NKDL un Minimālas kiberdrošības prasības

Kristiāns Teters

15.04.2025.

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

NKDL un Minimālas kiberdrošības prasības

- **NKDL**

Stājās spēkā 01.09.

- **Minimālas kiberdrošības Prasības**

Skaņošanas fāzē.

LIKUMI

Izdevējs: Saeima
Veids: likums
Pieņemts: 20.06.2024.
Stājas spēkā: 01.09.2024.

Publicēts:
Latvijas Vēstnesis, 128A, 04.07.2024.
OP numurs: 2024/128A.1

Saeima ir pieņēmusi un Valsts prezidents izsludina šādu likumu:

Nacionālās kiberdrošības likums

I nodaļa
Vispārīgie noteikumi

1. pants. Likumā lietotie termini

Likumā ir lietoti šādi termini:

1) **augstākā līmeņa domēnu nosaukumu reģistra uzturētājs** — institūcija, kam deleģēts konkrēts augstākā līmeņa domēns un kas atbild par šā augstākā līmeņa domēna pārvaldību, tai skaitā veic domēnu nosaukumu reģistrāciju šajā augstākā līmeņa domēnā un nodrošina augstākā līmeņa domēna tehnisko darbību, kā arī tā nosaukumu serveru darbību, datubāzu uzturēšanu un augstākā līmeņa domēna zonas datņu sadalīšanu starp nosaukumu serveriem neatkarīgi no tā, vai kādu no minētajām darbībām veic pati institūcija, izņemot situācijas, kad tā augstākā līmeņa domēnu nosaukumus izmanto tikai savām vajadzībām, vai veic ārpakalpojuma sniedzējs;

Subjekta kalendārs

Minimālas kiberdrošības prasības

- **Vispārīgie jautājumi**
- **Statusa paziņošanas kārtība**
- **Pamatprasības subjektiem**
  - **Kiberdrošības pārvaldnieks**
  - **Kiberdrošības pārvaldības dokumentācija**
  - **Kiberdrošības politika**
  - **IKT resursu un informācijas sistēmu katalogs**
  - **Kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns**
  - **Kiberincidentu pārvaldība un kiberincidentu žurnāls**
  - **Lietotāju un piekļuves tiesību pārvaldība**
  - **Tīklu pārvaldība**
  - **Žurnālfailu pārvaldība**
  - **Rezerves kopiju pārvaldība**
  - **Kiberhigiēnas pasākumi**
  - **Šifrēšanas prasības**
- **Ārpakalpojumu prasības**
  - **Vispārīgās ārpakalpojumu prasības**
  - **Īpašās ārpakalpojumu prasības IKT kritiskajai infrastruktūrai**
  - **Īpašās ārpakalpojumu prasības būtisko pakalpojumu sniedzējiem**
- **Papildu prasības IKT kritiskajai infrastruktūrai**
- **Papildu prasības kiberincidentu novēršanas institūcijām**
- **Kiberincidentu vadība**
- **Subjektu kiberdrošības uzraudzība**
  - Atbilstības audits
  - Ielaušanās testi un drošības skenēšana
  - Pašvērtējuma ziņojums
  - Neatbilstību novēršana valsts un pašvaldību institūcijās
  - Piekļuves slēgšana elektronisko sakaru tīklam
- **Noslēguma jautājumi**

Prasības Kiberdrošības pārvaldniekiem

IKT kritiskā infrastruktūra	Būtisko pakalpojumu sniedzējs	Svarīgo pakalpojumu sniedzējs
• Spēkā esošs, starptautiski atzīts sertifikāts (piem., CISM, CISSP) **vai** • Vidējā profesionālā vai augstākā izglītība kiberdrošības pārvaldībā vai saistītā jomā **un** vismaz 2 gadu darba pieredze kiberdrošības pārvaldībā, kas iegūta pēdējo 5 gadu laikā	• Spēkā esošs, starptautiski atzīts sertifikāts (piem., CISM, CISSP) **vai** • Vidējā profesionālā vai augstākā izglītība kiberdrošības pārvaldībā vai saistītā jomā **vai** • Vismaz 2 gadu darba pieredze kiberdrošības pārvaldībā, kas iegūta pēdējo 5 gadu laikā	• Spēkā esošs, starptautiski atzīts sertifikāts (piem., CISM, CISSP) **vai** • Vidējā profesionālā vai augstākā izglītība kiberdrošības pārvaldībā vai saistītā jomā **vai** • Vismaz 2 gadu darba pieredze kiberdrošības pārvaldībā

Dokumentācijas prasības

- **Kiberdrošības politika**
- **Kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns**
- **Resursu un IS katalogs**
- **Kiberincidentu žurnāls**

Kiberincidentu ziņošana

- **Kiberincidenta gadījumā**

Ziņo CERT.LV

- **Nozīmīga kiberincidenta gadījumā**

Specifiskas ziņojuma (sākotnējā, progresa un gala ziņojuma formas)

Pašnovērtējuma anketa

Iekļaujama informācija par subjekta :

- **Kiberdrošības politiku**
- **Resursu katalogu**
- **Kiberdrošības pārvaldnieku**
- **Kiberrisku pārvaldības plānu**
- **Lietotāju tiesību pārvaldību**
- **Kiberdrošības incidentu uzskaiti.**
- **Utt.**

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.

CERT.LV pakalpojumi

Pieejami gan Pašvaldībām, gan citiem NKDL subjektiem.

	CERT.LV nodrošinātie pakalpojumi	Nacionālās kiberdrošības likuma subjekti	Valsts un pašvaldību iestādes	Pārējie
1	Kiberdrošības incidentu risināšana un diennakts atbalsts	✓	✓	✓
2	Koordinēta ievainojamību atklāšana	✓	✓	✓
3	Pikšķerēšanas uzbrukumu simulācija	✓	✓	✗
4	Kiberapdraudējumu simulācija	✓	✓	✗
5	**DNS ugunsmūris**			
5.1.	DNS ugunsmūra pakalpojums ikvienam Latvijas iedzīvotājam un uzņēmumam	✓	✓	✓
5.2.	DNS ugunsmūra pakalpojums ar RPZ tehnoloģiju tiem, kas paši uztur savus DNS rekursīvos serverus	✓	✓	✓
6	Informācijas tehnoloģiju drošības apdraudējumu agrās brīdināšanas sistēma	✓	✓	✓*
7	Sabiedrības izglītošana – lekcijas un dalība pasākumos	✓	✓	✓
8	Latvijas kiberdrošības kopienas ziņapmaiņas platforma	✓	✓	✓
9	NTP laika serveris	✓	✓	✓
10	CERT.LV MISP - ar ļaunatūru saistītās informācijas apmaiņas platforma	✓	✓	✓**
11	Kiberdrošības draudu medības	✓	✓	✓**
12	Drošības operāciju centrs (SOC)	✓	✓	✓**
13	Industriālās automatizācijas un vadības sistēmu drošības laboratorijas pakalpojums	✓	✗	✗
14	IT sistēmu drošības testi	✓	✓	✓*


CERT.LV
Sakārtota kiberdrošības vide, mazāk incidentu.
certlv
certlv