

Bryssel den 30.5.2016
COM(2016) 363 final

2013/0027 (COD)

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET

enligt artikel 294.6 i fördraget om Europeiska unionens funktionssätt

om

**rådets ståndpunkt angående antagandet av Europaparlamentets och rådets direktiv om
åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i
hela unionen**

(Text av betydelse för EES)

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET

enligt artikel 294.6 i fördraget om Europeiska unionens funktionssätt

om

rådets ståndpunkt angående antagandet av Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen

(Text av betydelse för EES)

1. BAKGRUND

Överlämnande av förslaget till Europaparlamentet och rådet
(COM(2013) 48 final, 2013/0027 (COD)):

7.2.2013

Europeiska ekonomiska och sociala kommitténs yttrande:

22.5.2013

Europaparlamentets yttrande vid första behandlingen:

13.3.2014

Antagande av rådets ståndpunkt:

17.5.2016

2. SYFTE MED KOMMISSIONENS FÖRSLAG

För det första ålägger direktivet alla medlemsstater att se till att de har en miniminivå av nationell kapacitet genom att

- inrätta nationella myndigheter för nät- och informationssäkerhet (NIS),
- inrätta enheter för hantering av datasäkerhetsincidenter,
- anta nationella NIS-strategier och nationella NIS-samarbetsplaner.

För det andra bör de behöriga nationella myndigheterna samarbeta inom ett nätverk som tillåter säker och effektiv samordning, inbegripet ett samordnat informationsutbyte samt upptäckt och insatser på EU-nivå. Genom detta nätverk bör medlemsstaterna utbyta information och samarbeta för att bekämpa nät- och informationssäkerhetshot och nät- och informationssäkerhetsincidenter på grundval av den europeiska planen för samarbete inom detta område. För att se till att alla berörda myndigheter involveras på rätt sätt och vid rätt tidpunkt innehåller förslaget också krav på att brottsbekämpande organ ska underrättas om incidenter som omfattas av straffrätten och att Europol ska delta i EU:s system för samordning.

För det tredje syftar förslaget till att utifrån samma modell som ramdirektivet för elektronisk kommunikation se till att en riskhanteringskultur utvecklas och att information utbyts mellan privat och offentlig sektor. Företag inom specifika kritiska sektorer och offentliga förvaltningar kommer att åläggas att bedöma de risker som de står inför och vidta ändamålsenliga åtgärder som står i proportion till hoten för att garantera nät- och

informationssäkerheten. De kommer att vara skyldiga att underrätta de behöriga myndigheterna om alla incidenter som utgör ett allvarligt hot mot deras nät och informationssystem och som på ett allvarligt sätt påverkar kontinuiteten för kritiska tjänster och tillhandahållandet av varor.

3. KOMMENTARER TILL RÅDETS STÅNDPUNKT

Rådets ståndpunkt stöder överlag de viktigaste målen i kommissionens förslag, dvs. att säkerställa en hög gemensam säkerhetsnivå för nät och informationssystem. Rådet har emellertid gjort en rad ändringar i fråga om hur man ska uppnå detta mål.

Nationella cybersäkerhetskapaciteten

Enligt rådets ståndpunkt ska medlemsstaterna åläggas att anta en nationell NIS-strategi som fastställer de strategiska målen och lämpliga politiska åtgärder och lagstiftningsåtgärder för cybersäkerhet. Medlemsstaterna kommer också att vara skyldiga att utse en nationell behörig myndighet för direktivets genomförande och efterlevnad samt enheter för hantering av datasäkerhetsincidenter som ansvarar för hanteringen av incidenter och risker.

Även om rådets ståndpunkt inte ålägger medlemsstaterna att anta en nationell NIS-samarbetsplan, vilket ingick i det ursprungliga förslaget, kan ståndpunkten stödjas eftersom vissa aspekter i samarbetsplanen finns kvar i bestämmelsen om NIS-strategin.

