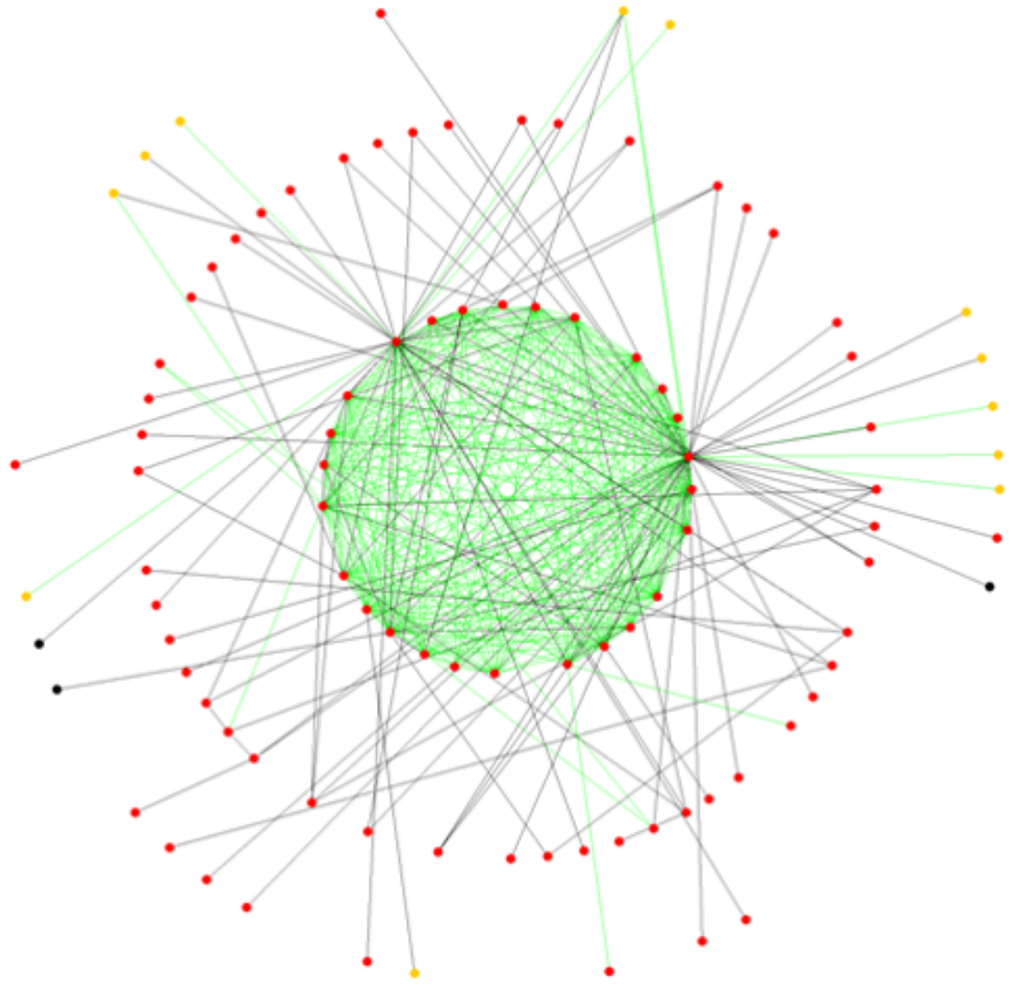
Kibernetinio saugumo vertinimas Lietuvoje ir saugumo reikalavimai informacijos prieglobos teikėjams

Dr. Rytis Rainys | rrt.lt

Kaunas, Domreg.lt, 2017



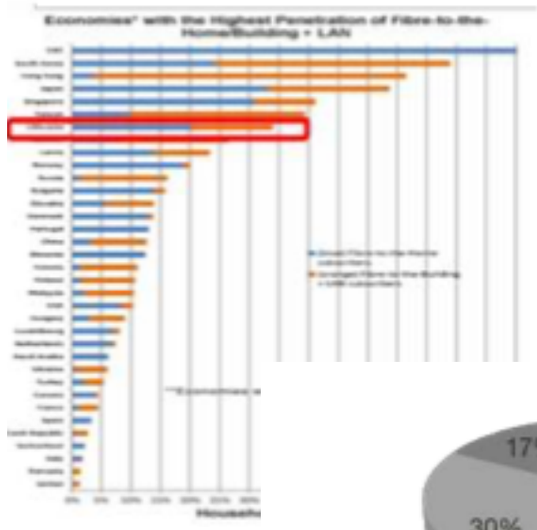
e-LT privalumai

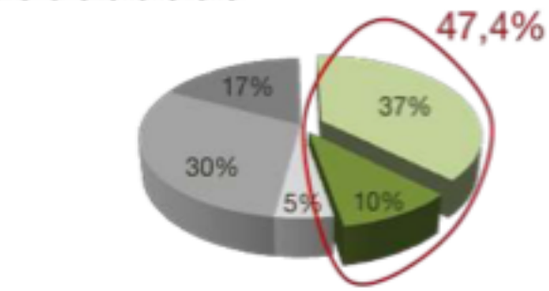
1) Technologiškai moderni interneto tinklo infrastruktūra

