Aizsardzības ministrija

Jaunās likumdošanas iniciatīvas kiberdrošības jomā

Edgars Kiukucāns
Kiberdrošības politikas departamenta direktors

2023. gada 30. martā

Aizsardzības ministrija

Kiberdrošības pārvaldības reforma #1
Izaicinājumi

Nevienmērīgs kiberdrošības līmenis valsts pārvaldē

Jaunas funkcijas, kas izriet no ES normatīvajiem aktiem un inicitatīvām

Grūtības piesaistīt un noturēt kvalificētu personālu AM un CERT.LV

Aizsardzības ministrija

Kiberdrošības pārvaldības reforma #2
Risinājumi

Nacionālā kiberdrošības centra izveide un attīstība

Valsts informācijas sistēmu drošības prasību izvērtēšana

NIS2 direktīvas/Nacionālās kiberdrošības likuma īstenošanas uzraudzība

Kompetenču centri un datu centru klasifikācija atbilstoši drošības prasībām

SOC centri (*Security Operations Centers*) kompetenču centros

Personāla piesaiste un konkurētspējīgs atalgojums

Aizsardzības ministrija

Nacionālais kiberdrošības likums (NKDL) I

NKDL tiks noteikts normatīvais regulējums attiecībā uz: kiberdrošību atbildīgajām institūcijām; NKDL subjektu identifikāciju un to uzskaiti; NKDL subjektu kiberdrošības pārvaldību; rīcību kiberincidenta gadījumā; koordinētu ievainojamību atklāšanu un novēršanu; subjektu uzraudzību; nacionālās kiberdrošības stratēģijas izstrādi.

NIS1 direktīvas saistošie sektori
Enerģētika
Transports
Banku darbība, finanšu tirgus infrastruktūra, veselības aprūpe
Dzeramais ūdens, notekūdeņi (gadījumā, ja tā ir galvenā darbība)
Digitālā infrastruktūra

NIS2 direktīvas saistošie sektori
Digitālie pakalpojumi (meklētājprogrammas, tiešsaistes tirgi, sociālie tīkli)
Kosmoss
Pasta un kurjeru pakalpojumi
Atkritumu apsaimniekošana
Ķimikālijas (ražošana un izplatīšana)
Pārtika (ražošana, pārstrāde un izplatīšana)
Ražošana

Aizsardzības ministrija

Būtiskie un svarīgie pakalpojumu sniedzēji

To, vai pakalpojumu sniedzējs ir svarīgs vai būtisks, nosaka nozare, kurā tas darbojas:

Būtiskās nozares (NKDL 16. pants)
Enerģētika
Transports
Banku darbība, finanšu tirgus infrastruktūra, veselības aprūpe
Dzeramais ūdens, notekūdeņi (gadījumā, ja tā ir galvenā darbība)
Digitālā infrastruktūra
IKT pakalpojumu pārvaldība
Valsts pārvalde
Kosmoss

Svarīgās nozares (NKDL 17. pants)
Pasta un kurjeru pakalpojumi
Atkritumu apsaimniekošana
Ķimikāliju izgatavošana, ražošana un izplatīšana
Pārtikas ražošana, pārstrāde un izplatīšana
Ražošana
Digitālo pakalpojumu sniedzēji
Pētniecība

Aizsardzības ministrija

Nacionālais kiberdrošības likums (NKDL) II

NKDL subjekti:

- **NKDL attiecas uz būtisko un svarīgo pakalpojumu sniedzējiem, kā arī informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem.**

Būtiskākās NKDL izmaiņas pret ITDL:

1) tiek izveidots Nacionālais kiberdrošības centrs;

2) likumprojekts papildināts ar normām, kas izriet no NIS2 direktīvas, tostarp, nosakot subjektus, paredzot koordinētu ievainojamību atklāšanu, uzraudzības mehānismus un sodīšanu;

3) iekļautas tiesību normas, kas regulē:

   1) IKT resursu aizsardzību **pret pakalpojumatteices (Ddos)** uzbrukumiem;

   2) koplietošanas datu centru kiberdrošību;

   3) vienotā valsts interneta apmaiņas punkta **(GLV-IX) pakalpojumu** nodrošināšanu;

   4) kiberkrīžu pārvaldības plānu izstrādi un koordinēšanu, kā to nosaka NIS2 direktīva;

4) NKDL, atšķirībā no ITDL, izdala atsevišķi subjekta rīcību kiberincidenta gadījumā (ITDL – drošības incidenti; NKDL – kiberincidenti).

