**Informatīvais ziņojums par Aizsardzības ministrijas sagatavoto Latvijas Republikas nacionālo pozīciju Nr. 1 par Eiropas Komisijas 2017. gada 13. septembra „Kiberdrošības pakotni”**

Aizsardzības ministrija ir sagatavojusi nacionālās pozīcijas projektu par Eiropas Komisijas (turpmāk – EK) 2017. gada 13. septembra **„**Kiberdrošības pakotni**”.**

Pozīcijas projekts skar vairāku valsts pārvaldes iestāžu kompetenci, tādēļ saskaņā ar Ministru kabineta 2009. gada 6. februāra noteikumu Nr. 96 „Kārtība, kādā izstrādā, saskaņo, apstiprina un aktualizē Latvijas Republikas nacionālās pozīcijas Eiropas Savienības jautājumos” prasībām, nacionālā pozīcija tiek virzīta apstiprināšanai Ministru kabinetā.

2017. gada 13. septembrī EK nāca klajā ar vairākiem priekšlikumiem un iniciatīvām „Kiberdrošības pakotnes” ietvaros Eiropas Savienības (turpmāk – ES) kiberdrošības spēju attīstīšanai. „Kiberdrošības pakotne” ietver:

1) EK paziņojums Eiropas Parlamentam un Padomei „Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību” (JOIN(2017) 450 *final*),

2) EK priekšlikums Eiropas Parlamenta un Padomes regulai par ENISA – Eiropas Kiberdrošības aģentūru – un Regulas (ES) 526/2013 atcelšanu un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju („Kiberdrošības akts”) (COM(2017) 477 *final*),

3) EK ieteikums (ES) 2017/1584 par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm (C(2017) 6100 *final*),

4) EK paziņojums Eiropas Parlamentam un Padomei „TID direktīvas potenciāla maksimāla izmantošana - kā efektīvi īstenot Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā” (COM(2017) 476 *final*).

**1. EK paziņojumi un priekšlikumi**

Paziņojums Eiropas Parlamentam un Padomei „Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību” paredz, ka ES pāriet no reaģējošas pieejas uz proaktīvu pieeju kiberdrošības jautājumiem, lai aizsargātu ES labklājību, sabiedrību un vērtības, kā arī pamatvērtības un pamatbrīvības, reaģējot uz pastāvošajiem un iespējamiem kiberdrošības draudiem. Paziņojums ietver pasākumus, ar kuriem paredzēts attīstīt ES spējas labāk reaģēt uz kiberdrošības draudiem, veicināt ES kiberdrošības noturību un kiberdrošības autonomiju, palielinot ar tehnoloģiju un prasmēm saistītās iespējas. Tāpat ir paredzēts paātrināt kibernoziegumu atklāšanu, izsekošanu un vainīgo saukšanu pie atbildības un sniegt ES dalībvalstīm atbalstu valsts kiberdrošības spēju attīstībai un uzlabošanai.

Priekšlikums Eiropas Parlamenta un Padomes regulai par ENISA – Eiropas Kiberdrošības aģentūru – un Regulas (ES) 526/2013 atcelšanu un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju („Kiberdrošības akts”) ietver divas daļas – regulējumu, kas nodrošinās ES Tīklu un informācijas drošības aģentūrai (ENISA) pastāvīgas darbības pilnvaras un regulējumu vienotam informācijas un komunikācijas tehnoloģiju (turpmāk - IKT) izstrādājumu, preču un pakalpojumu sertifikācijas satvaram Eiropā. Būtiskākā izmaiņas, ko priekšlikums paredz:

1. ENISA palīdzēs ES dalībvalstīm kosekventi īstenot ES politiku un tiesību aktus kiberdrošības jomā, īpaši saistībā ar Tīklu un informācijas drošības direktīvu (turpmāk – NIS direktīva; Direktīva (ES) 2016/1148);
2. ENISA veicinās ES kiberdrošības tirgus izaugsmi, tostarp izstrādājot Eiropas kiberdrošības sertifikācijas shēmas (regulas priekšlikuma 8. pants);
3. ENISA veicinās ES dalībvalstu operatīvo sadarbību kiberdrošības incidentu gadījumā (regulas priekšlikuma 7. pants).

Priekšlikuma daļa regulējumam par vienotu Eiropas kiberdrošības sertifikācijas satvaru paredz ar vispārīgu normu izveidot IKT produktu un pakalpojumu Eiropas kiberdrošības sertifikācijas satvaru (turpmāk – sertifikācijas satvars). Sertifikācijas satvara pametmērķis ir izveidot Eiropas kiberdrošības sertifikācijas shēmas, kas apliecina, ka IKT produkti un pakalpojumi, kas ir sertificēti saskaņā ar šādu shēmu, atbilst noteiktajām prasībām attiecībā uz to spēju noteiktā apliecinājuma līmenī pretoties darbībai, kas veikta nolūkā apdraudēt tādu glabāto, pārsūtīto vai apstrādāto datu vai funkciju, vai pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, ko piedāvā izmantot minētie produkti, procesi, pakalpojumi un sistēmas vai kam, tos izmantojot, var piekļūt (regulas priekšlikuma 43. pants).

