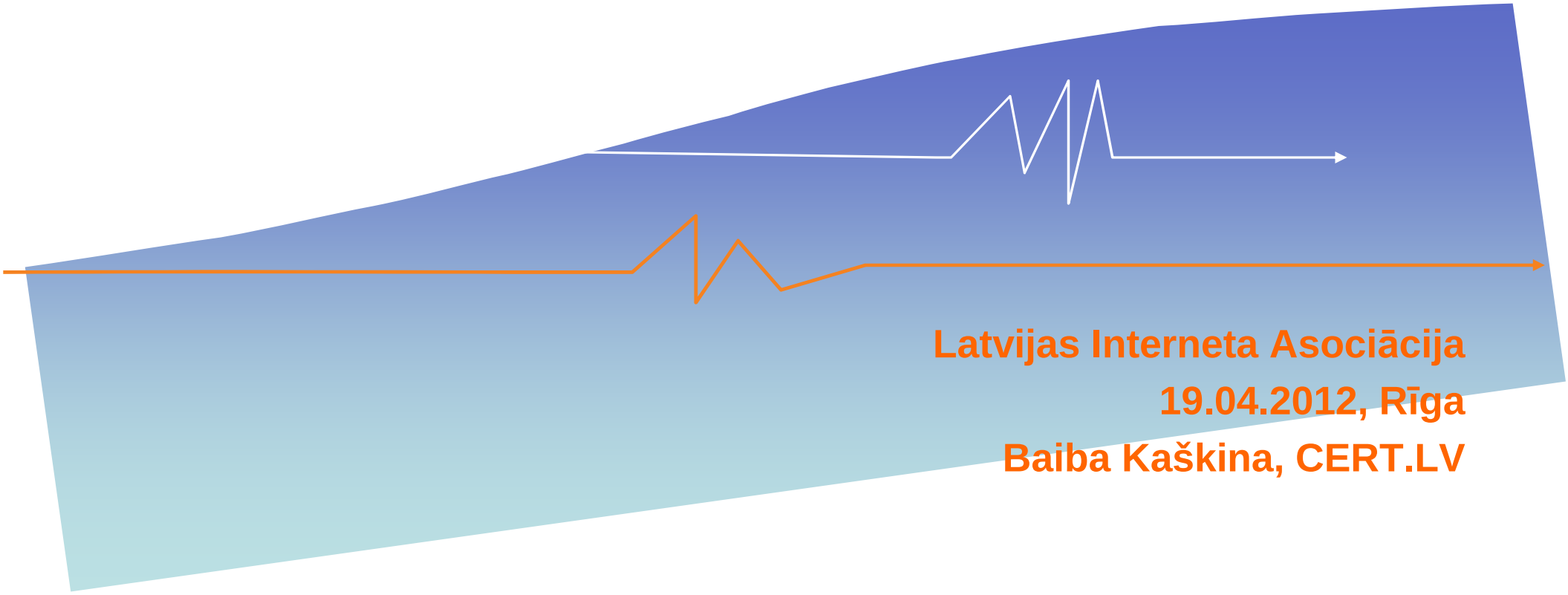
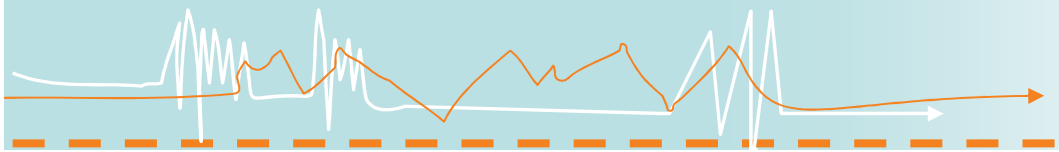
Situācija IT drošības jomā Latvijā



Latvijas Interneta Asociācija

19.04.2012, Rīga

Baiba Kaškina, CERT.LV



CERT.LV

Par CERT.LV

Kas ir CERT.LV?

