Europeiska unionens råd

Bryssel den 17 maj 2021
(OR. en)

8640/21

Interinstitutionellt ärende:
2020/0359(COD)

LIMITE

CYBER 138
JAI 523
DATAPROTECT 125
TELECOM 194
MI 332
CSC 190
CSCI 78

NOT

från:	Ordförandeskapet
till:	Ständiga representanternas kommitté (Coreper)/rådet
Ärende:	Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148 – Lägesrapport

Denna rapport har utarbetats under överinseende av ordförandeskapet och föregriper inte enskilda medlemsstaters särskilda intressen eller ytterligare bidrag. I rapporten redogörs för det arbete som hittills har utförts i rådets förberedande organ och för hur långt man har kommit i behandlingen av ovannämnda förslag. Rådet uppmanas att notera rapporten.

I. INLEDNING

1. Den 16 december 2020 antog kommissionen förslaget till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (det reviderade NIS-direktivet eller NIS 2)[1] i syfte att ersätta det nuvarande direktivet om säkerheten i nätverks- och informationssystem (NIS-direktivet)[2]. Förslaget var en av de åtgärder som planeras i EU:s strategi för cybersäkerhet för ett digitalt decennium[3] för att bygga upp motståndskraft mot cyberhot och säkerställa att allmänheten och företagen kan dra nytta av tillförlitlig digital teknik.

2. Syftet med förslaget, som grundas på artikel 114 i EUF-fördraget, är att ytterligare förbättra motståndskraften och incidenthanteringskapaciteten hos offentliga och privata entiteter, behöriga myndigheter och unionen som helhet. Förslaget breddar i betydande grad det nuvarande NIS-direktivets tillämpningsområde, tar upp säkerheten i leveranskedjor, skärper säkerhetskraven och rationaliserar rapporteringsskyldigheterna, samtidigt som strängare tillsynsåtgärder och striktare efterlevnadskontroll införs. Det innehåller dessutom bestämmelser om informationsutbyte och samarbete om cyberkrishantering på nationell nivå och unionsnivå. I förslaget föreskrivs dessutom reglering av databaser som innehåller domänregistreringsuppgifter.

---

1 Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148, COM(2020)823 final.

2 Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

3 Dok. 14133/20.

3. I Europaparlamentet är utskottet för industrifrågor, forskning och energi (ITRE) ansvarigt utskott för förslaget, medan utskottet för utrikesfrågor (AFET), utskottet för den inre marknaden och konsumentskydd (IMCO), utskottet för transport och turism (TRAN) och utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor (LIBE) är rådgivande utskott. Föredragande för ärendet är Bart Groothuis (Renew, Nederländerna). Det portugisiska ordförandeskapet höll en informell diskussion om ärendet med ITRE-utskottets föredragande den 29 januari 2021. Den 12 april 2021 tog ordförandeskapet kontakt med företrädare för föredraganden för IMCO-utskottets yttrande, Morten Lokkegaard (Renew, Danmark). Den 16 april höll det portugisiska ordförandeskapet en informell diskussion om ärendet med enhetschefen och andra handläggare från ITRE-utskottet. Föredraganden lade fram sitt förslag till betänkande för ITRE-utskottet den 3 maj 2021[4].

4. Europeiska ekonomiska och sociala kommittén antog sitt yttrande den 28 april 2021[5].

5. Den 3 februari 2021 beslutade Coreper att höra Europeiska regionkommittén om förslaget[6]. Hittills har Europeiska regionkommittén inte yttrat sig.

6. Europeiska datatillsynsmannen antog sitt yttrande den 11 mars 2021[7].

7. I sitt uttalande[8] av den 26 februari 2021 uppmanade Europeiska rådet medlagstiftarna att skyndsamt fortsätta arbetet, särskilt med det reviderade direktivet om säkerhet i nätverks- och informationssystem (NIS 2-direktivet).

---

4 2020/0359(COD).
5 TEN/730-EESC-2020
6 Dok. 5573/21.
7 *Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive*.
8 https://www.consilium.europa.eu/en/press/press-releases/2021/02/26/statement-of-the-members-of-the-european-council-25-26-february-2021/

8. I sina slutsatser[9] av den 22 mars 2021 om EU:s strategi för cybersäkerhet för ett digitalt decennium var rådet medvetet om vikten av en övergripande och horisontell strategi för cybersäkerhet i unionen, samtidigt som medlemsstaternas befogenheter och behov respekteras fullt ut, samt av vikten av kontinuerligt stöd till tekniskt bistånd och samarbete för att bygga upp medlemsstaternas kapacitet. Rådet noterade, med beaktande av cyberhotbildens utveckling, det nya förslaget till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen som bygger på NIS-direktivet och upprepade sitt stöd för att stärka och harmonisera nationella cybersäkerhetsramar samt för kontinuerligt samarbete mellan medlemsstaterna. Det betonade dessutom behovet av anpassning och harmonisering av sektorsspecifik lagstiftning på detta område.