Ieteikuma (ES) 2017/1584 par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm mērķis ir vērst dalībvalstu uzmanību uz augošo kiberapdraudējuma risku. Galvenās atbildīgās par reaģēšanu plašapmēra kiberdrošības incidentos vai krīzēs ir ES dalībvalstis, kuras skar incidenti. Ieteikumā EK ir definējusi kiberincidentus, kas uzskatāmi par Savienības mēroga krīzi. Kiberdrošības incidentu var uzskatīt par Savienības mēroga krīzi tad, ja izraisītais traucējums ir tik plašs, ka tā skartā dalībvalsts nespēj viena ar to tikt galā, vai skar divas vai vairāk dalībvalstis tik plašā apmērā un ar tādu tehnisku un politisku nozīmi, ka prasa laicīgu koordinēšanu un reaģēšanu Savienības politiskajā līmenī. Saskaņā ar reaģēšanas plānā norādīto, iestājoties ES mēroga krīzei ar kiberelementiem, reakciju Savienības politiskajā līmenī koordinē ES Padome, izmantojot Integrēto politiskās krīzes reaģēšanas (IPCR) mehānismu. EK koordinācija notiek saskaņā ar ātrās brīdināšanas sistēmu ARGUS. Ja krīzei ir nozīmīga ārējā vai Kopējās drošības un aizsardzības politikas (KDAP) dimensija, tiek aktivizēts Eiropas Ārējās darbības dienesta (EĀDD) mehānisms reaģēšanai krīzes situācijās.

Paziņojuma Eiropas Parlamentam un Padomei „TID direktīvas potenciāla maksimāla izmantošana - kā efektīvi īstenot Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā” pamatā ir EK sagatavošanās darbs un analīze, kas saistīta ar NIS direktīvas līdzšinējo ieviešanu, ENISA sniegto informāciju un pārrunām, kas notikušas ar dalībvalstīm NIS direktīvas pārņemšanas periodā. Paziņojuma pielikuma mērķis ir veicināt NIS direktīvas efektīvu piemērošanu, ieviešanu un izpildi un palīdzēt dalībvalstīm nodrošināt ES tiesību aktu efektīvu piemērošanu. Konkrētāk, tam ir definēti trīs specifiski mērķi:

1) nodrošināt lielāku skaidrību valstu iestādēm par direktīvā iekļautajiem pienākumiem, kas skar šīs iestādes,

2) nodrošināt to direktīvā noteikto pienākumu efektīvu izpildi, kas piemērojami vienībām, kurām ir pienākumi, kas skar drošības prasības un incidentu paziņošanu, un

3) kopumā veicināt juridisko noteiktību visiem iesaistītajiem dalībniekiem.

Diskusijas par priekšlikumiem notiek ES Padomes Horizontālo kiberdrošības jautājumu darba grupā (HWPCI).

**2. Latvijas nostāja**

Latvija kopumā atbalsta EK paziņojuma iniciatīvas, kas paredz plašāku starpnozaru un publiskā un privātā sektora sadarbību ES kiberaizsardzības spēju stiprināšanā un kibernoziedzības apkarošanā, ES kiberdrošības un kiberaizsardzības ietvara stiprināšanu tehniskā līmenī, kā arī kiberdrošības izpratnes palielināšanu sabiedrībā un kiberdrošības ekspertu skaita palielināšanu.

Latvija atbalsta pastāvīgu pilnvaru noteikšanu ENISA un atbalsta vienota Eiropas kiberdrošības sertifikācijas satvara izveidi ar ES regulu, ja šāda regula respektē ES pastāvošo vispārējo atbilstības novērtēšanas sistēmu Regulas (ES) 765/2008 ietvaros.

Latvija piesardzīgi vērtē EK paziņojumā paustās iniciatīvas, kas paredz jaunu institūciju veidošanu ES dalībvalstīs. Rūpīgi jāizvērtē šādu institūciju lietderība un jāizvairās no funkciju dublēšanas ar esošajām institūcijām un iniciatīvām.

Latvija atbalsta EK ieteikums par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm. ES ir būtiska nepieciešamība izveidot ES satvaru reaģēšanai kiberdrošības krīzēs.

EK sagatavojusi analīzi par īstenojamiem pasākumiem NIS direktīvas (Direktīva (ES) 2016/1148) efektīvai pārņemšanai nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību ES. Latvija atbalsta NIS direktīvas (Direktīva (ES) 2016/1148) pilnīgu īstenošanu līdz 2018. gada 9. maijam un pamata pakalpojumu un digitālo pakalpojumu sniedzēju noteikšanu NIS direktīvas ietvaros līdz 2018. gada 9. novembrim.

Detalizēta Latvijas pozīcija ir pieejama Aizsardzības ministrijas sagatavotajā nacionālajā pozīcijā par 2017. gada 13. septembra EK „Kiberdrošības pakotni”.

Aizsardzības ministra vietā

Iekšlietu ministrs R. Kozlovskis