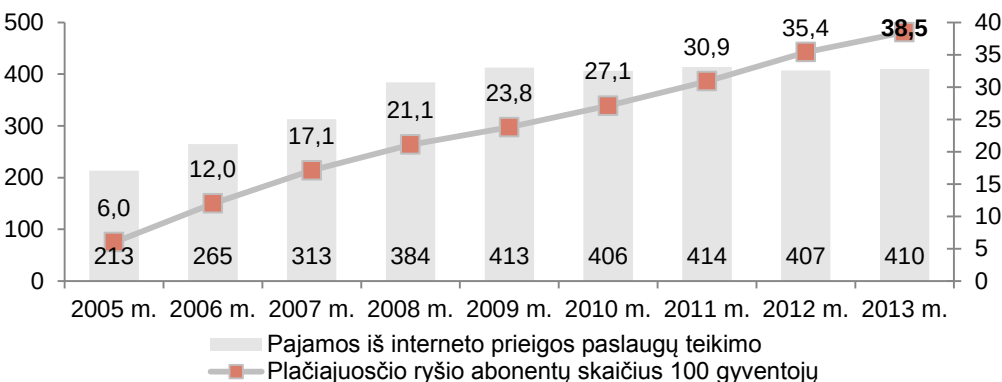


LIETUVOS RESPUBLIKOS
RYŠIŲ REGULIAVIMO TARNYBA

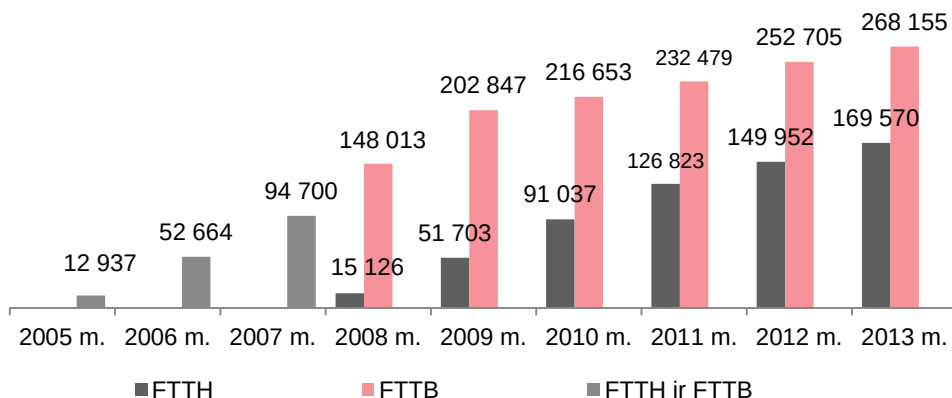
Kibernetinio saugumo situacijos Lietuvoje apžvalga bei tendencijos

dr. Rytis Rainys, RRT
„Europos savaitė 2014“ diskusija
2014 m. balandžio 30 d., Vilnius

INTERNETO RINKA



Pajamos iš interneto prieigos paslaugų teikimo, mln. Lt, ir plėčiamosios ryšio technologijas naudojančių abonentių, įskaitant abonentus, prisijungusius judriuoju telefono ryšio tinklu, skaičius 100 gyventojų



2013 m. interneto prieigos paslaugų, teikiamų plėčiamosiu ryšiu, skvarba pasiekė 38,5 proc. gyventojų.

2013 m. į elektroninių ryšių tinklo infrastruktūrą investavo daugiau. 2013 m. investicijos padidėjo 43 mln. Lt arba 16,2 proc.

38,6 proc. visų interneto prieigos paslaugų abonentių interneto prieigą gavo šviesolaidinio ryšio linijomis.

