



**SECURITY
DAYS**

DUOMENŲ SAUGUMAS VALSTYBĖS SEKTORIUJE: AR KARALIUS TIKRAI NUOGAS?



ANTANAS RAGUOTIS

„Registų centro“
IT direktorius

Registų centras - pagrindinių duomenų šaltinis

- ▶ **Gyventojų registras**
- ▶ Vedybų sutarčių registras
- ▶ Testamentų registras
- ▶ Neveiksnių ir ribotai veikusių asmenų registras



Gyventojai

Nekilnojamo turto registras ▼

- Adresų registras ▼
- Nekilnojamojo turto kadastras ▼
- Turto arešto aktų registras ▼
- Miškų valstybės kadastras ▼



Nekilnojamas turtas

Verslas



- ▶ **Juridinių asmenų registras**
- ▶ Juridinių asmenų dalyvių IS
- ▶ Juridinių asmenų galutinių naudos gavėjų IS

Kita



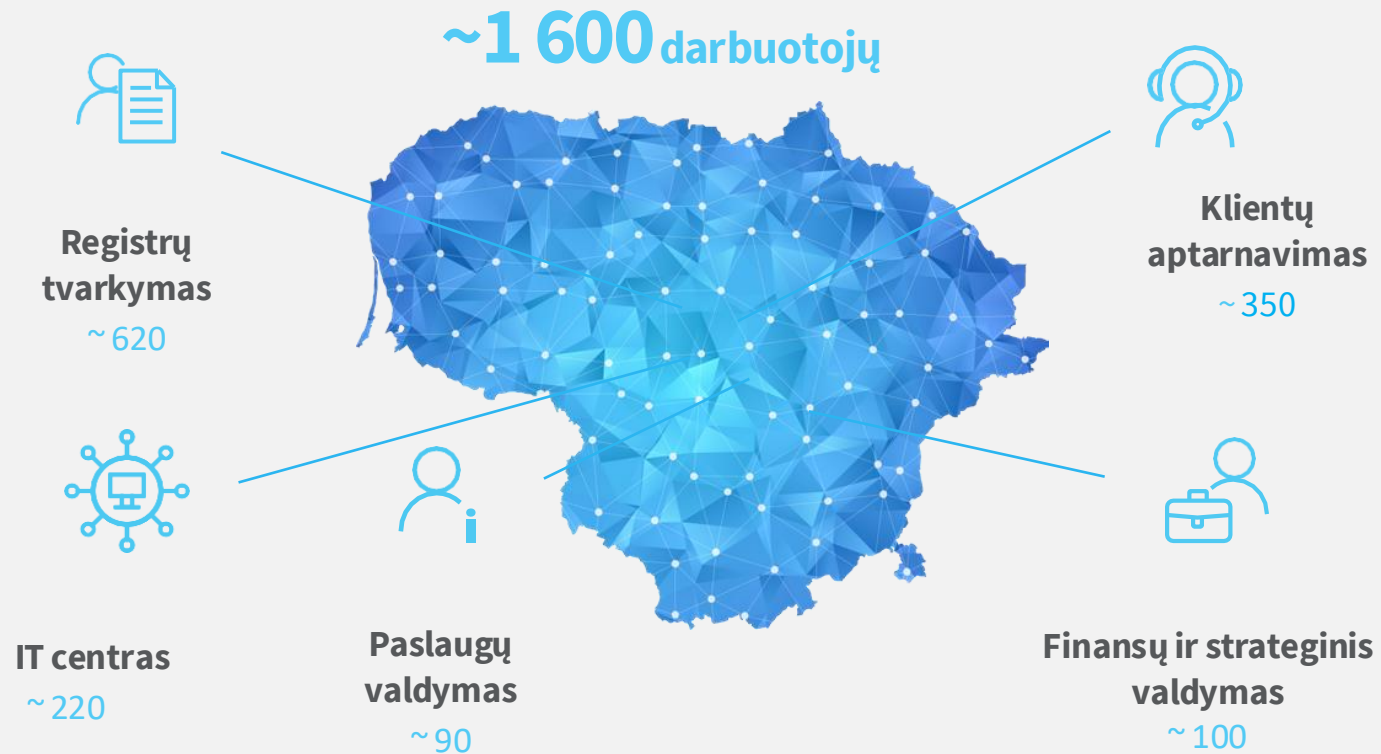
Įgaliojimų registras ▼

- Sutarčių ir teisių suvaržymų registras ▼

Informacinės sistemos

- ▶ Antstolių IS
- ▶ E. Sveikata
- ▶ Išankstinės pacientų registracijos IS
- ▶ Juridinių asmenų dalyvių IS
- ▶ Licencijų IS
- ▶ Piniginių lėšų apribojimų IS
- ▶ Politinių partijų narių sąrašų IS
- ▶ Teisinės pagalbos paslaugų IS
- ▶ Metrikacijos ir gyvenamosios vietos deklaravimo IS
