EVROPSKA
KOMISIJA

Bruselj, 30.5.2016
COM(2016) 363 final

2013/0027 (COD)

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU

v skladu s členom 294(6) Pogodbe o delovanju Evropske unije

v zvezi s

stališčem Sveta o sprejetju Direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

(Besedilo velja za EGP)

2013/0027 (COD)

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU

v skladu s členom 294(6) Pogodbe o delovanju Evropske unije

v zvezi s

stališčem Sveta o sprejetju Direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

(Besedilo velja za EGP)

1. OZADJE

Datum predložitve predloga Evropskemu parlamentu in Svetu (COM(2013) 48 – 2013/0027/COD):	7. 2. 2013
Datum mnenja Evropskega ekonomsko-socialnega odbora:	22. 5. 2013
Datum stališča Evropskega parlamenta, prva obravnava:	13. 3. 2014
Datum sprejetja stališča Sveta:	17. 5. 2016

2. CILJ PREDLOGA KOMISIJE

Prvič, predlog od vseh držav članic zahteva, da zagotovijo vzpostavitev minimalne ravni nacionalnih zmogljivosti, in sicer s/z:

- ustanovitvijo organov, pristojnih za varnost omrežij in informacij;
- ustanovitvijo skupin za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT);
- sprejetjem nacionalnih strategij za varnost omrežij in informacij in nacionalnih načrtov za sodelovanje na področju varnosti omrežij in informacij.

Drugič, pristojni nacionalni organi bi morali sodelovati v mreži, ki omogoča varno in učinkovito usklajevanje, kar med drugim vključuje usklajeno izmenjavo informacij ter odkrivanje incidentov in odzivanje nanje na ravni EU. Prek te mreže bi si države članice morale izmenjevati informacije ter sodelovati pri obvladovanju groženj in incidentov v zvezi z varnostjo omrežij in informacij na podlagi evropskega načrta za sodelovanje na tem področju. Da bi se zagotovilo ustrezno in pravočasno sodelovanje vseh zadevnih organov, predlog tudi zahteva, da morajo biti organi kazenskega pregona obveščeni o incidentih kriminalne narave ter da Europol sodeluje v mehanizmih usklajevanja na ravni EU.

Tretjič, na podlagi modela okvirne direktive o elektronskih komunikacijah naj bi predlog zagotovil, da se razvije kultura obvladovanja tveganja ter izmenjujejo informacije med zasebnim in javnim sektorjem. Podjetja v nekaterih ključnih sektorjih in javne uprave bodo morali oceniti tveganja, s katerimi se soočajo, ter sprejeti ustrezne in sorazmerne ukrepe za

zagotovitev varnosti omrežij in informacij. Pristojnim organom bodo morali poročati o vseh incidentih, ki resno ogrožajo njihova omrežja in informacijske sisteme ter znatno vplivajo na neprekinjenost kritičnih storitev in dobavo blaga.

3. PRIPOMBE K STALIŠČU SVETA

Na splošno stališče Sveta podpira temeljne cilje predloga Komisije, in sicer zagotoviti visoko skupno raven varnosti omrežij in informacijskih sistemov. Vendar pa Svet uvaja številne spremembe glede načina doseganja tega cilja.

Nacionalne zmogljivosti na področju kibernetske varnosti

Glede na stališče Sveta bodo morale države članice sprejeti nacionalno strategijo za varnost omrežij in informacij, v kateri bodo določeni strateški cilji ter ustrezni ukrepi politike in regulativni ukrepi za kibernetsko varnost. Države članice bodo prav tako morale imenovati pristojni nacionalni organ za izvajanje in izvrševanje direktive ter skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT), ki bodo odgovorne za obvladovanje incidentov in tveganj.

Čeprav stališče Sveta od držav članic ne zahteva, da sprejmejo nacionalne načrte za sodelovanje na področju varnosti omrežij in informacij, kot je predvideno v prvotnem predlogu, se stališče lahko podpre, saj so nekateri vidiki načrta za sodelovanje ohranjeni v določbi o strategiji za varnost omrežij in informacij.

