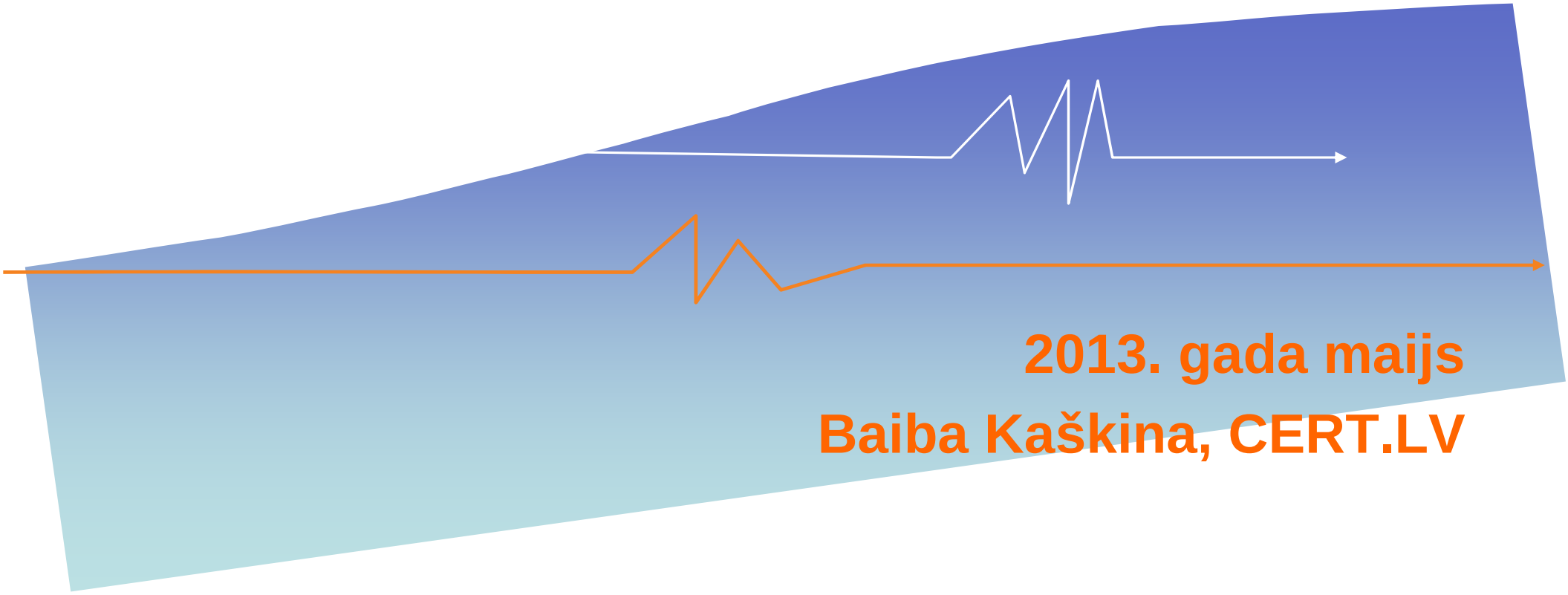
IT drošība Latvijā, atbildīgs IPS un citas CERT.LV aktivitātes



