Satversmes aizsardzības birojs

A/K 286, Rīga, LV-1001, tālr. 67025407, fakss 67025406, e-pasts pasts@sab.gov.lv

Aizsardzības ministrijai

Kopija:
Tieslietu ministrijai

2022. gada 15. decembrī
Nr.5.2-10/22/655
Uz 06.12.2022. Nr. MV-N/2484

Par 22-TA-3012

Satversmes aizsardzības birojs ir iepazinies ar Aizsardzības ministrijas izstrādāto likumprojektu "Nacionālās kiberdrošības likums" (turpmāk - likumprojekts) un informē, ka atbalsta tā tālāku virzību, vienlaikus izsakot šādus **iebildumus**:

1) svītrot likumprojekta 8. panta trešo daļu un izteikt likumprojekta 13. pantu šādā redakcijā:
"13. pants. Aizsardzības ministrijas, Satversmes aizsardzības biroja un kiberincidentu novēršanas institūciju sadarbība
(1) Aizsardzības ministrija un Satversmes aizsardzības birojs regulāri savstarpēji apmainās ar informāciju par aktualitātēm subjektu uzraudzībā.
(2) CERT.LV informē MilCERT par savā rīcībā esošo informāciju par kiberincidentiem Aizsardzības ministrijā, tās padotībā esošajās iestādēs un Nacionālajos bruņotajos spēkos.
(3) MilCERT sniedz informāciju CERT.LV, lai tas nodrošinātu šā likuma 11. panta pirmās daļas 3. punktā noteikto uzdevumu īstenošanu, kā arī citu tā rīcībā esošo informāciju par CERT.LV kompetencē esošajiem kiberincidentiem.
(4) Aizsardzības ministrija, Satversmes aizsardzības birojs un kiberincidentu novēršanas institūcijas sadarbojas un regulāri savstarpēji apmainās ar informāciju par aktualitātēm kiberincidentu jomā.";
2) izteikt likumprojekta 7. panta trešās daļas pirmo teikumu šādā redakcijā: "Šī panta pirmās daļas 1. un 2. punktā minētās tiesības Aizsardzības ministrija īsteno tikai attiecībā uz tiem būtisko pakalpojumu sniedzējiem un svarīgo pakalpojumu sniedzējiem, kuri nav informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieki vai tiesiskie valdītāji.";

3) izteikt likumprojekta 22. panta ceturtās daļas otro teikumu šādā redakcijā: "Ārēju auditu veic Ministru kabineta noteiktajām prasībām atbilstošs un noteiktajā kartībā saskaņots tiesību subjekts.";
4) izteikt likumprojekta 27. pantu šādā redakcijā:
"27. pants. Par kiberdrošību atbildīgā persona
(1) Šī likuma 4. pantā minēto subjektu kiberdrošības pārvaldību nodrošina un par to atbild attiecīgā subjekta vadītājs. Katra subjekta vadītājs nosaka atbildīgo personu, kura īsteno kiberdrošības pārvaldību attiecīgajā subjektā (turpmāk – par kiberdrošību atbildīgā persona). Ministru kabinets nosaka par kiberdrošību atbildīgajai personai izvirzītās prasības.
(2) Informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs nosaka par kiberdrošību atbildīgo personu pēc saskaņošanas ar Satversmes aizsardzības biroju.
(3) Par kiberdrošību atbildīgajai personai ir šādi pienākumi:
1) organizēt institūcijas informācijas un komunikācijas tehnoloģiju infrastruktūras drošības pasākumus;
2) ne retāk kā reizi gadā veikt informācijas un komunikācijas tehnoloģiju drošības pārbaudi un atbilstoši tās rezultātiem organizēt konstatēto trūkumu novēršanu;
3) vismaz reizi gadā apmeklēt kiberincidentu novēršanas institūcijas organizētu apmācību kiberdrošības jautājumos;
4) ne retāk kā reizi gadā veikt institūcijas darbinieku instruktāžu par aktuālajiem kiberriskiem un kiberdrošību.
(4) Subjekts par kiberdrošību atbildīgās personas noteikšanu ne vēlāk kā piecu darbdienu laikā informē Nacionālo kiberdrošības centru, Satversmes aizsardzības biroju un kompetento kiberincidentu novēršanas institūciju.".