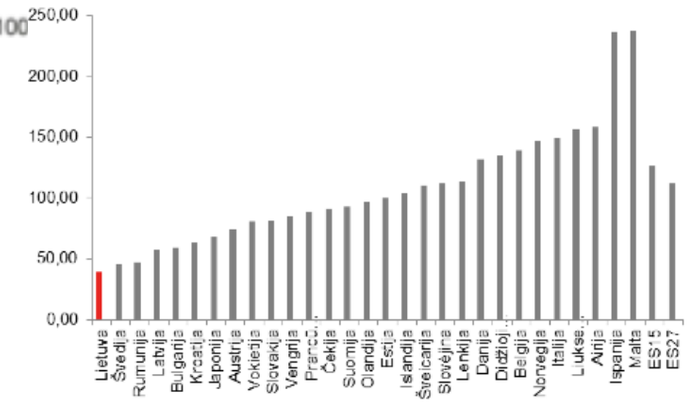
2) Didelis interneto greitis, aukšta tarptautinio interneto pralaida

3) Pigūs interneto mokesčiai vartotojams

4) Siekiamybė: nacionalinė kibernetinio saugumo užtikrinimo sistema







RRT kibernetinio saugumo reguliavimo rinkos

RRT Tinklų ir informacijos saugumo departamentas (TISD) atlieka kibernetinio saugumo priežiūrą:

2 skyriai TISD sudėtyje

14 darbuotojų

Interneto paslaugų teikėjai

Patikimumo užtikrinimo paslaugų teikėjai
- e. parašo
- e. spaudo
- laiko žymų
- Web tapatumo nustatymo
- ir kt.)

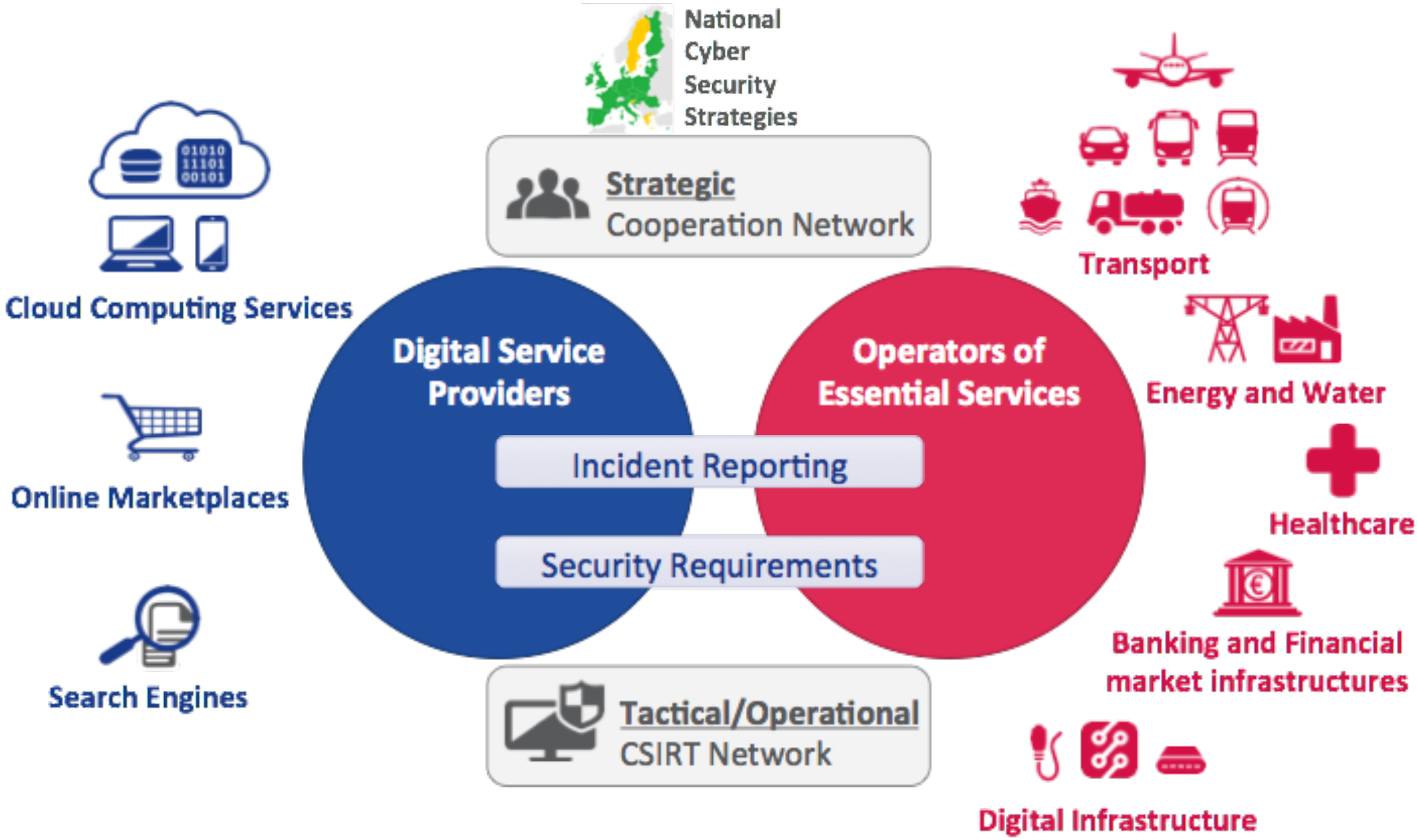
Debesų kompiuterijos teikėjai (tame tarpe hosting‘as)

