CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

IT Drošības seminārs «Esi drošs-2»

CERT.LV aktualitātes

Rīga, 2015.gada 29.aprīlis

Baiba Kaškina, Varis Teivāns, CERT.LV

«Esi drošs-2» programma

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

13:30 - 14:00 "**CERT.LV aktualitātes**" Baiba Kaškina, Varis Teivāns, CERT.LV

14:00 - 15:00 "**IT drošības likuma grozījumi: drošāka vide un papildus prasības**" Kirils Solovjovs, Latvijas Republikas Aizsardzības ministrija

15:00 - 15:30 Kafijas pauze *sadarbībā ar semināra atbalstītājiem Data Security Solutions*

15:30 - 16:00 "**Izplatītākie mobilo iekārtu lietošanas riski, kas apdraud organizācijas datu un informācijas sistēmu drošību**" Raivis Kalniņš, „Data Security Solutions" tehniskais direktors

16:00 - 16:30 "**Application Whitelisting - efektīva aizsardzība pret vīrusiem**" Toms Pēcis, SIA „Lattelecom" IT risku vadītājs

16:30 - 17:00 "**Piekļuves lieguma uzbrukumi prezidentūras laikā**" Didzis Ozoliņš, LVRTC

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Data Security Solutions
Riga, Latvia

Saturs

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Par semināru
- Statistika
- Sabiedrības izglītošana
- Sensoru tīkla izveide
- IT drošības mācības
- Konference

«Esi drošs-2»

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Jaunas telpas
- Tiešraide – nodrošina RTU
- Atbalstītājs – Data Security Solutions
- LMT stends
- Novērtējuma anketas
  - Izlozēsim 3 lietussargus

«Esi drošs-2»

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Hashtag jeb mirkļbirka twitter #esidross**
- **Wifi pieeja:**

  SSID: Esi dross

  Parole: welcome@RTU

Statistika un incidenti

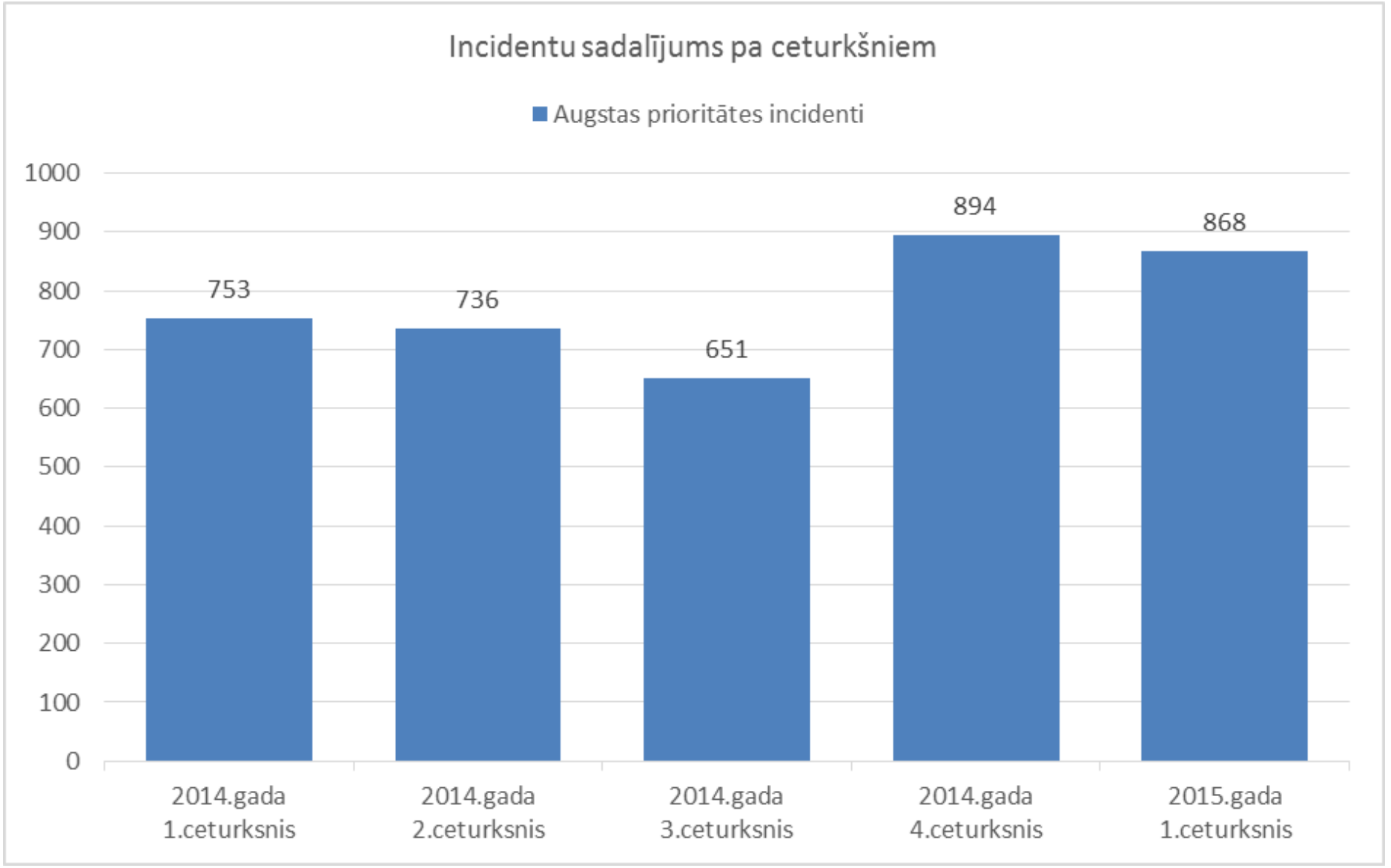
Incidenti ES prezidentūras kontekstā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Vairāki piekļuves lieguma uzbrukumi**
- **Pastiprināta interese un ielaušanās mēģinājumi dažādu sektoru tiešsaistes resursos**
- **Palielināta aktivitāte CERT.LV sensoros**

