Eiropas Savienības
Padome

Briselē, 2022. gada 22. martā
(OR. en)

7474/22
ADD 3

Starpiestāžu lieta:
2022/0085(COD)

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

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2022. gada 22. marts
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretārs *Jeppe TRANHOLM-MIKKELSEN*
K-jas dok. Nr.:	SWD(2022) 68 final
Temats:	KOMISIJAS DIENESTU DARBA DOKUMENTS IETEKMES NOVĒRTĒJUMA KOPSAVILKUMS Pavaddokuments dokumentam Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULAI, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās, birojos un aģentūrās

Pielikumā ir pievienots dokuments SWD(2022) 68 *final*.

Pielikumā: SWD(2022) 68 *final*

EIROPAS
KOMISIJA

Briselē, 22.3.2022.
SWD(2022) 68 final

KOMISIJAS DIENESTU DARBA DOKUMENTS

IETEKMES NOVĒRTĒJUMA KOPSAVILKUMS

Pavaddokuments dokumentam

Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULAI,

ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās, birojos un aģentūrās

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

1. Ievads

2020. gadā strauji pieauga tādu Savienības iestādes, struktūras un aģentūras ietekmējošu būtisku incidentu skaits, kurus izraisīja paaugstināta pastāvīga apdraudējuma (*APT*) rīcībspēki. To atspoguļo arī 2020. gadā *CERT-EU* veiktais kriminālanalīžu skaits, kas salīdzinājumā ar 2019. gadu ir vairāk nekā trīskāršojies, savukārt nozīmīgu incidentu skaits kopš 2018. gada ir palielinājies vairāk nekā desmitkārt.

Tomēr kiberdrošības spēju un IT drošības izdevumi Savienības iestādēs, struktūrās un aģentūrās dažos gadījumos ir pārsteidzoši nevienlīdzīgi, kā rezultātā Savienības iestāžu, struktūru un aģentūru kiberdrošības gatavības līmeņu spektrs ir ļoti plašs. Turklāt drošības apdraudējuma ainas analīze un IT drošības incidentu statistika liecina, ka Savienības iestāžu, struktūru un aģentūru pakļautība kiberuzbrukumiem tikai pastiprināsies.

2. Mērķi

Konstatēto trūkumu galvenais cēlonis ir nepietiekams kibernoturības līmenis Savienības iestādēs, struktūrās un aģentūrās, sadrumstaloti IT drošības resursi un nelīdzsvaroti IT drošības parametri.

Tiesību akta mērķis būtu nodrošināt pasākumus, lai Savienības iestādēs, struktūrās un aģentūrās nodrošinātu vienādi augsta līmeņa kiberdrošību. Tas veicinātu un nodrošinātu, ka kiberdrošības gatavība iet kopsolī ar Savienības iestāžu, struktūru un aģentūru aizvien straujāko digitalizāciju.

3. Iestāžu kiberdrošības padome un kiberdrošības satvars

Ar priekšlikumu par Iestāžu kiberdrošības padomi un kiberdrošības satvaru tiks ieviesti pasākumi nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās un aģentūrās, ļaujot pielāgoties regulējumam, kas pievēršas visu Savienības iestāžu, struktūru un aģentūru kiberdrošības apdraudējumiem, un tiks izveidota uzraudzība un ziņošana Iestāžu kiberdrošības padomei.

Priekšlikums paredz modernizēt *CERT-EU* misiju un uzdevumus, ņemot vērā izmaiņas Savienības iestādēs, struktūrās un aģentūrās un to pieaugošo digitalizāciju pēdējos gados, kā arī pieaugošo kiberdrošības apdraudējumu.

Priekšlikumam nav tiešas ietekmes uz dalībvalstīm vai ES iedzīvotājiem, vai budžetu.

Regulas juridiskais pamats ir Līguma par Eiropas Savienības darbību 298. pants, kurā paredzēts, ka, veicot savus uzdevumus, Savienības iestādes un struktūras saņem atvērtas, efektīvas un neatkarīgas Eiropas administrācijas atbalstu.

Šā priekšlikuma pamatā ir ES Drošības savienības stratēģija (COM(2020) 605 final) un ES kiberdrošības stratēģija digitālajai desmitgadei (JOIN(2020) 18 final).

4. Nobeigums

Iestāžu kiberdrošības padome un kiberdrošības satvars vairumu paredzēto mērķu sasniedz salīdzinoši efektīvi, lietderīgi un saskaņoti ar citām Savienības rīcībpolitikām, kā arī visplašāko ieinteresēto personu atbalstu. Šis risinājums ir izraudzīts kā visizdevīgākais, ņemot vērā dominējošās juridiskās robežas, saskaņā ar kurām mēs rīkojamies; turklāt pieeja "viens risinājums der visiem" nebūtu atbilstošs Savienības iestāžu, struktūru un aģentūru pašreizējai neviendabīgajai gatavībai un tehnoloģiskajiem riskiem un sarežģītībai, ar ko tās saskaras.