Nacionālais kiberdrošības centrs

KIBERDROŠĪBAS PIEZĪMES

IDENTIFICĒ:

- Apziniet kritiskos pakalpojumus un izveidojiet riskam pakļauto IKT resursu un informācijas sistēmu (sistēmas, datu kopas, infrastruktūra) katalogu.
- Regulāri veiciet kiberrisku novērtējumu un analīzi, nosakot apdraudējumus un to ietekmi.
- Sagatavojiet un uzturiet kiberrisku pārvaldības un darbības nepārtrauktības plānu (kritisko resursu un pakalpojumu identificēšana, lietotāju un piekļuves tiesību pārvaldīšana, ārpakalpojumu un piegādātāju apzināšana un kontrole).

AIZSARGĀ:

- Izstrādājiet un pārskatiet kiberdrošības politiku: kritisko pakalpojumu un resursu identificēšana, perimetra aizsardzība, fiziskā un loģiskā piekļuve, piekļuves tiesību kontrole, šifrēšana, dublēšana, piegādes ķēdes un ārpakalpojumi, uzraudzība, droša lietošana, glabāšana un likvidēšana.
- Veidojiet drošu konfigurāciju un veiciet atjauninājumus.
- Testējiet rezerves kopijas, atjauninājumus un drošības konfigurācijas.
- Pārskatiet nepārtrauktības plānu (BCP/DRP) un to testējiet.
- Veiciet darbinieku apmācības un nodrošiniet kiberhigiēnas ievērošanu.
- Iekļaujiet drošības prasības ārpakalpojumu līgumos.
- Uzturiet informācijas sistēmu aizsardzību (ugunsmūri, IDS/IPS, fiziskā drošība).
- Ieviesiet izmaiņu kontroli.

ATKLĀJ:

- Izveidojiet kiberincidentu žurnālu: žurnālfailu glabāšana, analīze un integritātes nodrošināšana.
- Izvietojiet un integrējiet agrās brīdināšanas sensorus.
- Drošības operāciju centra (SOC) integrācija vai alternatīva uzraudzības sistēma (SIEM).
- Veiciet pastāvīgu ievainojamību meklēšanu un drošības uzraudzību.

REAĢĒ:

- Sagatavojiet incidentu pārvaldības plānu un informācijas apmaiņas procedūras.
- Izolējiet incidenta vidi.
- Sekojiet līdzi incidentu ziņošanas termiņiem un izmantojiet tam paredzētās veidlapas.
- Sazinieties un koordinējieties ar uzraugošajām iestādēm un partneriem.
- Nodrošiniet, ka darbinieki zina, kam ziņot un kā koordinēt reaģēšanu.

ATJAUNO:

- Plānojiet izolēšanu un atjaunošanu, tāpat arī konfigurāciju, atjauninājumu un rezerves kopiju testēšanu.
- Uzlabojiet darbības nepārtrauktības plānu.

Aizsardzības ministrija

NCC-LV LATVIJAS KIBERDROŠĪBAS KOORDINĀCIJAS CENTRS

ECCC EIROPAS KIBERDROŠĪBAS KOMPETENČU CENTRS

Līdzfinansē Eiropas Savienība