ERĮ

eIDAS reglamentas

KSĮ

NIS Direktyva: imties schema (nuo 2018)



RRT kibernetinio saugumo reguliavimo rinkos

Įsigaliojus EU tinklų ir informacijos saugumo direktyvai (NIS Directive), prasiplėsRRT kibernetinio saugumo priežiūros rinkos

Skaitmeninių paslaugų teikėjai
- debesų kompiuterija
- e. prekybos vietos
- paieškos varikliai

RRT

Skaitmeninės infrastruktūros
- IXP
- DNS sistemos
- TLD registrai

NIS direktyva

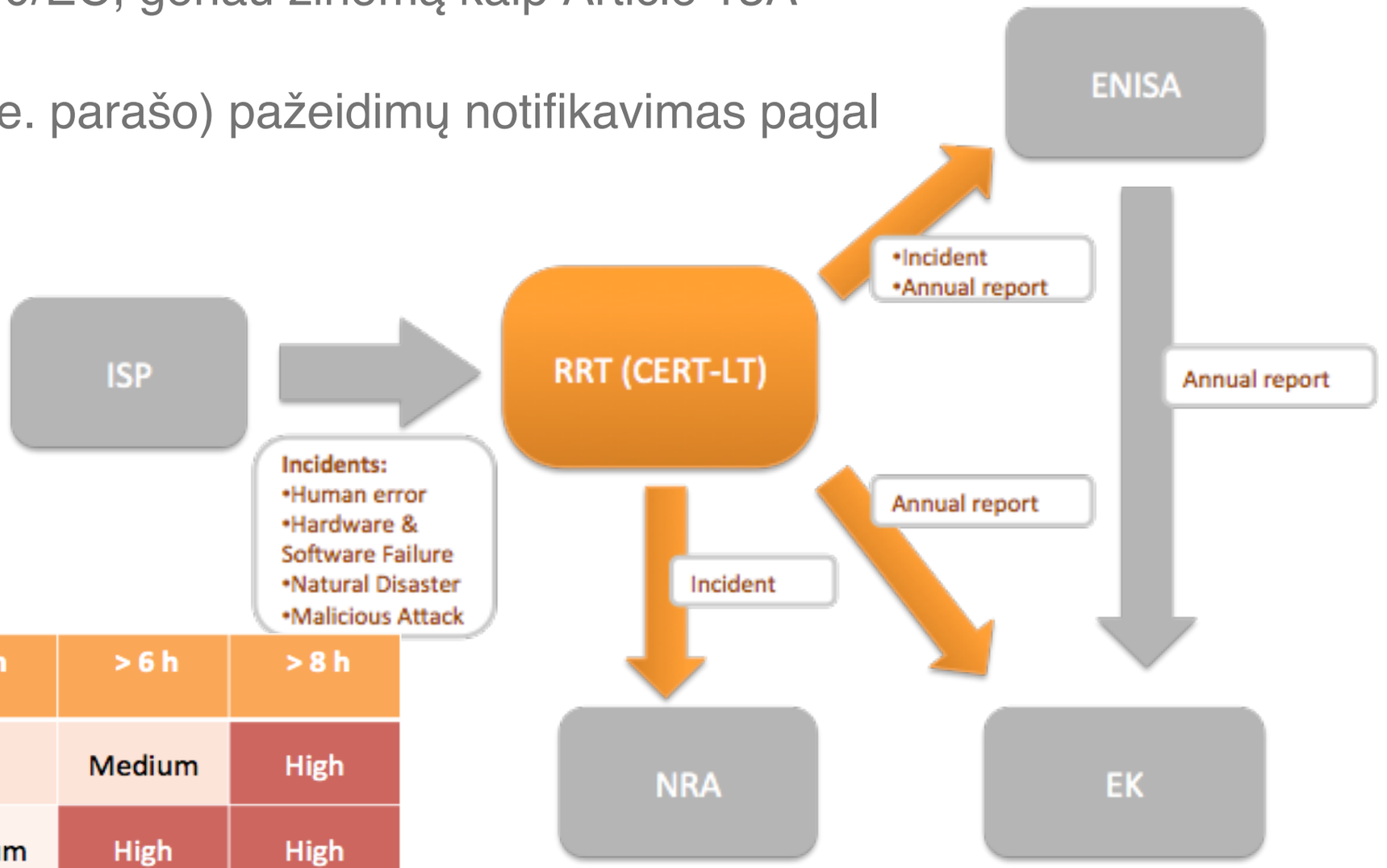
RRT kibernetinio saugumo veiklos apimtys