II. ARBETET I RÅDETS FÖRBEREDANDE ORGAN

9. I rådet behandlas förslaget i den övergripande arbetsgruppen för cyberfrågor (*den övergripande arbetsgruppen*) Vid det informella videokonferensmötet i den övergripande arbetsgruppen den 17 december 2020 presenterade kommissionen den nya strategin för cybersäkerhet och förslaget till översyn av NIS-direktivet. Därefter gav kommissionen en mer övergripande föredragning om förslaget den 12 januari 2021.

10. Vid det informella videokonferensmötet i den övergripande arbetsgruppen den 19 januari 2021 redogjorde det portugisiska ordförandeskapet för sin arbetsmetod för diskussionerna om NIS 2-direktivet. Ordförandeskapet planerade en noggrann genomläsning av förslaget, med beaktande av de viktiga nyheterna i det reviderade direktivet och med möjlighet för delegationerna till skriftliga synpunkter och frågor, följt av klargöranden från kommissionen.

[9] Dok. 6722/21.

11. Dessutom diskuterade den övergripande arbetsgruppen samspelet mellan NIS-direktivet och sektorsspecifik lagstiftning, framför allt direktivet om kritiska entiteters motståndskraft (*CER-direktivet*) och förordningen om digital operativ motståndskraft för finanssektorn (*DORA*). Kommissionen (generaldirektoratet för migration och inrikes frågor) presenterade det nya förslaget till CER-direktiv och underströk de viktigaste delarna av samspelet med NIS 2-direktivet. Vid mötena i den övergripande arbetsgruppen berördes även kopplingarna till den föreslagna förordningen om digital operativ motståndskraft för finanssektorn genom ett diskussionsunderlag från ordförandeskapet i arbetsgruppen för finansiella tjänster (som är ansvarig för DORA) och en presentation av det icke-officiella dokument som lades fram av tre medlemsstater inom arbetsgruppen för finansiella tjänster om sambandet mellan NIS-myndigheter och nationella behöriga myndigheter inom ramen för DORA. Den övergripande arbetsgruppens ordförande deltog även i ett möte i arbetsgruppen för civilskydd för att redogöra för läget i diskussionerna om NIS 2-direktivet. Ordförandeskapet höll den övergripande arbetsgruppen kontinuerligt underrättad om de berörda diskussionerna i arbetsgruppen för civilskydd och arbetsgruppen för finansiella tjänster om de berörda ärendena och upprepade att det krävdes nära samordning på nationell nivå mellan de olika ministerierna med ansvar för dessa ärenden.

12. Vid den övergripande arbetsgruppens informella videokonferensmöten den 2 och 9 februari 2021 inledde man behandlingen av förslaget med de två första artiklarna (*Innehåll* och *Tillämpningsområde*) och bilagorna I och II. Vid den övergripande arbetsgruppens möte den 2 februari fick man en föredragning från kommissionen och ordföranden i samarbetsgruppen för nät- och informationssäkerhet om arbetsläget i den gruppen och om dess roll när det gäller att underlätta genomförandet av NIS-direktivet. Vid det ovannämnda mötet presenterade dessutom Enisas verkställande direktör byråns arbetsprogram, inbegripet information om den studie om NIS-investeringar som Enisa genomfört och om byråns roll för att stödja medlemsstaterna och EU-institutionerna vid genomförandet av politik och råd med anknytning till NIS-direktivet. Under dessa möten diskuterades innehållet vad gäller tillämpningsområdet och frågor ställdes om proportionaliteten.

13. Vid mötet i den övergripande arbetsgruppen den 22 februari 2021 redovisade kommissionen konsekvensbedömningen för översynen av NIS-direktivet. och diskussionerna om förslaget fortsatte med artiklarna 3 och 4 (*Minimiharmonisering* och *Definitioner*).

14. Den 2 mars 2021 fortsatte den preliminära bedömningen av förslaget i den övergripande arbetsgruppen med omfattande diskussioner om artiklarna 5 och 6 (*Nationell strategi för cybersäkerhet* och *Samordnad information om sårbarheter och ett europeiskt sårbarhetsregister*) med en omfattande föredragning av kommissionen om samordnad information om sårbarheter och det europeiska sårbarhetsregistret.

