Svet
Evropske unije

Bruselj, 14. september 2017
(OR. en)

Medinstitucionalna zadeva:
2017/0225 (COD)

12183/17
ADD 2

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

SPREMNI DOPIS

Pošiljatelj:	za generalnega sekretarja Evropske komisije: direktor Jordi AYET PUIGARNAU
Prejemnik:	generalni sekretar Sveta Evropske unije Jeppe TRANHOLM-MIKKELSEN
Št. dok. Kom.:	SWD(2017) 501 final
Zadeva:	DELOVNI DOKUMENT SLUŽB KOMISIJE POVZETEK OCENE UČINKA Spremni dokument k predlogu uredbe Evropskega parlamenta in Sveta o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti)

V prilogi vam pošiljamo dokument SWD(2017) 501 final.

Priloga: SWD(2017) 501 final

EVROPSKA
KOMISIJA

Bruselj, 13.9.2017
SWD(2017) 501 final

DELOVNI DOKUMENT SLUŽB KOMISIJE

POVZETEK OCENE UČINKA

Spremni dokument

k predlogu uredbe Evropskega parlamenta in Sveta

o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti)

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. POTREBA PO UKREPANJU

V čem je problem in zakaj je to problem?

Digitalne tehnologije in internet so temelj gospodarstva in družbe EU. Ključni gospodarski sektorji, npr. promet, energetika, zdravstvo ali finance, so vse bolj odvisni od omrežij in informacijskih sistemov za opravljanje svojih temeljnih dejavnosti. Internet stvari povezuje predmete in ljudi prek komunikacijskih omrežij. Te nove razmere prinašajo priložnosti brez primere, pa tudi šibke točke. Kibernetski incidenti se vrstijo. Njihova kompleksnost in pogostost ter obseg njihovih posledic – od dostopa do bistvenih storitev do demokratičnih procesov – se bodo le še povečevali.

Glede tega so bili opredeljeni naslednji med seboj povezani problemi:

- razdrobljenost politik in pristopov h kibernetski varnosti po državah članicah;
- razpršenost virov in razdrobljenost pristopov h kibernetski varnosti v institucijah, agencijah in organih EU;
- nezadostna ozaveščenost državljanov in podjetij o kibernetskih grožnjah ter nezadostne informacije o varnostnih lastnostih izdelkov in storitev IKT, ki jih kupujejo, kot tudi naraščanje števila različnih nacionalnih in sektorskih certifikacijskih shem.

Ti problemi vplivajo na splošno kibernetsko odpornost EU in učinkovito delovanje notranjega trga.

Kaj bi bilo treba doseči?

Specifični cilji te pobude so naslednji:

1. povečanje zmožnosti in pripravljenosti držav članic in podjetij, zlasti glede kritičnih infrastruktur;
2. izboljšanje sodelovanja in usklajevanja med državami članicami ter institucijami, agencijami in organi EU;
3. povečanje zmožnosti na ravni EU, da se dopolni ukrepanje držav članic, zlasti v primeru čezmejnih kibernetskih kriz;
4. povečanje ozaveščenosti državljanov in podjetij o vprašanjih kibernetske varnosti;
5. povečanje splošne preglednosti zagotovil kibernetske varnosti izdelkov in storitev IKT za krepitev zaupanja v enotni digitalni trg in digitalne inovacije;
6. preprečevanje razdrobljenosti certifikacijskih shem v EU ter povezanih varnostnih zahtev in meril za ocenjevanje v različnih državah članicah in sektorjih.

Kakšna je dodana vrednost ukrepanja na ravni EU?

Ker sta digitalizacija in medsebojna povezanost gospodarstva in družbe razširjeni po vsem svetu, razsežnost problemov precej presega meje ozemlja posamezne države članice. Zato je potrebno ukrepanje na ravni Unije. Glede na sedanje razmere in prihodnje scenarije se zdi, da

ukrepi posameznih držav članic in razdrobljen pristop h kibernetski varnosti, zlasti pa njena čezmejna razsežnost, ne morejo povečati kolektivne kibernetske odpornosti Unije.

B. REŠITVE

Katere so različne možnosti za dosego ciljev? Ali ima katera od njih prednost?

V tej oceni učinka je preučen poseben sklop možnosti politike, ki zajemajo pregled Agencije Evropske unije za varnost omrežij in informacij (agencija ENISA) ter varnostnega certificiranja IKT.

