Regeringskansliet
Faktapromemoria 2021/22:FPM76

# Åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer

2021/22:FPM76

Justitiedepartementet

2022-04-21

## Dokumentbeteckning

COM(2022) 122 final
Förslag till EUROPARLAMENTETS OCH RÅDETS FÖRORDNING - om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer

## Sammanfattning

Kommissionen föreslår att unionens institutioner, organ och byråer blir skyldiga att inrätta ett internt ramverk för hantering, styrning och kontroll av cybersäkerhetsrisker. Vidare föreslås riskhanterings- och rapporteringsskyldigheter på cybersäkerhetsområdet för unionens institutioner, organ och byråer. Förslaget innebär även att EU:s Computer Emergency Response Team (CERT-EU) får nya uppgifter och en utökad roll. Kommissionen föreslår också att en cybersäkerhetsstyrelse skapas för att övervaka institutionernas, organens, byråernas och CERT-EU:s genomförande av förordningen.

Regeringen välkomnar åtgärder som leder till stärkt cybersäkerhet i EU:s institutioner, organ och byråer. Förordningen bör i möjligaste mån vara samstämmig med det nya NIS-direktivet (NIS 2) så att det ställs motsvarande cybersäkerhetskrav på EU:s institutioner, organ och byråer som på leverantörer av samhällsviktiga tjänster enligt nämnda direktiv.

# 1 Förslaget

## 1.1 Ärendets bakgrund

Förslaget bygger vidare på strategin för EU:s säkerhetsunion (COM(2020) 605) och EU:s strategi för cybersäkerhet för ett digitalt decennium (JOIN(2020) 18).

Enligt kommissionen är förslaget förenligt med direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS). Anpassningar görs också till förslaget till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148 [förslaget till NIS 2] (COM(2020) 823), förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten), förslag till förordning om informationssäkerhet inom unionens institutioner, organ och byråer (COM(2022) 119), kommissionens rekommendation av den 23 juni 2021 om att bygga en gemensam cyberenhet (C(2021) 4520) samt kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser.

## 1.2 Förslagets innehåll

Kommissionen föreslår att varje EU-institution, organ och byrå ska inrätta ett internt ramverk för hantering, styrning och kontroll av cybersäkerhetsrisker. Varje entitets högsta ledningsnivå ska godkänna entitetens egna grundläggande nivåer för cybersäkerhet. Institutionerna, organen och byråerna ska också genomföra regelbundna mognadsbedömningar av sin cybersäkerhet och anta varsin cybersäkerhetsplan.

Enligt förslaget får CERT-EU nya uppgifter och en utökad roll. CERT-EU ska ge institutionerna, organen och byråerna råd om cybersäkerhet, hjälpa dem att förebygga, upptäcka, begränsa och hantera incidenter samt fungera som entiteternas nav för utbyte av cybersäkerhetsinformation och samordning av incidenthantering. CERT-EU ska vidare tillhandahålla tjänster, i vissa fall kan dessa även vara avgiftsbelagda. Vidare föreslås CERT-EU inleda ett strukturerat samarbete med Enisa och bidra till den s.k. gemensamma cyberenheten (JCU).

Alla EU-institutioner, organ och byråer blir enligt förslaget skyldiga att underrätta CERT-EU om betydande cyberhot, utan onödigt dröjsmål och senast 24 timmar efter att de fått kännedom om dem.

Kommissionen föreslår även att en cybersäkerhetsstyrelse bestående av representanter från olika institutioner inrättas för att övervaka institutionernas, organens och byråernas genomförande av förordningen samt

övervaka CERT-EU:s genomförande av de allmänna prioriteringarna och målen samt ge CERT-EU strategisk vägledning.

### 1.3 Gällande svenska regler och förslagets effekt på dessa

Kommissionen menar att förslaget endast kommer att få konsekvenser för unionens institutioner, organ och byråer.