2013. gada maijs

Baiba Kaškina, CERT.LV

Par CERT.LV un likumdošanu

CERT.LV

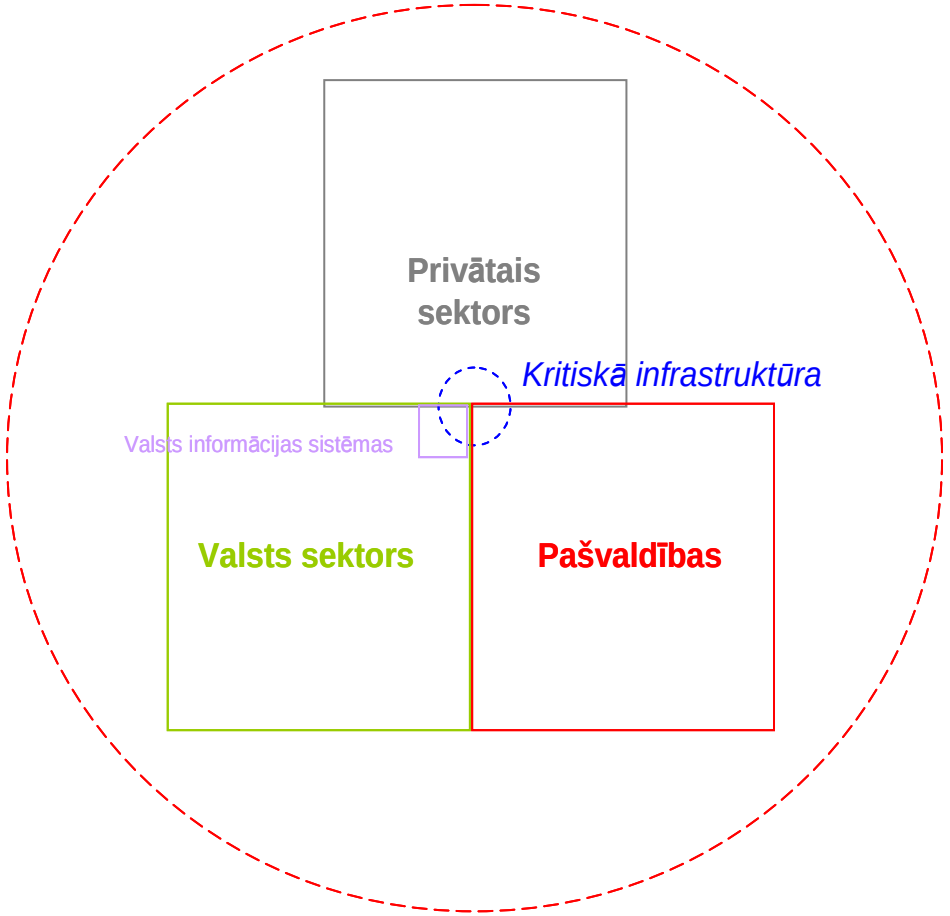
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Misija: “Veicināt IT drošību Latvijā”

CERT.LV

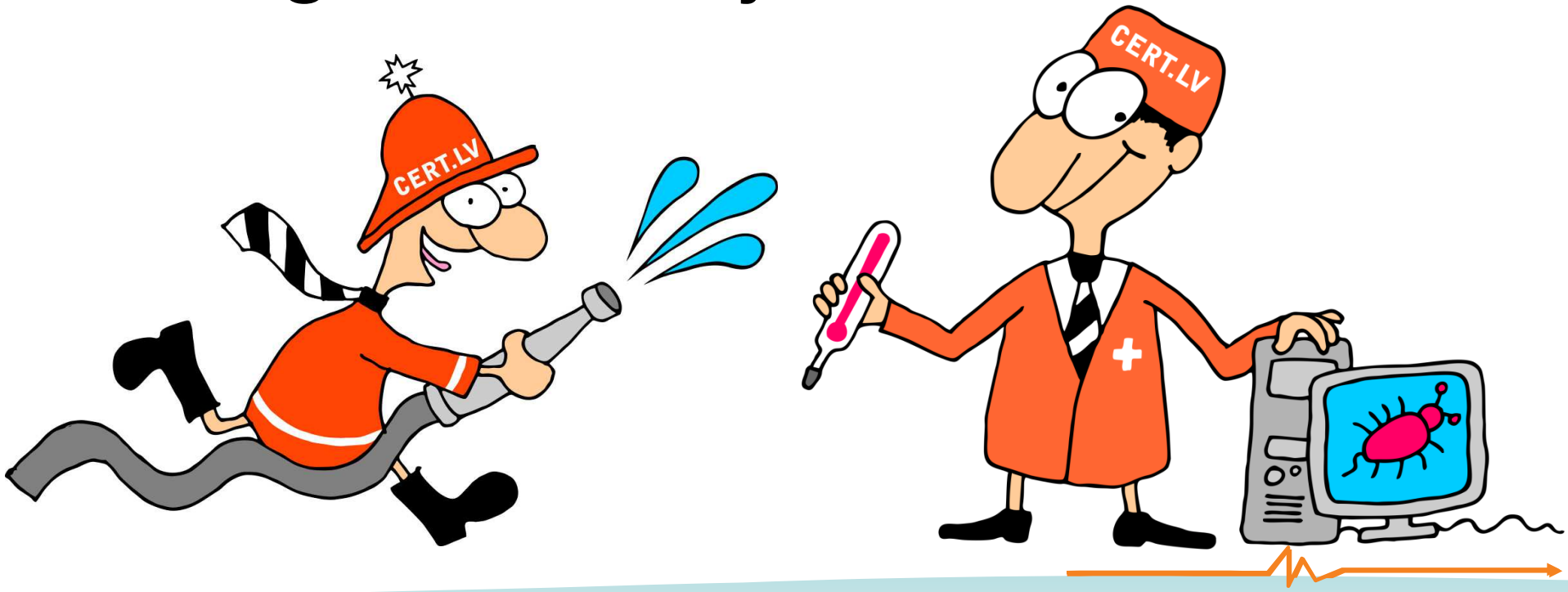
- Darbojas saskaņā ar “Informācijas tehnoloģiju drošības likumu” kopš 2011.gada 1.februāra
- Darbības uzdevumi un tiesības tiek deleģētas Latvijas Universitātes aģentūrai “Latvijas Universitātes Matemātikas un informātikas institūts”
- Finansēta no valsts budžeta
- Visi pakalpojumi ir bezmaksas