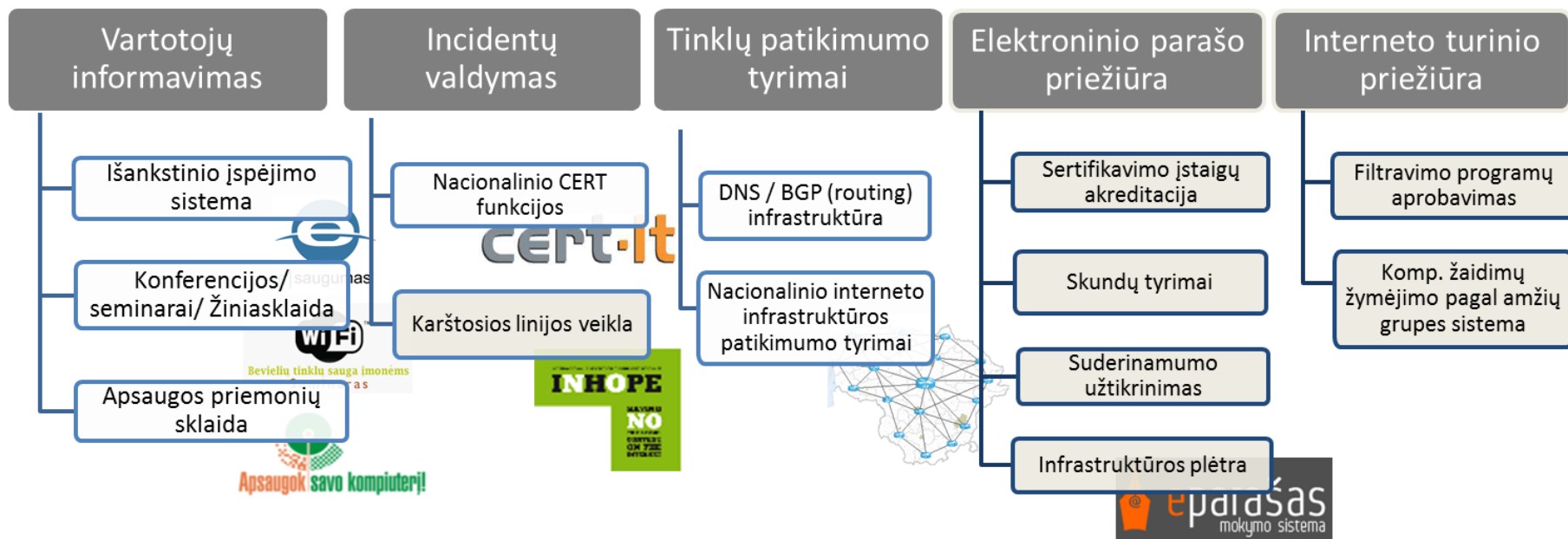
Nuo 2005 m. iki 2013 m. FTTx linijų skaičius išaugo 33,8 karto, o per 2013 m. šių linijų skaičius augo 8,7 proc. Lietuva pasauliniame kontekste yra viena pirmaujančių valstybių pagal naujos kartos tinklų plėtrą.

Judrusis ryšys – 26,1 proc.

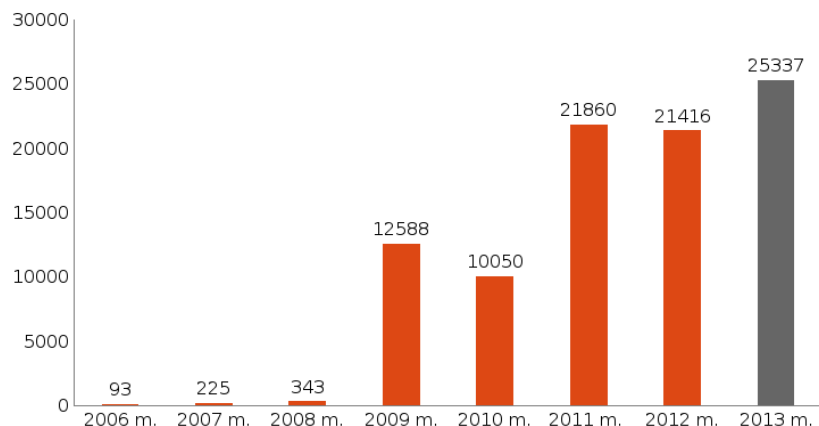


RRT SAUGUMO VEIKLA

TINKLŲ IR INFORMACIJOS SAUGUMO DEPARTAMENTAS



KIBERNETINIO SAUGUMO APŽVALGA



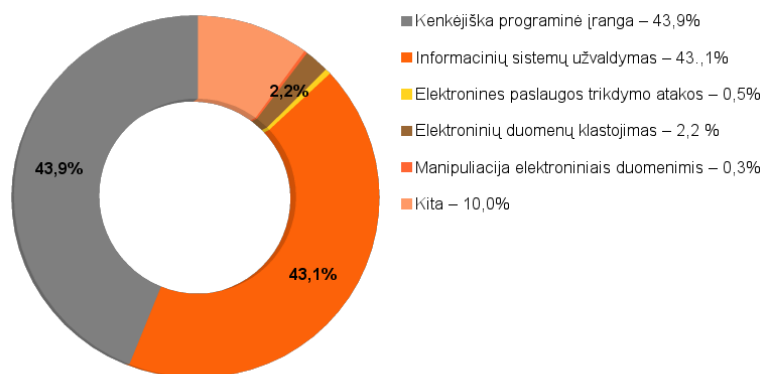
CERT-LT registruotų incidentų skaičius Lietuvoje

CERT-LT 2013-iais ištyrė 25 337 incidentus. Palyginti su 2012 metais (21 416 pranešimų), pranešimų buvo gauta 18 procentų daugiau.