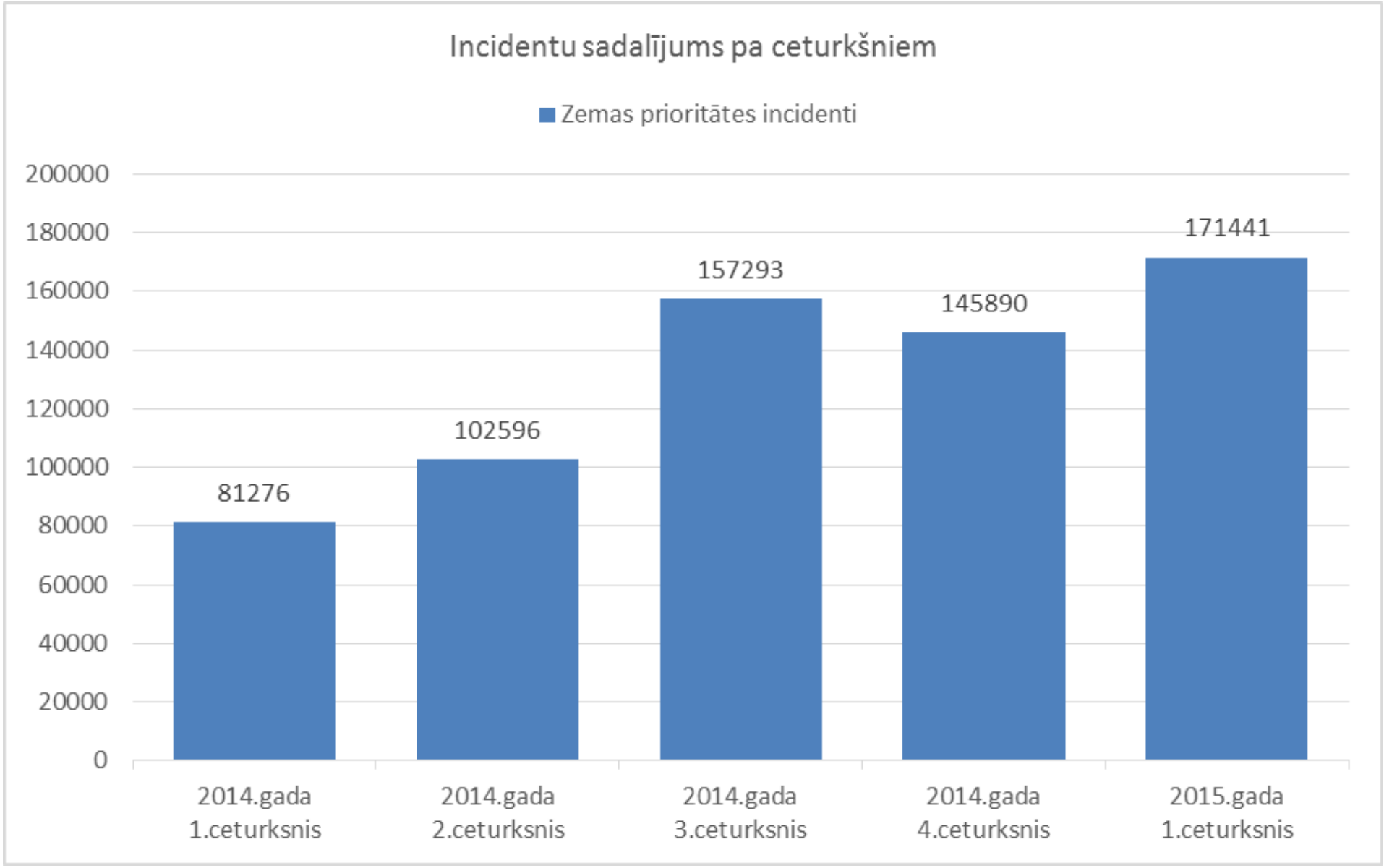
Augstas prioritātes incidenti

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija



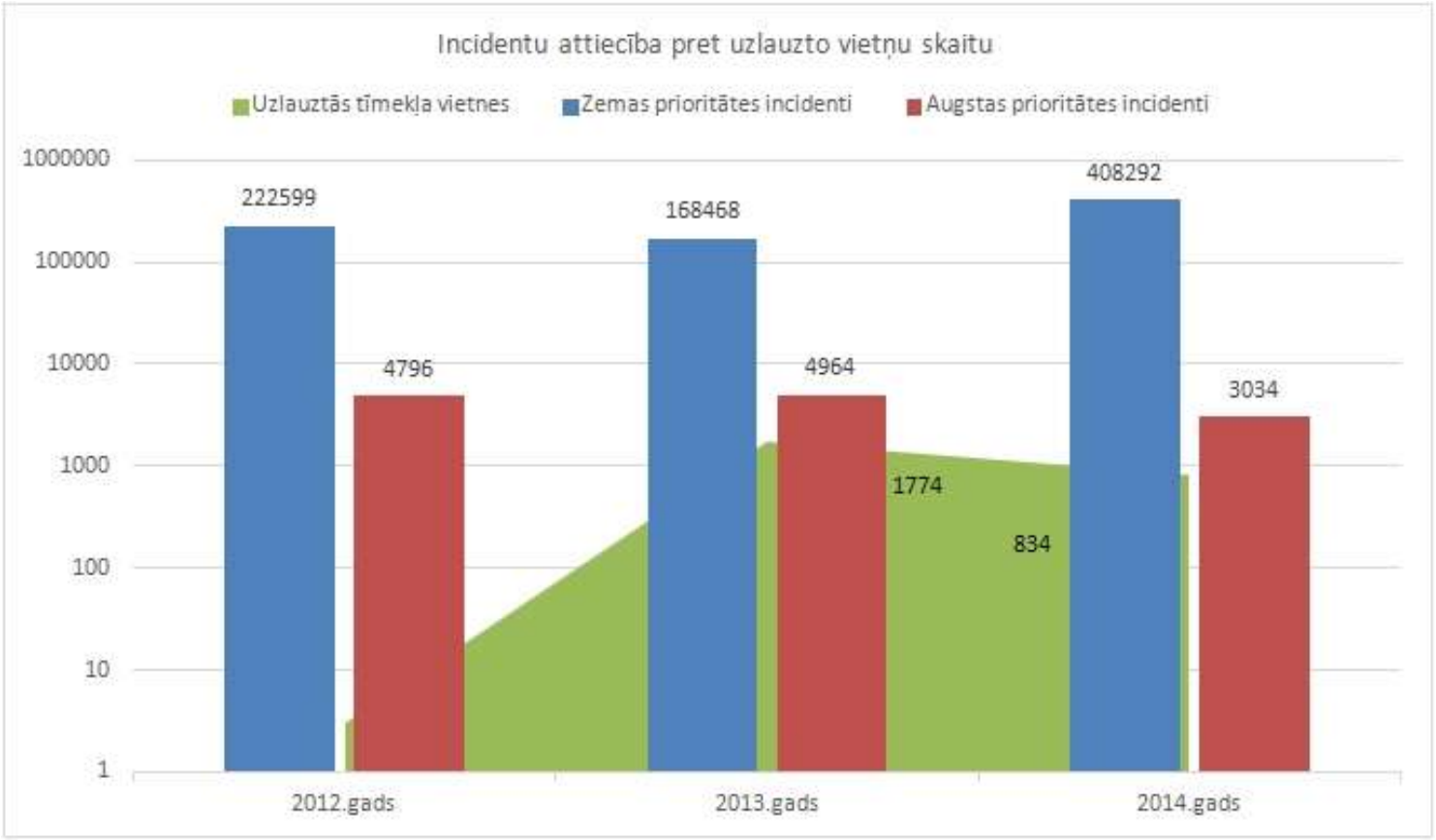
Zemas prioritātes incidenti

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija



Salīdzinājums 2012-2014.gads

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija



CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Tēma: Neapmaksāts rēķins

Labrit,

Pec musu gramatvedibas datiem, jums ir neapmaksats rekins pret musu uznemumu. Ludzam steidzami veikt apmaksu!!! Ludzam nosutit maksajuma uzdevumu!

Rekina kopija http://failiem.lv/u/qlfsujz

-----Original Message-----
From: gita eihmane [mailto:gita.eihmane@creditreform.lv]
Sent: Friday, February 27, 2015 3:33 PM
To: gita.eihmane@creditreform.lv
Subject: Maksājuma pieprasījums!

