Aizsardzības ministrija

NIS2 direktīva un Nacionālās kiberdrošības likums – kas mūs sagaida tuvākajos gados?

Edgars Kiukucāns
Kiberdrošības politikas departamenta direktors
Edgars.Kiukucans@mod.gov.lv

Aizsardzības ministrija

NIS2 direktīva

Direktīvas mērķis

nodrošināt vienādi augstu kiberdrošības līmeni visā Eiropas Savienībā

Atbilstības un ziņošanas pienākumi

Saskaņota kiberrisku pārvaldība

Direktīvas subjektu uzraudzība

Aizsardzības ministrija

NIS 2 direktīvas subjektu loks

NIS 1 saistošie sektori


Enerģētika


Veselības aprūpe


Transports


Dzeramais ūdens


Banku pakalpojumi


Notekūdeņi


Finanšu tirgus infrastruktūra

Digitālā infrastruktūra

Jauni sektori


Digitālie pakalpojumi


Ķimikālijas


Kosmoss


Pārtikas ražošana


Pasts


Industriālā ražošana


Kurjeru pakalpojumi

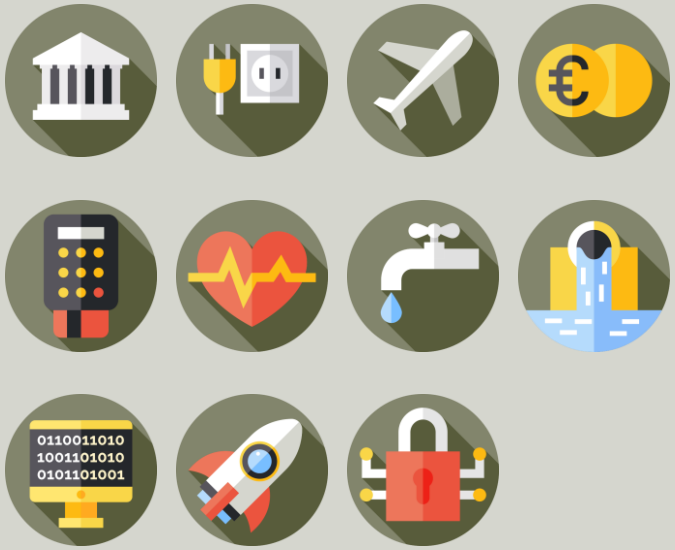

Atkritumu apsaimniekošana

Aizsardzības ministrija

NKDL subjekti

18. pants

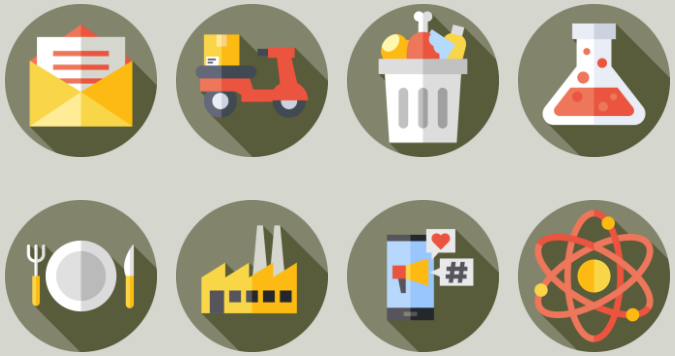
Būtisko pakalpojumu sniedzēji



+

19. pants

Svarīgo pakalpojumu sniedzēji



+

22. pants

Kritiskā IKT infrastruktūra

saskaņā ar Nacionālās drošības likumu

valsts un pašvaldību iestādes + lielie un vidējie uzņēmumi

Aizsardzības ministrija

NKDL subjekti

Pilns subjektu saraksts ir pieejams likumprojekta "Nacionālās kiberdrošības likums" aktuālajā redakcijā

Likumprojekts ir atrodams Saeimas likumdošanas datubāzē https://titania.saeima.lv/, sadaļā "Likumprojekti", meklējot pēc numura 553/Lp14 vai nosaukuma "Nacionālās kiberdrošības likums"

