EUROPA-
KOMMISSIONEN

Bruxelles, den 30.5.2016
COM(2016) 363 final

2013/0027 (COD)

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET

i henhold til artikel 294, stk. 6, i traktaten om Den Europæiske Unions funktionsmåde

vedrørende

Rådets holdning med henblik på vedtagelse af Europa-Parlamentets og Rådets direktiv om foranstaltninger, der skal sikre et højt fælles niveau af net- og informationssikkerhed i hele EU

(EØS-relevant tekst)

2013/0027 (COD)

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET

i henhold til artikel 294, stk. 6, i traktaten om Den Europæiske Unions funktionsmåde

vedrørende

Rådets holdning med henblik på vedtagelse af Europa-Parlamentets og Rådets direktiv om foranstaltninger, der skal sikre et højt fælles niveau af net- og informationssikkerhed i hele EU

(EØS-relevant tekst)

1. BAGGRUND

Forslag sendt til Europa-Parlamentet og Rådet (COM(2013) 48 – 2013/0027/COD):	7.2.2013
Udtalelse afgivet af Det Europæiske Økonomiske og Sociale Udvalg:	22.5.2013
Europa-Parlamentets førstebehandlingsholdning vedtaget:	13.3.2014
Rådets holdning vedtaget:	17.5.2016

2. FORMÅLET MED KOMMISSIONENS FORSLAG

For det første pålægger forslaget alle medlemsstaterne at sikre, at de har et minimum af national kapacitet ved at:

- oprette kompetente myndigheder for net- og informationssikkerhed (NIS)
- etablere enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)
- vedtage nationale NIS-strategier og nationale NIS-samarbejdsplaner.

For det andet bør de kompetente nationale myndigheder samarbejde i et netværk, der muliggør sikker og effektiv samordning, herunder også koordineret informationsudveksling samt detektering og en indsats på EU-plan. Gennem dette netværk bør medlemsstaterne med udgangspunkt i EU's NIS-samarbejdsplan udveksle oplysninger og samarbejde for at forebygge NIS-trusler og -hændelser. For at sikre, at alle relevante myndigheder inddrages behørigt og rettidigt, pålægges det ved forslaget også, at retshåndhævende myndigheder underrettes om hændelser af kriminel karakter, og at Europol inddrages i EU's koordineringsmekanismer.

For det tredje sigter forslaget – med rammedirektivet om elektronisk kommunikation som forlæg – mod at sørge for, at der udvikles en risikostyringskultur, og at der udveksles oplysninger mellem den private og offentlige sektor. Virksomheder i særlig kritiske sektorer og offentlige myndigheder vil blive forpligtet til at foretage en vurdering af de risici, de står overfor, og til at vedtage passende og forholdsmæssige foranstaltninger til at sikre net- og informationssikkerheden. De skal underrette de kompetente myndigheder om enhver

hændelse, som i alvorlig grad truer deres net- og informationssystemer, og som har væsentlig indvirkning på kritiske tjenesters kontinuitet og leveringen af varer.

3. BEMÆRKNINGER TIL RÅDETS HOLDNING

Rådets holdning udtrykker overordnet støtte til de væsentlige elementer i Kommissionens forslag, nemlig at sikre et højt fælles niveau af net- og informationssikkerhed. Rådet foretager imidlertid visse ændringer, hvad angår opnåelsen af dette mål.

National cybersikkerhedskapacitet

Det fremgår af Rådets holdning, at medlemsstaterne skal vedtage en national NIS-strategi, der fastlægger de strategiske mål og passende politiske og lovgivningsmæssige foranstaltninger for cybersikkerheden. Medlemsstaterne skal ligeledes udpege en kompetent national myndighed i forbindelse med gennemførelsen og håndhævelsen af direktivet samt enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), og som skal tage sig af hændelser og risici.

Selv om Rådets holdning ikke kræver, at medlemsstaterne vedtager en national NIS-samarbejdsplan, som det er anført i det oprindelige forslag, kan holdningen støttes, da visse aspekter af samarbejdsplanen er bibeholdt i bestemmelsen om NIS-strategien.