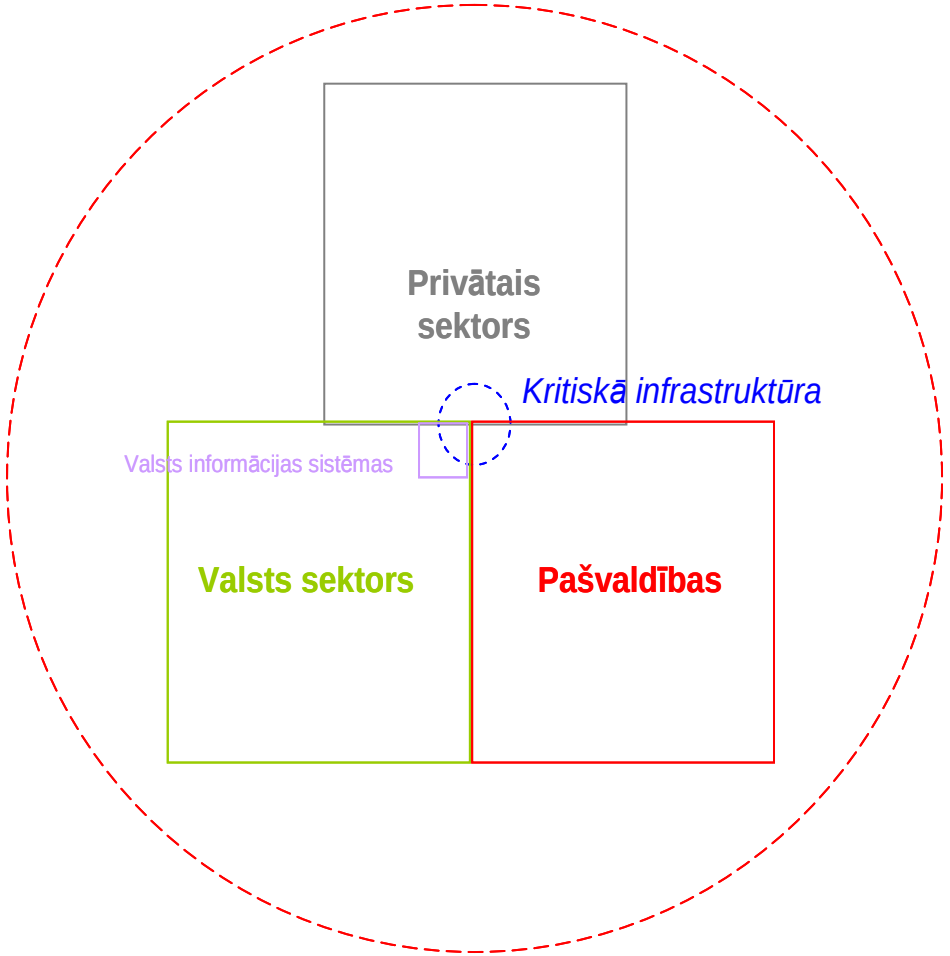
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Misija: “Veicināt IT drošību Latvijā”