Informavimas	**Incidentų valdymas**	**Tinklų infrast. patikimumo tyrimai**	**Patikimumo paslaugos** (e. parašas)	**Interneto turinio priežiūra**
• Išankstinio įspėjimo sistema • Info sklaida per media/web/seminarus	• Nationalinio CERT-LT funkcijos • Hot-line veikla	• Interneto topologijos žemėlapis • Kritinių tinklo elementų identifikavimas • Monitorinimas ir stebėsena	• Patikimumo paslaugų teikėjų priežiūra • Nacionalinis TSL sąrašas	• Debesų kompiuterijos saugumas • Safer Internet projektas • Turinio filtrų akreditacija

Direktyvos reikalavimų įgyvendinimas

1) Incidentų ICT sektoriuje notifikavimo mechanizmo užtikrinimas LT ir EU lygiu pagal 2009/140/EC, geriau žinomą kaip Article 13A

2) Patikimumo paslaugų (e. parašo) pažeidimų notifikavimas pagal Article 19



	< 2 h	> 2 h	> 4 h	> 6 h	> 8 h
> 2 % of users	Low	Low	Low	Medium	High
> 5 % of users	Low	Low	Medium	High	High
> 10 % of users	Medium	Medium	High	High	High
> 15 % of users	Medium	High	High	High	High

Incidentų detekcija Lietuvos IP perimetre

2016 m. CERT-LT atliko 49 463 incidentų elektroninėje erdvėje tyrimus, palyginti su 2015 m. (41 583), incidentų 19 proc. daugiau

20 490 saugumo spragų (SSDP, SSL, DNS ir t.t)

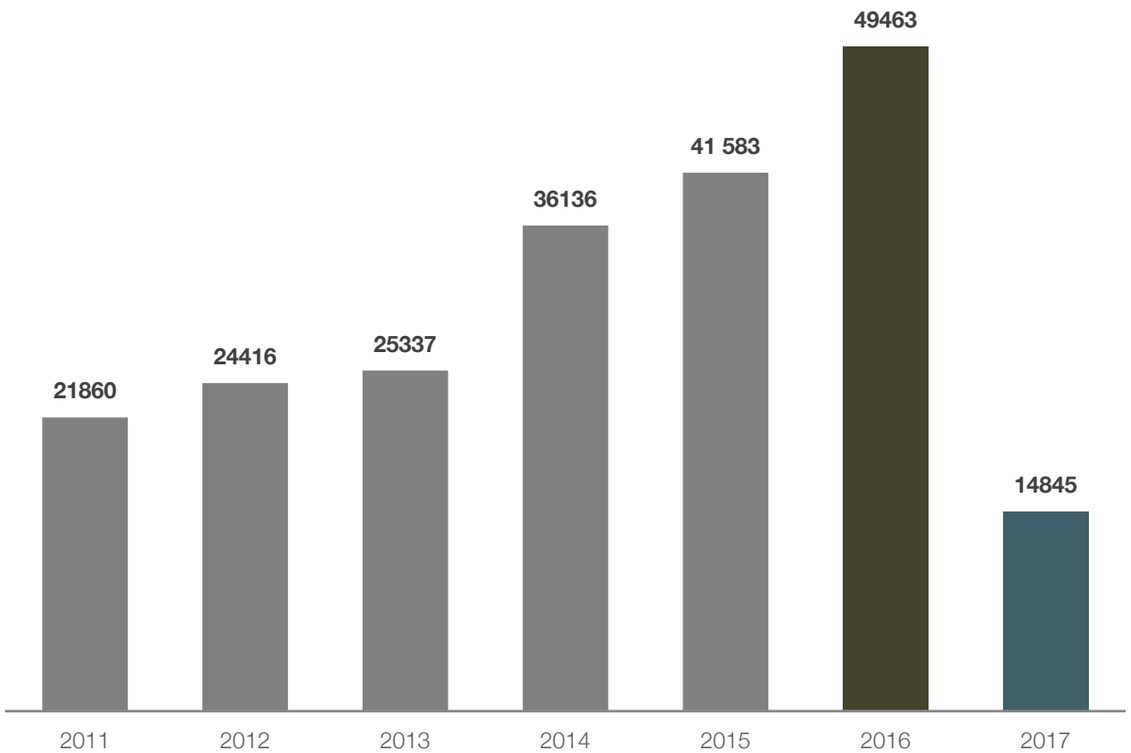
Kenkimo programinė įranga – 11 212 incidentų