- ▶ E. Siuntų pristatymo sistema „E. pristatymas“
- ▶ Viešosios informacijos rengėjų ir skleidėjų IS

Komanda



Žmonių ir organizacijos
vystymo departamentas

Teisės
departamentas

Prevencijos
departamentas

Vidaus audito
skyrius

Administracija

Komunikacijos
skyrius

~ 120

Apimtys



Registų centro kibernetinė branda

ENISA SIM3: pasiektas vidutinis brandos lygis

- ▼ Vertinimas atliktas 2026-04-24
- ▼ Vertinti 45 parametrai: organizacija, žmonės, įrankiai, procesai

- ▼ RC turi vidinį SOC, išorinio SOC paslaugas teikia "Santa Monica Networks".
- ▼ Vidinį SOC sudaro 7 pareigybės.

Organizacija



Žmonės



Įrankiai



Procesai



SIM3 ataskaitoje - Registų centro SOC atitinka ENISA vidutinį brandos lygį.

Bendra **brandą nėra vienoda**: formalūs mandatai, atsakomybės ir dalis procesų įvertinti aukštai, tačiau matomumo, įrankių formalizavimo ir kai kurių procedūrų srityse išlieka spragų.

Bendra situacija

Bendroje IT infrastruktūroje (tinklo įranga, serveriai, DB, OS) 2024 m. palaikoma tik apie 36 proc. komponentų. **Technologinė skola ~ 55 mln Eur.**