CERT.LV

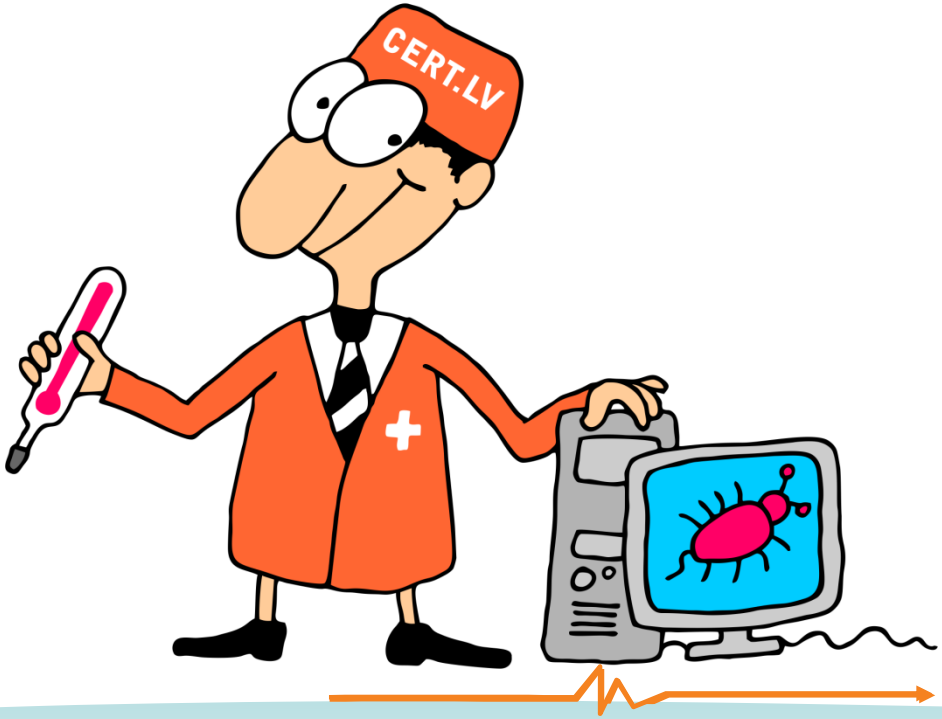
- Darbojas saskaņā ar “Informācijas tehnoloģiju drošības likumu” kopš 2011.gada 1.februāra
- Darbības uzdevumi un tiesības tiek deleģētas Latvijas Universitātes aģentūrai “Latvijas Universitātes Matemātikas un informātikas institūts”