2016 pabaigoje Lietuvoje buvo 351 „Mirai“ užkrėstų įrenginių (unikalių IP adresų)

2016 m. 19 reikšminių vientisumo incidentų, kuriuos pranešė IPT (2015 m. 10)

Problema: Informacinės sistemos užvaldymai – 10 673 (2015 m. 6 722) – 53 proc. daugiau

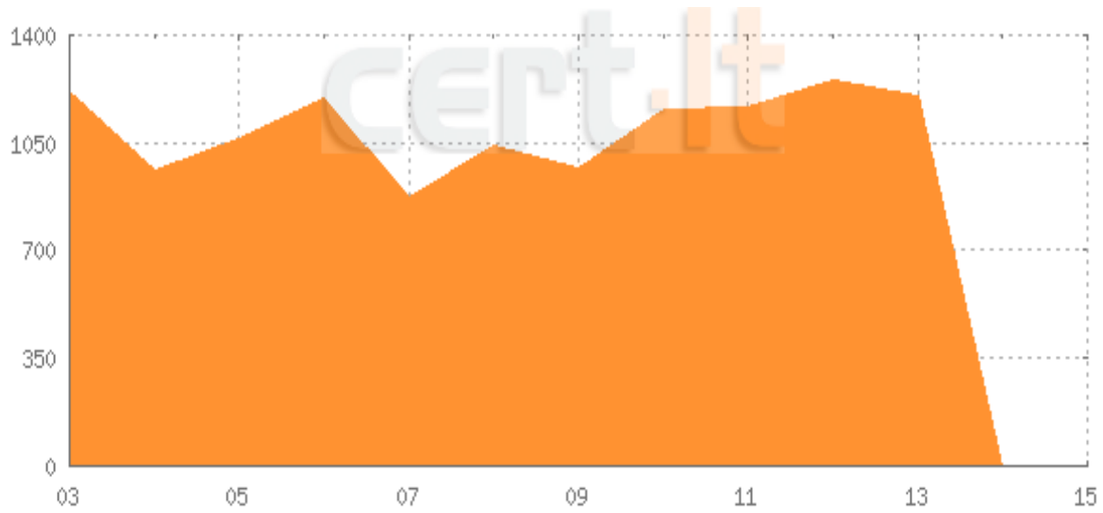
2010–2016 m. apdorotų incidentų suvestinė



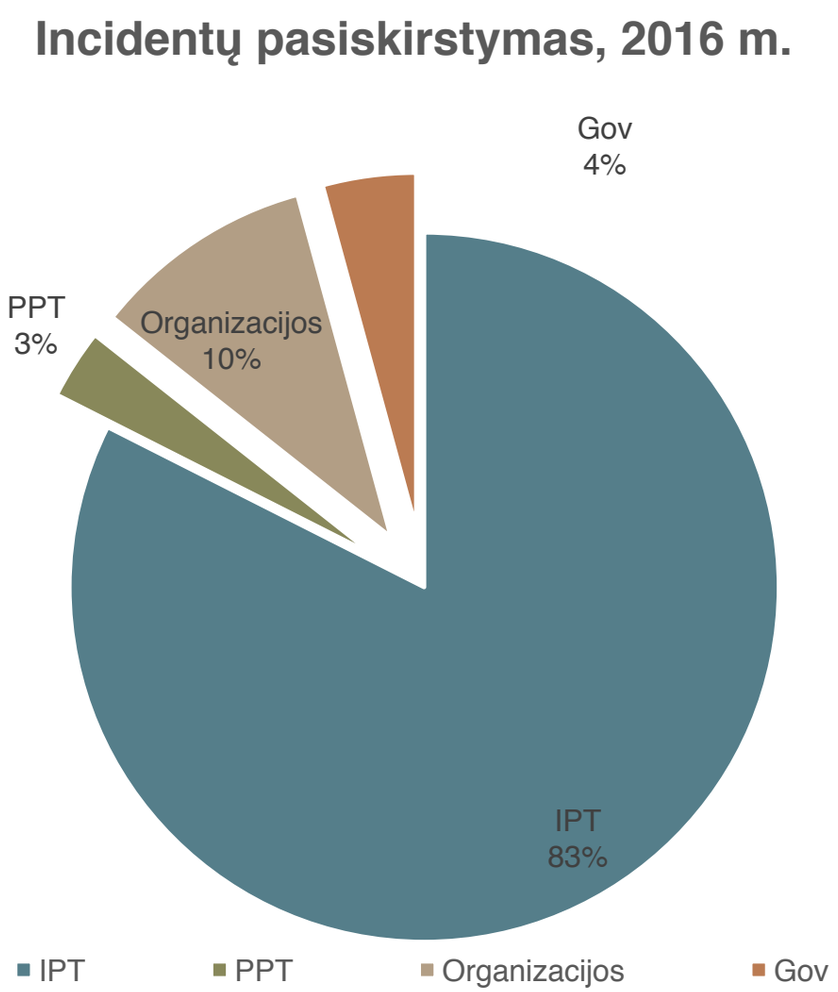
Incidentų tyrimas, valdymas

- ~ 1000-1400 incidentų per savaitę
- ~ 20% valdomi analitikų
  - Užvaldytos svetainės
  - DDoS atakos ir pan.
- ~ 80% valdomi automatiškai, XML (520 organizacijų)