Ištirta 10 924 informacinių sistemų užvaldymo incidentų – 19 proc. daugiau nei 2012 m. (9 148 atvejai), ir tai sudarė 43,1 proc. visų tirtų incidentų.

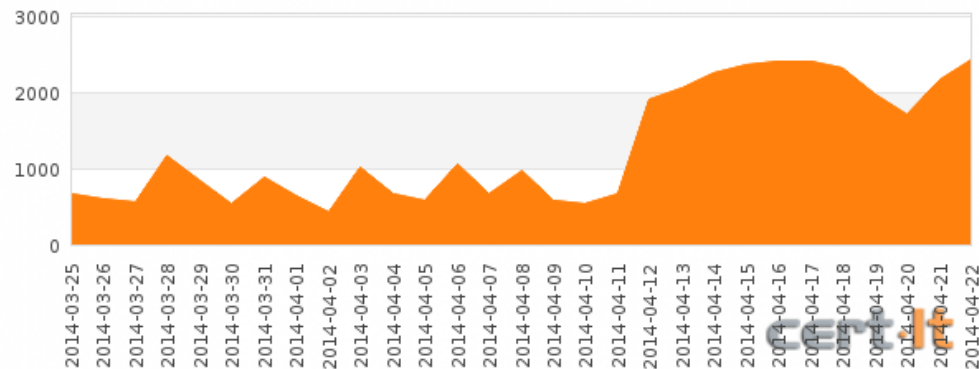
IS užvaldymo incidentai savo ruoštu yra ypatingai pavojingi, nes jų pasekoje įvyksta kiti incidentai: informacijos vagystės, kibernetinės atakos, virusų platinimas ir t.t.

Daugėjo klastojimo (angl. phishing) incidentų. Tirta 558 pranešimų – 3 kartus daugiau nei 2012 m. (185 pranešimai). Didžiąją dalį sudarė pranešimai apie suklastotas finansinių atsiskaitymų paslaugų ir bankų interneto svetaines, kurios veikdavo dažniausiai ne Europos Sąjungos tarnybinėse stotyse.

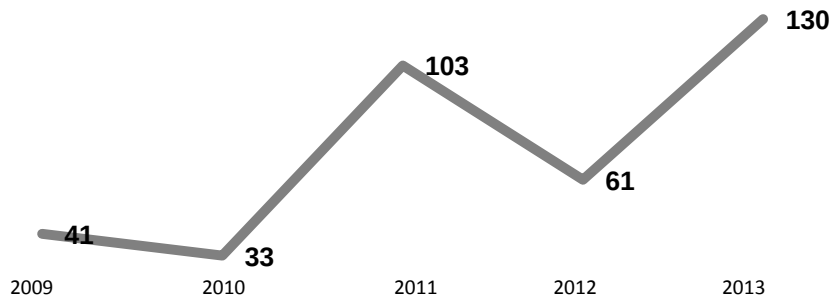


Ištirtų incidentų tipų pasiskirstymas, proc.

PAGRINDINĖS GRĖSMĖS



Botnet tinkluose veikiančių LT IP adresų grafikas, vnt. paroje



DDoS metinė statistika, vnt. per metus

Apie 2-3 tūkst. kompiuterių zombių Lietuvoje dalyvauja *botnet* veiklose kasdieną.

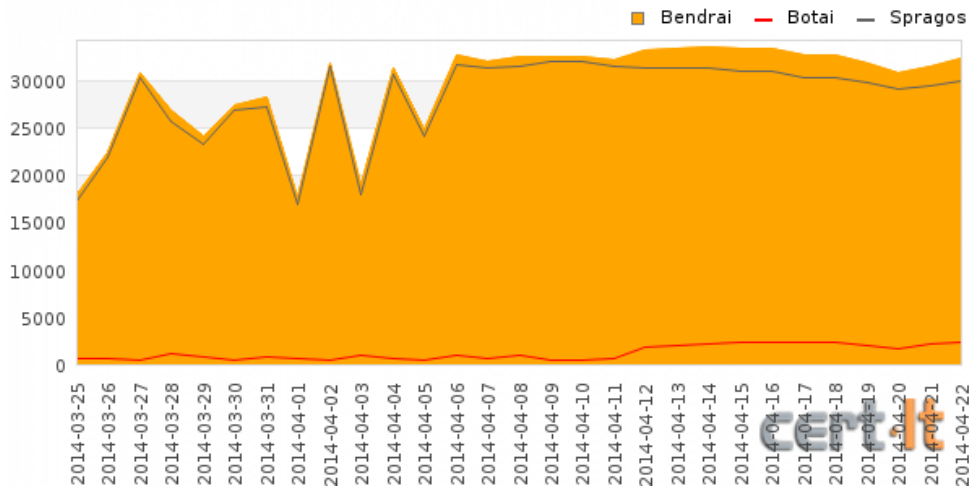
2013-09-09 neutralizuota LT veikęs botneto serveris, kuris galėjo valdyti 5400 kompiuterių visame pasaulyje, iš veikiančių 600, 75 iš LT.