- Finansēta no valsts budžeta
- Visi pakalpojumi ir bezmaksas

CERT.LV kopiena



Kas ir CERT.LV?

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



Aktuālā situācija

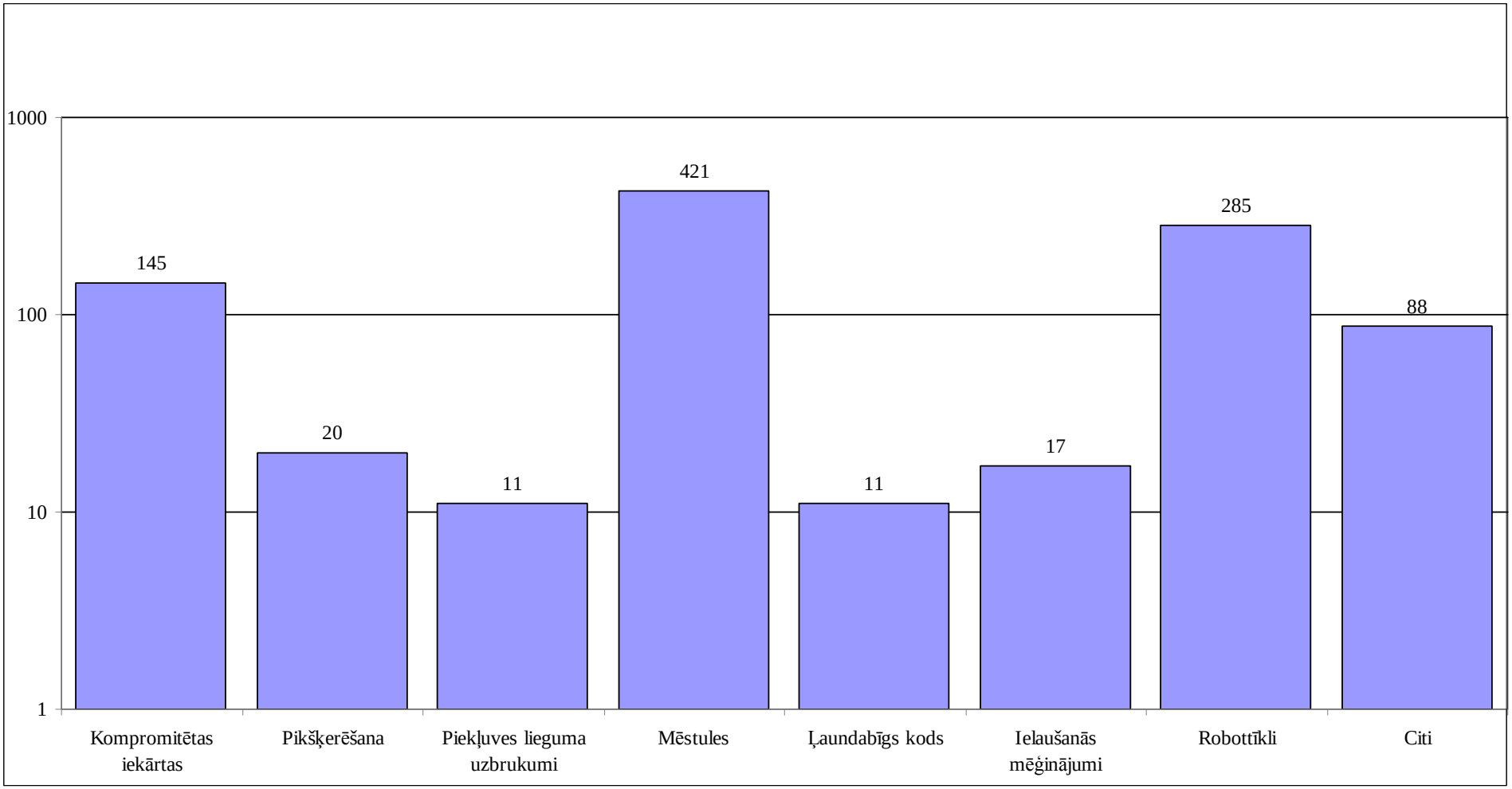
No kurienes nāk informācija?

