Europos Sąjungos
Taryba

Briuselis, 2022 m. kovo 22 d.
(OR. en)

7474/22
ADD 1

Tarpinstitucinė byla:
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

PASIŪLYMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2022 m. kovo 22 d.
kam:	Europos Sąjungos Tarybos generaliniam sekretoriui Jeppe TRANHOLMUI-MIKKELSENUI
Komisijos dok. Nr.:	COM(2022) 122 final - Annexes
Dalykas:	Pasiūlymo dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti, PRIEDAI

Delegacijoms pridedamas dokumentas COM(2022) 122 final - Annexes.

Pridedama: COM(2022) 122 final - Annexes

EUROPOS
KOMISIJA

Briuselis, 2022 03 22
COM(2022) 122 final

ANNEXES 1 to 2

PRIEDAI

prie

pasiūlymo dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO

kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti

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

I PRIEDAS

Pagrindiniuose kibernetinio saugumo standartuose turi būti atsižvelgta į šias sritis:

(1) kibernetinio saugumo politiką, įskaitant tinklų ir informacinių sistemų saugumo tikslus ir prioritetus, visų pirma susijusius su debesijos kompiuterijos paslaugų naudojimu (kaip apibrėžta Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 19 punkte) ir techninėmis priemonėmis, kuriomis sudaromos sąlygos nuotoliniam darbui,

(2) kibernetinio saugumo organizavimą, įskaitant funkcijų ir pareigų apibrėžimą,

(3) turto valdymą, įskaitant IT turto aprašą ir IT tinklo kartografiją,

(4) prieigos kontrolę,

(5) operacijų saugumą,

(6) ryšių saugumą,

(7) sistemų įsigijimą, plėtojimą ir techninę priežiūrą,

(8) santykius su tiekėjais,

(9) incidentų valdymą, įskaitant metodus, kuriais siekiama gerinti pasirengimą incidentams, reagavimą į juos ir atkūrimą įvykus incidentams, ir bendradarbiavimą su CERT-EU, kaip antai saugumo stebėsenos ir registravimo priežiūrą,

(10) veiklos tęstinumo ir krizių valdymą ir

(11) švietimą, informuotumo didinimą ir kibernetinio saugumo mokymo programas.

II PRIEDAS

Sąjungos institucijos, įstaigos ir agentūros, įgyvendindamos bazinius kibernetinio saugumo standartus ir savo kibernetinio saugumo planus pagal TKSV rekomendacinius dokumentus ir rekomendacijas, imasi bent šių konkrečių kibernetinio saugumo priemonių:

(1) imasi konkrečių veiksmų siekiant pereiti prie nulinio pasitikėjimo architektūros (nulinio pasitikėjimo architektūra – saugumo modelis, sistemos projektavimo principų rinkinys ir suderinta kibernetinio saugumo ir sistemos valdymo strategija, grindžiami pripažinimu, kad grėsmės egzistuoja tiek tradiciniuose tinkluose, tiek už jų ribų),

(2) patvirtina daugiaveiksnio tapatumo nustatymo būdą kaip visose tinklų ir informacinėse sistemose taikomą standartą,

(3) užtikrina programinės įrangos tiekimo grandinės saugumą, taikydamos saugios programinės įrangos kūrimo ir vertinimo kriterijus,

(4) sugriežtina viešųjų pirkimų taisykles, kad būtų sudarytos palankesnės sąlygos užtikrinti aukštą bendrą kibernetinio saugumo lygį:

   (a) pašalindamos sutartines kliūtis, kuriomis ribojamas IT paslaugų teikėjų keitimasis informacija apie incidentus, pažeidžiamumą ir kibernetines grėsmes su CERT-EU,

   (b) nustatydamos sutartinę prievolę pranešti apie incidentus, pažeidžiamumą ir kibernetines grėsmes ir užtikrindamos tinkamą reagavimą į incidentus bei jų stebėseną.