15. Diskussionerna fortsatte vid mötet i den övergripande arbetsgruppen den 9 mars 2021 med artiklarna 7–11 om nationella ramar för hantering av cybersäkerhetskriser, nationella behöriga myndigheter och gemensamma kontaktpunkter inom ramen för NIS-direktivet, enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) samt om kraven på dessa och deras uppgifter och samarbete på nationell nivå.

16. Vid sitt extra möte den 17 mars 2021 diskuterade den övergripande arbetsgruppen artiklarna 12–16 (kapitel III – *Samarbete*), som omfattar NIS samarbetsgrupp, CSIRT-nätverket, det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), rapporten om cybersäkerhetssituationen i unionen och frågan om sakkunnigbedömningar. I synnerhet de två sista artiklarna föranledde flera frågor och förtydliganden. Även artikel 17, *Styrning*, berördes vid detta möte, och chefen för gruppen för förebyggande och utåtriktad verksamhet vid Europols europeiska it-brottscentrum gav en föredragning om de brottsbekämpande myndigheternas syn på det reviderade NIS-direktivet.

17. Vid mötet den 24 mars 2021 behandlade den övergripande arbetsgruppen kapitel IV, *Riskhanterings- och rapporteringskrav för cybersäkerhet*: artiklarna 18 (*Riskhanteringsåtgärder för cybersäkerhet*), 19 (*EU-samordnade riskbedömningar av kritiska leveranskedjor*) och 20 (*Rapporteringsskyldigheter*). Den sistnämnda artikeln anses vara en av de viktigaste bestämmelserna i NIS 2-direktivet.

18. Vid mötet den 14 april behandlade den övergripande arbetsgruppen artiklarna 21 (*Användning av europeiska ordningar för cybersäkerhetscertifiering*), 22 (*Standardisering*) och 23 (*Databaser över domännamn och registreringsuppgifter*) samt de påföljande artiklarna 24 och 25 (*Jurisdiktion och registrering*). Även kapitlen V och VI (om informationsutbyte respektive tillsyn och efterlevnadskontroll) diskuterades vid mötet. Artiklarna 29 och 30 om tillsyn och efterlevnadskontroll i fråga om väsentliga respektive viktiga entiteter föranledde många synpunkter och frågor från medlemsstaterna på grund av att dessa bestämmelser är mycket omfattande och detaljerade. På samma sätt framfördes väsentliga synpunkter och frågor om artiklarna 31, 32 och 33 om administrativa sanktionsavgifter, om överträdelser som innebär personuppgiftsincidenter och om sanktioner. Medlemsstaterna begärde också ytterligare klargöranden om artikel 34 om ömsesidigt bistånd.

19. Den övergripande arbetsgruppen behandlade kapitel VII, *Övergångsbestämmelser och slutbestämmelser* (artiklarna 35–43), vid mötet den 19 april och slutförde därmed genomläsningen av artiklarna.

20. Vid mötet den 28 april 2021 slutförde den övergripande arbetsgruppen den fullständiga genomläsningen av förslaget genom att ta sig an ingressen. Detta var det första fysiska mötet för arbetsgruppen om NIS 2-direktivet under det portugisiska ordförandeskapet. I förväg tillhandahöll kommissionen en jämförelsetabell om skälen och de berörda artiklarna i texten den 15 februari 2021.

21. Vid mötet den 5 maj 2021 höll den övergripande arbetsgruppen en första diskussion i syfte att börja utforma ärendet. För att göra framsteg i ärendet har ordförandeskapet beslutat att inleda utarbetandet med frågan om samspelet mellan det reviderade NIS-direktivet och relevant sektorsspecifik lagstiftning. Beslutet fattades på grundval av diskussionerna i den övergripande arbetsgruppen under genomläsningen av ärendet och det faktum att frågan redan hade identifierats som viktig av medlemsstaterna med hänsyn till den specifika hänvisningen till frågan i rådets slutsatser av den 22 mars om EU:s strategi för cybersäkerhet för ett digitalt decennium. Medlemsstaterna har uppmanats att lämna in konkreta textförslag i denna fråga till och med den 14 maj 2021.

22. Hittills under det portugisiska ordförandeskapet har den övergripande arbetsgruppen ägnat 17 möten åt presentation och genomläsning av förslaget. Under dessa diskussioner har några medlemsstater anmält granskningsreservationer mot hela eller delar av förslaget.