Pregled agencije ENISA

Možnost 0 – **osnovni scenarij**. Ta možnost pomeni ohranitev sedanjega stanja. Mandat agencije ENISA bi se podaljšal ter cilji in naloge Agencije bi ostale večinoma nespremenjene, pri čemer bi se upoštevale naloge, ki jih agenciji ENISA dodeljuje poznejša zakonodaja EU (npr. direktiva o varnosti omrežij in informacij).

Možnost 1 – **potek mandata agencije ENISA** (konec delovanja agencije ENISA). Ta možnost bi pomenila konec delovanja agencije ENISA ob koncu njenega mandata (junija 2020) in po možnosti prerazporeditev pristojnosti/dejavnosti na ravni EU in/ali nacionalni ravni.

Možnost 2 – **„reformirana agencija ENISA“**. Ta možnost bi temeljila na sedanjem mandatu agencije ENISA, sprejete pa naj bi bile izbrane spremembe, ki bi upoštevale razvoj na področju kibernetske varnosti. Agencija bi dobila stalni mandat na podlagi naslednjih ključnih elementov: podpore oblikovanju in izvajanju politik EU, krepitve zmogljivosti, znanja in informacij, s trgom povezanih nalog, raziskav in inovacij ter operativnega sodelovanja in kriznega upravljanja.

Možnost 3 – **Agencija EU za kibernetsko varnost s polnimi operativnimi zmožnostmi.** Ta možnost pomeni reformo agencije ENISA z združitvijo treh glavnih nalog: 1. naloga oblikovanja politike / svetovalna naloga, 2. center informacij in strokovnega znanja ter 3. skupina za odzivanje na računalniške grožnje (CERT). Ta možnost bi v veliki meri pomenila enako spremembo obsega mandata kot možnost 2. Dodane pa bi bile dodatne naloge na področju odzivanja na incidente in kriznega upravljanja, tako da bi Agencija pokrivala celotni kibernetski življenjski cikel ter se ukvarjala s preprečevanjem in odkrivanjem kibernetskih incidentov ter odzivanjem nanje.

Certificiranje

Možnost 0 – osnovni scenarij – brez spremembe. Komisija bi pri tej možnosti ohranila sedanje stanje in ne bi sprejela nobenega političnega ali zakonodajnega ukrepa.

Možnost 1 – **nezakonodajni ukrepi (ukrepi „mehkega prava“)**. Komisija bi pri tej možnosti uporabila mehke instrumente politike (npr. razlagalna sporočila, podporo vseevropskim samoregulativnim pobudam in dejavnosti standardizacije), da bi izboljšala preglednost in zmanjšala razdrobljenost.

Možnost 2 – zakonodajni akt EU za razširitev sporazuma SOG-IS na vse države članice. Komisija bi pri tej možnosti predlagala zakonodajni akt za pravno razširitev članstva na vse države članice.

<u>Možnost 3</u> – splošni okvir EU za varnostno certificiranje IKT. Ta možnost pomeni vzpostavitev evropskega okvira za varnostno certificiranje IKT (vključno s skupino strokovnjakov, ki jo sestavljajo nacionalni organi), ki – kolikor je to mogoče – temelji na obstoječih shemah za varnostno certificiranje IKT. Okvir bi torej omogočil vzpostavitev certifikacijskih shem EU, ki bi bile sprejete v vseh državah članicah.

Prednostna možnost je kombinacija možnosti 2 za agencijo ENISA in možnosti 3 za certificiranje.

Kdo so različne zainteresirane strani? Kdo podpira katero možnost?

Velika večina zainteresiranih strani v vseh kategorijah (države članice, industrija, institucije EU in raziskovalna skupnost), ki so sodelovale v posvetovanjih, se strinja s prednostno možnostjo, saj podpirajo okrepitev vloge agencije ENISA in vzpostavitev evropskega okvira za varnostno certificiranje IKT.

Zlasti obstaja soglasje o tem, da bi morali imeti (najmanj) dobro delujočo agencijo EU s stalnim mandatom, ki ima ustrezne vire in pooblastila, da lahko rešuje sedanje in prihodnje izzive na področju kibernetske varnosti. Med zainteresiranimi stranmi obstaja tudi široko soglasje glede vzpostavitve prostovoljnega, stopnjevalnega evropskega okvira.