Išspręstų incidentų skaičius per savaitę



Incidentų pasiskirstymas tarp subjektų



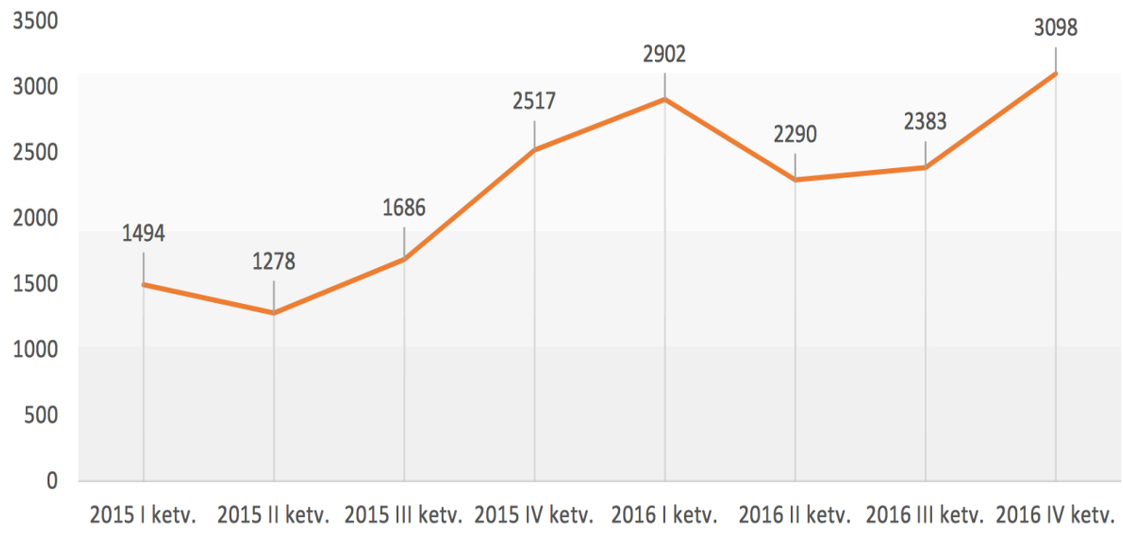
Incidentų tipai

Tipas	2016	2017	Pokytis %
Kenkimo programinė įranga	10 928	11 212	+3
Informacinių sistemų užvaldymas	6 975	10 673	+53
E. paslaugų trikdymo atakos	50	61	+22
E. duomenų klastojimas	559	555	-1
Vientisumo pažeidimai	10	21	+110
Įrenginių saugumo spragos	18 427	20 490	+11
Įvairaus pobūdžio	4 634	6 451	+39

IS užvaldymo incidentai

- **Informacinės sistemos užvaldymai – 10 673 (2015 m. 6 722) – 53 proc. Daugiau**
  - Fake Jquery
  - Exploit kit (RIG, Neutrino, Angler)
  - Ir pan.
- El. Duomenų klastojimas (phising) - 555 atvejai
- *Defacment* – ~300 atvejų

Informacinių sistemų užvaldymo atvejai 2015–2016 m.



Priežastys:

- Nepakankamas sistemų ir tinklalapių savininkų išprusimas saugumo srityje.
- Nepakankamas tinklalapių kūrėjų ir sistemų administratorių dėmesys saugumo klausimams ir menkas saugumo svarbos vertinimas.
- Didelis atviro kodo turinio valdymo sistemų populiarumas ir jų priežiūros trūkumas.

Situacijos vertinimas statistiškai

2016-iais unikalūs IP dalyvavę kenkimo veikloje, arba turintys saugumo spragų (dalis dalyvavę DDoS atakose):

- Viso kenkimo ip: 45 476 (be dinaminių ip 13 667) (2015 m. - 31 135)
- Viso spragų ip: 136 383 (be dinaminių ip 85 107) (2015 m. - 114 910)
- Pasikartojančių kenkimo ip: 2016 - 3 691 (27 proc.) (2015 - 10 386 (33 proc.))
- Pasikartojančių spragų ip: 2016 - 43 820 (51 proc.) (2015 - 58 453 (51 proc.))