Aizsardzības ministrija

Nacionālais kiberdrošības likums (NKDL) III

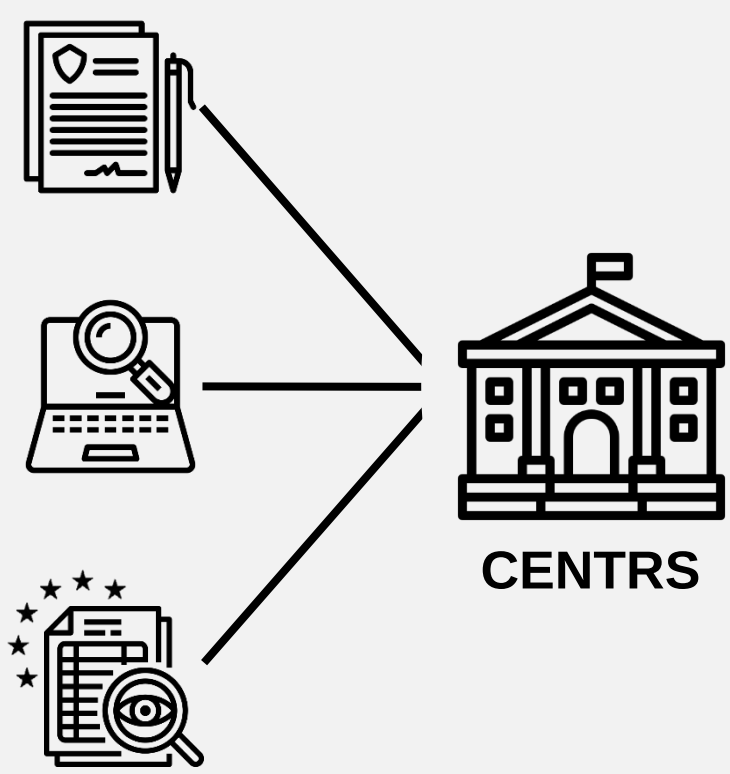
<u>Līdz 2023. gada 1. oktobrim MK izdod noteikumus, kas noteiks:</u>

- IKT **kritiskās infrastruktūras drošības pasākumus** un to plānošanas un īstenošanas kārtību;
- **Kiberrisku pārvaldības plānā** iekļaujamās informācijas kopumu;
- **minimālās kiberdrošības prasības** subjektiem un kārtību, kādā subjekti nodrošina savu IKT sistēmu atbilstību minimālajām kiberdrošības prasībām, kā arī prasības un veicamos pasākumus subjektu informācijas sistēmu pieejamības, autentiskuma, integritātes vai konfidencialitātes nodrošināšanai un datu atjaunošanai;
- NKDL subjekta **darbības nepārtrauktības plānā obligāti iekļaujamās informācijas veidu un apjomu**, kā arī plāna izpildes kontroles kārtību;
- **datu centru drošības prasības**, atbilstības novērtēšanas, reģistrācijas un uzraudzības kārtību, kā arī datu centra uzturētāja pienākumus;
- kiberdrošības operāciju centru **(SOC) izveides un darbības noteikumus** datu centros.

<u>Līdz 2024. gada 1. janvārim MK izdod noteikumus, kas noteiks:</u>

- Prasības un kārtību IKT infrastruktūras un interneta resursu **aizsardzībai pret pakalpojumatteices (DDoS)** uzbrukumiem;
- kiberhigiēnas pasākumu pamatelementus un **prasības kiberhigiēnas pasākumu īstenošanai** (valsts un pašvaldību institūcijām).

