allvarlig cyberincident inom en sektor eller medlemsstat kan direkt eller indirekt påverka – eller spridas till – andra sektorer eller andra medlemsstater. En viktig faktor när man ska bedöma risken för och konsekvenserna av en storskalig cyberincident är graden av dessa beroenden. Kommissionen avser därför att genom olika initiativ arbeta för att främja utvecklingen av samarbetet mellan sektorerna och öka kunskapen om beroendeförhållandena.

1.2.2 Utmaningar för Europas inre marknad för cybersäkerhet

Initiativen och förslagen när det gäller Europas inre marknad för cybersäkerhet syftar till att främja en mer integrerad inre marknad för cybersäkerhetsprodukter och tjänster för att underlätta införandet av mer praktiska och överkomliga lösningar. Kommissionens bedömning är att tillgången på IKT-säkerhetsprodukter och tjänster på den inre marknaden fortfarande är mycket fragmenterad geografiskt sett. Detta gör det svårt för de europeiska företagen att konkurrera på nationell, europeisk och global nivå. Det minskar också utbudet av fungerande och användbar cybersäkerhetsteknik. Certifiering är mycket viktig för att öka förtroendet och säkerheten när det gäller varor och tjänster. Företag kan idag behöva genomgå flera certifieringsprocesser för att kunna sälja i flera medlemsstater. I sämsta fall kan det hända att en IKT-produkt eller IKT-tjänst som utformats för att uppfylla cybersäkerhetskrav i en medlemsstat inte får släppas ut på marknaden i en annan medlemsstat.

För att skapa en fungerande inre marknad för cybersäkerhet, och på så sätt långsiktigt öka den gemensamma säkerheten i Europa, bör enligt kommissionen en eventuell ram för säkerhetscertifiering av IKT-produkter och IKT-tjänster skapas. För detta ändamål kommer kommissionen att inrätta en särskild arbetsgrupp för säkerhetscertifiering av IKT-produkter och IKT-tjänster som kommer att bestå av experter från medlemsstaterna och näringslivet. Syftet är att i samarbete med Enisa och det gemensamma forskningscentrumet före utgången av 2016 ta fram en färdplan för att undersöka möjligheten att lägga fram ett förslag till en sådan europeisk IKT-säkerhetscertifieringsram före utgången av 2017. Kommissionen kommer också att undersöka olika alternativ för hur man bäst kan beakta IKT-säkerhetscertifiering i framtida sektorsspecifik lagstiftning, som också avser säkerhetsaspekter. Förutom möjliga lagstiftningsalternativ kommer kommissionen också att undersöka möjligheten att införa ett europeiskt, kommersiellt inriktat, frivilligt och enkelt märkningssystem för säkerheten i IKT-produkter. Märkningssystemet skulle komplettera certifieringen och syfta till att öka läsbarheten för cybersäkerheten i kommersiella produkter för att på så sätt öka deras konkurrenskraft på den inre marknaden och globalt.

Offentliga förvaltningar kommer att engageras för att främja användning av gemensamma specifikationer och hänvisning till certifiering vid offentlig upphandling. Kommissionen kommer också att övervaka och rapportera om användningen av relevanta certifieringskrav inom offentlig upphandling på nationell nivå, särskilt när det gäller sektorspecifika system (t.ex. energi, transport, hälso- och sjukvård och offentlig förvaltning).

Kommissionen beskriver även initiativ och förslag för att öka investeringarna i cybersäkerhet i Europa och stödja små och medelstora företag vilka går ut på att använda befintliga verktyg för stöd till små och medelstora företag för att öka kunskaperna om befintliga finansieringsmekanismer bland cybersäkerhetsaktörer.