Samarbete mellan medlemsstaterna

Enligt rådets ståndpunkt kommer direktivet att föreskriva inrättandet av en samarbetsgrupp bestående av företrädare för medlemsstaterna, kommissionen och Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), för att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna. Genom direktivet kommer det också att skapas ett nätverk av enheter för hantering av datasäkerhetsincidenter för att främja snabbt och ändamålsenligt operativt samarbete om särskilda it-säkerhetsincidenter och för utbyte av information om risker.

Även om rådets ståndpunkt i sak avviker väsentligt från den ansats som ursprungligen föreslogs, kan kommissionen stödja den eftersom den som helhet ligger i linje med målet att förbättra samarbetet mellan medlemsstaterna.

Säkerhets- och anmälningskrav för leverantörer av samhällsviktiga tjänster

Enligt rådets ståndpunkt kommer ”leverantörer av samhällsviktiga tjänster” (likvärdigt med ”operatörer av kritisk infrastruktur” i det ursprungliga förslaget) att åläggas att vidta lämpliga säkerhetsåtgärder och att anmäla allvarliga incidenter till de berörda nationella myndigheterna. Rådet kunde emellertid inte ge sitt stöd till att införa en skyldighet för behöriga nationella myndigheter att anmäla incidenter som omfattas av straffrätten till de brottsbekämpande myndigheterna.

I likhet med det ursprungliga förslaget omfattar rådets ståndpunkt leverantörer inom energi, transport, bankverksamhet, finansmarknadsinfrastrukturer samt hälso- och sjukvården. Rådets ståndpunkt inkluderar dock även infrastruktur för vatten och digitala infrastrukturer.

Medlemsstaterna kommer att åläggas att identifiera dessa leverantörer på grundval av vissa kriterier, såsom huruvida tjänsten är nödvändig för upprätthållandet av viktig samhälls- eller ekonomisk verksamhet. Även om sådan identifiering inte ingick i det ursprungliga förslaget kan tillägget godtas med tanke på att medlemsstaterna är skyldiga att förse kommissionen med den information som den behöver för att bedöma om medlemsstaterna använder enhetliga tillvägagångssätt för att identifiera leverantörer av samhällsviktiga tjänster.

Offentliga förvaltningar tas i sig inte upp i rådets ståndpunkt. Om de uppfyller de kriterier som fastställs i artikel 5 måste de dock identifieras av medlemsstaterna som en leverantör av samhällsviktiga tjänster, eftersom sådana leverantörer kan vara både offentliga eller privata organ.

Säkerhets- och anmälningskrav för leverantörer av digitala tjänster

Enligt rådets ståndpunkt ska medlemsstaterna se till att leverantörer av digitala tjänster vidtar lämpliga säkerhetsåtgärder och anmäler incidenter till den behöriga myndigheten. Rådets ståndpunkt omfattar elektroniska marknadsplatser (motsvarande e-handelsplattformar i det ursprungliga förslaget), molntjänster och sökmotorer. Jämfört med det ursprungliga förslaget har följande inte tagits med i rådets ståndpunkt:

- Internetbetalningsslussar. – de omfattas nu av det reviderade betaltjänstdirektivet.
- Onlineförsäljning av tillämpningar – dessa ska förstås som en typ av elektroniska marknadsplatser.
- Sociala nätverk – i enlighet med rådets politiska överenskommelse med Europaparlamentet.

Enligt rådets ståndpunkt ges kommissionen genomförandebefogenheter att fastställa de förfaranden som krävs för verksamheten i samarbetsgruppen samt att närmare ange vissa faktorer rörande leverantörer av digitala tjänster, inbegripet format och förfaranden som gäller för anmälningskraven för dessa leverantörer.

Kommissionen kan stödja ovanstående.

Efter informella trepartsdiskussioner den 14 oktober 2014, den 11 november 2014, den 30 april 2015, den 29 juni 2015, den 17 november 2015 och den 7 december 2015 har parlamentet och rådet kommit fram till en preliminär politisk överenskommelse om texten.

Denna politiska överenskommelse bekräftades av rådet den 18 december 2015. Den 17 maj 2016 antog rådet sin ståndpunkt vid första behandlingen.

4. SLUTSATS

Kommissionen ger sitt stöd till resultaten av förhandlingarna mellan institutionerna och kan därför godta rådets ståndpunkt vid första behandlingen.