Svet
Evropske unije

Bruselj, 22. marec 2022
(OR. en)

Medinstitucionalna zadeva:
2022/0085(COD)

7474/22
ADD 3

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	22. marec 2022
Prejemnik:	generalni sekretar Sveta Evropske unije Jeppe TRANHOLM-MIKKELSEN
Št. dok. Kom.:	SWD(2022) 68 final
Zadeva:	DELOVNI DOKUMENT SLUŽB KOMISIJE POVZETEK OCENE UČINKA Spremni dokument predlog UREDBE EVROPSKEGA PARLAMENTA IN SVETA o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije

Delegacije prejmejo priloženi dokument SWD(2022) 68 final.

Priloga: SWD(2022) 68 final

EVROPSKA
KOMISIJA

Bruselj, 22.3.2022
SWD(2022) 68 final

DELOVNI DOKUMENT SLUŽB KOMISIJE

POVZETEK OCENE UČINKA

Spremni dokument

predlog UREDBE EVROPSKEGA PARLAMENTA IN SVETA

o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije

{COM(2022) 122 final} - {SWD(2022) 67 final}

1. Uvod

Leta 2020 se je močno povečalo število pomembnih incidentov, ki so prizadeli institucije, organe in agencije Unije ter so jih izvedli akterji naprednih trajnih groženj. To dokazujejo številni forenzični posnetki, ki jih je CERT-EU analiziral v letu 2020 in so se v primerjavi z letom 2019 več kot potrojili, število pomembnih incidentov pa se je od leta 2018 povečalo za več kot desetkrat.

Vendar so zmogljivosti za kibernetsko varnost in poraba za varnost IT v institucijah, organih in agencijah Unije v nekaterih primerih izjemno neenake, zaradi česar se ravni zrelosti kibernetske varnosti med institucijami, organi in agencijami Unije zelo razlikujejo. Poleg tega analiza groženj in statistični podatki o varnostnih incidentih IT kažejo, da se bo izpostavljenost institucij, organov in agencij Unije kibernetskim grožnjam le še povečevala.

2. Cilji

Opredeljene pomanjkljivosti na koncu vodijo do nezadostne ravni kibernetske odpornosti v institucijah, organih in agencijah Unije, razdrobljenih virov za varnost IT in neuravnoteženega odnosa do varnosti IT.

Cilj zakonodajnega akta bi bil zagotoviti ukrepe za visoko skupno raven kibernetske varnosti v institucijah, organih in agencijah Unije. To bi spodbudilo in zagotovilo, da bo zrelost kibernetske varnosti sledila vse večji digitalizaciji institucij, organov in agencij Unije.

3. Medinstitucionalni odbor za kibernetsko varnost in okvir za kibernetsko varnost

Predlog za Medinstitucionalni odbor za kibernetsko varnost in okvir za kibernetsko varnost bo uvedel ukrepe za visoko skupno raven kibernetske varnosti v institucijah, organih in agencijah Unije, omogočil uskladitev z okvirom, ki obravnava kibernetske grožnje vseh institucij, organov in agencij Unije, ter vzpostavil spremljanje in poročanje Medinstitucionalnemu odboru za kibernetsko varnost.

Predlog posodablja namen in naloge CERT-EU glede na spremenjeno in večjo digitalizacijo institucij, organov in agencij Unije v zadnjih letih ter razvijajoče se okolje kibernetskih groženj.

Za države članice ali državljane EU ni neposrednega vpliva ali proračunskih posledic.

Pravna podlaga za Uredbo je člen 298 Pogodbe o delovanju Evropske unije, ki določa, da institucije, organe, urade in agencije Unije pri izvajanju njihovih nalog podpira odprta, učinkovita in neodvisna evropska uprava.

Ta predlog temelji na strategiji EU za varnostno unijo (COM(2020) 605 final) in strategiji EU za kibernetsko varnost v digitalnem desetletju (JOIN(2020) 18 final).

4. Sklepna ugotovitev

Medinstitucionalni odbor za kibernetsko varnost in okvir za kibernetsko varnost uresničujeta večino predvidenih ciljev razmeroma uspešno in učinkovito ter skladno z drugimi politikami Unije, in sicer z najširšo podporo deležnikov. Ta izbrana rešitev je glede na prevladujoče pravne omejitve, v okviru katerih delujemo, najustreznejša, poleg tega pa enak pristop za vse ne bi bil ustrezen glede na sedanjo raznovrstno zrelost institucij, organov in agencij Unije ter razlike v tehnološkem tveganju in kompleksnosti, s katerimi se soočajo.