Pavadinimas	Pradžios metai	Atnaujinimų metai	Informacinių išteklių kritiškumas	Pažeidžiamumų vertinimo rezultatai
Pagrindiniai valstybės registrai ir IS				• Pasenusi programinė įranga didina kenkėjiškų atakų riziką • Rizika pažeisti duomenų vientisumą, konfidencialumą ir prieinamumą • Rizika nutekinti vidinę ar klientų informaciją dėl silpnų saugumo priemonių • Gresia DDoS atakos ir paslaugų nepasiekiamumas • Neįdiegtos Operacinių sistemų komponentų pataisos leidžia išnaudoti spragas nuotoliniu būdu • Galimybė įterpti kenksmingą kodą ir pasiekti vidinius resursus • Nesaugus aplikacijų dizainas didina kibernetinių atakų riziką • Konfigūracijos klaidos leidžia pasiekti jautrius duomenis • Pasenę arba nebepalaidomi komponentai, kuriems nebeleidžiami saugumo pataisymai, todėl didėja išnaudojimo tikimybė • Dalies duomenų saugojimas ar perdavimas nėra tinkamai šifruojamas arba naudojamos silpnos šifravimo schemos, leidžiančios nutekinti jautrią informaciją • Susidaro galimybės apeiti ugniasienes, pasiekti vidinius tinklo išteklius
Nekilnojamojo turto registras ir Nekilnojamojo turto kadastras (NTR / NTK)	1998	NTR – 2009, NTK – 2016 m.	5 - Labai didelis	
Gyventojų registras (GR)	2011	Modernizavimo projektas nespėdė tech. skolos	5 - Labai didelis	
Adresų registras (AR)	2007	2016	5 - Labai didelis	
Juridinių asmenų registras (JAR)	2004	2025	5 - Labai didelis	
Sutarčių ir teisinių suvaržymų registras (STSR)	2022	Nebuvo	5 - Labai didelis	
Ypatingos svarbos registrai ir IS, nepriskiriami prie pagrindinių				
Elektroninė sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema (ESPBI)	2015	2024	5 - Labai didelis	
Lietuvos Respublikos miškų valstybės kadastras (MVK)	2004	Nebuvo	6 - Labai didelis	
Neveiksnių ir ribotai veikiančių asmenų registras (NIRVAR)	2011	Nebuvo	4 - Didelis	
Turto arešto aktų registras (TAAR)	2002	2012	8 - Labai didelis	
Integruotų paslaugų platforma (IPP)	1999	Nebuvo	3 - Vidutinis	
Mažieji valstybės registrai				
• Antstolių informacinė sistema (AIS), • Nacionalinė elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinė sistema (E. PRISTATYMAS), • Išankstinės pacientų registracijos informacinė sistema (IPR), • Įgaliojimų registras (ĮR), • Juridinių asmenų dalyvių informacinė sistema (JADIS), • Licencijų informacinė sistema (LIS), • Piniginių lėšų apribojimų informacinė sistema (PLAIS), • Politinių organizacijų narių registras (POLONR), • Teisinės pagalbos paslaugų informacinė sistema (TEISIS), • Testamentų registras (TR), • Vedybų sutarčių registras (VSR), • Viešosios informacijos rengėjų ir skleidėjų informacinė sistema (VIRSIS)	2001-2023 m. (vienas registras bus pradėtas eksploatuoti tik 2026 m.)	6 sistemos / registrai neatnaujinami, 2015-2024	3 - Vidutinis / 4 - Didelis	

Į ką fokusavomės paskutiniais metais?



▶ **Monitoringo įrankių kūrimas**

- ▶ Rizikų žinynas, ~ 20 rizikų
- ▶ Prioritetai pagal rizikos lygį
- ▶ Darbai keliauja į bendrą backlogą

Viskas prasideda nuo matymo!

- ▶ BDAR ataskaitos, 20 tūkst. užklausų per mėn. vidurkis
- ▶ Fizinė infra – dubliuoti DC
- ▶ Atnaujinta tinklo topologija, viename iš DC
- ▶ Sisteminiai Penetration testai, bent 50 vnt.
- ▶ Vidinio tinklo MFA
- ▶ Emailo, MS MFA
- ▶ Atnaujinti TLS į ne žemiau 1.2
- ▶ SOC įsteigimas ir paslaugos pirkimas
- ▶ Monitoringo centro *outsource*
- ▶ XDR
- ▶ WAF
- ▶ xx auditų, vertinimų

Investicijos į kibernetinę saugą 2023-2026 m.

Pirkimai	Suma, be PVM
Saugumo specialisto kompetencijos	38 500
XDR/EDR	50 650
El. pašto apsauga	23 990
WAF praplėtimas	29 940
Pažeidžiamumų valdymo įrankis	18 725
PEN TESTAI	200 000
SIEM	298 400
WAF praplėtimas	170 420
SIEM praplėtimas	838 020
XDR	559 075
Sandbox	515 210
Testavimai	53 585
SOC	101 400
SOC2	241 200
VISO	3 139 115



3 metų dedikuotų
saugumo specialistų
DU ~ 1,5 mln Eur.

Kas įvyko?

- ▶ Kompromituotos
autorizuoto duomenų
gavėjo paskyros
- ▶ Per kliento paskyras
pavogti duomenys



Kodėl įvyko vagystė?