Nacionālā kiberdrošības centra izveide un funkcijas



Aizsardzības ministrija

Kiberdrošības stratēģija 2023-2026

Attēls: Pixabay

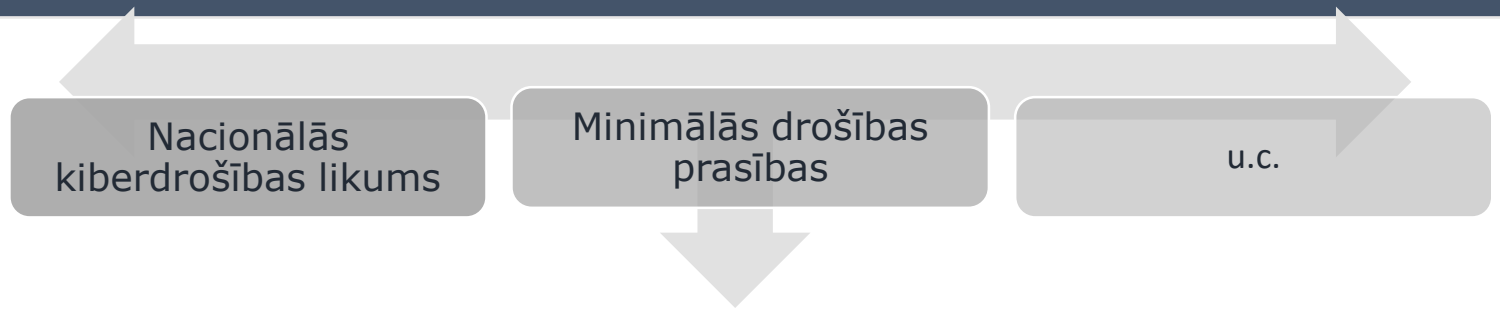
- **<u>Lielie virzieni nemainīgi</u>**:
  - Kiberdrošības pārvaldības pilnveidošana,
  - Kiberdrošības veicināšana un izturētspējas stiprināšana
  - Sabiedrības izpratne, izglītība un pētniecība
  - Starptautiskā sadarbība un tiesiskums kibertelpā,
  - Kibernoziedzības novēršana un apkarošana.
- **<u>Galvenie jaunie elementi</u>**:
  - Jaunais pārvaldības modelis
  - Publiskā-privātā sektora sadarbības uzlabošana
  - Vienotas kiberhigiēnas vadlīnijas
  - Kiberdrošības pratības veicināšana, izglītošanas veicināšana
  - Plašāka kiberelementu izspēle teorētiskās un praktiskās mācībās

Aizsardzības ministrija

2023. gada prioritātes

Nacionālā kiberdrošības centra izveide

NIS2 direktīvas pārņemšana (direktīva par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā)



Kiberdrošības stratēģijas 2023.-2026. gadam ieviešanas uzsākšana

Aizsardzības ministrija

Ar ES saistītās aktualitātes 2023. gadam – Kiberdrošības noturības akts

- ieviesīs **obligātas kiberdrošības prasības produktiem ar digitāliem elementiem** visā to aprites ciklā;
- noteiks kiberdrošības prasības produktiem ar digitāliem elementiem, izvietojot tos tirgū, t.sk. atbilstības novērtēšanas un paziņošanas procesus, pamatprasības par ievainojamību novēršanas procesiem, noteikumus par tirgus uzraudzību un iepriekš minēto noteikumu un prasību izpildes panākšanu;

Aizsardzības ministrija

Ar ES saistītās aktualitātes 2023. gadam – Digitālā Eiropa

Programma "Digitālā Eiropa" (DEP):

- DEP ir jauna ES programma, lai paātrinātu digitālo pārveidi uzņēmumiem, publiskajam sektoram un plašākai sabiedrībai.
- Š.g. 15. februārī noslēdzās DEP uzsaukums, kas paredzēts Nacionālo koordinācijas centru tīklam, kurā piedalījās arī Latvijas Nacionālais koordinācijas centrs (NCC-LV) iesniedzot projektu;
- ieviešanas uzsākšana ir gaidāma ar 2023. gada trešo ceturksni;
- Finansiālā atbalsta programma trešajām personām, kuras mērķis ir **veicināt inovatīvu kiberdrošības risinājumu ieviešanu un izplatīšanu mazos un vidējos uzņēmumos (MVU),** atvieglojot to kiberdrošības pārveidi.

!! NCC-LV aicina ar kiberdrošību saistīto industriju, akadēmiskās un pētniecības organizācijas, kā arī citas attiecīgas pilsoniskās sabiedrības apvienības reģistrēties NCC-LV kiberdrošības kopetences kopienā.

Vairāk info: https://www.mod.gov.lv/lv/nozares-politika/kiberdrosiba/eccc-nacionalais-koordinacijas-centrs

E-pasts: NCC@mod.gov.lv

Aizsardzības ministrija

Paldies!

Prezentācijā izmantoti attēli, kas izgūti no www.flaticon.com