



**Nacionālais
kiberdrošības
centrs**

IDENTIFICĒ - AIZSARGĀ - ATKLĀJ - REAĢĒ - ATJAUNOJIES



Kiberdrošības pārvaldība un galvenie kontroles pasākumi

1.

Kiberdrošības pārvaldība un atbildība

Iecel kiberdrošības pārvaldnieku un nodrošini pārvaldības struktūru, pienākumu un atbildības sadali, budžetu, rezerves un tehniskos līdzekļus drošībai.

2.

Kritisko funkciju un resursu identifikēšana

Nosaki kritiskos pakalpojumus un resursus, veic ietekmes un atkarību analīzi.

3.

Resursu uzskaitē un klasifikācija

Inventarizē sistēmas, klasificē pēc konfidencialitātes, integritātes un pieejamības.

4.

Risku pārvaldība un kiberdrošības politika

Izstrādā un ievieš kiberdrošības politiku, veic regulāru risku novērtējumu, nosaki pasākumus.

5.

Tīkla un sistēmu aizsardzība

Nodrošini tīkla segmentāciju, ugunsmūrus un automatizētus drošības risinājumus. Filtrē pielikumus un saites, lieto pretļauņatūras risinājumus, praktizē drošu konfigurāciju un atjauninājumus.

10.

Trešo pušu un ārpalpojumu drošība

Līgumos iekļauj drošības prasības, kontrolē piegādes ķēdes riskus, veic uzraudzību.

9.

Nepārtrauktība un atjaunošana

Izstrādā nepārtrauktības un atjaunošanas plānu, testē datu dublēšanu un atjaunošanas spēju.

8.

Incidentu pārvaldība un ziņošana

Izstrādā incidentu pārvaldības kārtību, uzturi reģistru, ziņo atbildīgajai iestādei noteiktajos termiņos.

7.

Auditācijas un žurnālu pārvaldība

Nodrošini žurnālfailu reģistrēšanu, glabāšanu, aizsardzību un analīzi.

6.

Piekļuves kontrole un identitātes pārvaldība

Ievieš drošu datu ievadi, piekļuves tiesību kontroli, periodisku tiesību pārskatīšanu, drošu daudzfaktoru autentifikāciju, pārskati un dzēs neaktīvos kontus.

11.

Datu aizsardzība un privātums

Nodrošini atbilstību VDAR, datu maskēšanu un šifrēšanu, drošu glabāšanu un dzēšanu.

12.

Uzraudzība un telemetrija

Ievieš centralizētu uzraudzību, anomāliju un draudu identifikēšanu reāllaikā.

13.

Drošības testēšana un auditi

Regulāri veic ievainojamību skenēšanu, testus un iekšējos auditus. Iesniedz pašvērtējuma ziņojumu atbilstoši veidlapai un prasībām.

14.

Darbinieku apmācība un kiberkultūra

Organizē regulāras apmācības, kiberhigiēnas pārbaudes, simulācijas.

15.

Sadarbība ar valsts institūcijām

Sadarbojies ar NKDC, CERT.LV, nozares kopienu, nodrošini informācijas apmaiņu.



Aizsardzības ministrija



NCC-LV
LATVIJAS KIBERDROŠĪBAS
KOORDINĀCIJAS CENTRS



ECCC
EIROPAS KIBERDROŠĪBAS
KOMPETENCŪ CENTRS



Līdzfinansē
Eiropas Savienība

Vairāk informācija pieejama: www.cyber.gov.lv