- ▶ Fokusas į kitas, pagal vertinimą didesnes rizikas
- ▶ Fokusas į projektus ir palaikymą
- ▶ Dar 2014 m. nepavyko pereiti prie patikimo MFA dėl didelio politinio ir suinteresuotų šalių pasipriešinimo
- ▶ Sutartys ir jų keitimas (per 20 tūkst.)
- ▶ Esantis MFA sprendimas *email* pagrindu buvo vertinamas kaip pakankamas
- ▶ Duomenų imties vertinimo neapibrėžtumas

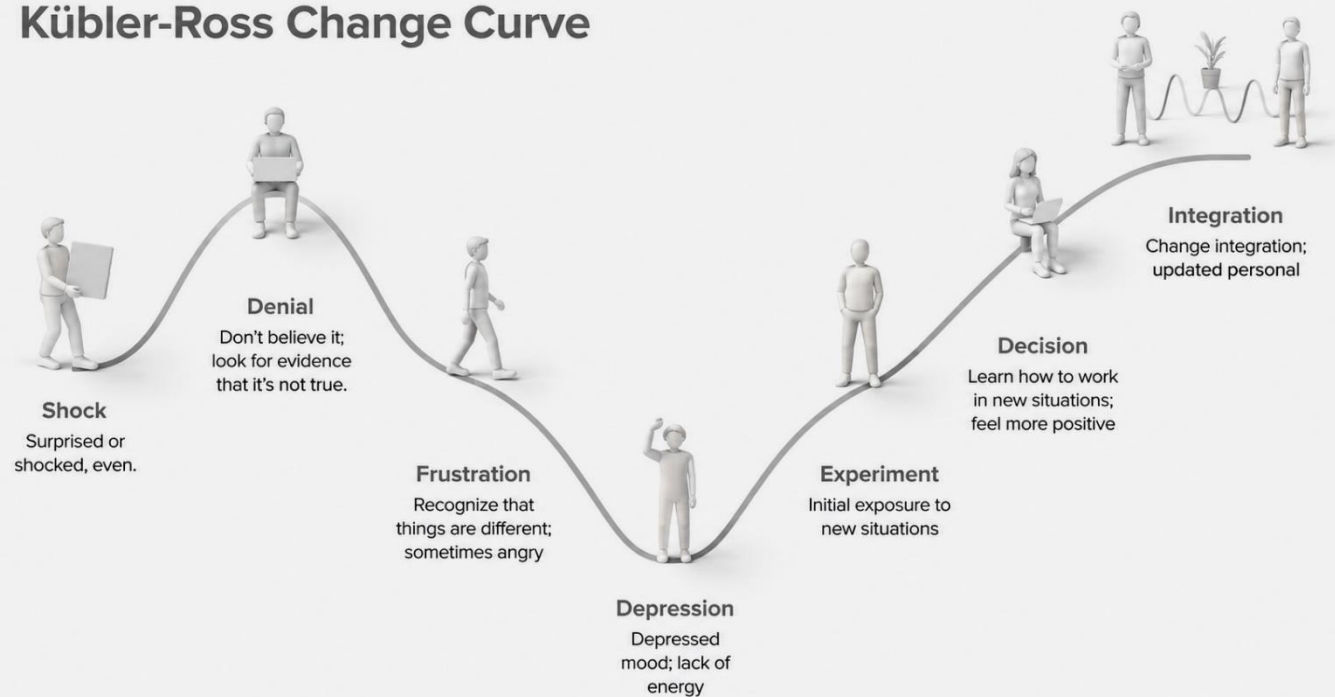


Incidentą lėmė ne viena konkreti techninė spraga ar organizacinės / techninės priemonės nebuvimas, o nepakankamai suvaldytų saugos rizikų visuma

Kaip jautėsi organizacija?

- ▶ Šokas visiems vs šokas tik daliai
- ▶ GD atstatydinimas
- ▶ Visiškas darbų perplanavimas
- ▶ Iškart pasikeitė prioritetai
- ▶ Įmonė mobilizavosi
- ▶ Politinis pasipriešinimas, sutartys, diplomatija tapo mažareikšmiais
- ▶ Patikros ir kontrolė iš visur – VSD, NKSC (5 punktai), Prokuratūra, Kriminalinė Policija, Antrasis operatyvinių tarnybų departamentas prie KAM, Seimas
- ▶ Suplanuotų darbų niekas neatidėjo

Kübler-Ross Change Curve



Ką darėme?