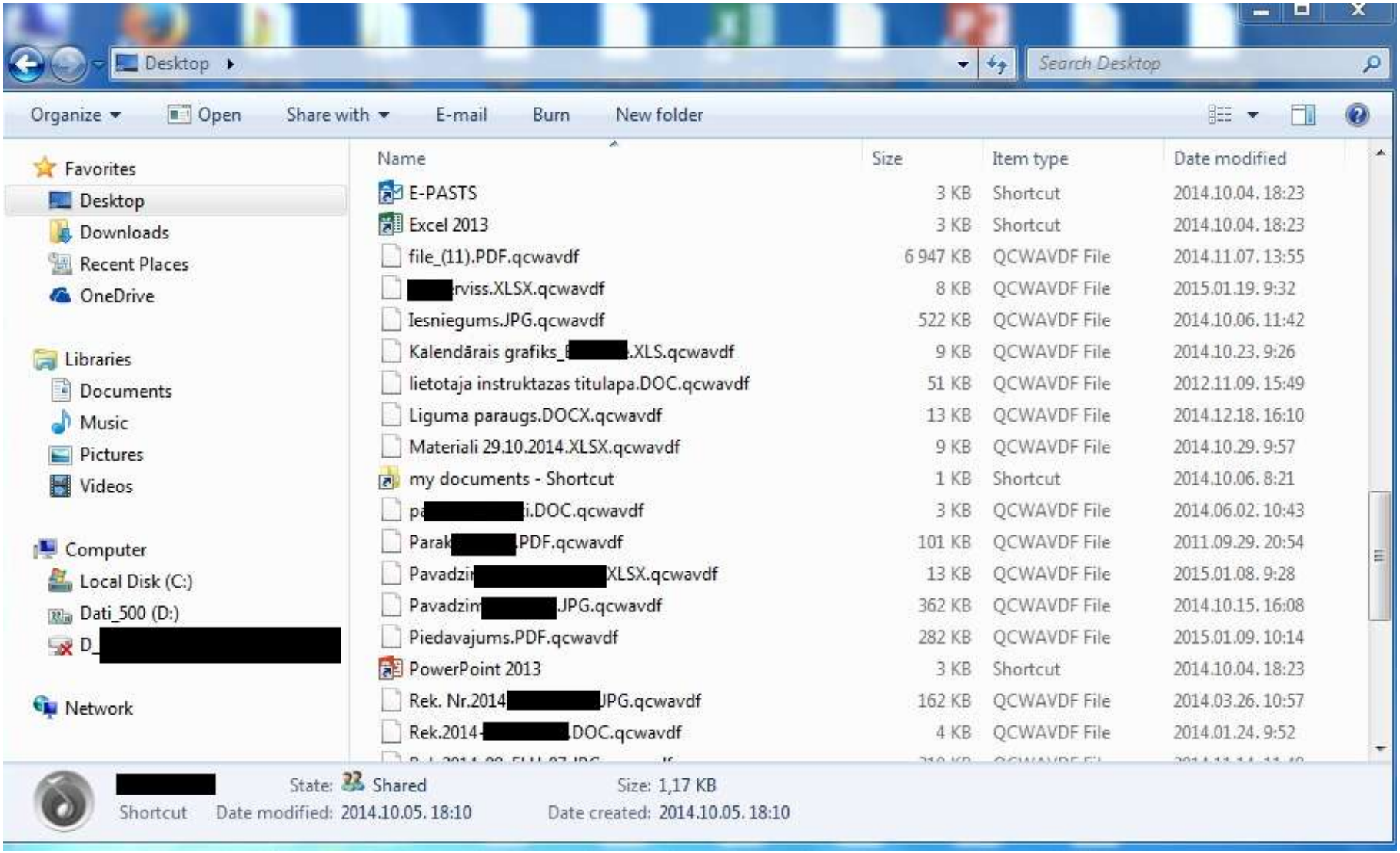
Labdien,
Atgādinām, ka šodien iestājas Jums dotais parāda apmaksas termiņš lietā par parāda atgūšanu SIA "Rīgas Satiksme" uzdevumā Nr 20147822. Ja parāds vēl nav apmaksāts, lūdzam to nekavējoties izdarīt.

