Eiropas Savienības
Padome

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

7474/22
ADD 1

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

PRIEKŠLIKUMS

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.:	COM(2022) 122 final - Annexes
Temats:	PIELIKUMI 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 COM(2022) 122 *final - Annexes*.

Pielikumā: COM(2022) 122 *final - Annexes*

EIROPAS
KOMISIJA

Briselē, 22.3.2022.
COM(2022) 122 final

ANNEXES 1 to 2

PIELIKUMI

dokumentam

Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULAI,

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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

I PIELIKUMS

Kiberdrošības pamatparametros jāpievēršas šādām jomām:

(1) kiberdrošības rīcībpolitika, tostarp tīklu un informācijas sistēmu drošības mērķi un prioritātes, jo īpaši attiecībā uz mākoņdatošanas pakalpojumu izmantošanu (Direktīvas 4. panta 19. punkta nozīmē [priekšlikums TID 2]) un tehniskiem pasākumiem tāldarba nodrošināšanai;

(2) kiberdrošības organizācija, tostarp uzdevumu un pienākumu definēšana;

(3) aktīvu pārvaldība, tostarp IT aktīvu inventarizācija un IT tīkla kartogrāfija;

(4) piekļuves kontrole;

(5) darbības drošība;

(6) komunikāciju drošība;

(7) sistēmas iegāde, attīstība un uzturēšana;

(8) attiecības ar piegādātājiem;

(9) incidentu pārvaldība, tostarp pieejas, lai uzlabotu sagatavotību incidentiem, reaģēšanu uz tiem un atgūšanos no tiem, un sadarbība ar *CERT-EU*, piemēram, drošības uzraudzības un reģistrēšanas uzturēšana;

(10) darbības nepārtrauktības pārvaldība un krīžu pārvarēšana, un

(11) izglītošanas par kiberdrošību, izpratnes veicināšanas un apmācības programmas.

II PIELIKUMS

Savienības iestādes, struktūras un aģentūras kiberdrošības pamatparametru īstenošanā un savos kiberdrošības plānos saskaņā ar *IICB* norādījumiem un ieteikumiem pievēršas vismaz šādiem konkrētiem kiberdrošības pasākumiem:

(1) konkrēti pasākumi virzībai uz nulles uzticēšanās arhitektūru (t. i., drošības modelis, sistēmas izstrādes principu kopums un koordinēta kiberdrošības un sistēmas pārvaldības stratēģija, kuras pamatā ir atzinums, ka draudi pastāv gan tradicionālās tīkla robežās, gan ārpus tām);

(2) daudzfaktoru autentifikācijas pieņemšana par normu tīklu un informācijas sistēmās;

(3) programmatūras piegādes ķēdes drošības izveide, izmantojot programmatūras drošas izstrādes un izvērtēšanas kritērijus;

(4) iepirkuma noteikumu uzlabošana, lai veicinātu vienādi augsta līmeņa kiberdrošību:

   (a) likvidējot līgumiskos šķēršļus, kas ierobežo to, kā IT pakalpojumu sniedzēji var informēt *CERT-EU* par incidentiem, ievainojamībām un kiberdraudiem;

   (b) ievērojot līgumā noteikto pienākumu ziņot par incidentiem, ievainojamībām un kiberdraudiem, kā arī ieviest atbilstīgu reaģēšanu uz incidentiem un to uzraudzību.