23. Ordförandeskapet är övertygat om att den noggranna genomgången av NIS 2-direktivet har gjort det möjligt för medlemsstaterna att få detaljerade förklaringar från kommissionen om de grundläggande ändringarna av det reviderade direktivet och samtidigt lyfta fram sina huvudsakliga farhågor när det gäller förslaget, vilket underlättar och effektiviserar det framtida arbetet för att i god tid nå fram till en allmän riktlinje.

III. SAKFRÅGOR

24. Under diskussionerna i den övergripande arbetsgruppen välkomnade medlemsstaterna generellt det reviderade NIS-direktivet men tog upp ett antal viktiga frågor och farhågor som bör diskuteras under förhandlingarna om förslaget.

25. En av de återkommande problemen som tagits upp under diskussionerna har varit samspelet mellan det reviderade NIS-direktivet och sektorsspecifik lagstiftning. Vid diskussionerna hittills har en betydande majoritet av medlemsstaterna sagt att det är absolut nödvändigt att betrakta förslaget till reviderat NIS-direktiv som den övergripande ramen för cybersäkerhet i EU och att det bör fungera som en referensstandard för minimiharmonisering av all berörd sektorsspecifik lagstiftning på området.

26. För det andra uttrycktes många farhågor om den betydande utvidgningen av tillämpningsområdet för det reviderade NIS-direktivet: omfattningen av de väsentliga och viktiga entiteter som omfattas av direktivets tillämpningsområde, medlemsstaternas ansvar för att identifiera väsentliga och viktiga entiteter, följderna för de nationella behöriga myndigheternas kapacitet att övervaka dessa förteckningar över entiteter, det som särskilt kännetecknar bilagorna. som närmare beskriver de väsentliga och viktiga entiteter som omfattas av tillämpningsområdet, t.ex. den omfattande inkluderingen av livsmedels- och transportsektorerna oavsett deras betydelse för respektive sektor, begränsningarna genom införande ett storleksbaserat tröskelvärde, särskilt när det gäller entiteter som tillhandahåller mer än en tjänst eller när det gäller små entiteter och mikroentiteter med starkt beroende av andra tjänster, vilket leder till dominoeffekter.

27. För det tredje har även frågan om de storleksbaserade kriterierna som enda faktor att överväga när det gäller identifiering av väsentliga och viktiga entiteter som ska omfattas av direktivets tillämpningsområde tagits upp av en del medlemsstater som kumulativt skulle föredra att en riskbaserad metod eller ytterligare kvalitativa kriterier införs på nationell nivå. Kommissionen har varit tydlig med att de storleksbaserade kriterierna är de mest optimala, om än möjligen inte idealiska, måttstocken för att ta itu med en ineffektiva identifieringsprocessen enligt nuvarande NIS-direktiv och på så sätt undvika fragmentering av tillämpningen av det framtida instrumentet.

28. En del medlemsstater har ifrågasatt huruvida den rättsliga grunden om inre marknaden (artikel 114 i EUF-fördraget) gör det möjligt att låta den offentliga förvaltningen omfattas av tillämpningsområdet för det reviderade direktivet. Tre medlemsstater uttrycker sitt intresse för att få ett skriftligt yttrande från rådets juridiska avdelning i denna fråga. Dessutom ifrågasattes kriterierna för att identifiera offentliga förvaltningsentiteter (den gemensamma nomenklaturen för statistiska territoriella enheter – Nuts).

29. En femte fråga som har lyfts fram av flera medlemsstater vid diskussionerna rör nationella säkerhetsintressen och tillämpningen i praktiken av undantaget av offentliga entiteter som deltar i upprätthållandet av allmän säkerhet, försvar och nationell säkerhet från tillämpningsområdet för det reviderade direktivet.

30. Andra frågor av intresse som tagits upp av medlemsstaterna med anknytning till kopplingar och eventuellt dubbelarbete mellan de olika strukturerna, nätverken och mekanismerna inom cybersäkerhet på EU-nivå, framför allt i och med införandet av EU-CyCLONe, men även för att föregripa kommande förslag och/eller initiativ såsom inrättandet av ett nätverk av säkerhetscentrum (SOC) eller förslaget om den gemensamma cyberenheten.

31. När det gäller införandet av sakkunnigbedömningar har vissa medlemsstater ifrågasatt att detta förfarande och mekanismen för fastställande av respektive metod ska vara obligatoriska, ställt frågor om den utbytta informationens konfidentialitet och tillgänglighet och betonat bristen på resurser för att genomföra sådana granskningar, särskilt i mindre medlemsstater.