Samarbejde mellem medlemsstaterne

Det fremgår af Rådets holdning, at der i henhold til direktivet skal oprettes en samarbejdsgruppe bestående af repræsentanter for medlemsstaterne, Kommissionen og Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA), som skal støtte og fremme et strategisk samarbejde og udvekslingen af oplysninger mellem medlemsstaterne. Ifølge Direktivet skal der også skabes et netværk af enheder, der håndterer IT-sikkerhedshændelser (såkaldte CSIRT-netværk) for at fremme et hurtigt og effektivt operationelt samarbejde om specifikke cybersikkerhedshændelser og udveksling af oplysninger om risici.

Selv om den indholdsmæssigt afviger fra tilgangen i det oprindelige forslag, kan Rådets holdning støttes, da den som helhed svarer til målet om at forbedre samarbejdet mellem medlemsstaterne.

Sikkerheds- og anmeldelseskrav for operatører af væsentlige tjenester

Det fremgår af Rådets holdning, at "operatører af væsentlige tjenester" (svarende til "operatører af kritisk infrastruktur" i det oprindelige forslag) skal træffe passende sikkerhedsforanstaltninger og indberette alvorlige hændelser til den kompetente nationale myndighed. Rådet støttede imidlertid ikke en forpligtelse for de kompetente nationale myndigheder til at indberette hændelser af kriminel karakter til de retshåndhævende myndigheder.

I det oprindelige forslag omfattede Rådets holdning operatører inden for energi, transport, bankvæsen, finansmarkedsinfrastrukturer og sundhedssektoren. Rådets aktuelle holdning inkluderer imidlertid også vand og digital infrastruktur.

Medlemsstaterne skal identificere disse operatører på grundlag af bestemte kriterier, f.eks. hvorvidt tjenesten er af afgørende betydning for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter. Selv om denne identificeringsproces ikke udgjorde en del af det oprindelige forslag, kan den accepteres på grundlag af medlemsstaternes forpligtelse til at forelægge Kommissionen de oplysninger, den behøver for at vurdere, om medlemsstaterne anvender konsekvente metoder til identificering af operatører af væsentlige tjenester.

Offentlige myndigheder som sådan er ikke omfattet af Rådets holdning. Hvis de opfylder de kriterier, der er fastsat i artikel 5, skal de identificeres af medlemsstaterne som en operatør af væsentlige tjenester, da operatører af væsentlige tjenester kan være både offentlige og private enheder.

Sikkerheds- og anmeldelseskrav til udbydere af digitale tjenester

Det fremgår af Rådets holdning, at medlemsstaterne skal sikre, at udbydere af digitale tjenester træffer passende sikkerhedsforanstaltninger og indberetter hændelser til den kompetente myndighed. Rådets holdning omfatter onlinemarkedspladser (svarende til e-handelsplatforme i det oprindelige forslag), cloudcomputing-tjenester og søgemaskiner. I forhold til det oprindelige forslag omfatter Rådets holdning ikke:

- internetbetalingsportaler – disse er nu omfattet af det reviderede betalingstjenestedirektiv
- applikationsforhandlere – disse skal forstås som værende en form for onlinemarkedsplads
- sociale netværk – i henhold til Rådets politiske enighed med Europa-Parlamentet.

I henhold til Rådets holdning har Kommissionen fået tildelt gennemførelsesbeføjelser til at fastlægge proceduremæssige ordninger, der er nødvendige for samarbejdsgruppens funktion samt for at præcisere visse elementer vedrørende udbydere af digitale tjenester, herunder formater og procedurer for anmeldelseskrav til udbydere af digitale tjenester.

Kommissionen støtter ovennævnte resultat.

Efter de uformelle trepartsdrøftelser den 14. oktober 2014, den 11. november 2014, den 30. april 2015, den 29. juni 2015, den 17. november 2015 og den 7. december 2015 er Parlamentet og Rådet nået til foreløbig politisk enighed om teksten.

Denne politiske enighed blev bekræftet af Rådet den 18. december 2015. Den 17. maj 2016 vedtog Rådet sin førstebehandlingsholdning.

4. KONKLUSION

Kommissionen støtter resultaterne af de interinstitutionelle forhandlinger og kan derfor acceptere Rådets førstebehandlingsholdning.