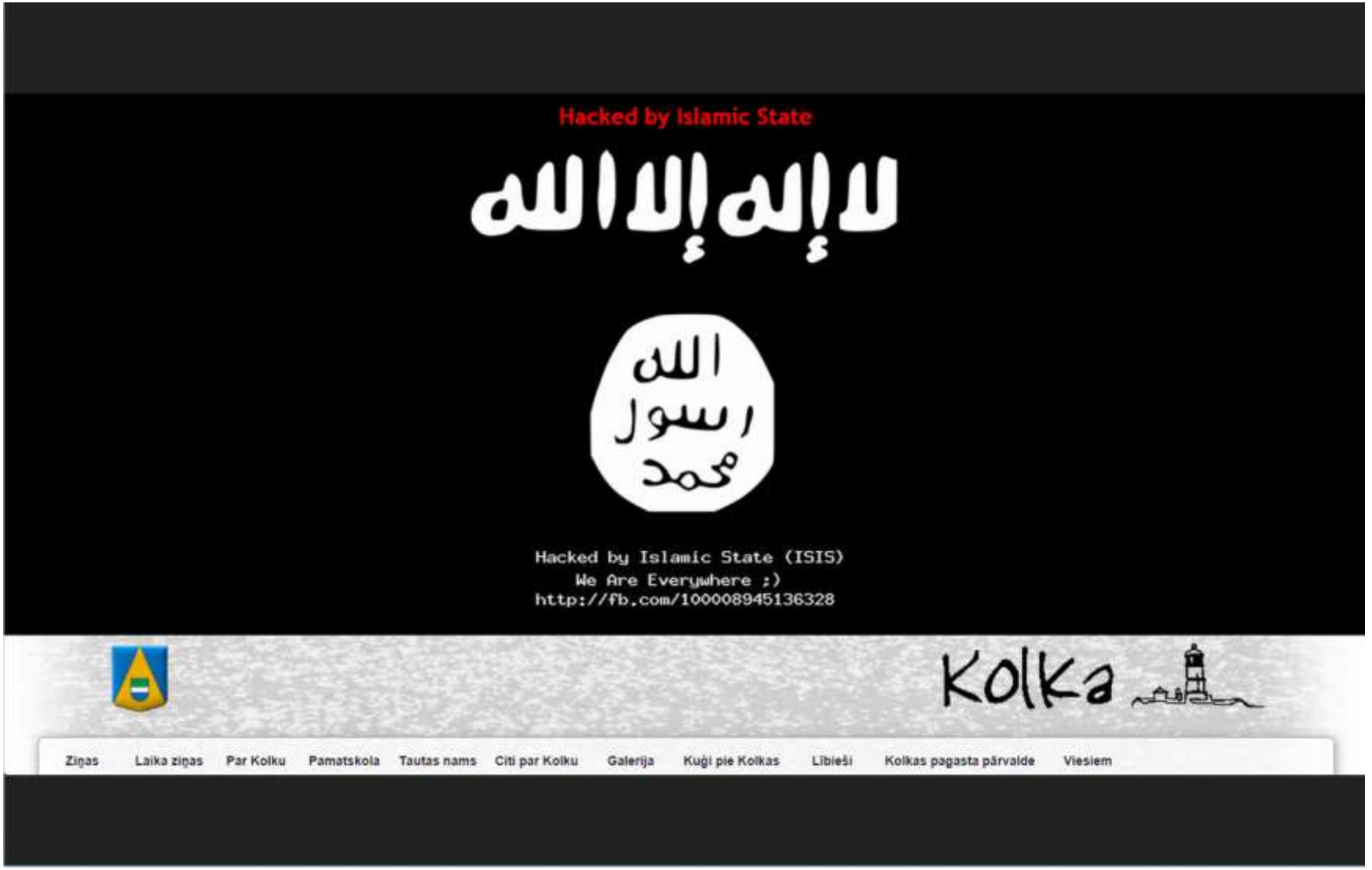
Jūsu lieta:
http://creditreform.su/piedzina/bridinajums.php?id=