CERT.LV kopiena



Kas ir CERT.LV?

- “Ģimenes ārsts” un “ugunsdzēsējs” e-vidē



IT drošības likums

- Pieņemts Saeimā 2010.gada 28.oktobrī
- Stājas spēkā 2011.gada 1.februārī
- Nosaka CERT.LV izveides kārtību
- Saistītie MK noteikumi par:
  - Kritiskās infrastruktūras drošības pasākumu plānošanu (spēkā no 2011.gada 1.februāra)
  - Elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanu (spēkā no 2011.gada 1.maija)
- Nosaka Nacionālās informācijas tehnoloģiju drošības padomes izveidi

Elektronisko sakaru komersantu pienākumi

- Nodrošināt maksimāli iespējamo pakalpojumu sniegšanas nepārtrauktību
- Informēt CERT.LV būtisku incidenta gadījumā
- Sniegt CERT.LV pieprasīto informāciju saistībā ar incidentiem
- Pēc CERT.LV pieprasījuma slēgt galalietotājam piekļuvi elektronisko sakaru tīklam
- Pēc CERT.LV pieprasījuma, ja ir būtiski drošības vai integritātes pārkāpumi, organizēt auditu

CERT.LV

MK noteikumi nr.327 “Noteikumi par elektronisko sakaru komersantu rīcības plānā ietveramo informāciju, šā plāna izpildes kontroli un kārtību, kādā galalietotājiem tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam”

Rīcības plāns

1. Vispārīgas ziņas par komersantu, juridiskā adrese, elektroniskā pasta adreses
2. Persona vai struktūrvienība, kas nodrošina drošības pasākumu īstenošanu (tālruņa numurs, fakss, e-pasts)
3. Elektronisko sakaru tīkla uzbūves vispārīgs apraksts un shēma
4. Elektronisko sakaru tīkla risku analīze
5. Reaģēšanas kārtība uz drošības incidentiem
6. Tīkla darbības atjaunošanas pasākumu apraksts

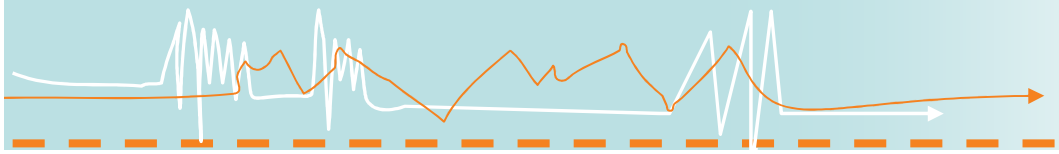
Rīcības plāna paraugs pieejams CERT.LV mājas lapā

