Regeringskansliet
Faktapromemoria 2020/21:FPM70

EU:s strategi för cybersäkerhet för ett digitalt decennium

2020/21:FPM70

Justitiedepartementet

2021-01-20

Dokumentbeteckning

JOIN (2020) 18
Gemensamt meddelande till Europaparlamentet och rådet ”EU:s strategi för cybersäkerhet för ett digitalt decennium”

Sammanfattning

EU:s nya cybersäkerhetsstrategi bygger vidare på den strategi som lanserades 2013 och fokuserar på åtgärder för hur EU kommer att skydda sina medborgare, företag och institutioner från cyberhot och hur internationellt samarbete kan utvecklas i syfte att säkerställa ett globalt och öppet internet.

Strategin är uppdelad i tre huvudsakliga delar: (1) Resiliens, teknisk suveränitet och ledarskap, (2) Operativ kapacitet för att förebygga, avskräcka och bemöta cyberattacker och (3) En global och öppen cyberrymd genom ökat samarbete. I strategin föreslås även hur cybersäkerheten ska stärkas inom EU:s egna institutioner.

Regeringen välkomnar strategins breda anslag, som understryker vikten av en horisontellt samordnad politik på cyberområdet, såväl mellan politikområden som mellan de inrikes- och utrikespolitiska dimensionerna. Regeringen anser vidare att det är viktigt att medlemsstaternas ansvar för att skydda nationell säkerhet säkerställs.

Regeringen återkommer till riksdagen avseende enskilda initiativ när de har presenterats.

1 Förslaget

1.1 Ärendets bakgrund

EU:s nya cybersäkerhetsstrategi bygger på den cybersäkerhetsstrategi som lanserades 2013, ”EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd”. Strategin bygger även vidare på kommissionens och den höga representanten för utrikesfrågor och säkerhetspolitik meddelande om ”Resiliens, avskräckning och försvar: stärkt cybersäkerhet för EU” från 2017.

EU:s cybersäkerhetsstrategi för det digitala decenniet är vidare ett centralt inslag i meddelandet om EU:s digitala framtid, Kommissionens återhämtningsplan, EU:s strategi för säkerhetsunionen, den globala strategin för EU:s utrikes- och säkerhetspolitik och EU:s strategiska agenda 2019–2024.

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

Kommissionen och den höga representanten för utrikesfrågor och säkerhetspolitik har den 16 december 2020 presenterat EU:s nya cybersäkerhetsstrategi.

1.2 Förslagets innehåll

Strategin handlar om att stärka cybersäkerheten i digitala verktyg och anslutningar, att stärka möjligheterna för en EU-gemensam lägesbild och agerande vid cyberattacker och att EU tillsammans med likasinnade värnar en cyberrymd baserad på rättsstatens principer och mänskliga rättigheter.

Strategin är uppdelad i tre huvudsakliga delar: (1) Resiliens, teknisk suveränitet och ledarskap, (2) Operativ kapacitet för att förebygga, avskräcka och bemöta cyberattacker och (3) En global och öppen cyberrymd genom ökat samarbete. I strategin föreslås även hur cybersäkerheten ska stärkas inom EU:s egna institutioner.

Resiliens, teknisk suveränitet och ledarskap

Strategin föreslår att direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen revideras, se separat faktaPM.

Strategin föreslår också att ett nätverk av säkerhetsoperationscentrum (SOCs), ska inrättas i hela EU. Centrumen ska utgöra en ”cybersäkerhetssköld” för EU och ska med stöd av artificiell intelligens kunna upptäcka tecken på cyberattacker för att möjliggöra proaktiva insatser. Strategin föreslår även en säker kommunikationsinfrastruktur. Vidare anges att ny horisontell reglering för att förbättra cybersäkerheten i uppkopplade produkter och tjänster som bjuds ut på inre marknaden ska övervägas.

Vidare pekar strategin på möjligheter att driva på arbetet med industristrategin och uppnå europeiskt ledarskap inom digital teknik och cybersäkerhet. Små och medelstora företag föreslås få stöd inom ramen för digitala ”innovationsknutpunkter”. Kommissionen avser också att investera i forskning och innovation som är öppen, konkurrenskraftig och baserad på spetskompetens. Utbildning, utvecklad cybersäkerhetskompetens och bättre motståndskraft mot stöld av immateriella tillgångar lyfts även fram.

Kommissionen aviserar också att genomförandet av 5G-verktygslådan ska färdigställas under andra kvartalet av år 2021.

Operativ kapacitet för att förebygga, avskräcka och bemöta

Strategin lanserar förslaget om att inrätta en gemensam cyberenhet (Joint Cyber Unit) som ska stärka samarbetet mellan EU-organen och medlemsstaternas myndigheter med ansvar för att förebygga, avskräcka och bemöta cyberattacker. Arbetet mot cyberbrottslighet, inklusive arbetet med att bättre skydda barn mot sexuell exploatering på nätet, ska stärkas genom ökad kapacitet och förbättrat samarbete mellan cybersäkerhetssektorn och brottsbekämpande myndigheter.

I strategin finns också förslag som ska stärka EU:s verktygslåda för cyberdiplomati för att förebygga och motverka skadlig cyberverksamhet, särskilt sådan verksamhet som påverkar kritisk infrastruktur, leveranskedjor och demokratiska institutioner och processer. En ny arbetsgrupp för delning av cyberrelaterad underrättelseinformation föreslås.

Strategin föreslår att EU och dess medlemsstater lägger ytterligare kraft på utvecklingen av cyberförsvarsförmågor genom olika EU-strategier och instrument samt, att där det är lämpligt, bygger vidare på samarbeten med Europeiska försvarsbyrån EDA. Strategin föreslår också att en öppen, europeisk domännamnssystemtjänst utvecklas, liksom förbättrat samarbete vad gäller cybersäkerhet och rymdfrågor.