Daugiau *on-line* statistikos dėl *botnet*, *spam* ir kitų grėsmių pateikiama www.cert.lt.

2013 metais CERT-LT ištyrė 130 pranešimų apie elektronines paslaugos trikdymo atakas (angl. denial of service, DoS). Palyginti su 2012 m. (61 pranešimas), pranešimųskaičius padidėjo daugiau nei 2 kartus.

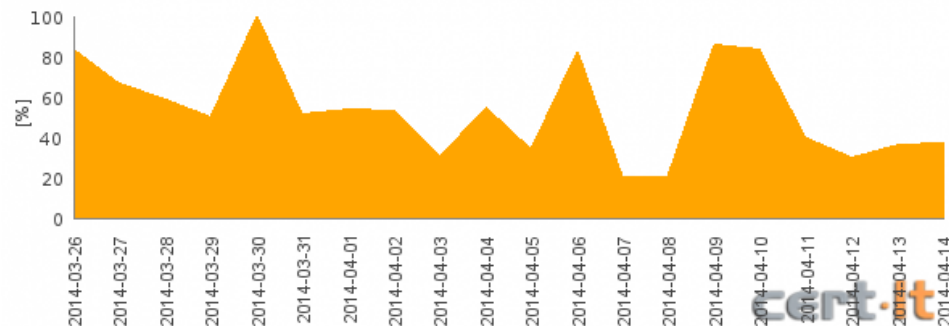


INCIDENTŲ PREVENCIJA



Šiais metais CERT-LT pradėjo nagrinėti Lietuvos interneto tinkle veikiančių įrenginių spragas, kurios gali būti naudojamos paslaugos trikdymo atakoms ar kitai kenkimo veiklai vykdyti. Per 2014-ųjų I ketv. nustatyti 1673 pavojingų spragų egzistavimo atvejai.

Bendras įrenginių, kurie gali būti išnaudoti kenkėjiškai veiklai internete, skaičius



CERT-LT pateiktų rekomendacijų interneto naudotojams efektyvumas

Šis grafikas vaizduoja interneto naudotojams CERT-LT pateiktų rekomendacijų ir priemonių, padėjusių interneto naudotojams, efektyvumą – kiek kompiuterių (procentais nuo visų apkrėstų kompiuterių) visiškai išvalyta taikant CERT-LT siūlomas priemones.



LIETUVOS INTERNETO TINKLO INFRASTRUKTŪROS STEBĖSENA (LITIS)



Kibernetinio saugumo incidentų valdymas yra būtinybė, tačiau dar svarbiau yra interneto tinklo infrastruktūros sklandi ir patikima veika.

LITIS projekto tikslas yra įvertinti Lietuvos interneto tinklo infrastruktūros patikimumą ir vertinti galimas grėsmes saugumui.

Pagrindiniai uždaviniai:

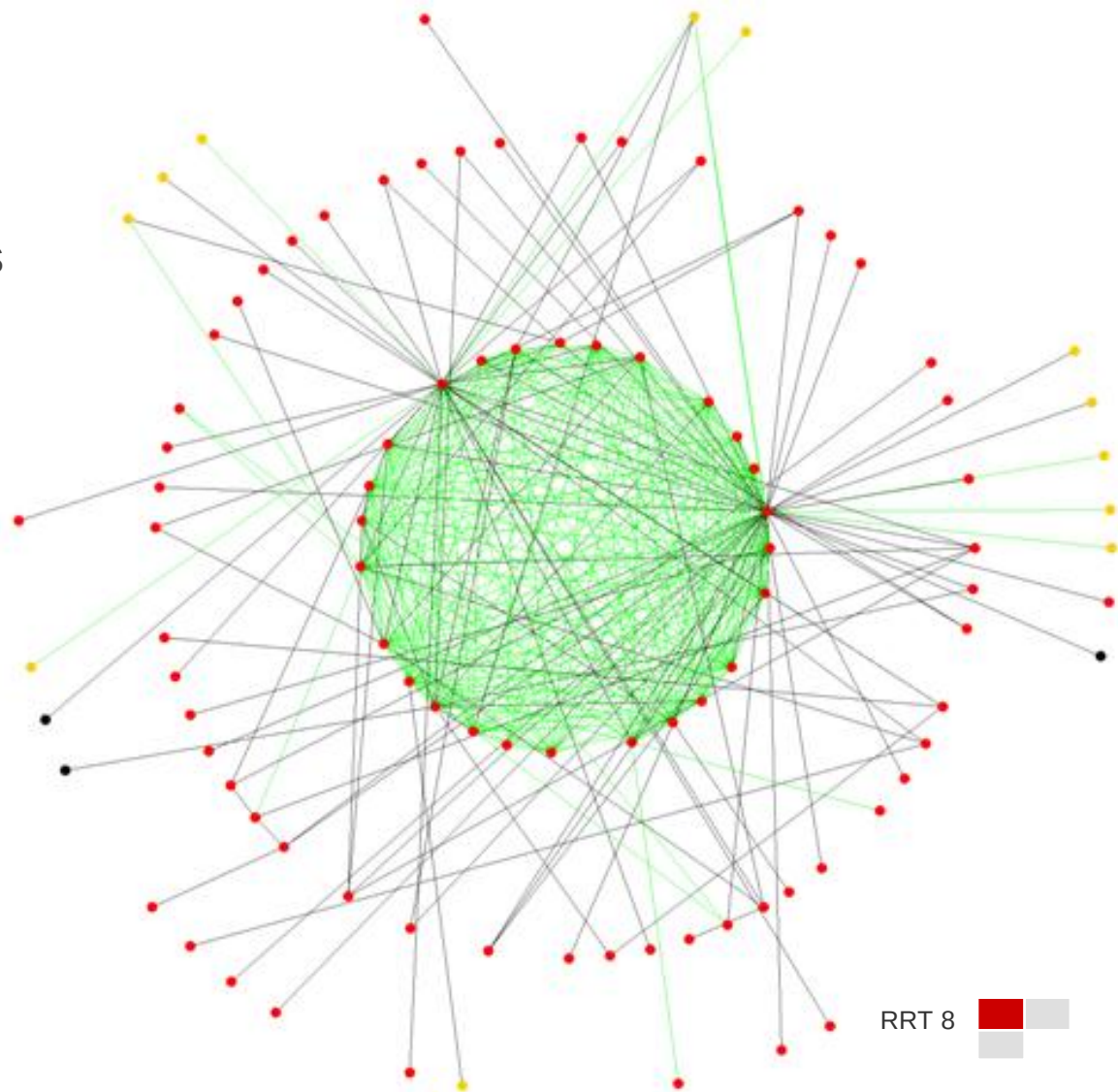
1. Lietuvos interneto tinklo topologijos sudarymas ir virtualizacija (tinklo modelio sudarymas);
2. Kritinių tinklo infrastruktūros elementų identifikavimas (metrikos sudarymas);
3. Kritinių elementų monitorinimas (on-line stebėseną).



LITIS VEIKLA. I ETAPAS

Kai kurie interneto topologijos tyrimo rezultatai

- 114 Lietuvos IPT
- 39 IPT autonominės sistemos
- > 660 tarptinklinių sujungimų
 - > 210 tranzito sujungimų
 - > 450 peering sujungimų



LITIS VEIKLA. I ETAPAS

SQL duomenų bazė ir LITIS vizualizacija.

LITIS ir CERT-LT incidentų valdymo sistemos apjungtos ir koreliuoja tarpusavyje.



Pagrindinis
Iterpti
Paieška
Trinti
Vizualizacija
Monitoringas
Ataskaitos
Apie tyrimą

DB: 2008 ☒

...Pasirinkti...

IPT: ☒

...Rodyti...

Lietuvos Interneto infrastruktūra

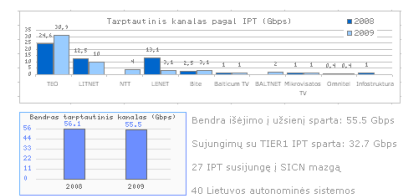
2009 metų duomenimis

Informacija pateikta iš: 64 IPT

Piering'ų skaičius Lietuvoje

Eil.	IPT pav.	ASN	Peering? sk.
1	Infostuktūra	6769	23
2	LITNET	2847	22
3	LRTC	15419	22
4	Dokeda	39354	20
5	Mikrovisatos TV	28679	20
6	So(21211)	21211	19
7	BALTNET(15440)	15440	19
8	BALTNET(8486)	8486	19

