NS2 direktīvas ieviešana Jelgavas valstspilsētas pašvaldībā

18.10.2024.

JVPI «Jelgavas digitālais centrs»

Reglamentējošie akti

- **Nacionālais kiberdrošības likums (NKDL)**
- **MK noteikumi Nr. 422 «Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām»***

**Izdoti saskaņā ar Nacionālā kiberdrošības likuma 12. panta trešo daļu, 24. panta otro daļu, 25. panta pirmo daļu, 26. pantu, 28. panta otro daļu, 29. pantu, 33. pantu, 34. panta pirmo, septīto un desmito daļu, 36. panta pirmo daļu, 42. panta trešo daļu, 43. panta otro daļu un 44. panta otro daļu un Elektronisko sakaru likuma 8. panta pirmo un otro daļu*

Uzdevumi publiskā un privātā sektora organizācijām (saskaņā ar MK N:442)

- Līdz 2025.gada 1.aprīlim

–jānosaka statuss un jāreģistrējas

- Līdz 2025.gada 1.oktobrim

–jāieceļ kiberdrošības pārvaldnieks

–jāiesniedz pirmais pašvērtējuma ziņojums

Foto: pixabay.com

Kiberdrošības dokumentācija


Foto: pixabay.com

- Kiberdrošības politika
- IKT resursu un informācijas sistēmu katalogs
- Kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns
- Kiberincidentu žurnāls
- Lietotāju un piekļuves tiesību pārvaldības politika
- Rezerves kopiju pārvaldības politika

Drošības tehnoloģijas Jelgavas valstpilsētas pašvaldībā

- Centralizētais ugunsmūris
- Centralizētais SPAM filtrs
- Microsoft System Center (darba stacijas licences kontrolei un atjauninājumu uzstādīšanai)
- IPswitch aktīvo iekārtu monitoringa sistēma
- Centralizēta Antivīrusa vadības sistēma
- CISCO VPN serveris u.c.

Foto: Jelgava.lv

Sadarbība ar CERT

Pakalpojumi:

- ABS informācijas tehnoloģiju drošības apdraudējumu agrās brīdināšanas sistēmas pakalpojumi
- MISP (Malware Information Sharing Platform) ar ļaunatūru saistītās informācijas apmaiņas platformas
- RPZ domēna vārdu sistēmas ugunsmūra pakalpojumi ar RPZ (Response policy zone) tehnoloģiju
- SOC drošības operāciju centra (Security operation center SOC) pakalpojumi

Sadarbība ar CERT

Ieguvumi

- Centralizēta pārvaldība: žurnālfailu, izvēlētu notikumu savākšana un glabāšana (risinājums ir fokusēts uz karstajiem drošības telemetrijas datiem)
- Procesu meklēšana vai bloķēšana
- Gala iekārtas izolēšana tīkla līmenī (antivīrusa režīms, host izolēšana, sanitizācija)
- Anomāliju un drošības pārkāpumu identificēšana, trauksmes ziņojumu sūtīšana
- Jebkura kiber uzbrukuma artifakta analīze un sanitizācija

CERT drošības operāciju centra darbība

Foto: pixabay.com


PALDIES
Laiks jautājumiem!
8787
POIC
@poicjelgava
@poic_jelgava
jelgava
@Jelgavas pilsēta
@Jelgavas pilsēta
@jelgavas_pilseta
@jelgavaLV