- Automātiskie ziņojumu avoti (~20)
- Incidentu ziņojumi no Latvijas
- Incidentu ziņojumi no citām valstīm
- CERT.LV vāktie dati

Aktuālā situācija

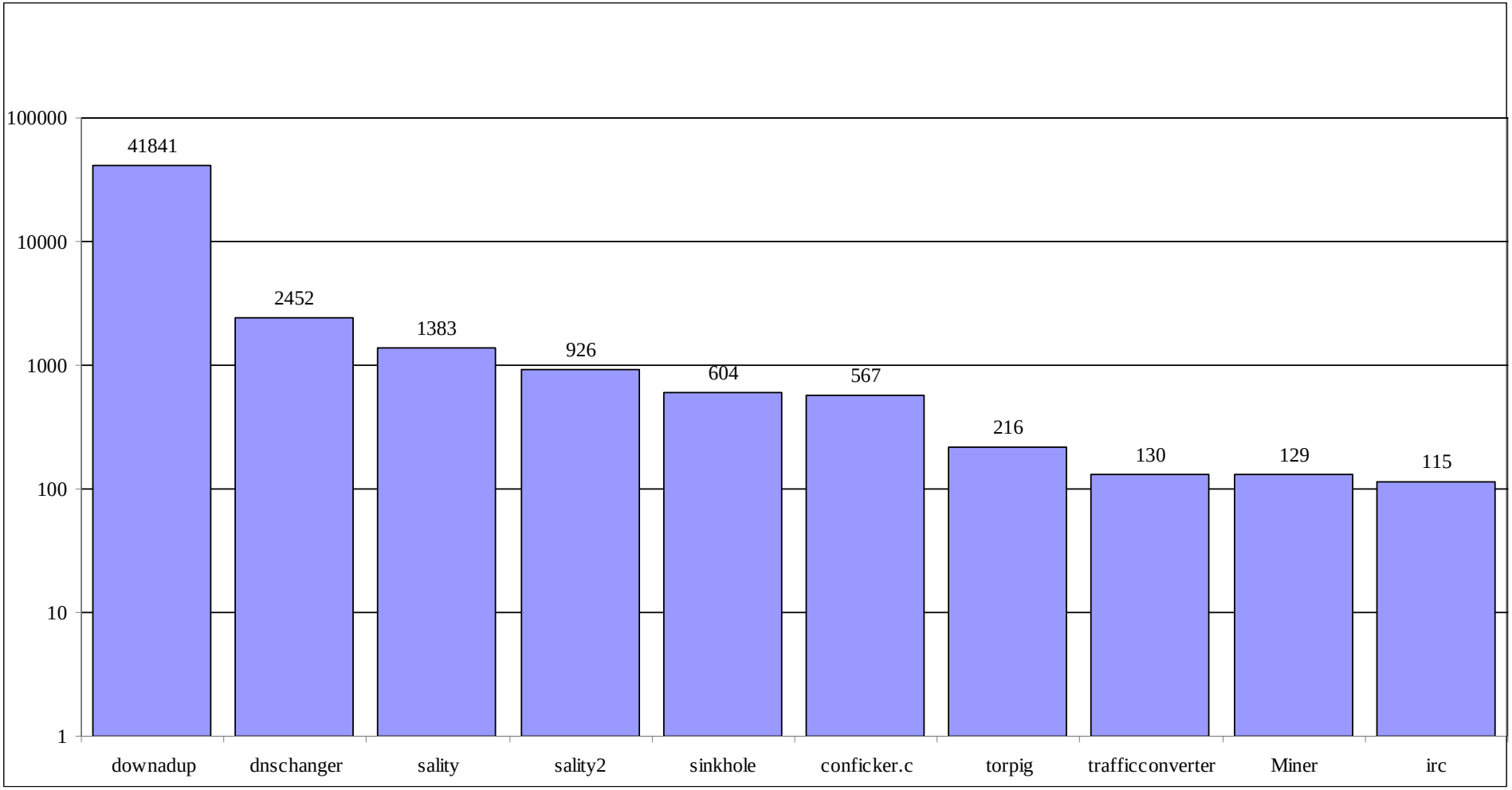
- Milzīgs skaits incidentu ziņojumu katru dienu
- Augstas un zemas prioritātes incidenti
- Sadarbība ar IPS
  - 5 IPS pieņem incidentu ziņojumus katru dienu
  - Domājam par sadarbības apliecinājumu/zīmi