Info



Abonentų skaičius

Eil. Nr.	IPT pav.	Abonentų skaičius	%
1	TEO	307601	39.55
2	Ornimitel	95038	12.22
3	Bite	60506	7.78
4	Dokeda	31636	4.07
5	LRTC	31264	4.02
6	So(21211)	26793	3.44
7	Viginta	23039	2.96

Sujungimai su TIER1

Eil.	Iš IPT	I IPT	Technologija	Sparta [Gbps]
1	TEO	TeliaSonera	Optika	10
2	TEO	TeliaSonera	Optika	10
3	TEO	TeliaSonera	Optika	10
4	LENET	Level3	Optika	1.5
5	Bite	Global Crossing	Optika	1.244

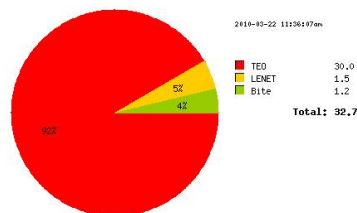


Lietuvos Interneto infrastruktūra

2009 metų duomenimis

in

Sujungimai su Užsienio IPT (TIER1)



Eil.	Iš IPT	I IPT	Technologija	Sparta [Gbps]
1	TEO	TeliaSonera	Optika	10
2	TEO	TeliaSonera	Optika	10
3	TEO	TeliaSonera	Optika	10
4	LENET	Level3	Optika	1.5
5	Bite	Global Crossing	Optika	1.244

LITIS VEIKLA. II ETAPAS

RRT viešųjų pirkimų būdu atliko galimybių studiją, kurioje BAIP, kartu su KTU ekspertais, suformulavo gaires būsimoms RRT studijoms dėl interneto patikimumo tyrimų.

Apsibrėžta, kad IP adresai, IP adresų režiai, domenų vardai, tinklų maršrutizacija ir autonominės sistemos yra esminiai komponentai interneto tinklo infrastruktūros funkcionalumui apibūdinti.

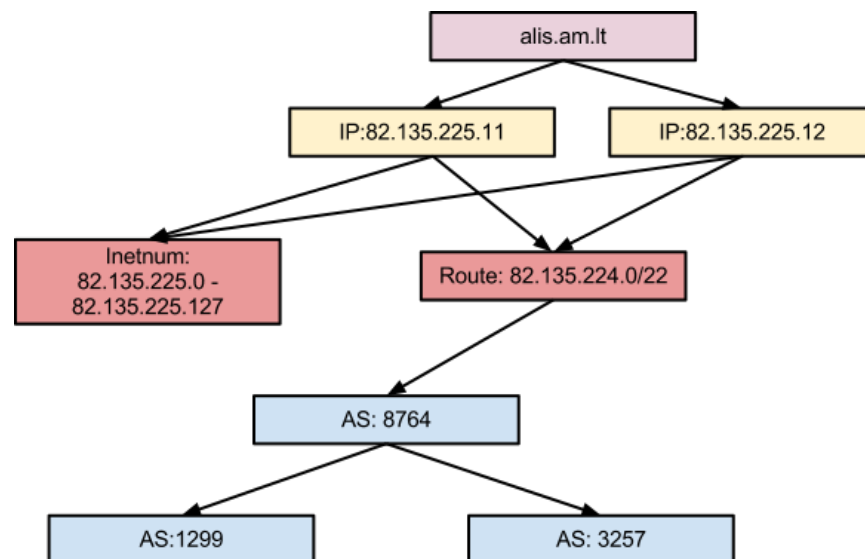
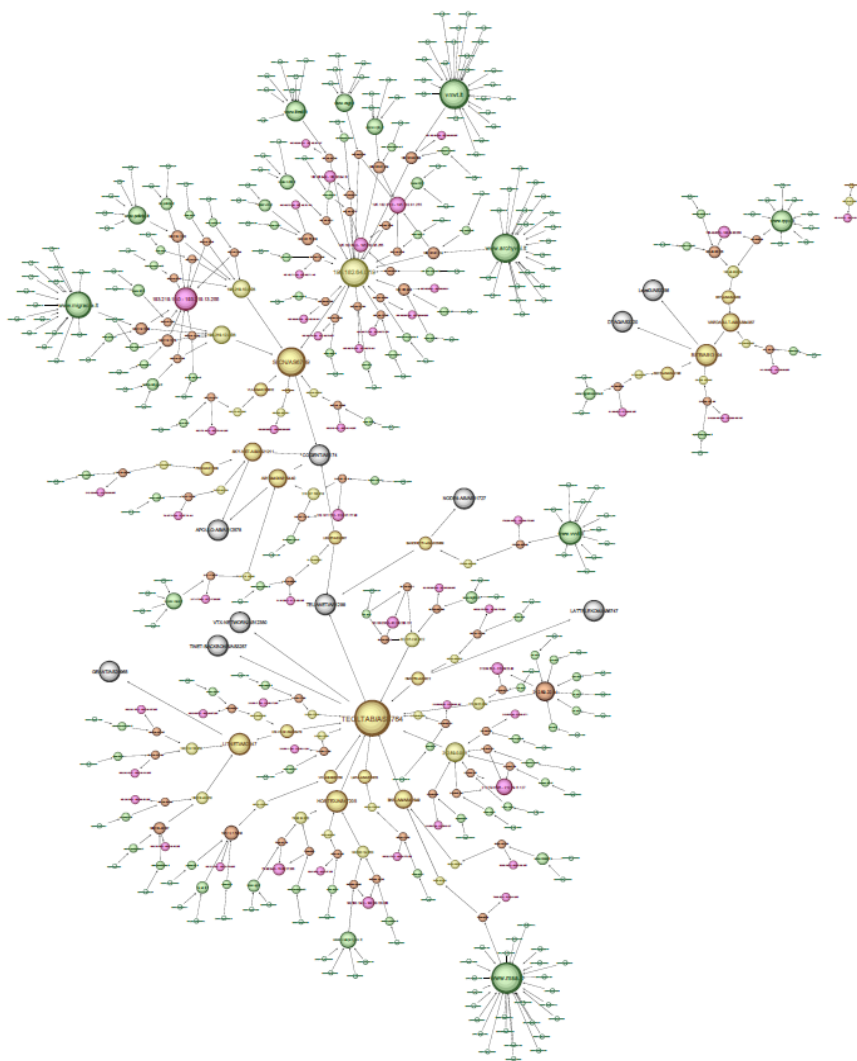
Kritiniai interneto tinklo elementai yra infrastruktūra (*domain name, IP address, IP address ranges, routes and autonomies systems*), kuri yra tiesiogiai susijusi su šių sektorių elektroninėmis sistemomis internete:

1. Informacijos ir ryšių technologijos;
2. Energetikos;
3. Finansų sistemos;
4. Viešo sektoriaus;
5. Gėlo vandens ir maisto tiekimo;
6. Sveikatos priežiūros;
7. Transporto.



LITIS VEIKLA. II ETAPAS

Kritinių e. paslaugų infrastruktūros pvz. (*url*->*ISPs*->*transit ISPs*)

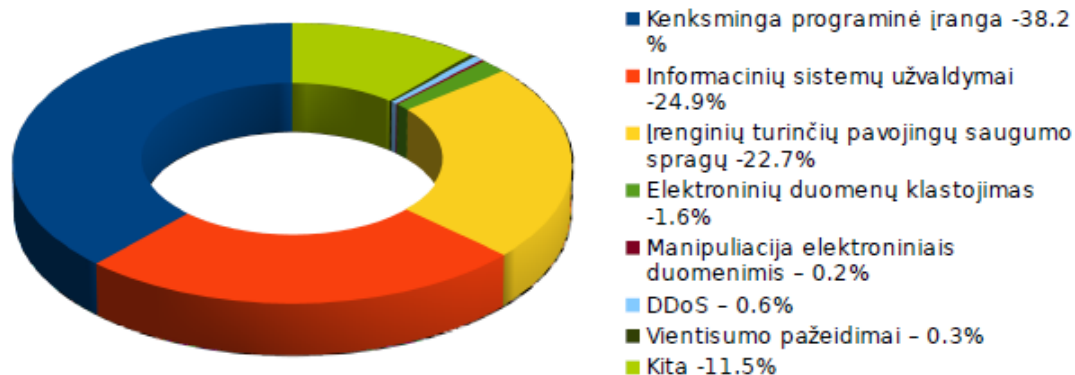


DEBESŲ KOMPIUTERIJA



Daugėjant debesų kompiuterijos pagrindu teikiamų paslaugų, kibernetinės atakos yra orientuojamos į **debesų kompiuterijos paslaugų teikėjus**, o dėl debesų kompiuterijos paslaugų specifikos tokių kibernetinių atakų padaroma **žala yra didelė** (pvz., ataka prieš vieną interneto svetainių prieglobos paslaugų teikėją galėtų pakenkti daugybei interneto svetainių).

atsižvelgiant į ypatingą teikiamų paslaugų svarbą, dažnai kyla klausimai dėl debesų kompiuterijos paslaugų saugumo, patikimumo ir duomenų apsaugos, kas kelia vartotojų nepasitikėjimą debesų kompiuterijos paslaugų teikėjais.



2014 m. I ketvirtį CERT-LT užfiksuotų incidentų statistika, proc.