En global och öppen cyberrymd genom ökat samarbete

Strategin understryker vikten av intensifierat samarbete med internationella partners för att stärka den regelbaserade världsordningen, främja internationell säkerhet och stabilitet i cyberrymden och skydda mänskliga rättigheter och grundläggande friheter på nätet. Ett ökat engagemang för och ledarskap i internationella standardiseringsprocesser föreslås. Arbetet med att inom FN-systemet utveckla gemensamma normer för staters uppförande ska stärkas. En EU-gemensam syn på internationell rätts tillämpbarhet i cyberrymden ska tas fram. Dialogen med tredjeländer och samarbetet med såväl regionala som internationella organisationer ska förstärkas ytterligare, liksom med andra aktörer inom flerpartsmodellen för internets styrning. Vidare föreslås att ett informellt nätverk för cyberfrågor etableras mellan EU-delegationerna och medlemsstaternas utlandsmyndigheter för att mer effektivt främja en gemensam syn på cyberrymden.

Cybersäkerhet i EU-institutioner, organ och byråer

Strategin föreslår förordningar med gemensamma informations- och cybersäkerhetsregler för EU:s institutioner, organ och byråer. Vidare förslås en ny rättslig grund för ett nätverk av europeiska organisationer för incidenthantering (CERT-EU).

1.3 Gällande svenska regler och förslagets effekt på dessa

Inte aktuellt. Meddelandet utgör inte bindande lagstiftning.

1.4 Budgetära konsekvenser / Konsekvensanalys

Inte aktuellt. Förslaget har inte några budgetära konsekvenser.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen välkomnar strategins breda anslag, som understryker vikten av en horisontellt samordnad politik på cyberområdet, såväl mellan politikområden som mellan de inrikes- och utrikespolitiska dimensionerna. Regeringen anser vidare att det är viktigt att medlemsstaternas ansvar för att skydda nationell säkerhet säkerställs. Medlemsstaterna ska kunna vidta de åtgärder som de anser nödvändiga för att skydda den nationella säkerheten.

Det är även av vikt att det är synergier som i första hand eftersträvas och att det tydliggörs hur de olika förslagen förhåller sig till varandra och till redan pågående arbete och lagstiftning på området. Förslagen är omfattande och långtgående och behöver analyseras närmare, bl.a. för att säkerställa att förslagen inte går in på nationella kompetensområden. Regeringen anser att det vidare är viktigt att tillvarata erfarenheter från andra processer inom EU som har bäring på strategin.

Regeringen instämmer i att cybersäkerhet måste integreras i alla digitala produkter och tekniker, till exempel i tekniker som artificiell intelligens, kryptering och kvantberäkning. Regeringen stödjer fortsatt EU-samarbete för att bekämpa cyberbrottslighet och brottslighet där man använder ny teknik. Det är dock enligt regeringen viktigt att förslagen till olika tekniksatsningar för ökad säkerhet inte i ett initialt skede låser sig till enskilda icke-beprövade lösningar. Det är prioriterat att samarbeta på EU-nivå för att förbättra tillgång till information och elektroniska bevis för brottsbekämpningen, till exempel genom en balanserad reglering rörande datalagring, tillgång till information och en effektiv gränsöverskridande tillgång till elektronisk bevisning. Nya regleringar ska vara förenliga med mänskliga rättigheter, särskilt rätten till respekt för privat- och familjelivet samt skyddet för personuppgifter, online såväl som offline, samt innefatta adekvata rättssäkerhetsgarantier.

Vidare anser regeringen att det är positivt att kommissionen prioriterar att genomförandet av 5G-verktygslådan blir färdig under andra kvartalet av innevarande år. Regeringen vill dock framhålla att det fortsatt är viktigt att användandet av verktygslådan är frivillig givet dess påverkan på nationell säkerhet som är en nationell kompetens.

Regeringen ser med oro på effekterna som den geopolitiska utvecklingen får för cyber- och teknikområdet, såväl vad gäller antagonistiska aktörers agerande som risken för ökad fragmentering och välkomnar därför förslagen i strategin för att stärka den globala cybersäkerheten. Ett mer samordnat EU kan bli en proaktiv och central aktör i de globala diskussionerna om internets framtid. Regeringen understryker vikten av att det europeiska agerandet på säkerhetsområdet är noga avvägt för att inte ge understöd till aktörer som vill se en ökad fragmentering av internet och informationsrymden. Regeringen instämmer i att EU:s engagemang i arbetet med internationell standardisering behöver öka.

Regeringen understryker vikten av ett nära transatlantiskt samarbete och samarbete med strategiska partners för att möta nya utmaningar på cyberområdet, inte minst vad gäller etablerandet av globala normer för utveckling och användning av nya tekniker.

Det är viktigt att Sverige verkar konstruktivt för att medel används så effektivt som möjligt när det gäller de utgifter som ingår i uppgörelsen om EU:s långtidsbudget 2021–2027. Tillkommande uppgifter ska huvudsakligen 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 ännu inte kända.

2.4 Remissinstansernas ståndpunkter

Förslaget har inte remitterats.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Ej tillämpligt. Meddelandet avser en strategi som informerar om kommande politiska initiativ och åtgärder.

3.2 Subsidiaritets- och proportionalitetsprincipen

Ej tillämpligt. Meddelandet avser en strategi som informerar om kommande politiska initiativ och åtgärder

4 Övrigt

4.1 Fortsatt behandling av ärendet

Kommissionens meddelande väntas bland annat diskuteras i den horisontella arbetsgruppen för cyberfrågor (HWP Cyber). Rådslutsatser förväntas att antas under våren 2021.

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.