Papildus, Satversmes aizsardzības birojs izsaka šādus **priekšlikumus**:

1) svītrot likumprojekta 21. pantu, izsakot likumprojekta 24. pantu šādā redakcijā:
"24. pants. Subjektu pienākumi
(1) Subjektiem ir šādi pienākumi:
1) veikt piemērotus un samērīgus tehniskus un organizatoriskus pasākumus, lai atbilstīgi novērtētu un pārvarētu kiberapdraudējumus;
2) izstrādāt kiberrisku pārvaldības un darbības nepārtrauktības nodrošināšanas plānu;
3) nodrošināt darbiniekiem regulāras apmācības efektīvai šī panta pirmās daļas 2. punktā minētajā plānā iekļauto pasākumu īstenošanai;
4) nozīmīga kiberapdraudējuma gadījumā informēt informācijas un komunikācijas tehnoloģiju tīkla, sistēmas vai pakalpojuma galalietotājus, kurus šāds apdraudējums varētu skart, kā arī informēt par iespējamajiem kiberdrošības pasākumiem vai līdzekļiem, ko galalietotāji

var izmantot. Vajadzības gadījumā subjekts informē galalietotāju arī par pašu kiberapdraudējumu;

5) pēc kompetentās kiberincidentu novēršanas institūcijas vai Nacionālā kiberdrošības centra pieprasījuma ne ilgāk kā uz piecām dienām slēgt galalietotājam piekļuvi elektronisko sakaru tīklam, ja galalietotājs būtiski apdraud citu lietotāju tiesības vai elektronisko sakaru tīkla, informācijas sistēmas vai pakalpojuma drošību. Pieprasījumā norāda kiberapdraudējumu, piekļuves ierobežojuma ilgumu un, ja nepieciešams, citas papildu darbības, kas veicamas subjektam (piemēram, datu plūsmas pārvirzīšana uz kompetentās kiberincidentu novēršanas institūcijas infrastruktūru).

(2) Ministru kabinets nosaka šī panta pirmās daļas 2. punktā minētajā plānā ietveramās informācijas kopumu, plāna izpildes kontroles kārtību, kā arī kārtību, kādā galalietotājam tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam.";

2) svītrot likumprojekta 25. panta pirmajā daļā vārdu "kopumu";

3) izteikt likumprojekta 32. pantu šādā redakcijā:

"32. pants. Agrās brīdināšanas sensori

Ministru kabinets nosaka kritērijus kiberdrošības agrās brīdināšanas sensoru obligātai uzstādīšanai valsts un pašvaldību institūcijās, un informācijas un komunikācijas tehnoloģiju kritiskajā infrastruktūrā.";

4) papildināt likumprojekta 36. pantu ar piekto daļu šādā redakcijā:

"(5) Pirms šī panta pirmajā daļā minētā lēmuma pieņemšanas Nacionālais kiberdrošības centrs informē Satversmes aizsardzības biroju.". Satversmes aizsardzības biroja ieskatā pirms 36. panta pirmajā daļā minētā lēmuma pieņemšanas ir nepieciešama informācijas apmaiņa, jo pastāv varbūtība, ka attiecībā uz notiekošo kiberincidentu tiek veiktas operatīvās darbības un konkrētajā brīdī to pārtraukšana būtu nevēlama, vai nacionālās drošības interesēs ir nepieciešams iegūt informāciju par kiberincidenta avotu, kas pēc iepriekšminētā lēmuma pieņemšanas var būt apgrūtināta, ja ne neiespējama;

5) iekļaut likumprojektā pantu par rīcību kiberdrošības nepilnības konstatēšanas gadījumā. Likumprojekta versijā, kas tika izplatīta publiskai apspriešanai šāds pants (pēc tā brīža numerācijas 37. pants) bija iekļauts un nav saprotama tā svītrošana no likumprojekta teksta.

Direktors E.Zviedris

ŠIS DOKUMENTS PARAKSTĪTS AR DROŠU ELEKTRONISKO PARAKSTU UN SATUR LAIKA ZĪMOGU