Aizsardzības ministrija

Nacionālās kiberdrošības likums

Galvenās izmaiņās, salīdzinot ar IT drošības likumu

Nacionālais kiberdrošības centrs
Statuss, funkcijas, tiesības un pienākumi; precizētas AM un CERT.LV funkcijas

NIS2 direktīvas normas
Subjekti, koordinēta ievainojamību atklāšana, uzraudzība, sodīšana

DDoS aizsardzība
Valsts IT resursu un infrastruktūras aizsardzības noteikumi pret pakalpojumatteices uzbrukumiem

Koplietošanas datu centri
Deleģējums MK noteikt drošības prasības; drošības operāciju centru (SOC) izveide

Kiberkrīžu plāns
Noteikumi par nacionālo kiberdrošības krīžu vadības plānu

Aizsardzības ministrija

Galvenās prasības subjektiem

Statusa noteikšana un reģistrācija

Kiberdrošības pārvaldnieka noteikšana

Minimālo kiberdrošības prasību ievērošana

Risku pārvaldības un darbības nepārtrauktības plāns

Ziņošana par incidentiem un ievainojamībām

Ikgadējs pašnovērtējuma ziņojums

Aizsardzības ministrija

Pakārtotie MK noteikumi

Noteikumi par minimālajām kiberdrošības prasībām

Kiberhigiēnas vadlīnijas valsts un pašvaldību institūcijām

Datu centru pakalpojumu drošības prasības

Prasības kiberincidentu novēršanas institūcijām

Centralizētās DDoS aizsardzības noteikumi

Aizsardzības ministrija

Noteikumi par minimālajām prasībām

MK noteikumi Nr.442, Nr.100, Nr.15, Nr.43, Nr.327

- Minimālās prasības subjektiem
- Prasības IKT KI
- Prasības kiberdrošības pārvaldniekam
- Kiberrisku pārvaldības un darbības nepārtrauktības plāns
- Agrās brīdināšanas sensori
- Incidentu nozīmīguma kritēriji

- Prasības kiberdrošības auditoriem
- Drošības skenēšana
- Elektronisko sakaru tīklu drošības prasības
- Incidentu ziņošanas kārtība
- Piekļuves slēgšana elektronisko sakaru tīklam
- Pašnovērtējuma ziņojums

NIS2 + nacionālās prasības

Aizsardzības ministrija

Noteikumi par minimālajām prasībām

- Fokuss uz subjektu kiberdrošību kopumā (nevis informācijas sistēmām, kā MK442)
- Mazāk specifisko prasību (piem., paroļu garums), uzsvars uz labu kiberpārvaldību
- Konsolidētas dokumentācijas prasības (politika + katalogs + plāns + žurnāls)
- Prasības aptver visus piecus NIST soļus (Identify, Protect, Detect, Respond, Recover)
- Ņemti vērā nozares ekspertu komentāri
- Prasības salāgotas ar ISO:27001 standartu

Kiberdrošības politika

Kiberincidentu un ievainojamību žurnāls

Resursu un informācijas sistēmu katalogs

Risku pārvaldības un darbības nepārtrauktības plāns

Aizsardzības ministrija

Kāda informācija jāiesniedz subjektam?

Subjekta statusa atbilstības paziņojums

līdz 01.04.2025

Informācija par kiberdrošības pārvaldnieku

līdz 01.07.2025

Pirmreizējs pašnovērtējuma ziņojums

līdz 01.07.2025

Aizsardzības ministrija

Subjektu uzraudzība

Uzraudzības iestādes (NKDC un SAB) būs tiesīgas veikt subjektu dokumentu un IKT infrastruktūras pārbaudes un vajadzības gadījumā izteikt subjektam brīdinājumu vai uzdot:

- novērst konstatētās neatbilstības,
- veikt ārēju auditu,
- informēt pakalpojumu saņēmējus par kiberapdraudējumu.

Ja minētie pasākumi nebūs efektīvi, uzraudzības iestādes būs tiesīgas:

- apturēt informācijas sistēmas, resursa vai e-pakalpojuma darbību līdz neatbilstību novēršanai,
- apturēt produkta tirdzniecību vai pakalpojuma sniegšanu līdz neatbilstību novēršanai,
- noteikt pagaidu aizliegumu subjekta vadītājam pildīt pienākumus līdz neatbilstību novēršanai.