Bendras procentas pasikartojančių: 48%. Kitaip sakant kas antro vartotojo atžvilgiu veiksmai (CERT-LT -> IPT -> vartotojas) yra efektyvūs

Dėl pasikartojančių ir vengiančių įgyvendinti CERT-LT nurodymus IP, dirbama su Kriminaline policija dėl laikino 48 val. Interneto atjungimo

Turinio internete incidentai

- 2016-iais RRT gavo 842 pranešimus apie neteisėtą ar žalingą turinį internete (išaugo 38 proc.)
- http://www.draugiskasinternetas.lt/lt/main/report

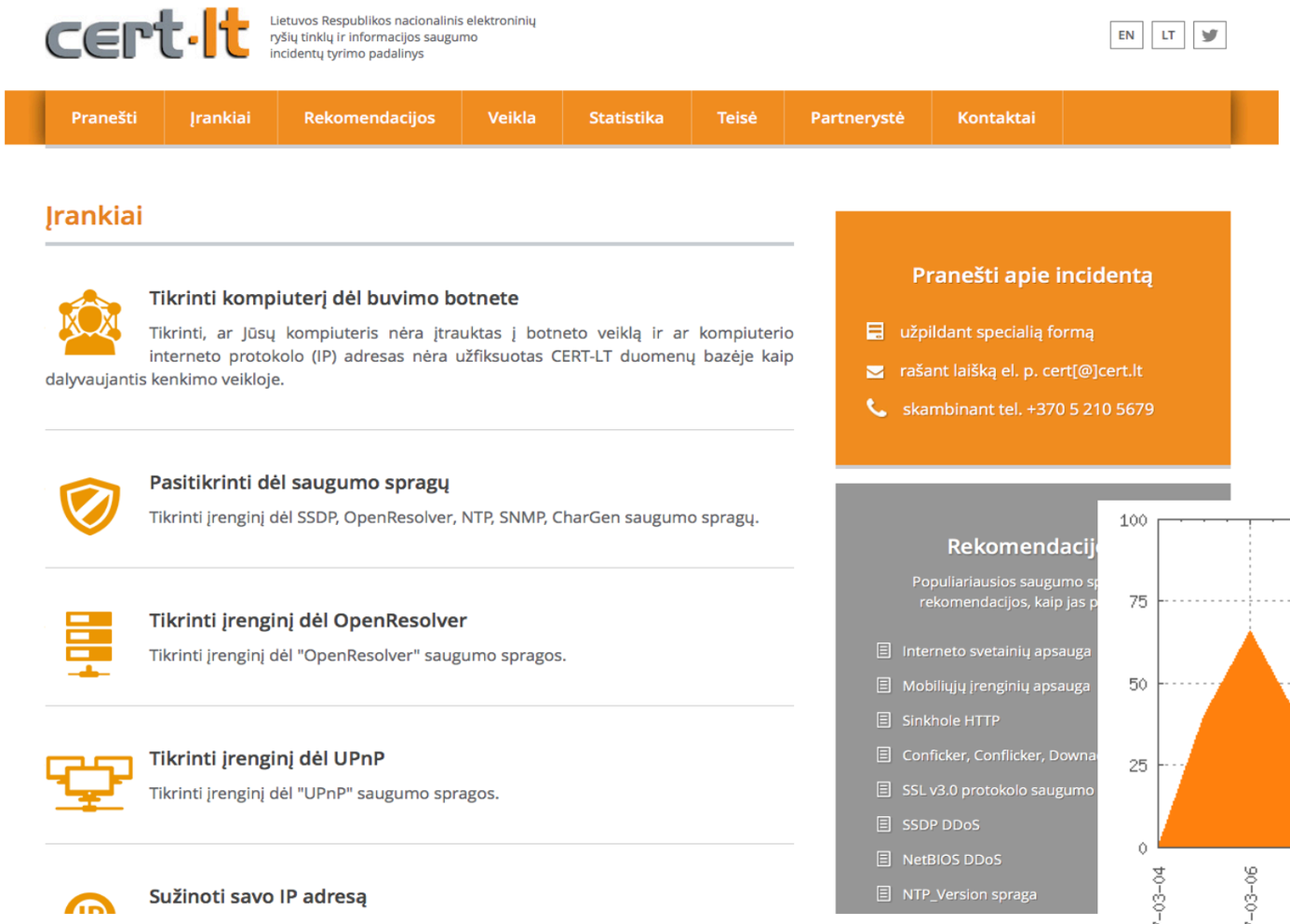
36 pranešimus persiuntė tolesniam tyrimui Policijos departamentu Įtariamas neteisėtas turinys Lietuvos tarnybinėse stotyse – seksualinis vaikų išnaudojimas, pornografija;

26 pranešimus persiuntė tolesniam tyrimui Žurnalistų etikos inspektoriaus tarny Įtariama neigiamą poveikį nepilnamečiams daranti informacija;

265 pranešimus apie vaikų seksualinio išnaudojimo vaizdus persiuntė kitų šalių karštosioms linijoms, tarptautinės interneto karštųjų linijų asociacijos INHOPE narėms;

78 pranešimus persiuntė įvairių šalių interneto paslaugų teikėjams su NTD

Informacijos sklaida



- Naujienos
- Įrankiai
- Pranešimo forma
- Rekomendacijos (~200)

2017 m.
- Sandbox
- WEB audito įrankis
- Rekomendacijos WEB

,,Taisyklės” – paprastai

- Viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų saugumo ir vientisumo užtikrinimo taisyklės [aktuali redakcija: 2015 m. birželio 24 d.]