32. När det gäller säkerheten i leveranskedjan, och mer specifikt de riskhanteringsåtgärder för cybersäkerhet som fastställs i artikel 18 och de EU-samordnade riskbedömningarna av kritiska leveranskedjor i artikel 19 i det förslaget till reviderat direktiv, har kommissionen meddelat att den för närvarande överväger en övergripande strategi som omfattar eventuella nya horisontella regler för att förbättra cybersäkerheten för alla uppkopplade produkter och tillhörande tjänster som släpps ut på marknaden.

33. Såsom nämnts ovan tog medlemsstaterna upp flera frågor om samordnad information om sårbarheter och Enisas inrättande av ett europeiskt sårbarhetsregister. Kommissionen redogjorde närmare för dessa båda frågor och angav att de skulle utvecklas på grundval av befintlig nationell och internationell bästa praxis och befintliga nationella och internationella bästa förfaranden på området.

34. När det gäller rapporteringen hade medlemsstaterna synpunkter på de administrativa bördorna, ansvarsaspekter till följd av det, tidsramen för underrättelse inom 24 timmar och rapporteringen om betydande cyberhot och tillbud.

35. Även hänvisningen till praktiska och rättsliga överväganden när det gäller upphävandet av de relevanta bestämmelserna i eIDA-förordningen och europeiska kodexen för elektronisk kommunikation har tagits upp av många medlemsstater som har begärt ytterligare klargöranden från Europeiska kommissionen om detta.

36. Medlemsstaterna har också ifrågasatt de omfattande befogenheter som det är tänkt att kommissionen ska få i det reviderade NIS-direktivet när det gäller antagandet av delegerade akter och genomförandeakter. Detta inbegrep frågor om kopplingarna till cybersäkerhetsakten när det gäller certifiering.

IV. SLUTSATSER

37. Ordförandeskapet uttrycker sin uppriktiga uppskattning för kommissionens helhjärtade engagemang under den noggranna genomläsningsprocessen och när det gällde att försöka besvara och klargöra medlemsstaternas frågor och synpunkter under diskussionerna.

38. Vidare erkänner ordförandeskapet medlemsstaternas engagemang för denna process, vilket framgår av de många detaljerade synpunkter och frågor som framfördes under diskussionerna. Ordförandeskapet är fullt medvetet om medlemsstaternas stora ansträngningar när det gäller samordningen mellan ministerierna på nationell nivå i ärendet.

39. På grundval av diskussionerna i den övergripande arbetsgruppen för cyberfrågor, som beskrivs ovan, är ordförandeskapet övertygat om att vissa avgörande delar av det reviderade förslaget till NIS-direktiv ännu inte är tillräckligt mogna för att möjliggöra givande framsteg i överläggningarna mellan medlemsstaterna om deras utformning. Ordförandeskapet anser därför att man genom att ta itu med frågan om samspelet mellan det reviderade NIS-direktivet och relevant sektorsspecifik lagstiftning kommer att möjliggöra framsteg i ärendet och bidra till det nödvändiga klargörandet mellan de relevanta motsvarande bestämmelserna i NIS 2 och andra rättsakter som för närvarande och/eller snart kommer att diskuteras i rådets förberedande organ (bl.a. DORA och CER-direktivet). Man måste också komma ihåg att varje rättsakt i detta samspel befinner sig i olika skeden av förhandlingsprocessen i rådets behöriga förberedande organ. Att redan från början ta itu med frågan om samverkan med relevant sektorsspecifik lagstiftning vid utarbetandet av NIS-direktivet bör göra det möjligt för förhandlingarna om de olika rättsakterna att gå smidigt, oberoende och på solid grund.

40. I slutet av juni 2021 kommer den övergripande arbetsgruppen, enligt det portugisiska ordförandeskapets nuvarande planering, att ha hållit totalt 19 möten om det reviderade NIS-direktivet. Ordförandeskapet anser att rådet, genom att den noggranna och, enligt vår uppfattning, nödvändiga genomgången av det reviderade direktivet har slutförts och utarbetandet därefter har inletts, till fullo har hörsammat uppmaningen från Europeiska rådet vid dess möte den 26 februari att skyndsamt fortsätta arbetet med det reviderade direktivet om säkerhet i nätverks- och informationssystem.

41. Det portugisiska ordförandeskapet är fast beslutet att ha ett nära samarbete med det tillträdande slovenska ordförandeskapet för att underlätta fortsatta diskussioner i den övergripande arbetsgruppen och för att säkerställa smidiga framsteg med ärendet i rådet.

42. Mot ovanstående bakgrund uppmanas Coreper och rådet att notera de framsteg som gjorts med behandlingen av förslaget till direktiv.