Svarīgi no MK noteikumiem

- Izņēmumi attiecībā uz Kritisko infrastruktūru
- Ja ir izmaiņas – plāns jāaktualizē
- Mēneša laikā par izmaiņām jāinformē CERT.LV
- Jānorāda, ja informācija ir Ierobežotas pieejamības
- CERT.LV izvērtē plānu un var lūgt izdarīt labojumus
- CERT.LV izmanto informāciju, īstenojot IT drošības likumā noteiktos uzdevumus un tiesības

Galalietotāju īslaicīga atslēgšana

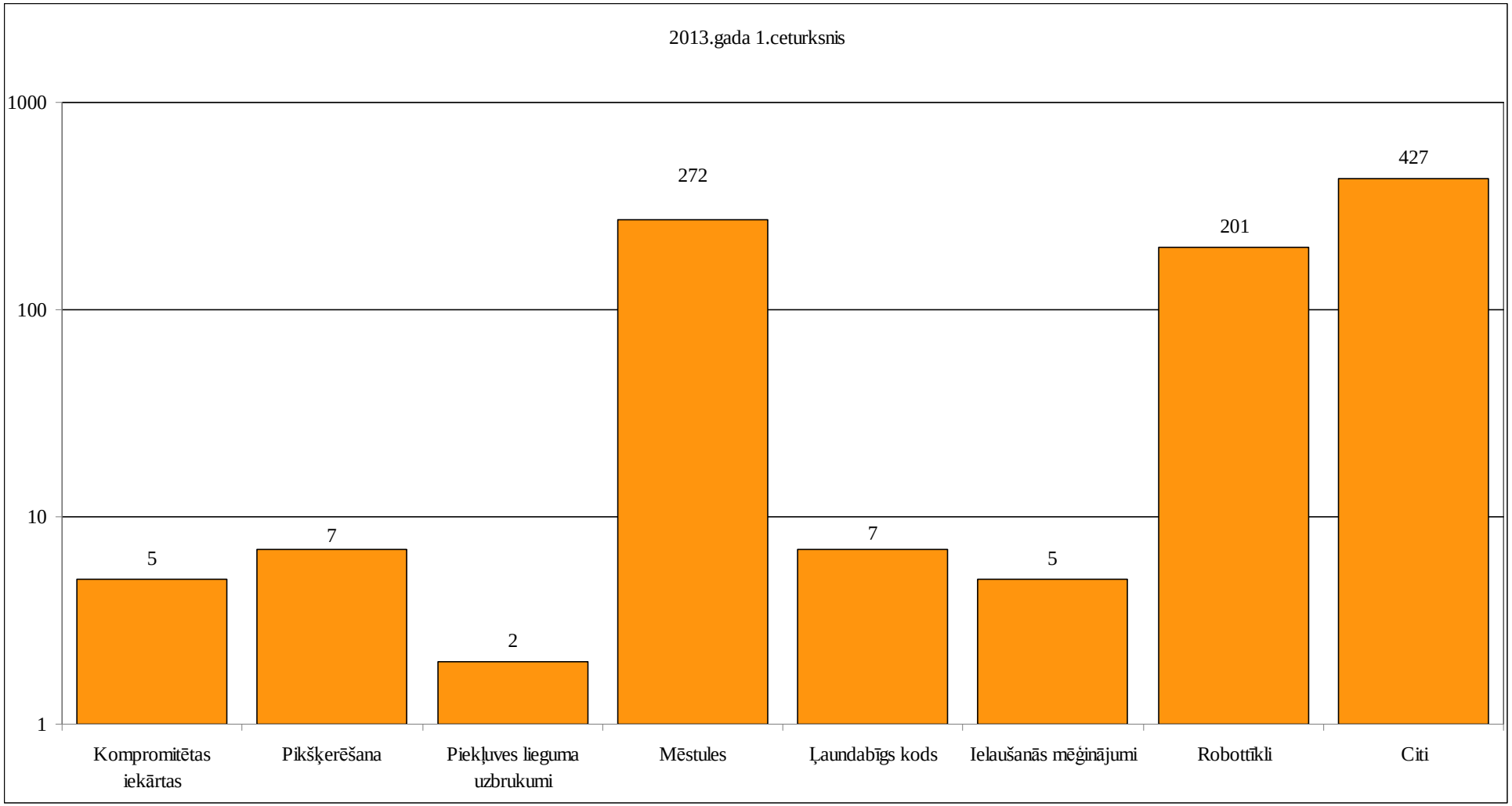
- CERT.LV var pieprasīt atslēgt galalietotāju uz laiku līdz 24h
- Pieprasījums tiek nosūtīts elektroniski
- CERT.LV informē arī telefoniski gan IPS, gan VP
- Jāatslēdz stundas laikā
- Atslēgšana – lai darbība skartu pēc iespējas mazāku skaitu citu galalietotāju