DEBESŲ KOMPIUTERIJA



RRT, kaip institucija, kurios viena iš svarbiausių **funkcijų yra užtikrinti saugumą elektroninėje erdvėje**, stebi **debesų kompiuterijos paslaugų rinką** ir siekia aiškumo dėl:

1. Šių paslaugų teikėjų reguliavimą (tiek ES, tiek Lietuvos mastu);
2. Duomenų apsaugos, paslaugų saugumo, patikimumo užtikrinimo sąlygas;
3. Šioje srityje galiojančius standartus, reglamentavimą.

Atliekant tyrimą **aiškėja**:

1. Šiuo metu debesų kompiuterijos paslaugų teikėjų veikla **nėra reguliuojama**. Tiek Lietuvoje, tiek ES **nėra minimalių informacijos apsaugos reikalavimų ar rekomendacijų** šios paslaugos teikėjams, taip pat **teikėjai nėra įpareigoti pranešti apie įvykusius incidentus CERT padaliniams**.
2. Kiekvienas teikėjas savo paslaugų teikimo sutartyse individualiai nurodo teikiamų paslaugų duomenų apsaugą, patikimumą, vartotojų įsipareigojimus ir atsakomybę, **nėra vartotojams skirtų rekomendacijų** renkantis, lyginant debesų kompiuterijos paslaugų teikėją, jo suteikiamas *garantijas*.





„PASLĖKTA“ PROBLEMATIKA

Kibernetinis saugumas yra sudėtingas, kompleksiškas ir ypatingai dinamiškas procesas, todėl mokslinių tyrimų reikšmė šiose srityje yra nepakankamai įvertinta akademijos, o interneto tinklo saugumo ir vientisumo tyrimų apskritai vyksta vienetai.

Nesvarbu koku lygiu sprendžiame kibernetinio saugumo klausimą (viešas-privatus-tinklo-vartotojo-...), praktikoje investuojame į arba technologinius (Firewall-IDS-IPS-...) arba procesinius (rizikų valdymas-auditas-standartai-...) sprendimus.

Nesvarbu kiek ir už kiek įsigysime įrangos, svarbu kokio lygio specialistai valdys procesus.

Akademiniis specialistų rengimas siaurėjant specializacijai yra neadekvatus:

Informatikos bakalauro programų: 13 (VU, VGTU, KTU, VDU, LEU, MRU, KU).

Informacijos saugumo magistro programų: 2 (KTU, VGTU).

Interneto inžinerijos programų: 1 (Kazimiero Simonavičiaus universitetas).



IŠVADOS

- Lietuvos elektroninių ryšių rinkoje internetas vystosi ypač dinamiškai.
- Moderni Lietuvos interneto infrastruktūra. Šviesolaidinės ryšio linijos (FTTx) Lietuvoje išlieka pagrindine plačiajuosčio ryšio paslaugų teikimo technologija.
- Kibernetinių incidentų mastas, ir ypač auganti jų įtaka tinklams ir IS, turi būti vertinama kaip rimta ir nuolatinė grėsmė tinklams, IS bei vartotojams.
- RRT vykdomas nacionalinio interneto tinklo infrastruktūros tyrimas sudaro geras prielaidas išsamiai ir objektyviai įvertinti nacionalinio interneto patikimumą, nustatyti kritinius elementus ir vykdyti jų nuolatinę stebėseną.
- Nustačius minimalius informacijos saugumo reikalavimus ir rekomendacijas *debesų kompiuterijos* paslaugų teikėjams ir prižiūrint šių reikalavimų įgyvendinimą, būtų užtikrinama, kad vartotojams būtų teikiamos patikimos *debesų kompiuterijos* paslaugos ir garantuojama jų duomenų apsauga. Įpareigojus *debesų kompiuterijos* paslaugų teikėjus teikti informaciją apie kibernetinius incidentus, būtų galimybė išnaudoti šią informaciją CERT-LT veikloje, siekiant sumažinti analogiškų incidentų pasikartojimo riziką kitiems *debesų kompiuterijos* paslaugų teikėjams. Kol kas vyksta RRT konsultacija su *debesų kompiuterijos* rinka.
- Mokslinių tyrimų ir akademijos indėlis vertinant kibernetinį saugumą, rengiant adekvačiai kibernetikai paruoštus specialistus bei suponuojant naujus efektyvius kibernetinio saugumo sprendimus yra būtinybė.

INFORMACIJOS ŠALTINIAI



- www.rrt.lt
- www.esaugumas.lt
- www.cert.lt
- www.draugiskasinternetas.lt



Ačiū už dėmesį!



rytis.rainys@rrt.lt
Ryšių reguliavimo tarnyba
Algirdo g. 27A
LT-03219 Vilnius