Ar cieņu,
Gita Eihmane
CreditReform Latvija SIA
67501030, 26515199

CTB Locker

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

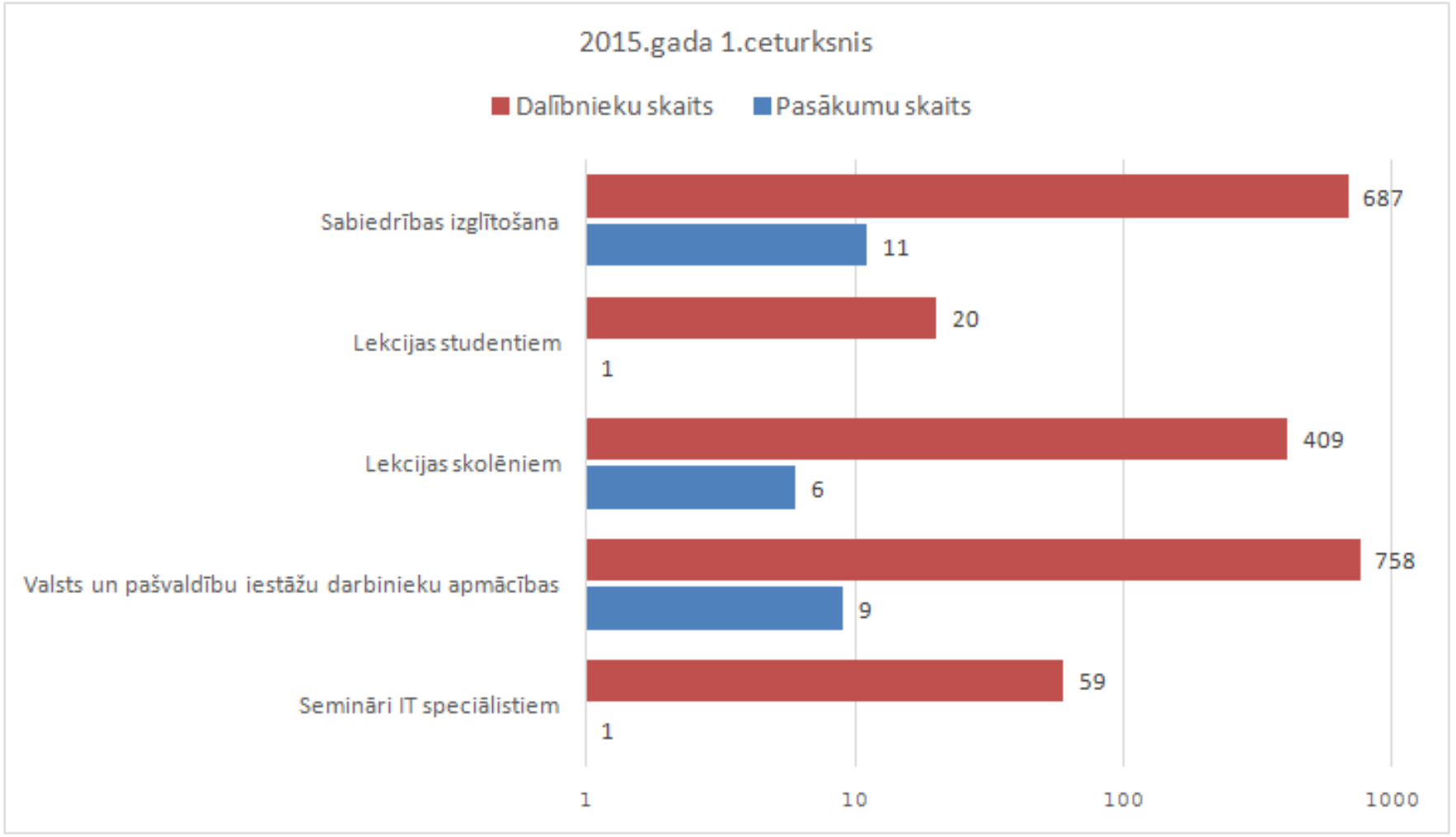

Desktop
Search Desktop
Organize
Open
Share with
E-mail
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
OneDrive
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Dati_500 (D:)
Network
Name
Size
Item type
Date modified
E-PASTS 3 KB Shortcut 2014.10.04. 18:23
Excel 2013 3 KB Shortcut 2014.10.04. 18:23
file_(11).PDF.qcwavdf 6 947 KB QCWAVDF File 2014.11.07. 13:55
[redacted]rviss.XLSX.qcwavdf 8 KB QCWAVDF File 2015.01.19. 9:32
Iesniegums.JPG.qcwavdf 522 KB QCWAVDF File 2014.10.06. 11:42
Kalendārais grafiks_[redacted].XLS.qcwavdf 9 KB QCWAVDF File 2014.10.23. 9:26
lietotaja instruktazas titulapa.DOC.qcwavdf 51 KB QCWAVDF File 2012.11.09. 15:49
Liguma paraugs.DOCX.qcwavdf 13 KB QCWAVDF File 2014.12.18. 16:10
Materiali 29.10.2014.XLSX.qcwavdf 9 KB QCWAVDF File 2014.10.29. 9:57
my documents - Shortcut 1 KB Shortcut 2014.10.06. 8:21
p[redacted]i.DOC.qcwavdf 3 KB QCWAVDF File 2014.06.02. 10:43
Parak[redacted].PDF.qcwavdf 101 KB QCWAVDF File 2011.09.29. 20:54
Pavadzi[redacted]XLSX.qcwavdf 13 KB QCWAVDF File 2015.01.08. 9:28
Pavadzim[redacted].JPG.qcwavdf 362 KB QCWAVDF File 2014.10.15. 16:08
Piedavajums.PDF.qcwavdf 282 KB QCWAVDF File 2015.01.09. 10:14
PowerPoint 2013 3 KB Shortcut 2014.10.04. 18:23
Rek. Nr.2014[redacted]JPG.qcwavdf 162 KB QCWAVDF File 2014.03.26. 10:57
Rek.2014-[redacted].DOC.qcwavdf 4 KB QCWAVDF File 2014.01.24. 9:52
[redacted]
State: Shared
Size: 1,17 KB
Shortcut
Date modified: 2014.10.05. 18:10
Date created: 2014.10.05. 18:10


Hacked by Islamic State
لا إله إلا الله
الله
رسول
محمد
Hacked by Islamic State (ISIS)
We Are Everywhere ;)
http://fb.com/100008945136328
Kolka
Ziņas
Laika ziņas
Par Kolku
Pamatskola
Tautas nams
Citi par Kolku
Galerija
Kuģi pie Kolkas
Lībieši
Kolkas pagasta pārvalde
Viesiem

