



Rīgas kiberdrošības attīstības vīzija & paveiktais



Misija



Rīgas digitālās aģentūras misija ir veidot drošu un stabilu digitālo ekosistēmu Rīgas iedzīvotājiem. Stiprināt digitālo noturību (digital resilience) un nodrošināt aizsardzību pret kiberuzbrukumiem, vienlaikus veicinot inovatīvu un efektīvu tehnoloģiju pielietojumu pilsētas pārvaldībā



Personāls un kiberdrošības vadība

In-house komanda

Paplašināta drošības komanda (+1 kolēģis ar drošības arhitektūras zināšanām)

Regulāra semināru, konferenču apmeklēšana

Sertifikācija - ITIL, CISM, u.c.

Sadarbība ar datu un informācijas aizsardzības centru

Darbinieku apmācības

Tiek veiktas regulāras darbinieku apmācības

Izstrādāta mācību vide, kur regulāri tiek kārtoti kiberdrošības un personas datu aizsardzības testi

Tiek izsūtīti informatīvi materiāli

Vadlīnijas personālam (droša datu apstrāde, risinājumi)

Starptautiska sadarbība

Dalība starptautiskās konferencēs, paneldiskusijās

Citu pilsētu pieredzes izmantošana

EU fondu projekti (plānā)



Atbilstība normatīvajam regulējumam

Kiberdrošības attīstības plāns

Balstīts uz ISO 27001 (vienota terminoloģija, izpratne)

- Kritisko resursu aizsardzība
- Incidentu monitorings, reaģēšana
- Auditi, pārbaudes,
- Risku pārvaldība
- Apmācības,
- Kiberhigiēnas izpratne
- u.c.

NIS2, Nacionālais kiberdrošības likums

Sadarbība ar CERT

Dalība NCC aktivitātēs

Uzskaitīti procesi, soļi, aktivitātes, kas jāveic, lai nodrošinātu atbilstību

Uzsākts izskatīt incidentu pārvaldības procesu

MK - Minimālās kiberdrošības prasības

Sniegts viedoklis MK projektam

Tiek veikti priekšdarbi (salīdzināta esošā/ nākotnē nepieciešamā drošības dokumentācija, apzināti trūkstošie risinājumi)

Sadarbība ar kompetentajām iestādēm



Kā ieviesīsim NIS2?

Izaicinājumi



- ✓ Ierobežots laiks, lai pilnvērtīgi ieviestu NIS2
- ✓ Ierobežoti finanšu resursi
- ✓ Zināšanu trūkums, nepieciešama prasmju pilnveide

Nacionālais līmenis



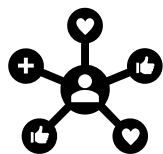
- ✓ Valsts līmeņa regulējums, vadlīnijas
- ✓ Centralizēts atbalsts (CERT > SOC)
- ✓ Komunikācija, atgriezeniskā saite

Rīga – praktisks pieredzes stāsts

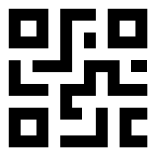


- ✓ Reāli piemēri ir nepieciešami, lai mazākas Pašvaldības varētu efektīvi ieviest NIS2
- ✓ Svarīgi mācīties no starptautiskās prakses un **nodrošināt pārrobežu sadarbību**

Kiberdrošības risinājumi



MFA



DDOS



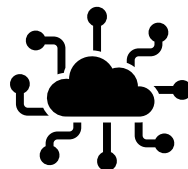
SIEM



SPF, *DMARC,
*DKIM



Ievainojamību
skenēšanas rīks



CERT
ABS/DNS



GDPR auditācijas
modulis

Plānotās aktivitātes

- Kiberdrošības stratēģija
- NIS2, MK aktivitātes
- Audits (pret jaunajām MK minimālo kiberdrošības noteikumu prasībām)
- Uzsvars uz BCP, DRP
- Lietotāju apmācības
- Digitālā noturība (*digital resilience*)
- EU fondu iespējas
- DC modernizācija
- AI normatīvu izstrāde



Paldies!