Aizsardzības ministrija

Sankcijas par prasību neievērošanu

VALSTS UN PAŠVALDĪBU INSTITŪCIJAS

Ziņošana amatpersonai, kura lemj par disciplinārsoda piemērošanu

PRIVĀTO TIESĪBU JURIDISKĀS PERSONAS

Administratīvā akta piespiedu izpilde, piemērojot piespiedu naudu

par valsts institūcijām	par pašvaldību institūcijām	būtisko pakalpojumu sniedzējiem un IKT KI	svarīgo pakalpojumu sniedzējiem
ziņo atbildīgajam Ministru kabineta loceklim un informē Ministru kabinetu	ziņo pašvaldības domes priekšsēdētājam un informē VARAM	līdz 10 miljoniem eiro vai līdz 2% no kopējā gada apgrozījuma pasaulē	līdz 7 miljoniem eiro vai līdz 1,4 % no kopējā gada apgrozījuma pasaulē

Aizsardzības ministrija

Par ko būs jādomā pašiem?

- **Kā nodrošināt savas IKT infrastruktūras un informācijas sistēmu atbilstību jaunajām minimālajām kiberdrošības prasībām?**
- **Kā plānot un īstenot kiberrisku pārvaldības pasākumus, kā nodrošināt darbības nepārtrauktību krīzes situācijā?**
- **Kā veicināt kiberhigiēnas ievērošanu un personāla apmācību kiberdrošības jautājumos?**

Aizsardzības ministrija

Tālākais darbs

NIS2 direktīvas ieviešana

- Likumprojekts ir iesniegts Ministru kabinetā
- Apstiprināšana Saeimā – 2024.gadā II. ceturksnis
- Saistīto MK noteikumu nodošana sabiedrības līdzdalībai TAP portālā – 2024. gada II. ceturksnis
- Darbs pie NIS2 ieviešanas jānoslēdz 2024. gada 17. oktobrī

NKDL subjektiem

Pēc likuma pieņemšanas – sektorāli informatīvie semināri par jaunajām prasībām

Reģistrācija (būtiskā vai svarīgā vienība), kiberdrošības pārvaldnieka paziņošana

Pašnovērtējuma anketas aizpildīšana un iesniegšana (NKDC vai SAB)

Aizsardzības ministrija

Finanšu atbalsta iespējas

ES programma "Digitālā Eiropa"

Tiešie granti
Aicinām sekot līdzi aktuālajai informācijai Eiropas Komisijas Funding & Tenders portālā
ec.europa.eu/info/funding-tenders/opportunities/portal/

Kaskādes granti
Eiropas Kiberdrošības kompetenču centra 2021-2027. gada plānošanas perioda grantu vadības likums

- Nacionālais koordinācijas centrs (NCC-LV)
- kiberdrošības kompetenču kopiena

Aicinām sekot līdzi informācijai www.cfla.gov.lv

"**Digitālās Eiropas**" kaskādes grantu projektu uzsaukums atvērts no 14. marta līdz 14. maijam

Līdz **60 000** eiro (50%) inovatīvu kiberdrošības risinājumu izstrādei un ieviešanai

Tiks atbalstīti **mazie un vidējie uzņēmumi**

Aizsardzības ministrija

Kiberdrošības kompetenču kopiena

Pašlaik kopienā ir

43 organizācijas

- valsts un pašvaldību iestādes,
- augstskolas,
- mazie, vidējie un lielie komersanti,
- nozares NVO

Kopienu var veidot

- tiešās un pastarpinātās pārvaldes iestādes,
- citas valsts institūcijas,
- atvasinātas publiskas personas,
- privāto tiesību juridiskās personas,
- tiesībspējīgas personālsabiedrības

Jautājumi?