Sabiedrības izglītošana

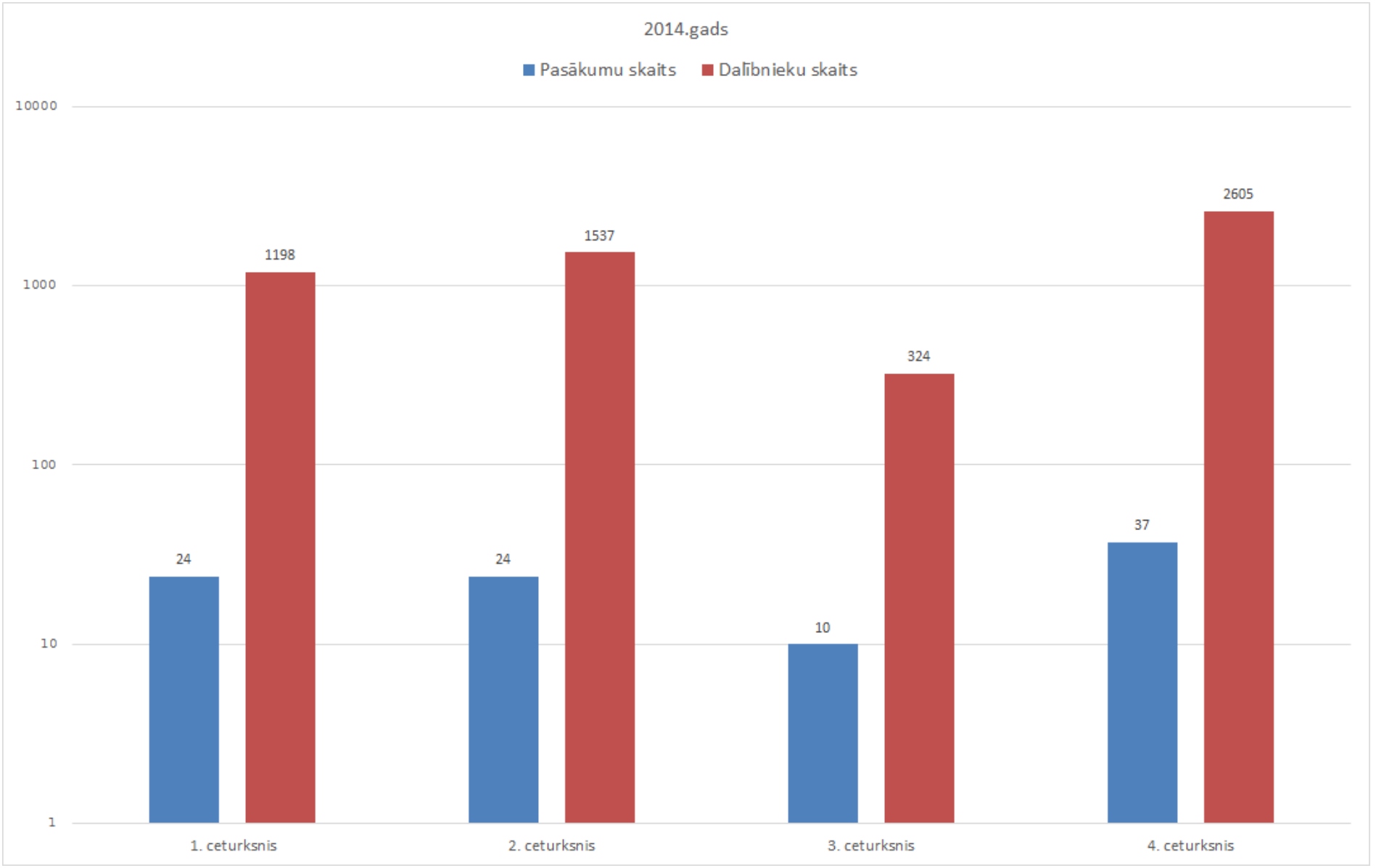
Sabiedrības izglītošana

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija



Sabiedrības izglītošana

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija



Sadarbojamies

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Valsts iestādes, pašvaldības**
  - **Valsts administrācijas skola**
- **Skolas, bibliotēkas, RTU**
- **Swedbanka – kampaņa, pasākumi**
- **LATA – par atvērtajiem datiem**
- **Latvijas sertificēto personas datu aizsardzības speciālistu asociācija**
- **E-prasmes, datorologs**
- **Netsafe drošāka interneta centrs**
- **ENISA**

Pūcītes

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Sensoru tīkla izveide

Sensoru tīkla izveide Latvijā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Motivācija**
  - **Incidenta analīzei nepietiekams saglabājamo datu apjoms valsts iestāžu datortīklos**
  - **Uzlabot valsts spēju apzināties IKT drošības situāciju valstī**
  - **Uzlabot reakcijas un preventīvās spējas**
  - **Identificēt arī nezināmo**

Sensoru tīkla izveide Latvijā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Rezultāti**
  - **Projekta 1. fāze - 20 sensori**
  - **118 000 augstas prioritātes notikumi**
  - **24 unikālas, sekmīgi veiktas un identificētas uzbrukumu kampaņas, >100 inficētas iekārtas 9 iestādēs**
  - **4 unikāli Android ļaunatūras gadījumi**