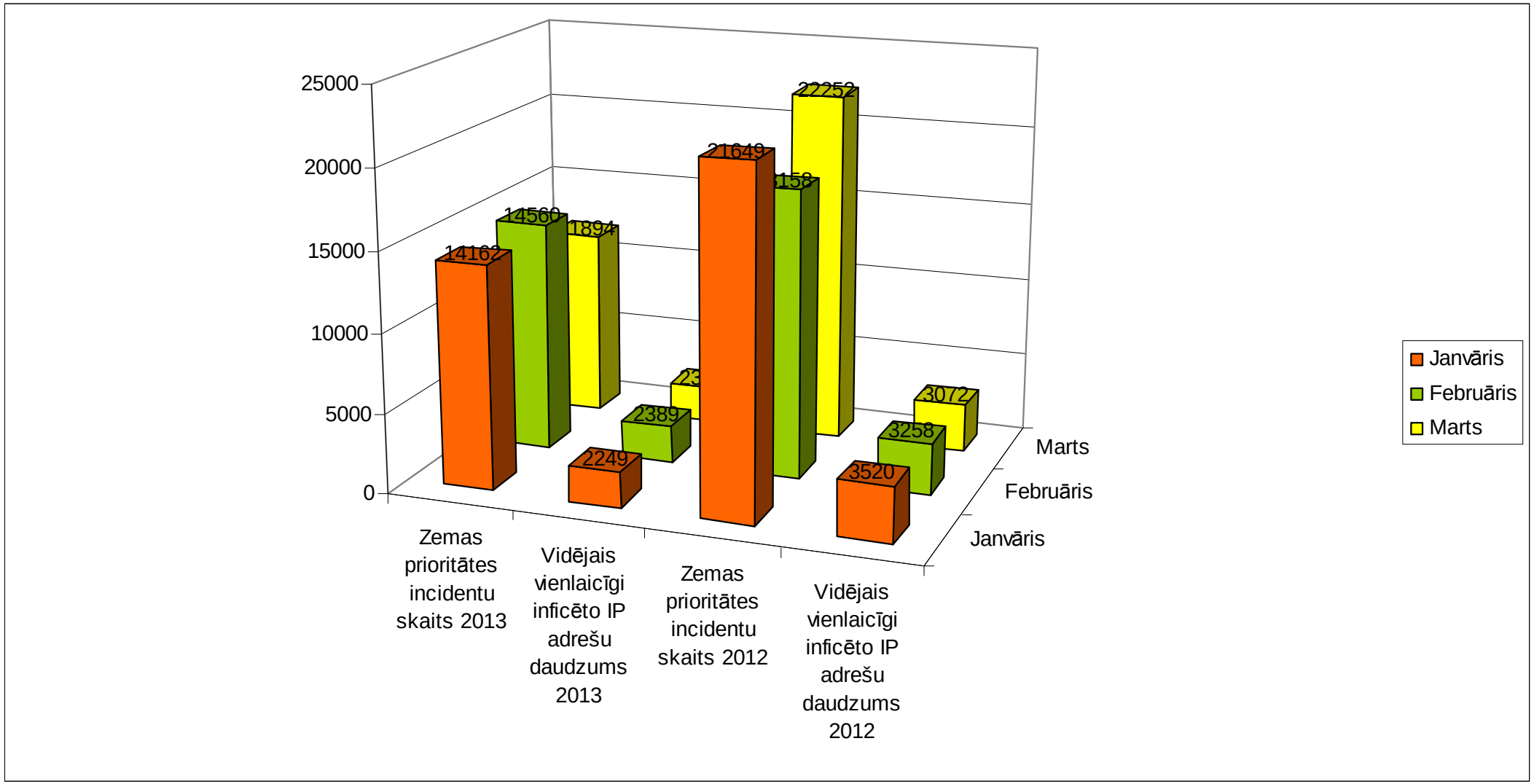
CERT.LV

2013.gada 1.ceturksnis

Augstas prioritātes incidenti - 926



Zemas prioritātes incidentu dinamika



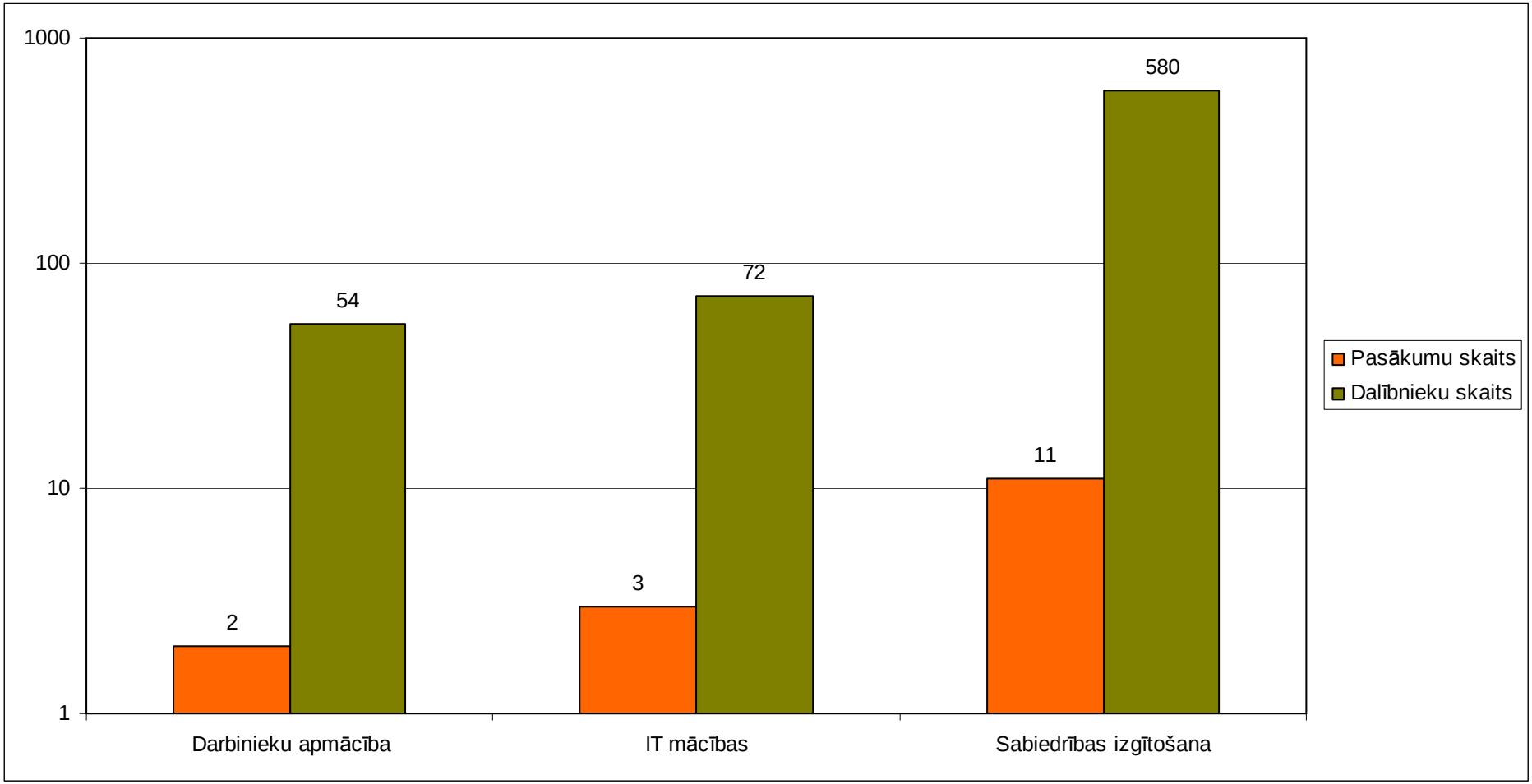
CERT.LV - 1.ceturksnis skaitļos

- 926 augstas prioritātes incidenti
- 31714 zemas prioritātes incidenti
- Vidēji 50 uzlauztas lapas mēnesī; janvārī, februārī - > 200