1.2.3 Främjande av industriell kapacitet på cybersäkerhetsområdet

När det gäller huvudområdet industriell kapacitet på cybersäkerhetsområdet vill kommissionen främja konkurrenskraft och innovation för den europeiska cybersäkerhetsbranschen. Avsnittet beskriver kommissionens redan påbörjade arbete med att underteckna ett avtal med branschen om ett privat-offentligt partnerskap för cybersäkerhet, så att arbetet kan inledas under det tredje kvartalet 2016 (cPPP). Partnerskapet för cybersäkerhet inleds inom ramen för EU:s ramprogram för forskning och innovation för perioden 2014–2020 (Horisont 2020). Partnerskapet kommer att mobilisera medel från två av programmets pelare: Ledarskap inom möjliggörande teknik och industriteknik och Samhällsutmaning – Säkra samhällen.

Partnerskapet kommer att genomföras med öppna och flexibla styrelseformer som är anpassade till cybersäkerhetsvillkorens snabba utveckling. Det kommer att beakta medlemsstaternas behov av att diskutera hur teknikutvecklingen påverkar möjligheterna till säker drift av nationella och gränsöverskridande infrastrukturer. Kommissionen kommer att inleda Horisont 2020-ansökningsomgångarna för partnerskapet under första kvartalet 2017 och samordna partnerskapet med relevanta sektorsstrategier, Horisont 2020-instrument och privat-offentliga partnerskap inom andra sektorer.

1.3 Gällande svenska regler och förslagets effekt på dessa

Kommissionens initiativ och förslag har i nuläget ingen påverkan på svensk reglering. Det kan dock inte uteslutas att något av förslagen kommer att utvecklas i den riktningen i framtiden.

1.4 Budgetära konsekvenser / Konsekvensanalys

Kommissionen redovisar ingen bedömning av de budgetära konsekvenserna. Regeringen anser att de åtgärder som föreslås i meddelandet inte ska medföra några extra kostnader.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Informations- och cybersäkerhet är ett viktigt område för regeringen och regeringen ställer sig generellt positiv till fortsatta satsningar på området inom ramen för EU. Regeringen anser dock att medlemsstaterna i första hand nu bör koncentrera sig på att införliva NIS-direktivet i nationell lagstiftning och genomföra de strukturer som anges i direktivet.

Regeringens är positiv till ett fortsatt starkt och proaktivt EU-arbete på området. Regeringen vill dock framhålla vikten av att de åtgärder som

meddelandet innehåller inte avleder resurser från det pågående arbetet med NIS-direktivet.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter är inte kända.

2.3 Institutionernas ståndpunkter

Institutioners ståndpunkter är inte kända.

2.4 Remissinstansernas ståndpunkter

Förslaget har inte varit föremål för remiss.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Meddelandet innehåller inte några konkreta förslag till nya rättsakter. Om nya rättsakter föreslås i ett senare skede bedöms följande artiklar vara relevanta. 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".

3.2 Subsidiaritets- och proportionalitetsprincipen

Meddelandet innehåller inte några konkreta förslag till nya rättsakter. Kommissionen anger inte i detta meddelande hur förslag och initiativ ansluter till subsidiaritets- och proportionalitetsprincipen.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Slovakien (ordförandeland) har aviserat att de avser att ta fram rådsslutsatser för att uttrycka rådets stöd för meddelandet. Arbetet med dessa har inletts inom ordförandeskapets vängrupp för cyberfrågor (FoP Cyber).

Cyberresiliens – IT-system, kritisk infrastruktur m.m. (t.ex. inom sjukvård eller banker) ska vara motståndskraftiga och kunna fortsätta leverera önskade tjänster vad som än händer (t.ex. it-incidenter orsakade av angrepp, elavbrott, olyckor etc.).

CSIRT – Enheter för hantering av it-säkerhetsincidenter (Computer Security Incident Response Team)

IKT – Informations- och kommunikationsteknologi

NIS-direktivet – EU-direktiv om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem (faktapromemoria 2012/13:FPM68)

EU:s Cybersäkerhetsstrategi – I EU:s strategi för it-säkerhet fastställs EU:s strategi för att förebygga och hantera avbrott i och angrepp mot Europas telekommunikationssystem (JOIN(2013)).

cPPP – Ett avtalsbaserat privat-offentligt partnerskap för cybersäkerhet (contruactual private public partnership).

FoP Cyber – Ordförandeskapets vängrupp för cyberfrågor (Friends of Presidency for Cyber Issues)