Sensoru tīkla izveide Latvijā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Attīstība**
  - **Projekta 2. fāze + 20 sensori**
  - **Uzraudzības interfeiss ir pieejams arī iestādei**
  - **Iestādes var piedalīties uzbrukuma/infekcijas pazīmju datu bāzes veidošanā**
  - **CERT.LV DNS RPZ / DNS Firewall servisa izveide ar augstas kvalitātes kaitniecisko resursu filtriem**

Sensoru tīkla izveide Latvijā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Attīstība**
  - **Seminārs CERT.LV sensora izvietošanas interesentiem**

IT drošības mācības

IT drošības mācības

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **«Kiberdzirnas»**
- **ENISA mācības**
- **«Marta migla»**
- **«Locked Shields»**

«Kiberdzirnas»

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Galvenais mērķis – pārbaudīt iestāžu gatavību iespējamiem IT drošības incidentiem ES prezidentūras laikā**
- **Dalībnieki – Iestāžu vadība un atbildīgie par IT drošību (CERT, SAB kā moderatori, LVRTC novērotāji)**
- **Norise – Moderatoru vadīta diskusija nelielās grupās par piedāvātajiem scenārijiem**
- **Rezultāts – Secinājumu dokuments izplatīšanai iestāžu vadībai**

«Cyber Europe 2014»

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Galvenais mērķis – pārbaudīt valstu spēju sadarboties nopietnas starptautiskas IT drošības krīzes novēršanai**

- **Dalībnieki – kopā vairāk kā 400 dalībnieki no 29 valstīm (no Latvijas - CERT.LV, Kibersardze, AIM, privātā sektora pārstāvji)**

- **Norise – 3 posmi Tehniskais, Operatīvais, Stratēģiskais. Katram posmam atšķirīgs mācību formāts. Rezultāti no katra iepriekšējā posma tika izmantoti nākamajā posmā**

- **Rezultātu apkopojums 2015.gada jūnijā**

- **Nākamās šāda veida mācības 2016.gadā - var sākt izrādīt interesi par dalību**

«Marta Migla»

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Galvenais mērķis – vingrināt dalībnieku komandas darbu un attīstīt spēju efektīvi reaģēt apjomīgu uzbrukumu gadījumā risinot tehniskus izaicinājumus**
- **Organizē CERT.LV & ZS Kiberaizsardzības vienība**
- **~ 70 dalībnieki, 3 komandas (BLUE), 1 komanda (RED)**
- **~ 30 sistēmas + tīkls**
- **Dalībnieku prasmes ar katru gadu būtiski uzlabojās**
- **Uzsvars uz tehnisko kompetenču vingrināšanu un attīstību**

«Locked Shields 2015»

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **NATO CCDCoE organizētas, pasaulē lielākās kiber krīzes mācības**
- **Scenārijs un mērķis: Fiktīvu valstu konflikts. Tehniskie un tiesiskie izaicinājumi, mediju aktivitātes, lielas krīzes risināšana un sarežģījumu pārvarēšana**
- **85 iekārtas + tīkls + SCADA(PLC) + Drone katrai komandai**
- **>400 dalībnieki, 16 komandas (BLUE), 5 komandas (RED)**

«Locked Shields 2015»

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Latvijas + Lietuvas komanda = 4. vietā

Lielā konference

„Kiberšahs. Stratēģija un taktika virtuālajā vidē”

- **IT drošības konference 2015.gada 1.oktobrī, LNB**
- **Referātu iesniegšana līdz 31.05.2015. Tēmas:**
  - IT drošības tehniskie izaicinājumi,
  - Droša programmatūras izstrāde,
  - Sabiedrības izglītošana un apmācība,
  - IT drošības pārvaldības izaicinājumi,
  - Stratēģiskie jautājumi un informācijas operācijas.
- **Atbalsta: LMT, DEAC, NIC.LV**

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

ISACA®
Gūstot vērtību no uzticamām informācijas sistēmām
Latvijas nodaļa

lmt

NIC

deac
DATU CENTRI

Paldies!

http://www.cert.lv

baiba.kaskina@cert.lv

«Esi drošs-2» programma

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

13:30 - 14:00 "CERT.LV aktualitātes" Baiba Kaškina, Varis Teivāns, CERT.LV

14:00 - 15:00 "IT drošības likuma grozījumi: drošāka vide un papildus prasības" Kirils Solovjovs, Latvijas Republikas Aizsardzības ministrija

15:00 - 15:30 Kafijas pauze *sadarbībā ar semināra atbalstītājiem Data Security Solutions*

15:30 - 16:00 "Izplatītākie mobilo iekārtu lietošanas riski, kas apdraud organizācijas datu un informācijas sistēmu drošību" Raivis Kalniņš, „Data Security Solutions" tehniskais direktors

16:00 - 16:30 "Application Whitelisting - efektīva aizsardzība pret vīrusiem" Toms Pēcis, SIA „Lattelecom" IT risku vadītājs

16:30 - 17:00 "Piekļuves lieguma uzbrukumi prezidentūras laikā" Didzis Ozoliņš, LVRTC

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Data Security Solutions
Riga, Latvia