- Suburta krizės valdymo grupė
- Išgrynintos koreguotinos sritys ir užduotys
- Sudėliotas ir įgyvendinamas veiksmų ir darbų planas:
 - Greita ir būtina
 - Būtina
 - Ilgalaikiai projektai

Papildomos saugumo priemonės Savitarnos sutartinių klientų prisijungimui

Naudotojų tipas

1. Visi, nepatenkantys į išimtis

2. Visos išimties

(blank)

Išimties tipas

2.1. XML duomenų teikimas

2.2. Robotai

2.3. Užsieniečiai

2.4. Saugumo institucijos ...

(blank)

Statusas

Nepradėta

Užbaigta

Vykdoma

(blank)

2026-05-28

Pagrindiniai iniciatyvos veiksmai

Pradinis naudotojų skaičius

Tikslas

Tikslo data

Panaikinta naudotojų

birželio 4 d.

birželio 11 d.

Naudotojai, kurie jungiasi naudotojo vardu ir slapta:

37 000

0

rugsėjo 2 d.

97%

2 415

2 266

1. Visi, nepatenkantys į išimtis

34 464

0

gegužės 29 d.

100%

0

Užbaigta

2026-05-29

Ijungti MFA

2. Visos išimties

2 536

0

TBD

63%

2 415

2 266

2.1. XML duomenų teikimas

200

0

TBD

76%

200

51

Užbaigta

2026-06-15

Pateikti

Užbaigta

2026-07-03

Informuoti 5 klientus,

Nepradėta

2026-09-01

Atjungti

Vykdoma

2026-07-24

Atlikti JAR

Nepradėta

TBD

Atjungti

2.2. Robotai

108

0

rugsėjo 2 d.

100%

49

49

Užbaigta

2026-06-11

Apriboti

Užbaigta

2026-06-15

Išsiųsti raštus, informuojan

Užbaigta

2026-06-23

Atjungti

Užbaigta

2026-07-17

Atjungti galimybę

2.3. Užsieniečiai

228

0

rugsėjo 2 d.

70%

166

166

Užbaigta

2026-05-28

Parengti

Užbaigta

2026-06-15

Išsiųsti raštus, informuojan

Užbaigta

2026-07-02

Atjungti

Vykdoma

2026-08-20

Pateikusiems IP sukurti

Nepradėta

2026-09-02

Atjungti

2.4. Saugumo institucijos (VIP7 --> VIP5)

2 000

0

rugsėjo 2 d.

59%

2 000

2 000

Užbaigta

2026-07-30

Organizuoti susitikimus

Užbaigta

2026-08-30

Paruošti

Vykdoma

2026-07-31

Išnagrinėti saugumo

Vykdoma

2026-09-01

Sukurti sprendimą

>

1. SSN_KPI

1. Savitarnos sutart naudotojai

2. DSM_KPI

2. Duomenų srautų monitoringas

3. VVP_KPI

3.Vidinių RC

Išvados ir išmoktos pamokos

- ▶ Visuomenės informavimas ir asmeninis informavimas pagal BDAR – du skirtingi dalykai
- ▶ Masiniam informavimui pagal BDAR įrankiui sukurti reikia laiko
- ▶ Teisiniai saugikliai neapsaugos nuo tikrų pasekmių
- ▶ Partnerių ir integratorių valdymas kritiškas
- ▶ Rizikų vertinimo prielaidos turi būti pastoviai kvestionuojamos
 - ▶ Ar dabartinis email, MFA yra tinkamas?
 - ▶ Ar dabar galime pasitikėti partneriais, integratoriais?
 - ▶ Asmens duomenų jautrumas šiandien ir vakar
- ▶ **Jeigu šiandien atrodo, kad rizikų valdymas yra pakankamas, rytoj galvokite iš naujo**
- ▶ Krizė – tai nauja galimybė įmonei



Ačiū už dėmesį



linkedin.com/company/RegistruCentras



linkedin.com/company/RegistruCentras
[FB.com/RegistruCentras](https://fb.com/RegistruCentras)



[@RegistruCentras](https://instagram.com/RegistruCentras)