1.ceturksnis - tendences

- Wordpress un Joomla! ievainojamības, Indonēzijas hakeri
- Atklātas ievainojamas mājas lapas un sistēmas – organizācijas ar to neko nedara, jo nav resursu
- Uzbrukums Spamhaus spoguļserverim
- Dažādu spiegu tīklu darbības pazīmju meklēšana
- Policijas izspiedējvīruss

Sabiedrības izglītošana



CERT.LV - 1.ceturksnis skaitļos

- Organizēti 17 semināri, apmācīti 772 cilvēki
- 9 raksti esidross.lv portālā
- 37 ziņas cert.lv
- 5 radio pārraides, 5 TV sižeti
- 16 ziņas dažādos portālos
- Informācija par 574 kontaktpersonām

CERT.LV

Atbildīgs Interneta pakalpojumu sniedzējs

CERT.LV

Atbildīgs interneta pakalpojumu sniedzējs

Sadarbības memorands starp:

- Latvijas Interneta asociācijas *Net-Safe Latvia* Drošāka interneta centru
- Informācijas tehnoloģiju drošības incidentu novēršanas institūciju *CERT.LV*
- Elektronisko sakaru pakalpojumu komersantu / Interneta pakalpojumu sniedzēju (IPS)

Mērķis, lai Interneta pakalpojumu sniedzējs:

- Iestātos par drošāku interneta vidi Latvijā
- Informētu gala lietotājus gadījumos, kad viņu datori ir inficēti ar kādu datorvīrusu
- Aktīvi iesaistītos cīņā ar kriminalizēto pornogrāfiju saturošu materiālu apriti internetā

Memoranda saturs:

- Centra atbildība un saistības
- CERT.LV atbildība un saistības
- IPS atbildība un saistības attiecībā uz Centru
- IPS atbildība un saistības attiecībā uz CERT.LV

CERT.LV atbildība un saistības:

- Apkopot un nosūtīt reizi dienā informāciju par inficētajām IP adresēm
- Izvietot mājas lapā informāciju par Atbildīgajiem IPS
- Konsultēt klientus par drošības incidentiem

IPS atbildība un saistības attiecībā uz CERT.LV:

- Deleģēt pārstāvi sadarbībai
- Saņemt un apstrādāt inficēto IP adrešu datu bāzi, piecu darba dienu laikā informējot IP adreses lietotāju par inficēto ierīci
- Noteikti ziņojumā jāietver šāda informācija:
  - Inficētā IP adrese un/vai incidenta identifikators, TCP/IP ports, uz kuru norādītajā laikā IP adrese pieslēdzas sensoram;
  - Datorvīrusa nosaukums, ieteikumi, kā problēmu risināt;
  - Norāde, ka informācija saņemta no CERT.LV.
- Informēt klientus, kā saņemt sīkāku informāciju (zvanot vai rakstot CERT.LV)

CERT.LV

Atbildīgie interneta pakalpojumu sniedzēji

IZZI

LATNET
biznesa klases internets

interneta pasaule

dtg
Datu tehnoloģiju grupa

spx IT

ILVA

sigma net

lattelecom

LATVIJAS UNIVERSITATE
ANNO 1919

FirstHost
Over expected

GARMTECH

EXTRANETS
HIGH QUALITY INTERNET PROVIDER

Business Class Internet®
VERSIJA

Citas CERT.LV aktivitātes

Drošības ekspertu grupa

Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupa (DEG):

- Dibināta 2012.gada 16.augustā LV CSIRT grupas vietā
- Statūti un Ētikas kodekss
- Noteikumi biedru uzņemšanai
- Sanāksmes reizi mēnesī
- Šobrīd 30 dalībnieki

esi drošs

Mēs atbildam par savu drošību informācijas tehnoloģiju laikmetā

Meklēt...