Na strani industrije to rešitev za certificiranje podpirajo podjetja, za katera že veljajo zahteve glede certificiranja in ki bi jim vseevropski mehanizem, ki bi temeljil na vzajemnem priznavanju certifikatov, prinesel koristi. Podpirajo jo tudi mala in srednja podjetja, ki bi utrpela največjo škodo, če že morajo ali bi morala opraviti več različnih certifikacijskih postopkov v različnih državah članicah. Nekatere države članice, zlasti tiste z manj sredstvi, kot tudi nekateri predstavniki industrije in institucij EU so izrazili pozitivno stališče tudi glede možnosti 3 za agencijo ENISA.

C. UČINKI PREDNOSTNE MOŽNOSTI

Kakšne so koristi prednostne možnosti (če obstaja, sicer glavnih možnosti)?

EU bi pri prednostni možnosti imela agencijo, katere glavna naloga bi bila podpirati države članice, institucije EU in podjetja na področjih, kjer bi to prineslo največjo dodano vrednost. Ta zajemajo: podpora izvajanju direktive o varnosti omrežij in informacij, oblikovanje in izvajanje politike, informacije, znanje in ozaveščenost, raziskave, operativno sodelovanje in krizno upravljanje ter trg. Agencija ENISA bi zlasti podpirala politiko EU na področju varnostnega certificiranja IKT, tako da bi zagotavljala upravno vzdrževanje in tehnično upravljanje evropskega okvira za varnostno certificiranje IKT. Takšen okvir bo praktično vzpostavil sklop pravil o upravljanju varnostnega certificiranja IKT v EU, ki bi spodbujal sistem vzajemnega priznavanja certifikatov, izdanih v različnih državah članicah. Rešitev, ki združuje te možnosti, velja za najučinkovitejšo in naj bi EU omogočila doseči opredeljene cilje: okrepiti zmogljivosti na področju kibernetske varnosti, pripravljenost, sodelovanje, ozaveščanje, preglednost in preprečevanje razdrobljenosti trga. Poleg tega je ta možnost najbolj skladna s prednostnimi nalogami politike, kot so opredeljene v strategiji za kibernetsko varnost in z njo povezanih politikah (npr. direktivi o varnosti omrežij in informacij), ter strategijo za enotni digitalni trg. Poleg tega bi s to možnostjo cilje dosegli z razumno uporabo virov.

Kakšni so stroški prednostne možnosti (če obstaja, sicer glavnih možnosti)?

„Reformirana agencija ENISA“ bi kljub novim vlogam ostala prilagodljiva. Zahtevani finančni prispevek iz proračuna EU bi bil višji, kot je sedaj, vendar še vedno precej nižji od drugih agencij, ki ravno tako delujejo na kritičnih področjih.

Vzpostavitev evropskega okvira za varnostno certificiranje IKT ne bi pomenila dodatnih začetnih stroškov za industrijo (vključno z malimi in srednjimi podjetji). Nasprotno, vodila bi k znatnim prihrankom za podjetja, ki že certificirajo svoje izdelke ali so pripravljena izvajati varnostno certificiranje, kar bi ugodno vplivalo na njihovo konkurenčnost na svetovni ravni. Na drugi strani pa bi bilo potrebnih nekaj proračunskih obveznosti, da bi zagotovili vzdrževanje okvira, ki bi jih zagotavljala predvsem „reformirana agencija ENISA“, kar zadeva tehnične in tajniške naloge.

Ali bo prišlo do znatnih učinkov na nacionalne proračune in uprave?

Ne. Stroški, povezani z okrepitvijo vloge agencije ENISA, bi se večinoma krili iz proračuna EU, države članice pa bi lahko še naprej zagotavljale prostovoljne finančne prispevke za Agencijo. Glede certificiranja bi na nacionalne proračune in uprave vplivala v glavnem vzpostavitev certifikacijskega organa, kadar bi bilo to primerno.

Bo imela pobuda druge pomembnejše učinke?

Ne.

Sorazmernost

Prednostna možnost vključuje uravnotežene ukrepe, ki se vsi zdijo potrebni za doseganje zadevnih ciljev brez nalaganja prevelikega bremena zadevnim zainteresiranim stranem. Ob upoštevanju navedenega se šteje, da je ta pobuda v skladu z načelom sorazmernosti.

D. NADALJNJI UKREPI

Kdaj bo politika pregledana?

Predlaga se, da se prva ocena pripravi pet let po začetku veljavnosti pravnega instrumenta. Komisija bo nato o svoji oceni poročala Evropskemu parlamentu in Svetu ter ji po potrebi priložila predlog za revizijo. Nadaljnja ocenjevanja bo Komisija izvajala vsakih pet let.