- http://www.rrt.lt/lt/teisine-informacija/teisine-informacija_1072/rrt-teises-aktu-paieska/650/download/20520.html

- Reglamentuoja ...**elektroninės informacijos prieglobos paslaugų teikėjų** (PPT) teises ir pareigas **užtikrinant** jų teikiamų elektroninės informacijos prieglobos paslaugų **saugumą ir vientisumą**, **informacijos** apie kibernetinius ar saugumo **incidentus** ..., taikytas incidentų valdymo priemones ... **teikimo** RRT tvarką ir sąlygas....

- III, IV skyriai

,,Taisyklės” – paprastai. Pareigos ir teisė

- PPT prievolės:
- 5.1. užtikrinti savo **teikiamų paslaugų** saugumą |(tech. ir org. priemonės);
- 5.3. užtikrinti savo paslaugų teikimui **naudojamos įrangos** saugumą;
- 5.4. nedelsiant informuoti paslaugų gavėjus apie **svarbius** incidentus.
- 5.5. informuoti paslaugų gavėjus apie **planinius** darbus
- 5.8. turėti nustatytą paslaugų gavėjų **įspėjimo** apie saugumo **pažeidimus tvarką** ir kokių **veiksmų** tokiu atveju privalo **imtis** gavėjai ir (ar) teikėjai
- PPT teisė:
- 6.1**. imtis** neatidėliotinų priemonių, **įskaitant laikiną** elektroninės informacijos prieglobos **paslaugų teikimo** šių paslaugų gavėjams **apribojimą**, kai incidentas ir (ar) vientisumo pažeidimas yra įvykęs arba yra akivaizdi incidento ir (ar) vientisumo pažeidimo grėsmė;
- 6.3. **laikinai apriboti** ar **nutraukti** elektroninės informacijos prieglobos **paslaugų teikimą** šių paslaugų gavėjams, prieš tai juos **įspėję**, jei nustatoma, kad elektroninės informacijos prieglobos paslaugų gavėjai, naudodamiesi jų teikiamomis paslaugomis, atlieka kenkimo veiką;

,,Taisyklės” – paprastai. Pranešimai

- IV skyrius
- PPT paslaugų teikėjai:
- - **privalo nedelsiant informuoti tarnybą** apie didelės įtakos incidentus ar incidentus, kurie gali turėti didėlės įtakos paslaugų teikimui jų gavėjams (7.2)
- - **privalo ne vėliau kaip per 1 darbo** dieną informuoti **tarnybą** apie vidutinės įtakos incidentus ar incidentus kurie gali turėti vidutinės įtakos paslaugų teikimui jų gavėjams (7.3)
- 7.4 pranešti cert@cert.lt arba https://www.cert.lt/report
- 7.5. pateikti tarnybai k/t pasiekiama 24/7

Paslaugos sutrikimo trukmė	Ilgiau nei viena valanda, bet trumpiau nei dvi valandos	Ilgiau nei dvi valandos
Paslaugų gavėjų skaičius arba % nuo bendro teikėjo paslaugų gavėjų skaičiaus	Įtaka	
>1000 arba > 5 %	Vidutinė	Didelė

CERT-LT kontaktai

- 24/7*
- El. p. cert@cert.lt
- PGP/GPG Key ID: 0xA3BACE47
- Tel. 8 5 210 56 79

** Nedarbo valandomis reguojama tik į svarbius incidentus*

Naudingos nuorodos

- Apia CERT-LT: www.cert.lt
- Metinė CERT-LT veiklos ataskaita: www.cert.lt/doc/2016.pdf
- CERT-LT RFC2350: www.cert.lt/doc/CERT-LT_RFC2350_LT_final.pdf
- Naujienos/įspėjimai: https://twitter.com/cert_lt
- Taisyklės: http://www.rrt.lt/lt/teisine-informacija/teisine-informacija_1072/rrt-teises-aktu-paieska/650/download/20520.html
- Apie grėsmes internete: www.esaugumas.lt

- XML aprašymas https://www.cert.lt/xml_info.html
- Pranešimo forma: www.cert.lt/report

Dr. Rytis RAINYS
Lietuvos Respublikos ryšių reguliavimo tarnyba
Tinklų ir informacijos saugumo departamento direktorius
Mortos 14, LT-03219 Vilnius
Mob. +370 611 14018
e-mail: rytis.rainys@rrt.lt
www.rrt.lt
www.cert.lt