Mājās | Darbā | Publiskās vietās | Ieteikumi | Par drošību | Pasākumi | Notikumi pasaulē

Tēmas

- Ap un par drošību (23)
- Darbā (16)
- Ieteikumu lāde (23)
- Mājās (24)
- Notikumi pasaulē (1)
- Pasākumi un notikumi (6)
- Publiskās vietās (16)

Saišu lenta

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija – CERT.LV
- LR Satiksmes ministrija
- LV CSIRT iniciatīva
- Net-Safe Latvia Drošāka interneta centrs

Publikāciju kalendārs

maijs 2012						
P	O	T	C	P	S	Sv
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			
« Apr						

Populārākie krāpšanas veidi internetā

Būtu jau labi, ja īstajā brīdī vienmēr varētu bez šaubīšanās pateikt šos vārdus. Vienkārši saprast, ka kāds cenšas Jūs apkrāpt...

AKTUĀLIE RAKSTI

2012. gada 27. februāris 2

Kā atpazīt pikšķerēšanu?

Jau iepriekšējos rakstos par pikšķerēšanu ("Pikšķerēšana jeb, kā atdot savu naudu katram gribētājam" un "3 padomi – kā pasargāt sevi...

2012. gada 23. februāris 2

Kas jāzina, lai droši lietotu „draugiem.lv"?

Šodien vairs neviens nerunā par sociālo tīklu un portālu augošo popularitāti pasaulē. Tas jau ir noticis fakts! Pasaule ir "socializējusies"...

CERT.LV | NIC

Laipni lūdzam mājaslapā

ESI DROŠS!

Šī mājaslapa ir paredzēta **ikvienam, kurš rūpējas par sava datora drošību un savu drošību internetā**. Mājas lapu uztur Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) un tajā informācijas tehnoloģiju speciālisti no LV-CSIRT iniciatīvas grupas sniedz padomus, dalās pieredzē, kā arī ir gatavi atbildēt uz Jūsu jautājumiem par Jūsu datora drošību un Jūsu drošību internetā.

Jaunākie raksti

- Populārākie krāpšanas veidi internetā
- Kāda vīrieša datorā Datorologs uzgājis 110 vīrusus!
- Pārbaudi sava datora veselību pie Datorologa!
- Kā atpazīt pikšķerēšanu?
- Kas jāzina, lai droši lietotu „draugiem.lv"?

Jaunākie komentāri

Citas aktivitātes

- Palīdzība IT drošības incidentu gadījumos
- IT drošības dokumentu paraugi
- Semināri, mācības, sabiedrības izglītošana
- Dalība “atbildīgo IPS” semināros
  - Prezentācijas
  - Plakāti, citi materiāli

Nākotne

- Latvijas izvēlētais ceļš – drošība caur sadarbību
- IT drošības līmeni valstī var paaugstināt tikai kopīgiem spēkiem
- IT drošībai jākļūst par katra ikdienu
- Lietotāji jāturpina izglītot un ieinteresēt IT drošībā

Paldies par uzmanību!

https://www.cert.lv/

baiba.kaskina@cert.lv

https://twitter.com/certlv

Semināra programma

13:00-13:30 IT drošība Latvijā, Atbildīgs IPS un citas CERT.LV aktivitātes

13:30-13:45 IT drošības incidentu veidi, kāda informācija tiek sūtīta inficētajiem lietotājiem, kur tā tiek iegūta

13:45 - 14:30 Ko ieteikt lietotājam, ja viņa dators inficēts: biežāk sastopamās infekcijas, kā tās izpaužas, kā izplatās un kuras ir bīstamākās

14:30 - 15:00 Kafijas pauze

15:00 - 16:00 Ko ieteikt lietotājam, ja viņa dators inficēts: datora ārstēšana un ieteicamie rīki, kā arī kas var notikt, ja dators netiek ārstēts

16:00 - 16:15 Informācija drošākai interneta lietošanai

16:15 – 16:30 Jautājumi/atbildes