- sazinies ar NCC-LV sekretariātu

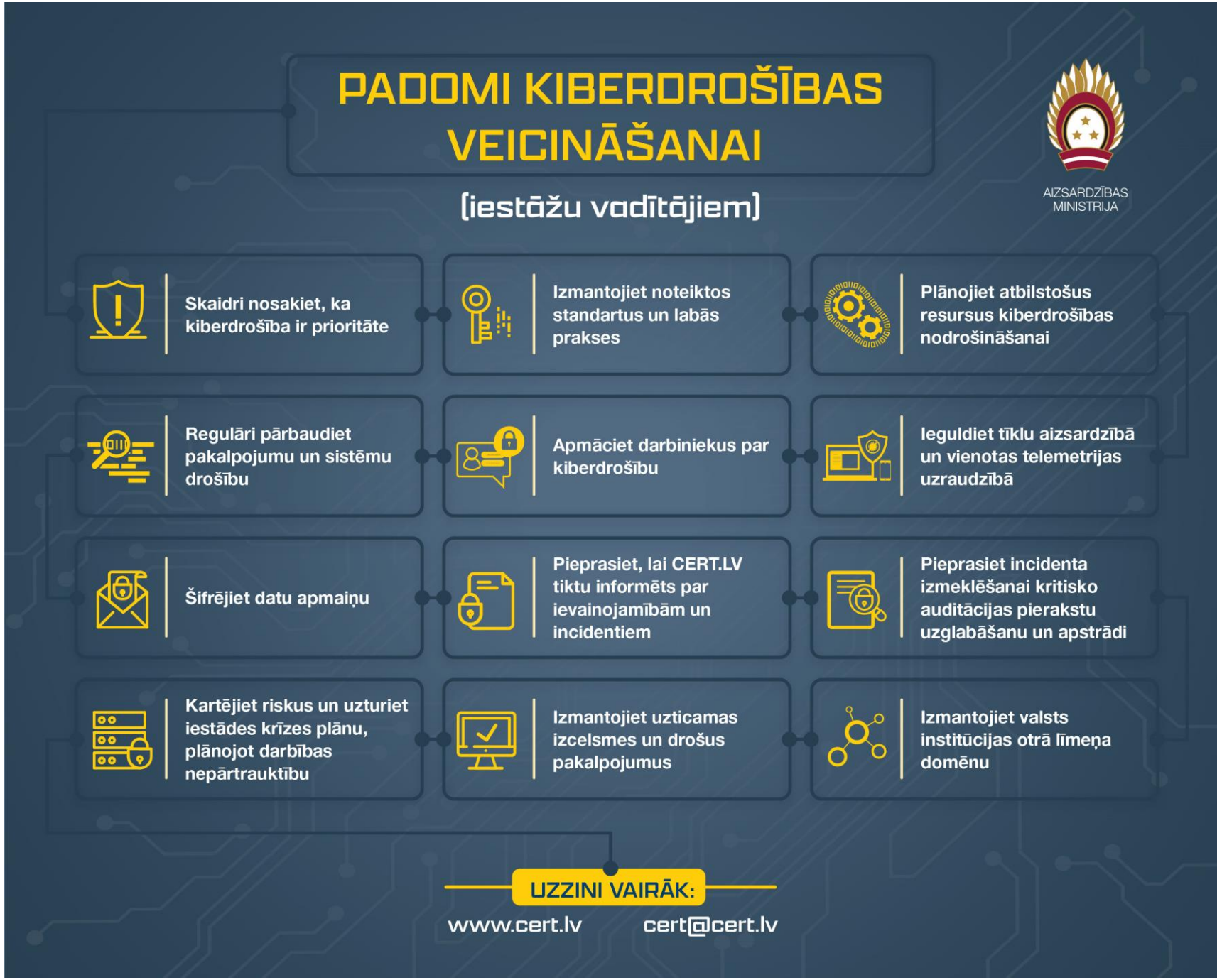
NCC@mod.gov.lv

6733 5352

Prasības dalībniekiem

- jāspēj sniegt ieguldījums ECCC un NCC-LV tīkla pamatuzdevumā
- jābūt kiberdrošības lietpratībai vismaz vienā no Regulā 2021/887 minētajām jomām

Aizsardzības ministrija



Aizsardzības ministrija

Paldies par uzmanību!

NIS2@mod.gov.lv