Augstas prioritātes incidenti – 1.ceturksnis - 998

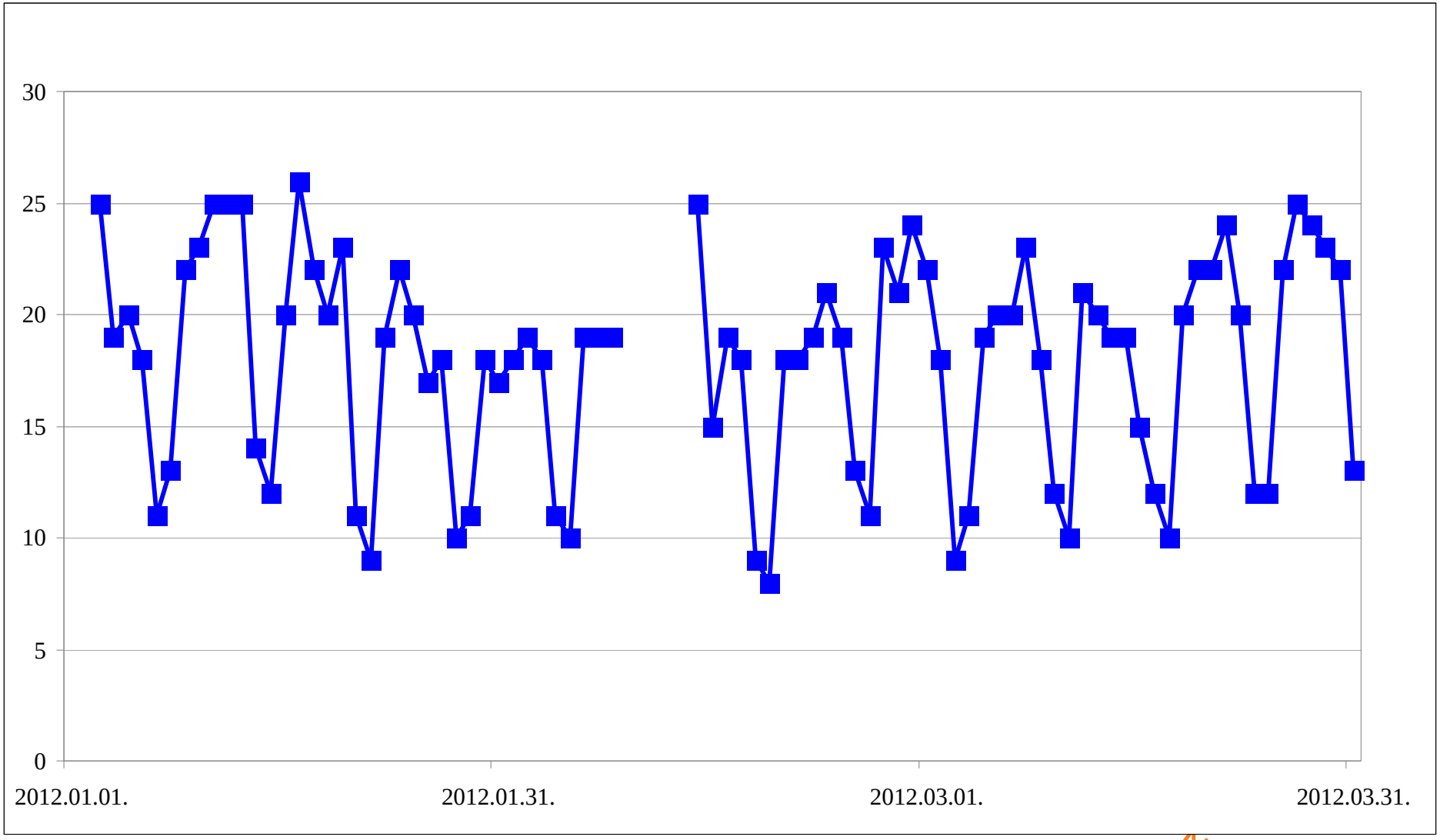


Zemas prioritātes incidenti – 1.ceturksnis – 48841

Infekciju TOP10



Inficētās IP adreses Valsts & pašvaldību iestādēs



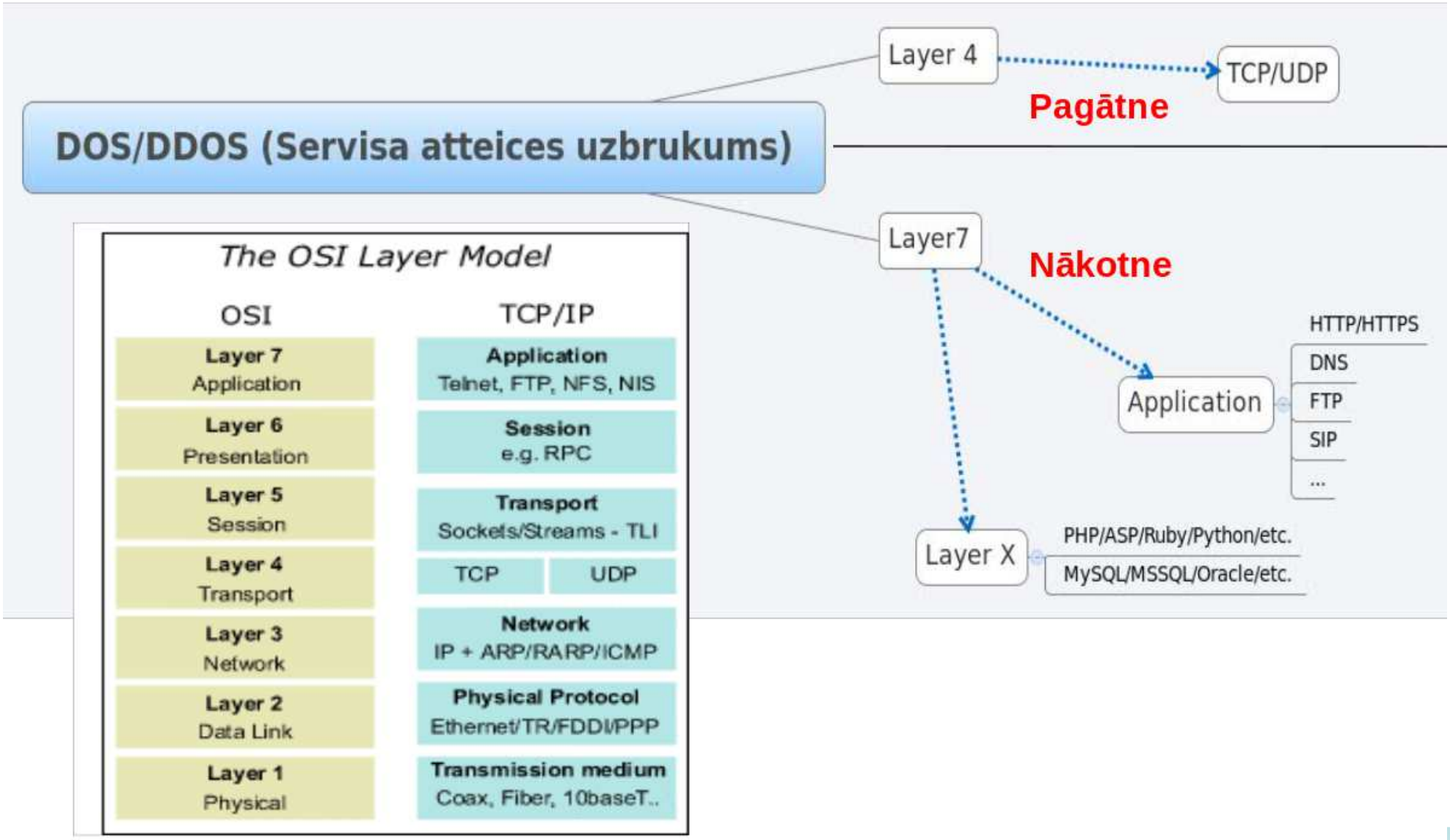
Aktuālā situācija

- Botnetos esošo datoru skaits joprojām liels
- Inficēšanās caur pārlūkprogrammām
- Serveru uzlaušanas, pikšķerēšana, piekļuves liegšanas uzbrukumi
- Uzbrukumi sociāli jūtīgos brīžos
- Ļaundabīgās programmatūras izplatīšana

Aktuālā situācija

- Spamhaus melnie saraksti – cīņa ar nelegālajiem hostētājiem
- Draudi
  - Politiskās situācijas saasinājumi
  - Mērķētie uzbrukumi
  - Ļaunatūras izplatīšana no uzlauztajām lapām
  - Pikšķerēšanas u.c. uzbrukumu ticamības palielināšanās

Piekļuves liegšanas uzbrukumi



Botneta piemērs

CERT.LV pētīts botnets:

38 : Darwin

161 : FreeBSD

378 : Linux

3 : SunOS

Neviena Windows servera!

Rīcības plāni

- 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”
- ES direktīvas ieviešana Latvijā
- Jāiesniedz CERT.LV līdz 2011.gada 31.oktobrim
- Saturs – MK noteikumos
- CERT.LV lapā ir plāns, paskaidrojumi

Īsumā

- CERT.LV aicina sadarboties
  - Informācija par inficētām IP adresēm
  - Sadarbības zīme
  - Rīcības plāni
  - LV-CSIRT sadarbības grupa
  - Izglītojoši pasākumi
- Lietotāji jāturpina izglītot un ieinteresēt IT drošībā
- IT drošības līmeni var paaugstināt tikai kopīgiem spēkiem

Tuvākie pasākumi

- “Esi drošs-1” seminārs – 25.aprīlī
- “Esi drošs-2” seminārs – 17.maijā

Paldies par uzmanību!

http://www.cert.lv/

cert@cert.lv

baiba.kaskina@cert.lv