Eftersom ministerrådet består av medlemsstaterna, så kan förslaget få konsekvenser på svensk lagstiftning. Regeringen behöver därför närmare analysera om och i så fall i vilken utsträckning förslaget påverkar svensk lagstiftning.

### 1.4 Budgetära konsekvenser / Konsekvensanalys

Kommissionen föreslår en omfördelning av personal och ekonomiska resurser från unionens berörda institutioner, organ och byråer till kommissionens budget. De resurser som behövs för att CERT-EU ska kunna fullgöra sin utökade roll tas, enligt förslaget, genom årligt ekonomiskt bidrag från de EU-institutioner, organ och byråer som drar nytta av CERT-EU:s tjänster. Omfördelningen ska vara klar när den första årsbudgeten antas efter att den föreslagna förordningen träder i kraft.

Förslaget bedöms inte ha några konsekvenser för statsbudgeten. Eventuella ökade kostnader för EU-institutioner, organ och byråer bör hanteras genom omprioriteringar i den fleråriga budgetramen (MFF) i linje med vad som föreslagits i förordningen.

## 2 Ståndpunkter

### 2.1 Preliminär svensk ståndpunkt

Regeringen välkomnar åtgärder som leder till stärkt cybersäkerhet i EU:s institutioner, organ och byråer. Förordningen bör i möjligaste mån vara samstämmig med NIS2-direktivet (COM(2020) 823) som just nu förhandlas, så att det ställs motsvarande cybersäkerhetskrav på EU:s institutioner, organ och byråer som på leverantörer av samhällsviktiga tjänster enligt nämnda direktiv.

Regeringen anser att förslagets konsekvenser behöver analyseras närmare. Det rör särskilt hur bestämmelserna om informationshantering (art. 18), delningsskyldigheter (art. 19) och underrättelseskyldigheter (art. 20) förhåller sig till information som finns hos nationella myndigheter. Vidare behöver kopplingen mellan detta förslag och förslaget till förordning om

informationssäkerhet inom unionens institutioner (COM(2022) 119) analyseras närmare.

Regeringen ställer sig också frågande till de referenser som i förslaget görs till en gemensam cyberenhet (JCU) eftersom en sådan enhet inte är beslutad samt att behovet av en eventuell sådan enhet ännu inte är klarlagd.

## 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

Kommissionen har som rättslig grund angett fördraget om Europeiska unionens funktionssätt, särskilt artikel 298, och fördraget om upprättande av Europeiska atomenergigemenskapen, särskilt artikel 106a.

Beslut fattas av rådet med kvalificerad majoritet efter ordinarie lagstiftningsförfarande med Europaparlamentet.

## 3.2 Subsidiaritets- och proportionalitetsprincipen

Enligt kommissionen omfattas förslaget av unionens exklusiva befogenhet. En prövning av subsidiaritetsprincipen är därför inte aktuell.

Kommissionen menar att de regler som föreslås i förordningen inte går utöver vad som är nödvändigt för att uppnå de specifika målen på ett tillfredsställande sätt. Regeringen anser att konsekvenserna av förslaget är svåra att överblicka och att det hade varit önskvärt med en utförlig konsekvensbedömning. Förslagets proportionalitet behöver analyseras närmare när förslagets eventuella konsekvenser för medlemsstaterna klarlagts.

# 4 Övrigt

## 4.1 Fortsatt behandling av ärendet

Kommissionens förslag väntas bland annat diskuteras i den horisontella arbetsgruppen för cyberfrågor (HWP Cyber).

## 4.2 Fackuttryck/termer

CERT-EU – Computer Emergency Response Team. En enhet bestående av cybersäkerhetsexperter från EU:s institutioner, organ och byråer som hanterar och förebygger it-incidenter. CERT-EU samarbetar med andra CERT:ar i medlemsländerna.

JCU – Joint Cyber Unit. Kommissionen rekommenderar att en gemensam cyberenhet inrättas som sammanför resurser och expertis inom EU för att förebygga och reagera på storskaliga cyberincidenter och cyberkriser.