Sodelovanje med državami članicami

Glede na stališče Sveta se bo z direktivo ustanovila „skupina za sodelovanje“, ki jo bodo sestavljali predstavniki držav članic, Komisije in Agencije Evropske unije za varnost omrežij in informacij (ENISA), da bi se podprla in spodbujala strateško sodelovanje in izmenjava informacij med državami članicami. Direktiva bo vzpostavila tudi mrežo skupin za odzivanje na incidente na področju računalniške varnosti, znano kot mrežo CSIRT, da se bosta spodbujala hitro in učinkovito operativno sodelovanje pri posameznih incidentih na področju kibernetske varnosti ter izmenjava informacij o tveganjih.

Čeprav se stališče Sveta vsebinsko razlikuje od pristopa v prvotnem predlogu, se njegovo stališče lahko podpre, saj na splošno ustreza cilju izboljšanja sodelovanja med državami članicami.

Varnostne zahteve in zahteve glede priglasitve za izvajalce osnovnih storitev

Glede na stališče Sveta bodo morali „izvajalci osnovnih storitev“ (v prvotnem predlogu „upravljavci kritične infrastrukture“) sprejeti ustrezne varnostne ukrepe ter resne incidente priglasiti ustreznim nacionalnim organom. Vendar pa Svet ni podprl obveznosti pristojnih nacionalnih organov glede priglasitve incidentov kriminalne narave organom kazenskega pregona.

V skladu s prvotnim predlogom stališče Sveta zajema take izvajalce v energetskem, prometnem in bančnem sektorju, sektorju infrastruktur finančnega trga ter zdravstvenem sektorju. Vendar pa stališče Sveta vključuje tudi vodni sektor in sektor digitalne infrastrukture.

Države članice bodo morale opredeliti te izvajalce na podlagi določenih meril, kot je vprašanje, ali je ta storitev bistvena za vzdrževanje ključnih družbenih ali gospodarskih dejavnosti. Čeprav ta postopek opredelitve ni bil del prvotnega predloga, ga je mogoče sprejeti, saj morajo države članice Komisiji predložiti informacije, ki jih potrebuje, da oceni, ali države članice uporabljajo dosleden pristop za opredelitev izvajalcev osnovnih storitev.

Javne uprave niso vključene v stališče Sveta. Toda če izpolnjujejo merila iz člena 5, jih bodo morale države članice opredeliti kot izvajalce osnovnih storitev, saj so lahko izvajalci osnovnih storitev javni ali zasebni subjekti.

Varnostne zahteve in zahteve glede priglasitve za ponudnike digitalnih storitev

Glede na stališče Sveta bodo morale države članice zagotoviti, da ponudniki digitalnih storitev sprejmejo ustrezne varnostne ukrepe in incidente priglasijo pristojnemu organu. Stališče Sveta vključuje spletne tržnice (v prvotnem predlogu platforme za e-trgovanje), storitve računalništva v oblaku in iskalnike. Stališče Sveta v primerjavi s prvotnim predlogom ne vključuje:

- portalov za spletna plačila, ki jih zdaj ureja revidirana direktiva o plačilnih storitvah;
- trgovin z aplikacijami, ki jih je treba razumeti kot vrsto spletne tržnice;
- družabnih omrežij, v skladu s političnim dogovorom Sveta z Evropskim parlamentom.

Glede na stališče Sveta so bila Komisiji podeljena izvedbena pooblastila za določitev postopkovnih ureditev, potrebnih za delovanje skupine za sodelovanje, ter za natančnejšo opredelitev nekaterih elementov v zvezi s ponudniki digitalnih storitev, vključno z oblikami in postopki, ki se uporabljajo za zahteve glede priglasitve za ponudnike digitalnih storitev.

Komisija te izide podpira.

Po neuradnih tristranskih razpravah 14. oktobra 2014, 11. novembra 2014, 30. aprila 2015, 29. junija 2015, 17. novembra 2015 in 7. decembra 2015 sta Parlament in Svet o besedilu dosegla okvirni politični dogovor.

Ta politični dogovor je Svet potrdil 18. decembra 2015. Svet je 17. maja 2016 sprejel svoje stališče v prvi obravnavi.

4. SKLEPNE UGOTOVITVE

Komisija podpira rezultate medinstitucionalnih pogajanj in lahko zato sprejme stališče Sveta v prvi obravnavi.